The Journal on Terrorism and Security Analysis

11th Edition (Spring 2016)

Syracuse University
Syracuse, New York 13244

Contents

Undergraduate Spotlight:

Message from the Editor-in-Chief

With this publication the Journal on Terrorism and Security Analysis (“JTSA”) has reached its 11th edition. We could not have come this far without inspiring authors, steadfast support from Syracuse University (notably the Syracuse University College of Law, the Maxwell School of Citizenship and Public Affairs, and the Institute for National Security and Counterterrorism), a dedicated team of editors (with special thanks to Zachary D. Johnson), and—perhaps—a little luck. We at JTSA hope you enjoy the latest installment of our journal and look forward to bringing you more engaging scholarship in the years to come.

Sincerely,

Kyle Lundin
Editor-in-Chief

Women in Islamic Armed Groups

Brittany L. Card, Laura McElroy, Maida Omerović, and Rebekah Glickman-Simon

Introduction

Women in Islamic armed groups, unseen and unmentioned by the international community, are relegated to the private sphere. When these women are depicted, they are often siloed into one of three categories: (1) the dutiful, supportive mother and wife, who cooks, cleans, and cares for her children, (2) the coerced victim, who participates out of devotion to her husband, or (3) the fetishized, sexual deviant, whose "un-Muslim" personal history is analyzed in an attempt to pinpoint which character flaw led her to commit such an "un-womanly" act.[1]

These one-dimensional depictions fail to recognize the inextricable internal and external factors that culminate in each woman's participation in an armed group. Therefore, a comprehensive analysis of the role of women in armed groups must contextually examine the history of the armed group; the societal role and status of women, including the impact of shifting economic, political and social factors; and the group's ideology. These elements create a framework through which to holistically analyze the involvement of women in a group.

By applying this framework to al-Shabaab in Somalia and al-Qaeda in Iraq ("AQI"), this paper demonstrates how examining these often disparate components together results in a more comprehensive understanding of the elements that dictate women's involvement and the essential nature of their participation. Singular and cross-cutting factors and trends are revealed, which can contribute to group-specific policy recommendations.

Al-Shabaab

Following Somalia's 1991-1992 civil war, young male hardliners from Al-Ittihad Al-Islami, a militant Salafi group, broke off

[1] Mia Bloom, *Bombshells: Women and Terror*, 28 GENDER ISSUES 1, 4 (2011), Springer.

and established al-Shabaab ("the Youth") in 2003.[2] The group aligned itself with the Islamic Courts Union ("ICU"), an alliance of Sharia courts in Somalia, and achieved early victories, including conquering Mogadishu and much of the country by the end of 2006.[3] Threatened by the expansion of hardline Islamism near its border, Ethiopia invaded Somalia with U.S. backing later that year.[4]

Ethiopia's invasion proved to be a turning point for al-Shabaab.[5] Somalia's disapproval of the invasion enabled al-Shabaab to position itself as a political alternative.[6] As a result, al-Shabaab simultaneously radicalized and gained a greater foothold. Al-Shabaab asserted that political Islam was the best alternative to the "failed Somali nationalism" that had caused widespread corruption, dysfunctional governance, and human rights abuses. As a result, al-Shabaab grew from hundreds of members to thousands.[7]

In 2010, al-Shabaab carried out its first foreign attack: a suicide bombing that killed seventy-four people in Kampala, Uganda. Shortly after, Kenya invaded Somalia, ejecting al-Shabaab from Mogadishu and other cities.[8] In 2012, al-Shabaab declared its allegiance to al-Qaeda and continued attacks in Somalia and abroad, including the infamous Westgate mall attack in Nairobi, Kenya. Yet, reflective of its origins, al-Shabaab's "modus operandi suggests an organization with a local focus, and its attacks since 2007 have been directly connected to local warfare, even when attacking outside Somalia."[9]

Today, al-Shabaab does not appear to have a single centralized leadership structure and it controls much of southern and central Somalia. The group has enjoyed relatively widespread community

[2] Jonathan Masters & Mohammed Aly Sergie, *CFR Backgrounders: Al-Shabaab*, COUNCIL ON FOREIGN RELATIONS (Mar. 13, 2015), http://www.cfr.org/2omalia/al-shabab/p18650.

[3] Paula Cristina Roque, *Somalia: Understanding Al-Shabaab*, INST. FOR SEC. STUDIES 2 (June 3, 2009), https://www.issafrica.org/uploads/SABAAB040609.pdf.

[4] Xan Rice, *Ethiopia Ends Somalia Occupation,* THE GUARDIAN (Jan. 26, 2009, 9:39 AM), http://www.theguardian.com/world/2009/jan/26/ethiopia-ends-somalia-occupation.

[5] Roque, *supra* note 3.

[6] Malkhadir Muhumed, *Somalis Balk at Plans For Ethiopian Troops*, AL JAZEERA (Feb. 3, 2014, 12:42 PM), http://www.aljazeera.com/indepth/features/2014/02/201422122028512719.html.

[7] Masters & Sergie, *supra* note 2.

[8] *Id.*

[9] STIG JARLE HANSEN, AL-SHABAAB IN SOMALIA: THE HISTORY AND IDEOLOGY OF A MILITANT ISLAMIST GROUP, 2005-2012 2 (C. Hurst & Co.,2013).

support, particularly among local clan leaders and elders. While some reports suggest that community support may have begun to wane,[10] "continuously expanding its local community infrastructure and support . . . has thus far been essential to al-Shabaab's strategy."[11]

Status of Women in Somali Society

During President Mohamed Siad Barre's rule from 1969 to 1991, prior to the civil war, women's political and economic participation was legally recognized. Increased access to education enabled women to become educators, professionals, and "an important part of the intellectual community."[12] The Family Law of 1975 also gave women equal rights to property, inheritance and divorce. The law abolished polygamy and raised the legal age of marriage for women to eighteen years. As a result, women attained higher levels of education and began having fewer children.[13]

During the civil war, women continued to serve in the public sphere, working at "the forefront of emergency care and social recovery efforts at the community level."[14] After the war, men were generally unable to work or support their families as they did before. As a result, many women took over as decision-makers and increasingly joined the workforce to meet the needs of their families.[15] While these women still faced discrimination in some areas due to Sharia law, they were generally able to live and work freely.[16]

[10] *Losing Streak – Public Support Fades for al-Shabab,* AFR. UNION MISSION IN SOM., http://amisom-au.org/2011/09/losing-streak-public-support-fades-for-al-shabab/.

[11] Roque, *supra* note 3, at 3.

[12] *Human Rights Brief: Women in Somalia,* IMMIGRATION & REFUGEE BD. OF CAN. (Apr. 1, 1994), http://www.refworld.org/docid/3ae6a83b8.html (last visited Jan. 19, 2016).

[13] *Id.*

[14] Judith Gardner, *Gender Profile for Somalia: An Executive Summary*, EUR. COMM'N SOM. UNIT, KENYA & NORAD 2–3 (Jan. 2007), http://www.eeas.europa.eu/delegations/somalia/documents/more_info/country_gender_profile_executive_summary_en.pdf.

[15] Dyan Mazurana, *Women, Girls and Non State Armed Groups*, *in* WOMEN & WARS: CONTESTED HISTORIES, UNCERTAIN FUTURES 146, 164 (Carol Cohn ed. 2013).

[16] *Harsh War, Harsh Peace*, HUMAN RIGHTS WATCH (Apr. 19, 2010), https://www.hrw.org/report/2010/04/19/harsh-war-harsh-peace/abuses-al-shabaab-transitional-federal-government-and-amisom.

When al-Shabaab came to power, women faced a backlash as the group sought to reverse women's newfound power and agency. Through the use of violence, al-Shabaab reasserted male dominance over women, reinstituting pre-war traditional and cultural values, as well as new values under the auspices of Sharia law. As a result, women were prohibited from working, walking unaccompanied, and were subjected to "sporadically applied decrees" governing their wardrobes, livelihoods, and personal interactions.[17] Ongoing violence and fear of abduction further impacted girls' mobility, like their ability to go to school.[18]

Female Participation in Al-Shabaab

Research conducted on the roles of women and girls within al-Shabaab is by no means comprehensive because the experiences of girls are often told to researchers by boys within al-Shabaab.[19] Nonetheless, these accounts can provide some insight into the gendered nature of boys' and girls' experiences within the group. Boys and girls are typically abducted on their way to school, while playing, or even from their homes. Once captured, the division of labor by gender becomes clear. Boys are used as suicide bombers or fighters, occupying the vast majority of roles in the public sphere. Conversely, girls serve mainly domestic functions, such as cooking and cleaning, while women serve as fundraisers and caregivers. Some girls also serve in support roles during combat, carrying "bullets, water, milk, and food to the front lines."[20] Finally, girls are subjected to forced marriage and sexual abuse. Al-Shabaab recruiters even explain to the families of young women that "before a man is given a gun, he must be given a woman, so that he can leave something behind," illustrating the importance of girls and women serving as wives and mothers.[21]

Samantha Lewthwaite appears to be the only exception to al-Shabaab's rigid exclusion of women from public roles. Lewthwaite, known as the "White Widow," is a British citizen who has seemingly risen through the ranks of al-Shabaab following the deaths of several

[17] *Id.*

[18] *No Place for Children*, HUMAN RIGHTS WATCH (Feb. 20, 2012), https://www.hrw.org/report/2012/02/20/no-place-children/child-recruitment-forced-marriage-and-attacks-schools-somalia.

[19] *Id.*

[20] *Id.*

[21] Mazurana, *supra* note 15, at 164.

of its leaders. Lewthwaite serves as a recruiter and trainer, and is also thought to have orchestrated the murders of about 400 people.[22]

The admittedly lacking research conducted on the group does not suggest that the role of women in al-Shabaab has changed significantly since the group's foundation. The marginalization of women to the group's private sphere is part of an intentional strategy designed to reinforce the Somali patriarchy, which benefits al-Shabaab. Indeed, the "exclusion of women from visible positions is in part a reaction to decades of internal warfare in Somalia which fundamentally altered the economic and social expectations placed upon women and girls, and consequently challenged patriarchal Somali notions of masculinity and manhood."[23] By doing this, al-Shabaab's reclaiming of masculinity is part of how it projects of power.

Al-Qaeda in Iraq

Following the 2003 U.S.-led invasion of Iraq and subsequent ousting of President Saddam Hussein, AQI was founded in 2004 when Abu Musab al-Zarqawi declared his allegiance to Osama bin Laden.[24] Zarqawi, a charismatic and skilled strategist, rose to prominence during the Iraqi insurgency due to his attacks against U.S. forces. As the insurgency continued, Zarqawi became known for his "high-profile" and "brutal" tactics, including the frequent use of suicide bombers, the enforcement of radical Islam, and extreme violence against Muslims.[25]

Throughout Zarqawi's violent rule, the Iraqi population became increasingly unhappy with AQI's actions. The leadership of al-Qaeda global, especially Osama bin Laden's successor, Ayman al-Zawahiri, emphasized the importance of maintaining popular support. Despite the call for Zarqawi to desist, the violent tactics continued and in 2005 "[t]he global backlash against Zarqawi and his group reached

[22] Morgan Winsor, *'White Widow' Samantha Lewthwaite Is Now Right Hand Of Al Shabaab Leader In Somalia: Report*, INT'L BUS. TIMES (May 18, 2015, 8:32 AM), http://www.ibtimes.com/white-widow-samantha-lewthwaite-now-right-hand-al-shabaab-leader-somalia-report-1926783.

[23] Mazurana, *supra* note 15, at 164.

[24] M. J. Kirdar, *Al Qaeda in Iraq*, CTR. FOR STRATEGIC & INT'L STUDIES (June 15, 2011), https://csis.org/publication/al-qaeda-iraq.

[25] *The Islamic State*, MAPPING MILITANT ORGS.: STANFORD UNIVERSITY (May 15, 2015), http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/1.

its peak following AQI's coordinated bombings of three Amman hotels that killed 60 people, most of them Muslims attending a wedding party."[26]

Following Zarqawi's death by U.S. forces in June 2006, the group's new leadership re-named the group the Islamic State in Iraq ("ISI"), in an attempt to unify the divided AQI factions under this "more Iraqi" brand.[27] ISI regained a foothold in Iraq following the withdrawal of U.S. forces in December 2011 and eventually took advantage of the instability caused by the Syrian Civil War. In April 2013, the leader of ISI, Abu Bakr al-Baghdadi, announced the formalization of ISI operations in Syria and changed the group's name to the Islamic State in Iraq and Syria (ISIS). Al-Qaeda global did not approve of this expansion and denounced its affiliation with ISIS in February 2014.[28]

Status of Women in Iraqi Society

The status and roles of women in Iraq have experienced a dramatic shift in the years since the Gulf War in 1991. Specifically, conflict and insecurity have led to a "rise in tribal customs and religiously-inspired political extremism, which have had a deleterious effect on women's rights, both inside and outside the home."[29]

Before 1991, Iraqi women largely enjoyed high levels of rights and social participation. These developments trace back to the Ba'ath Party's rise to power in 1968 when they increased the legal status of women in the public and private spheres as a means to achieve economic growth and increase its authority over the population. In the 1970's, women were formally granted equal legal and economic opportunity rights, compulsory education for both sexes was implemented and maternity benefits were institutionalized.[30]

[26] Kirdar, *supra* note 24.

[27] Eben Kaplan, *Abu Hamza al-Muhajir, Zarqawi's Mysterious Successor (aka Abu Ayub al-Masri)*, COUNCIL ON FOREIGN RELATIONS (June 13, 2006), http://www.cfr.org/iraq/abu-hamza-al-muhajir-zarqawis-mysterious-successor-aka-abu-ayub-al-masri/p10894.

[28] The Islamic State, *supra* note 25.

[29] *At a Crossroads: Human Rights in Iraq Eight Years after the US-Led Invasion*, HUMAN RIGHTS WATCH, February 21, 2011, https://www.hrw.org/report/2011/02/21/crossroads/human-rights-iraq-eight-years-after-us-led-invasion.

[30] *Id.*

After the Gulf War, the public status, mobility and protections of women declined as Saddam Hussein reduced the legal status of women in an attempt to gain support from conservative, religious and tribal groups. Women who organized against these changes were often subjected to gender-based violence by state security forces. Insecurity following the 2003 U.S. invasion further fueled the sectarian violence and the deterioration of women's rights.[31] The ideologies of militia and tribal groups that rose to power in this insecure vacuum emphasized keeping women out of public life. As a result, women were increasingly victimized, notably through practices such as honor killings and "pleasure marriages."[32]The prevalence of rapes and abductions also increased, causing women to fear public life.[33]

Scope of Female Participation

Unlike other Islamic armed groups, women in AQI serve a variety of roles in both the private and public spheres. In the private sphere, women serve as wives, mothers, and caregivers for their husbands and children. Women also fulfill logistical roles, like opening bank accounts, fundraising, translating documents, and conducting "bookkeeping" duties. In addition, female recruiters use the Internet to both spread AQI's ideology and recruit women far beyond the borders of Iraq,[34] sometimes resulting in the formation of "sisterhoods" after meeting in chat rooms.[35] Recruitment tactics have also been hands-on and manipulative. For example, Samira Ahmed Jassim, known as "the mother of believers," allegedly orchestrated the rapes of eighty women in order to shame them into becoming suicide bombers. Jassim was arrested in 2009 but not before twenty-eight of her "recruits" successfully perpetrated attacks.[36]

[31] *Id.*

[32] *Id.*

[33] *Iraq: Insecurity Driving Women Indoors*, HUMAN RIGHTS WATCH (Jul. 15, 2003), https://www.hrw.org/news/2003/07/15/iraq-insecurity-driving-women-indoors.

[34] Lori Poloni-Staudinger & Candice D. Ortbals, *Women Engaged in Violent Political Activity, in* TERRORISM AND VIOLENT CONFLICT: WOMEN'S AGENCY, LEADERSHIP, AND RESPONSES 42 (2013).

[35] Jennie Stone & Katherine Pattillo, *Al Qaeda's Use of Female Suicide Bombers in Iraq, in* WOMEN, GENDER, AND TERRORISM 159, 171 (2011).

[36] Deborah Haynes, *The 'Suicide Bomb Queen' Who Preyed On Shame Of Rape Victims To Turn Them Into Lethal Weapons,* THE TIMES, Feb. 5, 2009.

In the public sphere of AQI, women began functioning as suicide bombers inside and outside of Iraq in 2005. For example, on November 9, 2005 AQI carried out two suicide attacks using female bombers. In one, Myrium Goris, a Belgian citizen, bombed U.S. soldiers outside of Baghdad. At the same time, three men and one woman, Sajida Mubarak Atrous al-Rishawi, bombed a wedding party in Amman, Jordan.[37] By June of 2008, thirty-three women had successfully conducted suicide bombings in twenty-eight separate attacks in Iraq.[38]

In September 2008, women in ISI reportedly established the all-female, Naseeba al-Ansariya Martyrdom Battalion. This battalion was comprised of wives, sisters, or daughters of men killed by U.S. or Iraqi forces, most of whom are motivated by revenge. Notably, a woman who claimed to be second in command reported that the involvement of women in the Sunni insurgency was not new and that women had always played a variety of roles during the conflict. She said the women "treated wounded insurgents and carried explosive belts underneath their garments, taking advantage of conservative Muslim traditions."[39]

Shifting Role of Women

AQI's use of female as suicide bombers represents a marked shift from the traditional support roles of women in al-Qaeda global, which prohibited the use of women in violent jihad operations.[40] In contrast, AQI publically called for women to join and support the jihad. Shortly after a suicide bombing in 2005, a website linked to Zarqawi posted "May God accept our sister among the martyrs."[41] Mia Bloom describes this as the shift from the "revolutionary womb," in which women gave birth to and raised future jihadists, to the "exploding womb," in which women were encouraged to undertake

[37] Stone, *supra* note 35, at 165–66.

[38] Anne Speckhard, *Female Suicide Bombers In Iraq,* 5 DEMOCRACY & SECURITY 19, 20 (Mar. 17, 2009), available at Routledge.

[39] Sudarsan Raghavan, *Female Suicide Bombers Are Latest War Tactic,* WASH. POST (Sept. 17, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/09/16/AR2008091603697.html.

[40] Katharina Von Knop, *The Female Jihad: Al Qaeda's Women, in* 30:5 STUDIES IN CONFLICT & TERRORISM 397, 407 (2007), available at Routledge.

[41] Stone, *supra* note 35, at 164.

violent operations.[42]

There are several strategic reasons why AQI decided to use women as suicide bombers. First, women were seen as unexpected enemies. U.S soldiers had not been trained to look for female combatants. Instead, women were viewed as civilians or victims in need of protection.[43] Given local and religious customs, women were able to pass through checkpoints more easily than men were, usually without being searched.[44] Women also provided an untapped pool of recruits. Some Iraqi women wanted to avenge the death of a loved one, usually a husband or father.[45] AQI met this demand while also gaining valuable fighters. Women's public participation in AQI was also used as a tactic to shame men into joining the jihad. Zarqawi once asked: "Are there no men, so that we have to recruit women . . . Isn't it a shame for the sons of my own nation that our sisters ask to conduct martyrdom operations while men are preoccupied with life?"[46]

Finally, female bombers receive far more media attention than male bombers, as their participation in these violent acts is considered to be outside the accepted parameters of "female" action.[47] As a result, female suicide bombers within AQI inflicted physical damage and brought increased media coverage to Zarqawi's violence. This tactic allowed AQI to project power both inside and outside of Iraq. In particular, Western female suicide bombers served as a "global testament to the success of al-Qaeda's recruiting efforts" and "as an alarming indicator to the Western world" of AQI's capabilities.[48]

Analyzing Women's Involvement in Islamic Armed Groups

A contextualized, gendered analysis enables policymakers and analysts to better understand the role of women in Islamic armed groups. This type of analysis provides a nuanced assessment of the roles of male leadership, women's agency, as well as why and when women's roles may shift. The case studies of al-Shabaab and AQI

[42] Bloom, *supra* note 1, at 6.

[43] Christopher Dickey, *Women of Al Qaeda,* NEWSWEEK (Dec. 11, 2005, 7:00 PM), http://www.newsweek.com/women-al-qaeda-113757.

[44] Speckhard, *supra* note 38, at 28.

[45] *Id.* at 36.

[46] Dickey, *supra* note 43.

[47] Speckhard, *supra* note 38, at 42.

[48] Stone, *supra* note 35, at 165.

indicate that the roles women hold are not arbitrary. They are the result of strategic decisions made by male leaders. The locus of this decision is crucial to fully understand women's power and position in armed Islamic groups: regardless of a woman's dedication to a group or cause, her participation and the scope of her role is contingent upon male leaders' approval.

Even when women are permitted to participate in Islamic armed groups, men continue to dictate women's involvement. For example, al-Shabaab rigidly excludes women from violent roles. After the Westgate mall attack, al-Shabaab quickly countered media reports that Samantha Lewthwaite was part of the attack, tweeting: "We have an adequate number of young men who are fully committed and we do not employ our sisters in such military operations."[49] This statement reinforces al-Shabaab's promotion of masculinity and a patriarchal rule. In AQI, it was Zarqawi's decision to include women in suicide attacks. Interestingly, once women in AQI were permitted to hold public roles, it appears that some women were given increasing autonomy, exemplified by the all-female Naseeba al-Ansariya Martyrdom Battalion and by the actions of Samira Ahmed Jassim, "the mother of believers."[50]

Although many Islamic groups share ideological roots, a context-specific, gendered analysis reveals that these groups are not monolithic in their strategies and tactics, nor in roles they permit women to hold. This is evidenced by al-Shabaab and AQI. Thus, it is clear that there is no "universal role" for female participants in Islamic armed groups, as each organization uses women to help achieve its specific goals. Therefore, it is critical for policymakers and analysts to assess the context, ideological developments, leadership, and status of women in each society and within each armed group in order to fully understand the changing—or static—role of women.

Finally, the largely private nature of the roles held by women in Islamic armed groups does not diminish their importance. These roles are vital for the success and longevity of the group. Not only do they perform administrative functions that are crucial for the day-to-day maintenance of the group, but their roles serve to preserve the morale of fighters and to raise future generations of group members.

Given the current global landscape and the prevalence of non-state actors, it is critical for policymakers to recognize that not all

[49] *Al-Shabab Denies Women Involved in Kenya Mall Attack*, BBC NEWS (Sept. 24, 2013), http://www.bbc.com/news/uk-24235136.

[50] Haynes, *supra* note 36.

Islamic armed groups are the same. Countering these groups requires a nuanced strategy. An essential component of this refined approach is a context-specific analysis of women's participation in each group. Whether private or public, the roles each group permits women to hold provides invaluable insight into the group's specific ideology, strategy and future movements.

Key Findings

- A contextualized, gendered analysis reveals that the roles of women in Islamic armed groups are not uniform, despite the groups' shared ideological roots.
- Private roles, like that of wives and mothers, are essential to the success and sustainability of armed groups. Thus, analysts must examine roles beyond front-line positions. The case studies of al-Shabaab and al-Qaeda in Iraq ("AQI") reveal the varying roles of women and how they shift over time.
- Prior to the establishment of al-Shabaab and AQI, women in Somalia and Iraq held public roles in society. Later, conflict and insecurity in both countries provided political leaders with the opportunity to diminish the roles of women. As a result, women were relegated to the private sphere, enabling armed groups to exploit women's new social standing for their own benefit.
- Women in both al-Shabaab and AQI served in mainly private roles. Yet women in AQI also served in public, violent roles. Iraqi and Western women were used as suicide bombers inside and outside of Iraq. This tactic allowed AQI to project power locally and globally. In contrast, al-Shabaab denies any use of women in public, violent roles.
- Al-Shabaab's exclusion of women from public roles is likely due to the group's reliance on the premise of male domination over women and on support from local elders and some in the community. In contrast, AQI's brutal and violent tactics, including the use of women as suicide bomb attacks, heavily eroded the group's local support.

Countering ISIL: A Need for an Effective Strategy

LTC Pat Kaune, USA, Army War College Fellow

"The key to the art, not the science, but the art, of strategy is to design a multi-pronged approach tailored to each individual case . . . All activities affect all others and the overall success or failure of the outcome."
[1]

The current military strategy to counter the Islamic State of Iraq and the Levant ("ISIL") lacks sufficient means and effective ways to achieve our ends. First, Operation INHERENT RESOLVE lacks credible partners to effectively combat ISIL. Currently, the Iraqi Army ("IA"), the Kurdish Peshmerga, and so-called moderate Syrian rebel forces lack the training and or equipment to achieve the degradation of or destruction of ISIL. Secondly, the military campaign, a combination of bombing ISIL targets with a train, advise and assist approach yields inconclusive results at best. Lastly, if the United States is unwilling to consider alternatives such as employing its own forces as "boots on the ground", then it must partner with those forces it expects to achieve its strategic aims. General (R) David H. Petraeus recognized this as he testified that military actions need to support political settlements and "that context will not materialize on its own. We and our partners need to facilitate it—and over the past four years, we have not done so."[2] Failure to review our strategic approach or properly resource our allies fails to produce a strategy that will defeat ISIL's will to "last and expand."[3] Failure to assess the effectiveness of our military campaign at best, wastes precious resources and at worst risks placing the U.S at a strategic disadvantage in the region.

First our military strategy lacks an effective means in a credible ground force to effectively execute any way designed to "degrade, and

[1] John Blaney, *The Art of Strategy Creation for Complex Situations*, 5 PRISM, no. 3, at 30.

[2] Michael R. Gordon and Eric Schmitt. 2015, *David Petraeus Urges Stronger U.S. Military Effort in Syria*, N.Y. TIMES, (Sept. 22, 2015), http://www.nytimes.com/2015/09/23/world/middleeast/david-petraeus-urges-stronger-us-military-effort-in-syria.html?_r=0.

[3] CHARLES R. LISTER, THE ISLAMIC STATE A BRIEF INTRODUCTION 5 (Brookings Institution, 2015).

ultimately destroy, ISIL through a comprehensive and sustained counterterrorism strategy."[4] A central tenet of Winning in a Complex World is that our military operates as a joint multinational force and integrates multiple partners.[5] Iraqi Security Forces ("ISF"), Syrian rebels and the Kurdish Peshmerga have flaws which require various degrees of training or enhanced operational support. Limiting options involving increased "boots on the ground" inhibits U.S forces to effectively partner with these means to produce a force capable of defeating ISIL. Current national strategy directs the "arming and training of the Iraqi army, the Kurdish Peshmerga fighters and moderate Syrian Rebels."[6] However, this approach is flawed in assuming the ISF will achieve such a proficiency level without U.S operational support. Moreover, ISF faces serious manning deficits, lacks systemic accountability, and assigns more than 40 percent of their force to the Baghdad operations command.[7] The survey also found that Counter-Terrorism Services ("CTS")-Iraq Special Forces, faces critical manning shortfalls and remains at 40 percent of its manning level.[8] Another example in failing to produce an effective means is the failed attempt to train moderate Syrian Rebels. The program illustrates that creating a viable force entails more actions than just merely allocating 500 million dollars for training.[9] Failing to properly resource such a program undermines U.S credibility by failing to provide protection for potential partners and wasting resources. General Lloyd. J. Austin, Commander, United States

[4] Press Secretary, Office of the White House, *Fact Sheet: Strategy to Counter the Islamic state of Iraq and the Levant (ISIL)*, WHITE HOUSE, (Sept. 10, 2014), https://www.whitehouse.gov/the-press-office/2014/09/10/fact-sheet-strategy-counter-islamic-state-iraq-and-levant-ISIL.

[5] UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND (TRADOC), TRADOC PAMPHLET 525-3-1 THE UNITED STATES ARMY OPERATING CONCEPT 2016–2028 VI (Headquarters of the Army, Training and Doctrine Command 2014), www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

[6] Sanu Kainikara, *The Articulated Strategy to Fight the Islamic State: Is it Self-Defeating?*, STRATEGIC ANALYSIS 39, no.1, at 16–21 (July 27, 2015), http://dx.doi.org/10.1080/09700161.2014.980541.

[7] Linda Robinson, *An Assessment of the Counter-ISIL Campaign One Year After Mosul*, RAND, 2–3 (Aug. 25, 2015), http://www.rand.org/pubs/testimonies/CT435z1.

[8] *Id.* at 4.

[9] Lolita C. Baldor, *US Looking for Ways to Fix Syrian Rebel Program*, MARINE CORPS TIMES, (Sept. 8, 2015), http://www.marinecorpstimes.com/story/military/2015/09/08/us-looking-ways-fix-syrian-rebel-program/71903794/.

Central Command, testified that a ten month, $500 million effort resulted in only 4 or 5 trained fighters.[10] Moreover, identifying so-called "moderate" rebels presents an insurmountable task given the numerous threats to our potential allies in Syria. Furthermore, strategic environment itself presents many obstacles to protecting and training Syrian forces. As the Center for a New American Security concluded, "military training of Syrian rebels on the territory of regional allies will be complicated by the insistence of these allies that the rebels be encouraged to fight the Assad regime as well as ISIL."[11] Consequently, any strategy which relies upon an unreliable means is doomed to fail in that "[t]here are no rebels of the right hue and caliber to arm and train in Syria, unless such an action is initiated to support the government troops. This is anathema to the US and its allies, and rightly so, given the Bashar regime's track record so far . . . ."[12] Failing to properly prepare our partners jeopardizes the strategic approach in that it fails to produce a means capable of achieving a desired end.

Next, the military campaign lacks creativity in its utilization of a train, advise, and assist portion to partner with potential means identified above. CENTCOM employed a Defense Department "cookie-cutter" approach in the "$1.6 billion Iraq Train and Equip Fund, a scaled-down version of the massive U.S. programs that created Iraqi duplicates of U.S. brigades in 2005–2008."[13] However, such an approach incorrectly assumes the 2015 ISF matches the ISF which partnered with the U.S.in 2005–2008. Operations to retake ISIL controlled territory, a predominantly Sunni populace, will require not only enhancing but also influencing the actions of the Shia militias as part of the ISF and the Peshmerga. A Rand survey identified these challenges as it concluded U.S. strategy needed to be "more proactive

[10] Nancy Youssef and Tim Mack, *Obama's General Just Set His ISIS War Plan on Fire*, DAILY BEAST, (Sept. 16, 2015), http://www.thedailybeast.com/articles/2015/09/16/obama-s-general-just-set-his-ISIS-war-plan-on-fire.html?via=mobile&source=email.

[11] SHAWN BRIMLEY, ET AL., IDEAS TO ACTION SUGGESTIONS FOR THE 25TH SECRETARY OF DEFENSE, CTR. FOR NEW AM. SEC. 11 (2015).

[12] Kainikara, *supra* note 6, at 19.

[13] Michael Knights*, No One Talks About Liberating Mosul Anymore,* FOREIGN POL'Y (Aug. 11, 2015), http://foreignpolicy.com/2015/08/11/no-one-talks-about-liberating-mosul-anymore-iraq-islamic-state-military-pentagon/?utm_content=buffer92f03&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.

in coordinating with these forces on the battlefield to produce more gains in the anti-ISIL fight . . . vis-à-vis the Shia militias could also entail efforts to mitigate the two widely acknowledged risks of their currently large and growing role."[14] General Milley acknowledged training may not be enough in considering all bilateral military cooperation between the two countries.[15] For example, only a small number of U.S. trained soldiers reside in the ISF and Kurdish Special Forces due to the possibility that U.S. airpower could be manipulated to settle old scores.[16] Limited action on August 3, 2015, illustrates the need for more support as the coalition only intervened in eight locations on the ground while the war raged across a front line greater than 1200 miles.[17] Effective partnering should involve close combat advisors who "will have to accompany their supported units into battle, not just wave goodbye as they leave the base."[18] Simply put, enhancing our partner's performance not only increases their ability to achieve desired effects against ISIL, but also our ability to mitigate potential undesired outcomes in sectarian violence. General Mark A. Milley acknowledged this need as he opined "My experience . . . is that the indigenous force or the force you are advising typically performs better when advisors accompany them into various operations."[19]

Lastly, in failing to produce a credible ground force, the military's air campaign presents as the only effective dilemma faced by ISIL. Winning in A Complex World also prescribes that as part of a joint, inter-organizational, and multinational team, our military "operate across multiple domains, and present our enemies with *multiple* dilemmas."[20] As the enemy in Vietnam, ISIL adapted and

[14] Robinson, *supra* note 7*,* at 7–8.

[15] Michelle Tan, *Army Chief of Staff Makes Surprise Visit to Iraq*, MILITARY TIMES (Sept. 3, 2015, 3:17 PM), http://www.armytimes.com/story/military/pentagon/2015/09/03/army-chief-staff-makes-surprise-visit-iraq/71647490/.

[16] Knights, *supra* note 13.

[17] *Id.*

[18] David Kilcullen, *I See No Alternative to a Larger, More Intense Conventional War Against Isis*, GUARDIAN (July 10, 2015), http://www.theguardian.com/commentisfree/2015/jul/10/i-see-no-alternative-to-a-larger-more-intense-conventional-war-against-isis.

[19] Michelle Tan, *New Chief: We Cannot Allow a Hollow Army*, ARMY TIMES (Oct. 24, 2015, 10:04 AM), http://www.armytimes.com/story/defense/show-daily/ausa/2015/10/24/new-chief-we-cannot-allow-hollow-army/73560482/.

[20] TRADOC, *supra* note 5, at VI (emphasis added).

airpower effectiveness "declines as ISIL targets inevitably disperse."[21] Credible ground forces would introduce another dilemma to a force trying to retain its land and "increase their exposure to attack."[22] As a U.S. senior official admitted, the strategy lacks ground forces and that "[a]irstrikes are effective, but airstrikes alone will not win this fight."[23] Currently, ISIL remains capable of surviving and expanding through exerting force, collecting taxes and oil revenues as well as administering territory.[24] As of October 8, 2015, CENTCOM identified 13,781 damaged or destroyed targets to include tanks, vehicles, fighting positions, buildings, and oil infrastructure.[25] However, CENTCOM numbers may not substantially capture the effectiveness of the current approach. A campaign review concluded strikes averaged a total of twenty-five a day in Iraq and Syria combined and that ISIL forces adapted to it through dispersion or sheltering amongst populated areas.[26] Another reason for the air campaign's ineffectiveness is the approach lacks a proven method of Special Forces combat advising indigenous partners; instead the method opts to embed advisors in Iraqi headquarters.[27] A lack of ground forces and limited Intelligence, Surveillance, and Reconnaissance ("ISR") assets shows a lack of commitment in partnership. Such support proves untimely in relying upon the coordination between an ISF headquarters and the Combined Air Operations Center ("CAOC") in Qatar.[28] One system review

[21] RICHARD LIM, TERRORISTS, INSURGENTS AND THE LESSONS OF HISTORY 5–7 (AUSA Institute of Land Warfare, 2014).

[22] *Id.*

[23] W. J. Hennigan & Brian Bennett, *U.S. Faces Pressure to Change its Strategy in Syria*, L.A. TIMES (Sept. 9, 2015, 5:26 PM), http://www.latimes.com/world/europe/la-fg-us-syria-20150910-story.html.

[24] Graeme Wood, *What ISIS Really Wants*, ATLANTIC, (March 2015), http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/.

[25] Combined Joint Task Force, Operation Inherent Resolve, Post to Combined Joint Task Force—Operation Inherent Resolve Official Facebook Page, (last visited Oct. 19, 2015), https://www.facebook.com/CJTFOIR?fref=ts.

[26] Anthony H. Cordesman, *The Imploding U.S. Strategy in the Islamic State War*, CTR. FOR STRATEGIC & INT'L STUDIES (Oct. 23, 2014), http://csis.org/publication/imploding-us-strategy-islamic-state-war.

[27] Scott A. Vickery, *Operation Inherent Resolve: An Interim Assessment Policy Watch 2354,* WASH. INST. FOR NEAR EAST POL'Y (Jan. 23, 2015), http://www.washingtoninstitute.org/policy-analysis/view/operation-inherent-resolve-an-interim-assessment.

[28] *Id.*

determined that "Iraqi command-and-control appears too lethargic to pass targets to the CAOC in a consistently timely manner."[29] Furthermore, Information Handling Services ("IHS") of Jane's Terrorism and Insurgency Center concluded that ISIL daily average number of attacks actually rose to 11.8 from 8.3, between July 1 and September 30, 2015.[30] The IHS also found that ISIL's capacity to wage a territorial-focused insurgency in conjunction with a "punitive campaign of terrorist attacks remains undiminished."[31] Consequently, the military campaign's reliance upon a bombing campaign in concert with a train, advise, and assist methodology requires an assessment of its current means and ways to achieve any decisive results.

Without such an assessment, current military strategy to counter ISIL will continue to produce ineffective results. The U.S. military should consider its current methodology to countering ISIL and develop new options to increase the effectiveness of the military campaign. As General Milley aptly stated, "[w]hat you want to do in any war is you want to continually assess your assumptions, continually assess the ways and means you are going to achieve the end state."[32] A strategy that relies solely upon an air campaign to challenge the enemy will not allow us to partner effectively with ground forces to mitigate the "toleration of Sunni populations hostile to government forces" which allowed ISISIL to seize large territories in Iraq and Syria.[33] Employing U.S. ground forces to degrade and destroy ISIL is an option. Such an option need not include nation-building as part of its end state. Decision makers must recognize that "half-hearted measures and further delay will only strengthen ISIL's position and ensure confrontation at a later date in which the United States is at a greater strategic disadvantage."[34] Lastly, in reviewing all strategic elements of power, our senior leaders must begin with the end in mind and assess a drastically changed strategic environment. Strategists must acknowledge ISIL "is a problem that cannot be

[29] *Id.*

[30] Cassandra Vinograd, *ISIS Attacks Soared in Past 3 Months: IHS Jane's Database*, NBC NEWS (Oct. 22, 2015, 12:52 AM), http://www.nbcnews.com/storyline/isis-terror/isis-attacks-soared-past-3-months-ihs-janes-database-n448401.

[31] *Id.*

[32] Tan, *supra* note 19.

[33] Vickery, *supra* note 27.

[34] LIM, *supra* note 21, at 5–7.

divorced from the regional crisis that gave birth to it."[35] Root cause analysis finds it originated from both political crisis and sectarian tensions within Syria and Iraq.[36] Perhaps the current strategy serves as the best of bad options available in "continuing to slowly bleed it (ISIL) though air strikes and proxy warfare."[37] Regardless, a sound military strategy should assess *all* feasible options and rigorously identify how to develop the means and or modify the ways necessary to achieve strategic aims.

[35] Burak Kadercan, *Why Fighting Through Auxiliaries Often Fails*, NAT'L INTEREST, (Sept. 13, 2015), http://nationalinterest.org/feature/why-fighting-through-auxiliaries-usually-fails-13818?page=3.

[36] *Id*.

[37] Wood, *supra* note 24.

The Digital Dye Pack: Confronting Crypto-Currencies and the Modern Terrorist

John Caton

Introduction

Since the advent of Bitcoin in 2009, crypto-currencies are most widely known as an exclusively online form of payment for drugs, weapons and even assassins.[1] Touted for being virtually anonymous and free from the influence of any government, virtual currencies have taken on a life of their own with over 650 variants currently in circulation.[2] Recently, terrorist organizations such as the Islamic State have taken note of the potential these crypto-currencies have to offer and have taken active steps to finance their operations on a global scale.[3] While the United States government has taken steps to address the security risks such technology presents, inconsistent and often contradictory treatment of crypto-currencies by various federal agencies poses an immense risk to the country as a whole. This inconsistent treatment coupled with the non-physical and technological nature of cypto-currencies has precluded the federal government from fully utilizing the all anti-money laundering and anti-terrorism legislation at its disposal. It is the author's policy recommendation that the United States government take active steps to formally recognize all virtual coinage as a legitimate form of currency and therefore subject to all pre-existing laws relating to money laundering and terrorism financing.

History of Bitcoin & Terrorism

The first crypto-currency to enter circulation, Bitcoin, was created by either an individual or group of individuals under the

[1] *History of Bitcoin: The world's first decentralized currency*, http://historyofbitcoin.org/ (last visited Jan. 23, 2016).

[2] *Map of Coins*, http://mapofcoins.com/bitcoin (last visited Jan. 23, 2016).

[3] Brooke Satti, *ISIS. Are they Using Bitcoins to Fund Criminal Activities?*, Sec. Intelligence (Oct. 29, 2014), https://securityintelligence.com/isis-are-they-using-bitcoins-to-fund-criminal-activities/.

pseudonym Satoshi Nakamoto.[4] The original whitepaper released by Nakamoto states that Bitcoin was created with the aim of eliminating the "trust based model" established by third party vendors (banks) when it comes to processing electronic transactions.[5] The same document goes on to argue that high transaction costs and limitations on the size of such transactions, hinders not only the prospect of streamlining casual money transfers, but establishes "a broader cost in the loss of ability to make non-reversible payments for non-reversible services."[6] Bitcoin's structure decentralizes the electronic money transfer system; meaning it is not controlled by any single bank or government. Bitcoin replaces these "trust systems" with a cryptographic "proof of work" system which will be explored in greater detail later in this paper.[7]

Following the first Bitcoin exchange's creation in February 2010, terrorist organizations and governments alike began to take notice of the potential Bitcoin and other crypto-currency spin-offs had to offer in terms of anonymously transferring funds.[8] An inter-governmental anti-money laundering task force known as the Financial Action Task Force published a report outlining how virtual currencies can be used to enable criminal networks to hide their funds.[9] In October 2010, the largest crypto-currency exchange at the time, Mt. Gox, switched its payment service platform to a virtual currency service known as Liberty Reserve.[10] Liberty Reserve was ultimately shut down in 2013 by United States federal prosecutors for laundering over $6 billion for criminal and terrorist organizations. Additionally, Mt. Gox's website was shut down in February 2014, taking with it an estimated $450,000,000 worth of crypto-currencies.[11]

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin Project, https://bitcoin.org/bitcoin.pdf (last visited Jan. 22, 2016).

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] History of Bitcoin, *supra* note 1.

[9] *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FIN. ACTION TASK FORCE (June 2014), http://www.scribd.com/doc/231929964/Virtual-Currency-Key-Definitions-and-Potential-Aml-Cft-Risks.

[10] History of Bitcoin, *supra* note 1.

[11] PAUL ANNING, STUART HOEGNER, & JERRY BRITO, THE LAW OF BITCOIN (2015).

Financing Terrorism

Given the decentralized and near-anonymous nature of crypto-currencies, numerous terrorist organizations have taken steps to begin funding their nefarious operations via such technology. The Islamic State of Iraq and Syria ("ISIS") in particular has begun utilizing Bitcoins to "crowd source" its operations and potentially fund operatives in the United States.[12] An online anti-terrorist hacking collective, known as Ghost Security, or GhostSec, allegedly discovered a Bitcoin wallet linked to a known ISIS IP address. As of September 2015 the Bitcoins in the alleged ISIS wallet was valued at over 3 million dollars.[13] Given GhostSec's prior role in averting terrorist attacks in the City of New York as well as Tunisia, government authorities are taking serious note of this discovery.[14]

In light of the November 2015 attacks in Paris, much of the world has taken note of the danger crypto-currencies present in the modern world. In October of 2013, it was discovered that the Swedish crypto-currency conversion site, Yourserver.se, was being used to fund the ISIS blog website, Al-Khilafah Aridat.[15] This site provided directions on how to use Bitcoin to donate to ISIS.[16] Additionally, in 2014, seventeen-year-old Ali Shukri Amin was arrested in the United States for providing directions on how to use Bitcoin to support ISIS.[17]

[12] Danna Harman, *U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*, HAARETZ (Jan. 29, 2015), http://www.haaretz.com/middle-east-news/.premium-1.639542.

[13] Lewis Sanders, IV, *Bitcoin: Islamic State's Online Currency Venture,* Deutsche Welle (Sep. 20, 2015), http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856.

[14] Anthony Cuthbertson, *Anonymous affiliate GhostSec thwarts Isis terror plots in New York and Tunisia*, International Business Times (July 22, 2015, 5:27 PM), http://www.ibtimes.co.uk/anonymous-affiliate-ghostsec-thwarts-isis-terror-plots-new-york-tunisia-1512031.

[15] Satti, *supra* note 3.

[16] Al-Khilafah Aridat, https://alkhilafaharidat.wordpress.com/ (last visited Jan. 22, 2016).

[17] Deborah Hastings, *Va. teen gets 11 years in prison for tweeting about ISIS, aiding the terrorist group*, N.Y. Daily News (Aug. 28, 2015), http://www.nydailynews.com/news/national/va-teen-11-years-prison-aiding-isis-article-1.2340577.

Presently, the European Union is exploring options on how to limit the methods by which crypto-currencies can be used to fund ISIS.[18]

How Crypto-Currency Functions

The first issue to consider when examining how crypto-currencies may finance terrorism around the globe is to understand how a decentralized electronic currency functions without the support of a centralized financial system. In the modern age, most government tender is considered "fiat currency," meaning the money is not tied to any physical commodity.[19] Historically, a country's paper currency was tied to goods such as gold or silver.[20]

One of the many ways the United States Federal Reserve regulates the value of the dollar is to control the amount of money in circulation.[21] Charged, "to promote sustainable growth, high levels of employment, stability of prices to help preserve the purchasing power of the dollar and moderate long-term interest rates," this central banking system accomplishes this goal by studying the United States economy and forecasting future changes in the global marketplace.[22] Periodically, the U.S. Bureau of Engraving and Printing implements new security features in the American dollar so as to prevent forgers from illegally printing their own money.[23]

Today, crypto-currencies function very much in the same way as any government backed legal tender, with the exception that it is not controlled by any single centralized system. Crypto-currencies such as Bitcoin, Dogecoin, or Litecoin are not supported by any physical commodity, making them a "fiat currency," much like the dollar, euro,

[18] Mary-Ann Russon, *Paris attacks: EU to crack down on bitcoin transfers in attempt to strangle Isis funding*, Int'l Bus. Times (Nov. 20, 2015, 11:50 AM), http://www.ibtimes.co.uk/paris-attacks-eu-crack-down-bitcoin-transfers-attempt-strangle-isis-funding-1529693.

[19] Doug Levinson, *What gives a dollar bill its value?*, TedEd, https://www.youtube.com/watch?v=XNu5ppFZbHo&ab_channel=TED-Ed (last visited Jan. 22, 2016).

[20] *Id.*

[21] Mark Koba, *The Federal Reserve: CNBC Explains*, CNBC (Mar. 18, 2015, 9:21 AM), http://www.cnbc.com/id/43752521.

[22] *Id.*

[23] *U.S.* Currency, BUREAU OF ENGRAVING & PRINTING, http://www.moneyfactory.gov/uscurrency.html (last visited Jan. 22, 2016).

or peso.[24] The role of a centralized banking system, such as the U.S. Federal Reserve, is replaced by a given crypto-currency's open source core software.[25] Among other services, this software automatically regulates how much of the virtual coinage is placed in circulation at any given time and is in turn supported by the users of the given crypto-currency.[26]

Today, the vast majority of all crypto-currencies in circulation follow the Bitcoin model and algorithm of peer-to-peer currency exchange.[27] Crypto-currency users store their virtual money in electronic wallets, from which requests to send or receive funds are generated.[28] The manner in which these wallets encrypt requests to send/receive funds as well as the process by which digital currency "miners" verify and carry out transactions not only make crypto-currency use extremely reliable but nearly anonymous as well.[29] Should any security vulnerabilities be identified, the given crypto-currency's development team quickly patches the core software and pushes the update onto all of the users of the crypto-currency.[30]

Pools of online users, known as miners, run a given crypto-currency's core software on a single computer or banks of computers. These miners receive "blocks" of virtual currency transactions, which are encrypted with highly complex mathematical codes that take enormous computing power to solve.[31] By solving these transaction blocks, miners not only confirm the validity of a crypto-currency

[24] Kevin Drumm, *Bitcoin Is a Fiat Currency, But That's Not Its Big Problem*, Mother Jones (Feb. 25, 2014, 11:54 AM), http://www.motherjones.com/kevin-drum/2014/02/bitcoin-fiat-currency-thats-not-its-big-problem.

[25] Zulfikar Ramzan, *Bitcoin: Transactions Block Chains*, Khan Acad. (Nov. 11, 2015), https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-block-chains.

[26] Gheorghe Popescu, *The Economics of the Bitcoin System*, 2 J. OF SELF-GOVERNANCE & MGMT. ECONS. 57–62, no. 1 (2014).

[27] *See* James Trevaskis, *Bitcoin 101: What you need to know about Crypto-Currencies*, ABC.Net.Au (Sept. 25, 2013), http://www.abc.net.au/technology/articles/2013/09/25/3855973.htm.

[28] Zulfikar Ramzan, *supra* note 25.

[29] Edward Murphy, *Federation of American Scientists*, Cong. Research Serv. (Nov. 12, 2015), https://www.fas.org/sgp/crs/misc/R43339.pdf.

[30] Danny Bradbury, *Bitcoin Development Team Patches its Own Security Patch*, COINDESK (Dec. 18, 2015), http://www.coindesk.com/bitcoin-development-team-patches-its-own-security-patch/.

[31] Nakamoto, *supra* note 4.

transaction, but are awarded for their services with new virtual coinage by the given core software.[32] The difficulty of solving these transaction blocks increases or decreases depending on the amount of time it took for all of the miners in a given crypto-currency network to solve a pre-determined number of transaction blocks.[33] Likewise, the new crypto-currencies awarded to miners per block mined decreases over time.[34] These features were implemented by design so as to regulate the amount of a new crypto-currency entering the marketplace without any centralized banking system.[35]

All crypto-currency transactions are placed in a public ledger, known as a "blockchain," so the entire crypto-currency community is aware of how much of the given virtual coinage is in circulation.[36] By maintaining this public ledger, users of the given crypto-currency are able to safeguard against fraudulent transactions and counterfeit creation of the new crypto currency.[37]

Most crypto-currency wallets and free online services are able to generate Quick Response (QR) codes, a type of barcode, which when scanned, provides an individual with a virtual wallet address that he or she may then transmit funds to.[38] While this service was designed to provide traditional brick and mortar stores the ability for users to pay in crypto-currency with relative ease, such features can also be used for nefarious purposes. Once a QR code has been generated, a terrorist organizations could hypothetically discretely place QR codes nearly anywhere in the physical world and receive direct funding without having to contact their donors in person. The use of QR codes on The Onion Router ("TOR") webpages essentially

[32] *What is Bitcoin mining?*, Bitcoin Mining, https://www.bitcoinmining.com/ (last visited Jan. 22, 2016).

[33] Bitcoin Difficulty and Hashrate Chart, BITCION WISDOM, https://bitcoinwisdom.com/bitcoin/difficulty(last visited Jan. 22, 2016).

[34] Nikhil Gupta, *How Will 2017's Block Reward Halving Affect Bitcoin Price?*, NEWSBTC (Mar. 13, 2015, 6:19 PM), http://www.newsbtc.com/2015/03/13/how-will-2017s-block-reward-halving-affect-bitcoin-price.

[35] Popescu, *supra* note 26.

[36] Nakamoto, *supra* note 4.

[37] *Id.*

[38] Elbert Alias, *Bitcoin QR Code Generator*, http://bitcoinqrcode.org/ (last visited Jan. 22, 2016).

allows both lone wolf attackers and organized terrorists factions to "crowd source" their nefarious operations.[39]

The Flaws of Crypto-Currency

Relatively speaking, crypto-currency is in its infancy and is likely to experience growing pains over the next couple of decades. The largest issue facing the major virtual currencies is the very transparency it promotes. As more and more transaction blocks are solved and added to the blockchain, all users must continually download the entire blockchain to their virtual wallet if they wish to continue using their crypto-currency.[40] It is speculated, in the case of Bitcoin, that users must ultimately either accept a centralized system that handles participants' wallets or migrate to another crypto-currency altogether .[41] Given the collapse of the centralized Bitcoin exchange, Mt. Gox, crypto-currency users may be inclined to stay away from using other centralized services and instead use different crypto-currencies altogether.[42]

Another major drawback of using crypto-currencies is their high volatility. Even among the more established virtual currencies, such as Bitcoin, prices have never remained stable. An example of this was the price of $1000 per Bitcoin in early December 2013, which decreased in value to $382 by mid-December 2013.[43]

[39] Kara Foxx, *FBI Head Warns of 'Crowdsourced Terrorism' and Online Predators*, Fox19 News (Oct. 15, 2015, 10:10 PM), http://www.fox19.com/story/30264432/fbi-head-warns-of-crowdsourced-terrorism-and-online-predators.

[40] Pete Rizzo, *Researchers Tackle Tomorrow's Blockchain Problems with Bitcoin*, CoinDesk (Sept. 18, 2015), http://www.coindesk.com/cornell-research-blockchain-problems-bitcoin-ng.

[41] *Id.*

[42] John Boyd, *The Mt. Gox Bitcoin debacle: An update*, IEEE Spectrum (Nov. 3, 2015, 5:08 PM), http://spectrum.ieee.org/tech-talk/computing/networks/the-mt-gox-bitcoin-debacle-an-update.

[43] *Bitcoin in USD Price Rate Chart*, CoinPlorer, https://coinplorer.com/Charts?fromCurrency=BTC&toCurrency=USD (last visited Jan. 22, 2016).

Status Quo

At the present time, the United States Treasury's Financial Crimes Enforcement Network ("FINCEN") has ruled that virtual-currency exchanges fall under the category of "money transfer services," which subjects them to Money Services Business ("MSB") regulations under the U.S. Bank Secrecy Act ("BSA").[44] In a somewhat contradictory fashion, however, FINCEN has ruled that any company that is "purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is not a money transmitter," and therefore do not fall under any BSA or Patriot Act regulations.[45] While this announcement was designed to clarify mining issues surrounding an earlier FINCEN publication, the proclamation's lack of clarity has only served to muddy the waters of what constitutes a crypto-currency exchange versus a company that buys and sells virtual currency as an investment.[46] This lack of specificity clearly paves the way for terrorist shell corporations to act as de facto crypto-currency exchanges and money laundering stations.

Given the ease with which shell companies can be established, these foreign "virtual currency" investment companies have the potential to not only anonymously convert crypto-currencies into the U.S. dollar, but they could likewise convert any funds into a crypto-currency of their choice.[47] The fact that FINCEN specifically labels companies that engage in crypto-currency investments as "not money transmitters," and then fails to specify what constitutes normal investment behavior, opens an entirely new loophole by which terrorist organizations could anonymously fund their operations.[48] While FINCEN reserves the right to determine what constitutes a crypto-

[44] Murphy, *supra* note 29.

[45] Steve Hudak, *FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors*, U.S. Dep't of Treasury, Fin. Crimes Enf't Network (Jan. 30, 2014), https://www.fincen.gov/news_room/nr/html/20140130.html.

[46] *Id.*

[47] Jason Sharman, *Shopping for Anonymous Shell Companies: An Audit Study of Anonymity and Crime in the International Financial System*, 24 J. OF ECON. PERSPECTIVES 127, 127–140 (2010), http://www.jstor.org/stable/20799176.

[48] Jamal El-Hindi, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, (Jan. 30, 2014), http://www.jdsupra.com/legalnews/application-of-fincens-regulations-to-v-78635/.

currency exchange, the agency specifically states that the burden falls on the company to report itself as a virtual currency exchange, should it migrate away from purchasing and selling crypto-currencies for exclusively investment purposes.[49]

Current Legal Parameters on Money Laundering

The majority of financial crimes related to funding terrorism both in the United States and abroad fall under the purview of the BSA and specific sections of the Patriot Act. The BSA, otherwise known as the "Currency and Foreign Transactions Reporting Act," mandates "financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities."[50] The Patriot Act, officially known as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," has twelve sections dedicated to enhancing the BSA's pre-existing money laundering laws as well as "Know Your Customer" banking statues to include international financial institutions.[51]

Crypto-Currencies in the United States

Despite crypto-currencies being classified by the U.S. Treasury Department as a decentralized virtual currency, it is often not treated or even recognized by other government agencies as such.[52] The Federal Election Commission ("FEC") has ruled that donations in the form of Bitcoin are not liable to the same legal scrutiny as traditional

[49] *Id.*

[50] *FinCEN's Mandate from Congress*, U.S. Dep't of Treasury, https://www.fincen.gov/statutes_regs/bsa/ (last visited Jan. 22, 2016).

[51] *Id.*

[52] J. S. Calvery, *Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Growth, Tax and Capital*, https://www.fincen.gov/news_room/testimony/html/20131119.html (last visited Nov. 19, 2015).

currency donations.[53] While the FEC did rule that a campaign may only accept up to $100 worth of Bitcoins, given the high volatility of most crypto-currencies, the aforementioned $100 in Bitcoins could hypothetically appreciate to $1000 overnight.[54] The Internal Revenue Service identifies crypto-currency miners as self-employed workers and the currency they mine to be property liable for taxation.[55] This lack of a standard definition of crypto-currencies by all agencies of the federal government not only hinders the identification and capture of the financers of terrorism, but could result in tax fraud, and questionable campaign financing.

Three Near-Immutable Aspects of Crypto-Currencies

In a perfect world, virtual currencies would be treated as a commodity capable of being regulated, tracked and studied. Their inherit value would remain fairly stable and centralized in a single public or private organization. However, given that crypto-currencies are inherently volatile, non-physical, decentralized and constructed with anonymity in mind, many traditional solutions simply cannot be applied. The following three aspects of virtual currencies must be taken as fact when developing any meaningful anti-terror crypto-currency government policy:

1. Organizations seeking to use crypto-currencies for nefarious means will utilize any and all anonymity services available to make their financial transactions as close to completely anonymous as possible.
2. Crypto-currencies are inherently designed to be released into the virtual economy at a steady pre-determined rate, so as to prevent any one group from manipulating the currency.
3. Given the vast variety of crypto-currencies in circulation, should any single virtual currency collapse for any reason,

[53] Dave Levinthal, *What the FEC's Bitcoin ruling means*, Ctr. for Pub. Integrity (May 8, 2014, 1:36 PM), http://www.publicintegrity.org/2014/05/08/14739/what-fecs-bitcoin-ruling-means.

[54] *Id.*

[55] *Internal Revenue Service guidelines on reporting crypto-currency*, Internal Revenue Serv. 4 (2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

> users will switch to another crypto-currency rather than abandon using crypto currencies altogether.

While most virtual currencies are not entirely anonymous, near complete anonymity can be achieved by utilizing services such as TOR, crypto-currency laundry services, encrypted wallets and even specialized virtual currencies designed to be completely untraceable.[56] Likewise, crypto-currencies that follow the Bitcoin model of distribution are designed to be inflation proof, meaning the reward per transaction block is determined by the number of miners working on the aforementioned transaction block.[57] Aside from independently regulating how much of a given crypto-currency is released into the virtual marketplace at any given time, the manner in which the Bitcoin decentralized system is designed, it is nearly impossible for any single public or private entity from gaining control of how a given crypto-currency operates.[58]

The global online community of crypto-currency users value both the overall autonomy and anonymity such forms of money provide. Given there are over 650 crypto-currencies to choose from, unless an inherit flaw is found in the source code of every virtual currency, users are more likely to switch to a new crypto-currency rather than stay with a possibly corrupted model.[59] Additionally, since nearly all crypto-currency programming is open source, the online community is likely to identify any issue long before any government is able to capitalize on the flaw.

Wrong Solutions

While a first world solution to prevent the nefarious use of decentralized virtual currencies would be to place it under centralized control, the collapse of Mt. Gox and the online community's general desire to remain anonymous have largely removed any chance of government controlled crypto-currency exchanges from being widely accepted.[60] A secondary solution of taking over the crypto-currency market with the intent of removing all currency from circulation via

[56] Andy Greenberg, *5 Bitcoin projects that could make payments far more anonymous*, Wired (May 5, 2015, 6:30 AM), http://www.wired.com/2014/05/bitcoin-anonymous-projects/.

[57] Nakamoto, *supra* note 4.

[58] *Id.*

[59] *Map of coins*, *supra* note 2.

[60] Boyd, *supra* note 42.

government sponsored mining, while possible in theory, is again countered by Bitcoin's deflationary model of limiting the reward per block mined.[61] The vast variety of virtual currencies available online eliminates the risk of any government from completely removing all crypto-currencies from the Internet.

Another potential solution to preventing the use of digital currency by terrorist organizations would be for all crypto-currency exchanges to register with the U.S. Government in the same way banks are bound by Know Your Customer ("KYC") laws as outlined in the BSA and the Patriot Act.[62] At the present time, only the larger virtual currency exchanges are being actively regulated by FISCEN.[63] While this would superficially solve the anonymity issue virtual currencies present, crypto-currency users would again be more inclined to either migrate to a new unregulated crypto-currency or continue using their virtual coinage through services such as TOR.[64]

Given that none of the aforementioned policy suggestions would completely eliminate crypto-currencies use by terrorist groups, a fair question to address is why should the United States government not attempt to limit or eliminate the use of virtual currencies on the mainstream web since they pose a possible grave danger to the nation's security? While appealing at first blush, by driving crypto-currency use onto the dark web, law enforcement agencies will have a far more difficult time flagging individuals who are monetarily supporting terrorist organizations. As addressed earlier, most mainstream crypto-currencies do not offer complete anonymity.[65] By foregoing the option of eliminating crypto-currency use on the mainstream web, law enforcement agencies will be able to better identify donors to terrorist organizations who do not take the proper precautions to enhance their anonymity.

[61] *How Bitcoin's blockchain technology can build more businesses*, AFR (Nov. 6, 2015, 12:15 AM), http://www.afr.com/markets/currencies/bitcoins-blockchain-technology-is-a-machine-for-building-trust-20151102-gkonxr.

[62] *Federal Financial Institutions Examination Council*, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm (last visited Jan. 22, 2016).

[63] *Id.*

[64] Tamer Sameeh, *The dark web - the bitcoin slang market*, NewsBTC (Nov. 19, 2015), http://www.newsbtc.com/2015/11/19/the-dark-web-the-bitcoin-slang-market/.

[65] Adam Ludwin, *How Anonymous is Bitcoin? A Backgrounder for Policymakers*, CoinDesk (Jan. 25, 2015) http://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

As it stands, the greatest loophole in the American legal system regarding the use of crypto-currencies comes from companies which "invest" in crypto-currencies.[66] Companies which self-identify as crypto-currency investment firms do not fall under the purview of the BSA or the Patriot Act. This loophole allows any terrorist organization to establish a shell corporation and launder their funding as de facto virtual currency exchanges.[67] While FINCEN reserves the right to determine if any organization is laundering money under the guise of investment, the fact that such companies are not required to register with the U.S. Government immediately could hypothetically allow terrorists to fund their operations on American soil.

Policy Suggestions

At this point in time, the first step the federal government should take in addressing the issue of crypto-currencies is to pass legislation mandating that all federal agencies and departments recognize and treat virtual currencies in the same manner as other foreign currencies. With the implementation of this federal mandate, the aforementioned inconsistencies, such as the Federal Election Commission's definition of Bitcoin, will no longer clash with FINCEN's longstanding policies of recognizing crypto-currencies as a convertible decentralized virtual currency. While the Internal Revenue Service will be forced to adjust their stance on crypto-currencies as taxable property, by implementing a standardized definition the legal issues surrounding how virtual coinage affects the U.S. Uniform Commercial Code and the Commodity Futures Trading Commission would finally be clarified.

By bringing all virtual currencies under the definition of foreign currency, FINCEN will be able to make crypto-currency investment companies liable for any violations of the BSA or the Patriot Act in regards to indirectly laundering funds. Such companies would then have to register with the federal government as all major crypto-currency exchanges are currently required to do. FINCEN would furthermore be granted the powers established by all prior anti-money laundering laws to pursue any terrorist organization that is hiding its funds via crypto-currency.

[66] El-Hindi, *supra* note 48.

[67] *Id.*

As an aside, individual crypto-currency miners should be exempted from the registration requirement. The legislative language should reflect FINCEN's current stance that miners, while enabling transactions, have no direct knowledge of the source of the transactions they are validating.[68] Additionally, the fact that nearly all crypto-currencies follow the Bitcoin structure of cryptographic based validation, legally making the miners responsible for all transactions would assure that the operation of all virtual currencies would move underground to the deep web.

From a global perspective, the implementation of such proposed legislation would undoubtedly lend legitimacy to most major crypto-currencies in circulation. The price of virtual coinage would increase in value and thus inadvertently help fund the very terrorist organizations our nation is trying to stop. Given the high volatility of crypto-currencies, however, this spike in value would not last.

Conclusion

While Satoshi Nakamoto's creation of Bitcoin may have been well intentioned, the reality unfortunately remains that crypto-currencies today are associated with elements such as the dark web and the purchase of illegal weapons or drugs. Given the non-physical and decentralized nature of crypto-currencies, the United States has been forced to adopt reactive policies to counteract the dangers this new technology poses. Unfortunately, no digital dye pack could ever help the federal government identify those who wish to use crypto-currencies for wicked means. That being said, should the United States formally recognize virtual coinage as legitimate currency, the nation would be taking the first of many important steps in confronting the dangerous and complicated issues surrounding this new technology

[68] *Id.*

Thwarting Recruitment Efforts and Radicalization in the West: One Part of a Multipronged Approach to Combating ISIS

Bradley Dixon

Introduction

There are many factors contributing to the rise of the self-proclaimed Islamic State ("ISIS"). One contributor includes radicalization and recruitment of westerners. The United States, the United Kingdom, and other Western countries are greatly concerned with the ISIS recruitment capabilities. News articles as of late are littered with headlines like "ISIS message resonating with young people from U.S., West,"[1] "Teens Suspected Trying to join ISIS,"[2] and "Why do people join ISIS?"[3] News agencies are regularly reporting on new attempts and successes of teenagers and young adults leaving home in the West to join the violent group.

According to one report, "thousands of Westerners . . . are believed to be fighting alongside ISIS and other terror groups in Syria and Iraq."[4] Another report, citing the U.N. Security Council, suggests that foreigners are joining on an "unprecedented scale"[5] and more than 15,000 foreigners from over ninety countries have travelled to join or

[1] *FBI: ISIS Message Resonating with Young People from U.S., West*, CBS NEWS (Mar. 5, 2015), http://www.cbsnews.com/news/isis-targeting-young-people-from-u-s-western-countries-as-recruits/.

[2] Naomi Ng, *Australian Teens Suspected of Trying to Join ISIS Stopped at Airport*, CNN (Mar. 9, 2015, 3:34 AM), http://www.cnn.com/2015/03/09/asia/australia-teens-isis/index.html.

[3] Erin Banco, *Why Do People Join ISIS? The Psychology of a Terrorist*, INT'L BUS. TIMES (Sept. 5, 2014, 8:01 PM), http://www.ibtimes.com/why-do-people-join-isis-psychology-terrorist-1680444.

[4] CBS News, *supra* note 1.

[5] Spencer Ackerman, *Foreign Jihadists Flocking to Iraq and Syria on 'Unprecedented Scale' — UN*, GUARDIAN (Oct. 30, 2014, 5:13 PM), http://www.theguardian.com/world/2014/oct/30/foreign-jihadist-iraq-syria-unprecedented-un-isis.

support the fight in Syria and Iraq.[6] Another report, by Dr. Maha Hosain Aziz—a professor specializing in political risk, prediction, and strategy at New York University— submits that more than 3400 western men, women, and teenagers "have left their homes, families, and lives to go fight alongside ISIS in Syria and Iraq."[7] Nearly 2800 of those fighters have come from prominent Western states including the U.S., Canada, France, the U.K, Australia, and Germany.[8] In fact, so many westerners are joining the fight that even ISIS is becoming concerned and is tightening "recruitment requirements and security checks for westerners . . . as ISIS fears spies may be disguised as fighters [to] infiltrate the group."[9]

So, why are so many men, women, and teenagers joining, or attempting to join ISIS, and what can be done to stop them? This paper describes ISIS recruitment efforts in the West and why westerners are joining them in an effort to understand how to combat recruiting efforts and slow the growth of this radical group. In doing so, it is important to recognize that combating radicalization and recruitment in the West is not the only way to combat ISIS, but is one of many ways in a multipronged approach to combat ISIS.

Theories

To begin, it is important to understand some of the basic theories of conflict. Understanding basic theories of conflict will ultimately help us understand why people, or groups, become involved in violent conflict, such as the conflict revolving around ISIS. Thomas Homer-Dixon, in *Environmental Change and Violent Conflict: Understanding the Casual Links* (1990), offers several different typologies of conflict that provide a framework to analyze the causes

[6] Charles Lister, *Profiling the Islamic State*, BROOKINGS DOHA CENTER ANALYSIS PAPER, no. 13, at 34 (Dec. 1, 2014), http://www.brookings.edu/research/reports2/2014/12/profiling-islamic-state-lister.

[7] Dr. Maha Hosain Aziz, *Three Steps to Reduce ISIS Recruitment in Western Countries*, HUFFINGTON POST (Mar. 5, 2015, 3:19 PM), http://www.huffingtonpost.com/maha-hosain-aziz/how-we-can-stop-isis-recruitment_b_6776014.html.

[8] Joshua Berlinger, *The Names: Who Has Been Recruited to ISIS from the West*, CNN (Feb. 26, 2015, 4:13 PM), http://www.cnn.com/2015/02/25/world/isis-western-recruits/index.html.

[9] Alessandria Masi, *Westerners Joining ISIS Have Tougher Recruitment Requirements To Weed Out ISIS Spies*, INT'L BUS. TIMES (Nov. 9, 2014, 10:32 PM), http://www.ibtimes.com/westerners-joining-isis-have-tougher-recruitment-requirements-weed-out-isis-spies-1721314.

of conflict on individual, group, and systemic levels.[10] While some may suggest that we must consider issues of conflict on all levels, analyzing conflict one level at a time can prove more thorough and provide more explanatory power.

Three of the thirteen typologies offered by Homer-Dixon—including Frustration-aggression theories, group-identity theories, and structural theories—will be used in this paper to analyze why people from the West join ISIS, which will ultimately help us understand how to combat the Western recruitment and radicalization problem.

1. Frustration-Aggression Theories

Frustration-Aggression theories analyze conflict at an individual level. These theories suggest that when the strong desires of a person are blocked or go unfulfilled, that person will become aggressive toward the blocking agent, which may subsequently result in conflict.[11] Homer-Dixon provided simple illustrations that can help explain the different theories of conflict. Below is a diagram that helps explain frustration-aggression theories:

Blocked desires → Frustration → Aggressive Behavior → Conflict

2. Group-Identity Theories

Group-identity theories analyze conflict at a group level. These theories focus on group identity reinforcement and the "us vs. them" narratives that result. According to group-identity theorists, "conflict serves to satisfy the desire for group cohesion and strong group identity."[12] A strong desire for group recognition and identity can cause one group to discriminate against others. Thus, hostility begins to grow, which can lead to defensive behaviors. This cycle of hostility and defensive preparation can eventually spiral into conflict. Below is a diagram that helps explain group-identity theories:

Individual Desire for Satisfactory Group Identity → Group Discrimination Against Other Groups → Cycle of Hostility and Defensive Preparation → Conflict

[10] Thomas Homer-Dixon, *Appendix to a Typology of Common Theories of Conflict*, ENVTL. CHANGE & VIOLENT CONFLICT 26 (1990).

[11] *Id.*

[12] *Id.* at 28.

3. Structural Theories

Structural theories suggest that the context and structure of a situation are what ultimately lead to conflict. "A structuralist approach suggests that actors evaluate the possible outcomes of their interactions with other actors and pursue the best option available to them, even if this option entails conflict."[13] In other words, even rational actors may *choose* conflict if, through analysis of their situation, they feel that the only or less costly way of achieving their desires is through conflict. Below is a diagram that helps explain structural theories:

External Situation or Structure with an "Objective" Conflict of Interest → Actors' "Rational" Evaluation of Possible Outcomes → Actors' Choice of Action → Conflict

To apply these theories, cases of different westerners joining ISIS and Islamic extremists, as well as research performed by various scholars, think tanks, and news agencies, will be considered.

Who Is Joining ISIS and Other Violent Islamic Extremist Groups?

Many men, women, and even teenagers have left their homes in the West to join ISIS and other extremist groups. The average age of foreign fighters joining radical Islamist movements in the Middle East is between eighteen and twenty-nine years old, although some have been as young as fifteen and some have been in their thirties.[14] Below are some statistics from a report by Joshua Berlinger[15] approximating how many westerners have joined, or attempted to join ISIS from prominent Western states (these numbers are approximations, as new recruits have joined since the report was given in February 2015 and since this paper was written in April 2015): 180 Americans, 130 Canadians, 1200 French, fifty Australians, 600 U.K. nationals—including Mohamed Emwazi, a.k.a. "Jihadi John," and 600 Germans.

[13] *Id.* at 29.

[14] Richard Barrett, *Foreign Fighters in Syria*, SOUFAN GROUP 16 (June 2014), http://soufangroup.com/foreign-fighters-in-syria/.

[15] Berlinger, *supra* note 8.

A surprising and emerging trend is western women being recruited and volunteering to join ISIS.[16] Approximately 550 western women have traveled to join ISIS,[17] accounting for nearly one-fifth of all the western foreigners who have joined.[18] While the majority of recruits are obviously men who join as jihadi fighters, women play a prominent role in supporting the ISIS campaign, and women will be a major focus in this paper.

Why Are They Joining?

Previous explanations of what makes a terrorist have suggested that economic deprivation and lack of education can cause a person to "adopt extreme views and turn to terrorism."[19] However, while deprivation may be used as part of ISIS recruitment narratives—particularly in the Middle East where its main operations take place—deprivation and lack of education may not actually be reasons as to why *westerners* have joined ISIS.

Beenish Ahmed, a world reporter for Think Progress, reported on Aqsa Mahmood, a teenage girl from Glasgow, Scotland, who became an ISIS bride and is an active ISIS recruiter. Aqsa is quoted from one of her social media accounts, saying:

> The media at first used to portray the ones running away to join the Jihad as being unsuccessful, and say that they didn't have a future and came from broke down families etc. But that is far from the truth . . . Most sisters I have come across have been in

[16] Jeff R. Weyers, *From Canada to the Islamic State: A Canadian Woman On The Frontlines With ISIS*, TERRORISM RESEARCH & ANALYSIS CONSORTIUM, http://www.trackingterrorism.org/article/canada-islamic-state-canadian-woman-frontlines-isis (last visited Jan. 22, 2016).

[17] Carolyn Hoyle, Alexandra Bradford, & Ross Frenett, *Becoming Mulan? Female Western Migrants To ISIS*, INST. FOR STRATEGIC DIALOGUE 8 (Feb. 10, 2015), www.strategicdialogue.org/ISDJ2969_Becoming_Mulan_01.15_WEB.PDF.

[18] Rachel Obe Briggs & Tanya Silverman, *Western Foreign Fighters: Innovations in Responding To The Threat*, INST. FOR STRATEGIC DIALOGUE 12 (Feb. 19, 2015), www.strategicdialogue.org/ISDJ2784_Western_foreign_fighters_V7_WEB.pdf.

[19] Alan Kruger, *What Makes a Terrorist? It's Not Poverty and Lack of Education, according to Economic Research by Princeton's Alan Krueger. Look Elsewhere*, AM. ENTER. INST. (Nov. 7, 2007), www.aei.org/publication/what—makes—a—terrorist/.

> university studying courses with many promising paths, with big, happy families and friends and everything in the Dunyah (world) to persuade one to stay behind and enjoy the luxury. If we had stayed behind, we could have been blessed with it all from a relaxing and comfortable life and lots of money [sic].[20]

Evidence has shown that neither economic deprivation, nor lack of education is a catalyst to supporting or participating in terrorist activities, as confirmed in Aqsa Mahmood's statement.[21] So why are people joining such an extreme and violent terrorist group? Several reasons have been offered, including: disaffection, adventure, belief that it is a humanitarian mission, calls to action, opportunity, political participation, security, fear, perception that Islam and the West are irreconcilably opposed, fear of oppression, anger about the perceived treatment of Muslims, desire to contribute to the building of an Islamic State, and even romance.[22] For further analysis and application of theory, we will look at a few specific cases of radicalization and recruitment.

Perhaps the most significant case to consider is that of Mohammed Emwazi, also known as "Jihadi John." Emwazi is considered to be the face of ISIS, as it has been revealed that he is the man behind the black mask in many ISIS propaganda videos showing beheadings and mass executions of prisoners. He has personally performed executions and appeared in the beheading videos of James Foley, Steven Sotloff, David Haines, Alan Henning, Abdul-Rahman (Peter) Kassig, and Kenji Goto—western and Japanese reporters and aid workers.[23]

[20] Beenish Ahmed, *How A Teenage Girl Goes From Listening To Coldplay And Reading Harry Potter To Joining ISIS*, THINKPROGRESS (Feb. 24, 2015), www.thinkprogress.org/world/2015/02/24/3626720/women—isis/.

[21] Kruger, *supra* note 19.

[22] Katherine Brown. *Analysis: Why Are Western Women Joining IS?* BBC NEWS (Oct. 6, 2014), http://www.bbc.com/news/uk-29507410; *Case File Mohammed Emwazi*, CAGE UK (Mar. 9, 2015), www.cageuk.org/case/mohammed—emwazi; Joanna Paraszcuk, *Romance, Religion, & Idealism: Why Western Women Join IS*, RADIO FREE EUR. RADIO LIBERTY (Jan. 29, 2015), http://www.rferl.org/content/islamic-state-western-women-recruits/26819669.html; Ahmed, *supra* note 20; Briggs & Silverman, *supra* note 18 at 6–51; ; Hoyle et al., *supra* note 17, at 4–39.

[23] Cage UK, *supra* note 22.

Emwazi was born in 1988 in Kuwait. In 1994, at age six, Emwazi moved with his family to the U.K. where he was educated at Quintin Kynaston Community Academy. The head teacher at the academy, Jo Shuter, said she never suspected him of becoming "the man known as Jihadi John."[24] She described him as being "quiet, hardworking, and aspirational."[25]

Cage, a human rights advocacy group based in London, provided a somewhat controversial profile of the radicalization of Mohammed Emwazi. The Cage article, "Case File: Mohammed Emwazi," seems to take the stance that Emwazi may have been the real victim .[26] Although this perspective is certainly skewed, it does highlight some important events that may have contributed to the radicalization of Mohammed Emwazi that can be analyzed in an effort to prevent radicalization and recruitment in the West. The following case was derived from information in the Cage report:

For four years following his graduation from university in 2009, Emwazi was subjected to harassment by British security agencies. Such harassment included unwarranted detention at airports, deportation, and being barred from entering various countries.
In 2009, in an attempt to go to Tanzania for a summer holiday safari, Emwazi was stopped at the airport and denied entry without being given official reason. Shortly thereafter, he was taken to a police station, stripped of his clothing, and thrown into a jail cell where he stayed for 24 hours without food or drink. While there, he regularly had guns pointed at him and felt threatened. He was eventually deported and sent on a plane to Amsterdam.

Armed men were waiting in Amsterdam when he arrived and he was quickly taken into an interrogation room. There, he met two agents, one from Dutch intelligence, and another from British MI5. He was questioned about his trip to Tanzania and accused of wanting to travel to Somalia and of being a terrorist. Eventually, the conversation shifted to where the MI5 agent suggested Emwazi should work for MI5, an offer that Emwazi denied. The MI5 agent then informed him that he would be followed and that life would become very difficult for him.

Emwazi left Amsterdam for Dover, where he was stopped again by men from the Anti-Terror Unit and was, once again, taken to

[24] Dominic Casciani, *Islamic State: Profile of Mohammed Emwazi Aka 'Jihadi John',* BBC NEWS (Mar. 2, 2015), www.bbc.com/news/uk-31641569.

[25] *Id.*

[26] Cage UK, *supra* note 22.

an interrogation room. There, he was asked his thoughts regarding 7/7 and 9/11, and various questions about his personal life, similar to the questions received by the MI5 agent in Amsterdam. To his surprise, Emwazi was informed that the officers had visited and questioned his fiancé. According to Emwazi, this visit scared his fiancé, who subsequently called off their engagement.

Intelligence officials had also visited Mohammed Emwazi's family. Eventually, his family suggested that he move back to Kuwait to avoid harassment. While in Kuwait, he became engaged to another woman. Emwazi stayed in Kuwait for over eight months with extended family before returning to London to visit his immediate family and inform them of his engagement. Upon his return, he was again contacted by intelligence agents, but informed them that he had nothing to say to them.

In his attempt to travel back to Kuwait from London to marry his new fiancé, Emwazi was again subjected to harassment at airports, subjected to police brutality, and denied access to flights and travel. Eventually, he was informed that his visa had been rejected and he could not enter Kuwait. He then traveled to Dubai where he contacted the Kuwaiti embassy to find information about the reason for his visa rejection. He found that his rejection came "as a result of the UK Intelligence informing the Kuwaiti Intelligence not to let him enter."[27] As a result, he lost his job and another chance to marry his fiancé. Feeling disaffected by British government, Emwazi made his way to Syria for jihad.[28]

In response to Cage's report, MI6 ex-chief Sir John Sawyers stated, "extremists are not radicalized to the jihadi movement because of interactions with British security forces . . . these people draw attention to themselves because of their activity, because of their mixing participation in extremist and sometimes terrorist circles."[29] What Cage fails to consider and Emwazi fails to mention is that British

[27] *Id.*

[28] Michelle FlorCruz, *'Jihadi John' Mohammed Emwazi Not Radicalized By UK Security Forces: Ex-Chief Of MI6*, INT'L BUS. TIMES (Feb. 27, 2015), http://www.ibtimes.com/jihadi-john-mohammed-emwazi-not-radicalized-uk-security-forces-ex-chief-mi6-1831564.

[29] Cahal Milmo, *'Jihadi John': Mohammad Emwazi - From British Computer Programmer to ISIS Executioner*, INDEPENDENT (Feb. 26, 2015), http://www.independent.co.uk/news/uk/home-news/jihadi-john-was-a-computer-programmer-known-to-mi5-for-at-least-four-years-10073607.html.

intelligence was alerted to Emwazi because of his affiliations with other men "who were under surveillance by the security services."[30] Emwazi was "considered an associate of a number of high-profile suspected jihadists whom they [British intelligence] were tracking across the world."[31] Three of those suspected jihadists are now dead, "several others are serving prison sentences, and one is living in Sudan, stripped of his British citizenship."[32] Two of the suspects joined the terrorist organization al-Shabaab in Somalia, which is exactly what British intelligence suspected Emwazi might do.

All of the above Emwazi profile information can be verified with the transcripts of Emwazi's conversations with Cage advocates, which can be found in the Cage report "The Emwazi emails: Cage releases its correspondences with Emwazi in full," released February 28, 2015. While this information is one-sided and comes from the perspective of Emwazi himself, *his* perception of the events is important in understanding why he became radicalized and joined ISIS.

Homer-Dixon's frustration-aggression theory of conflict can be applied to Mohammed Emwazi's eventual joining of the ISIS conflict. According to Emwazi, in the Cage report, he was constantly faced with blocked desires, including being denied travel, prevented from seeing family, denied ability to return to his newly established home in Kuwait, and even twice being prevented from marrying his fiancée.[33] These blocked desires clearly contributed to Emwazi becoming frustrated, regardless of who was at fault. His frustrations obviously contributed to his radicalization and aggressive behavior, which ultimately led to his joining of a major contemporary conflict of which he is now a very significant player.

Daveed Gartenstein-Ross and Laura Grossman wrote a study published by the Foundation for Defense and Democracies entitled "Homegrown terrorists in the U.S. and U.K.: an empirical examination of the radicalization process."[34] In this, Gartenstein-Ross and

[30] Casciani, supra note 24.

[31] *Id.*

[32] Milmo, *supra* note 29.

[33] Cage UK, *supra* note 22.

[34] Daveed Gartenstein-Ross & Laura Grossman, *Homegrown Terrorists in the U.S. and U.K.: An Empirical Examination of the Radicalization Process*, FOUND. FOR DEF. & DEMOCRACIES 31–32 (Apr. 2009), www.defenddemocracy.org/content/uploads/documents/Homegrownterrorists_USandUK.pdf.

Grossman provide another case study of Western radicalization, that of Adam Gadahn. Gadahn became part of al-Qaeda, but his radicalization is similar to those who are radicalized and recruited by ISIS. The following case study was derived, in part, from information found in Gartenstein-Ross and Grossman's study:

> Adam Gadahn was raised in rural Southern California and eventually became a spokesman for al-Qaeda. After moving in with his grandparents, he began to explore different religions and was intrigued by Islam. Soon, he began attending a mosque and converted to Islam "in a small ceremony at the Islamic Society of Orange County."[35] Soon, he began spending a lot of time with a group of men who "had a profoundly legalistic interpretation of Islam,"[36] an approach that Gadahn began to adopt.
>
> After moving into an apartment with other Muslims, Gadahn became closely involved with two group members with "extremist views and connections to international militancy who would serve as [his] spiritual mentors."[37] During his mentorship, he began to embrace radical political views and "came to see Islam and the West as irreconcilably opposed."[38]
>
> In Gadahn's first propaganda video for al-Qaeda, he "expressed the idea of a fundamental schism between Islam and the West" and stated that "the allegiance and loyalty of a Muslim is to Allah, His Messenger, his religion, and his fellow believers before anyone and anything else . . . if there is a conflict between his religion and his nation and family, then he must choose the religion every time [sic]."[39]

It is a natural human desire to belong to a group, as a form of developing an identity and becoming something, or someone.[40] Before Gadahn began his mentorship, he was considered a loner and did not often interact with others. It is clear that with his rapid embrace of his

[35] *Id.* at 32.

[36] *Id.* at 33.

[37] *Id.* at 33–34.

[38] *Id.* at 33.

[39] Gartenstein-Ross & Grossman, *supra* note 34, at 33–34.

[40] DIPAK K. GUPTA, WAVES OF INTERNATIONAL TERRORISM AND THE GLOBAL SPREAD OF IDEAS: FROM UNDERSTANDING TO MANAGEMENT 1, 3 (2009).

mentors and their radical narratives that Gadahn had a strong individual desire for what Homer-Dixon described as "satisfactory identity within a group."[41] Gadahn's new identity led him to join in his new group's discrimination against the West, as professed in his claim of a "fundamental schism between Islam and the West,"[42] and constant demonization and criticism of anyone who did not follow a legalistic approach to Islam. The constant hostility of Gadahn and his group ultimately led him and his group to join in a contemporary conflict against the West.

Emwazi and Gadahn are significant cases of Western radicalization and recruitment. However there are other cases, particularly that of Western women joining ISIS and other radical Islamic groups, that have been studied. In the report "Becoming Mulan? Female Western Migrants to ISIS," the authors find that women traveling to join ISIS are divided into two categories, those traveling with male companions and those making the trip alone.[43] "Of those that travel alone, three primary reasons have been identified: grievances, solutions, and personal motivations."[44]

Western women who have migrated to ISIS territory often talk about the oppression of Muslims. Many post grisly images of violence against Muslim men, women, and even children, on their social media pages. "Different conflicts across the world are presented as part of a larger war against Islam by non-believers."[45] Many Westerners are grieved by such a narrative and blame western powers for perpetuating such conflicts.[46] Their sympathies are what drive them to take up jihad and join ISIS.

Westerners who have joined ISIS clearly believe that the West has failed to properly recognize and respect the Ummah (Muslim world) and have strong desires for recognition and respect of Muslim identity. The perception, whether true or false, that western powers perpetuate this problem leads many to discriminate against, and even demonize the West. This leads to hostility and the desire to join groups like ISIS to fight against the West in this perceived conflict.

[41] Homer-Dixon, *supra* note 10, at 28.

[42] Gartenstein-Ross & Grossman, *supra* note 34, at 33–34.

[43] Hoyle et al., *supra* note 17, at 4–39.

[44] *Id.* at 10.

[45] *Id.* at 11.

[46] *Id.*

Nimmi Gowrinathan, of Foreign Affairs, suggested that "the conflict in Iraq is . . . rooted in identity."[47] The "search for meaning, sisterhood, and identity is a key driving factor for women" that join ISIS.[48] The assumption can be made that men also search for meaning and camaraderie, which can also be a driving factor in their decisions to join ISIS.

For many, contribution to a cause can help them become something, or someone, and fulfill the individual desire for identity within a group. Some western women have felt as though their opportunities to contribute to society have been suppressed. One reason women are joining ISIS is "because it provides a new utopian politics—participating in jihad and being part of the creation of a new Islamic State."[49] For women, there is a great deal of romanticism in joining with ISIS. Not only do they look forward to marrying a strong, noble jihadi fighter, but romance is found in the idea of being part of a new political project and an "Islamic 'good life' built upon a particular idea of Islam and Sharia law" where women have new opportunities to contribute.[50] These opportunities include joining al-Khansaa, an all-female police force, participating in surveillance and intelligence gathering, political engagement, and participation in women's traditional daily responsibilities.[51] One of the main contributions women are making for ISIS is their ability to spread the ISIS narrative and recruit. Such contributions are very significant for ISIS and solidifies their important identity and role within the group. The identity of these women is, in part, determined by their ability to spread their group's discriminations against the West and non-believers, which creates hostility and perpetuates the conflict between ISIS and the West.

At this point, it is important to note that, while ISIS supporters generally have great disdain for the West, their main goal is to establish an Islamic State, or caliphate, where they can live in a society governed by a strict interpretation of Sharia law. One western woman who has joined ISIS, Umm Ubaydah, writes, "We don't resort to

[47] Nimmi Gowrinathan, *The Women of ISIS: Understanding and Combating Female Extremism*, FOREIGN AFFAIRS (Apr. 21, 2014), https://www.foreignaffairs.com/articles/middle-east/2014-08-21/women-isis.

[48] Hoyle et al., *supra* note 17, at 13.

[49] Brown, *supra* note 22.

[50] *Id.*

[51] *Id.*

violence because of the wrong America has done. We are trying to build an Islamic state that lives and abides by the law of Allah,"[52] denoting that the West is an obstacle in the development of an Islamic State and the only way to overcome it is by violence. Another woman, Umm Ibrahim, suggested that the most important reason for women migrating to ISIS-controlled territory is to establish the caliphate and be part of bringing honor to the Ummah.[53] These expressions illustrate one reason that women and others join ISIS is the "belief that Muslims are being systematically oppressed."[54] Building a Muslim caliphate is not only desirable to those who join ISIS, but they believe that it is their "mandatory religious duty to assist in this process" and "fulfilling their religious duty is crucial to securing their place in heaven."[55]

In this situation, Homer-Dixon's Structural theory can be applied. The West is seen as a barrier to the building of the caliphate with an obvious conflict of interest. Those involved with the fight against the West have rationalized that while a fight against the West may prove difficult and costly, religious duty and desire makes establishing the caliphate absolutely necessary. This has led to the only option of doing whatever it takes to fulfill that duty and desire to establish an Islamic State, which has resulted in significant conflict.

In short, many westerners are grieved by their perception of how the West has treated or is treating Muslims. They see establishing a caliphate as not only a duty, but also a solution to their grievances. Desires to contribute more in society, romance, camaraderie, identity, and personal duty all contribute to their eventual joining of ISIS.

How are they radicalized and recruited?

As social beings, all humans desire to belong to a group. According to Maslow's hierarchy of needs, the need to belong is second only to the physical needs of food, water, and shelter.[56] When we become part of a group, we "derive great satisfaction by adhering to their explicit rules and implicit norms" and we are "happy being

[52] Hoyle et al., *supra* note 17, at 12.

[53] *Id.*

[54] Paraszcuk, *supra* note 22.

[55] Hoyle et al., *supra* note 17, at 13.

[56] Gupta, *supra* note 40 at 3.

altruistic toward members of our chosen groups and opposing, sometimes violently, the rival groups."[57]

All extremist groups have *salesmen* who distribute their messages by persuading others to believe in them and join their causes.[58] These salesmen include religious leaders with ties to extremist organizations who work to convert new followers. The radicalization of Adam Gadahn is a perfect example of this. He was one who did not have a satisfactory identity and became attracted to a radical narrative. He was persuaded by his ideological leaders of the need to join jihad, which is what ultimately led him to develop a great disdain for the West and join a radical movement.

Technology has improved in ways that provide unprecedented opportunities for ideological salesmen.[59] ISIS, in particular, has utilized advances in communication and information technology to provide nearly all of its members and supporters the opportunity to act as salesmen. Social media outlets, particularly Twitter, YouTube, and Facebook, are very effective in spreading violent extremist ideology and play a very significant role in radicalization, recruitment, and even the fundraising efforts of ISIS today.[60]

According to one report, "ISIS produces as many as 90,000 posts every day on Twitter, YouTube, and other social media platforms with today's young people being the target market."[61] Once an individual is drawn into radical narratives online, they become part of a "pool of like-minded individuals from whom extremists can draw moral and material support, as well as recruits to replace losses and expand operations."[62]

Much research done on spreading the ISIS narrative via social media has been on how women, in particular, are greatly involved in spreading ISIS ideology by distributing propaganda and personalized messages through these outlets. The specific types of narratives provided by female supporters of ISIS are "key to ensuring that ever

[57] *Id.*

[58] *Id.* at 5.

[59] Matthew J. Morgan, *The Origins of the New Terrorism*, PARAMETERS: U.S. ARMY WAR COLL. 29, 34 (Spring 2004).

[60] Barrett, *supra* note 14, at 7.

[61] CBS News, *supra* note 1.

[62] Frank J. Cillufo, Sharon L. Cardash, & Andrew J. Whitehead, *Radicalization: Behind Bars and Beyond Borders*, 13 BROWN J. OF WORLD AFFAIRS 113, 115 (2007).

more women travel to join ISIS."[63] Both male and female supporters often post grievances against the West, celebrations of ISIS successes, and statements to encourage migration of others from the West to ISIS-controlled territory. They even provide "practical advice to those wishing to travel" to join the group, such as developing flight plans, advising on how to leave home without being suspected by family and friends, and who to meet with that can help someone get to ISIS-controlled territory. [64]

Some supporters also engage in encouraging attacks on the West. Umm Layth, a former westerner and ISIS recruit, encouraged via social media those who "cannot make it to the battlefield [should] bring the battlefield to [themselves]," suggesting the need to "be a Mujahid wherever you may be."[65] Social media has become the main focus of ISIS recruitment and radicalization efforts and has played a large role in convincing nearly all of the people who have recently attempted to leave their homes in the West and join ISIS.

What Can Be Done?

The answer to this question is not simple and involves several different ways to combat ISIS recruitment and radicalization efforts in the West. Such efforts include community engagement, developing and effectively spreading an anti-ISIS narrative, and the creation of exit programs.

Research has suggested that "underlying most Western recruitment is a sense of alienation from society and even government."[66] People are easily influenced by ISIS narratives because they don't feel they have a "stake or future in their community or country," so why should they stay? ISIS provides an exit strategy from this predicament. [67]

Because disaffection from society and government, as well as the perception of an irreconcilable opposition between Islam and the West are important parts of the radicalization process, one way to

[63] Hoyle et al., *supra* note 17, at 33–34.

[64] *Id.* at 33.

[65] *Id.* at 34.

[66] Aziz, *supra* note 7.

[67] *Id.*

counter radicalization is through "Muslim civic engagement efforts."[68] The United Kingdom's Prime Minister, David Cameron, stated that "every school, every university every college, every community [must] recognize they have a role to play, we all have a role to play, in stopping people from having their minds poisoned by this appalling death cult [sic]."[69] The Terrorism Research and Analysis Consortium ("TRAC") also expressed a community call-to-action, stating that "engagement at the community level may be the only way for dealing with actions that are not criminal in and of themselves . . . Prevention is the responsibility of everyone if we are to improve the chances of preventing radicalization."[70]

Stevan Weine, professor of psychiatry at the University of Illinois Chicago, provided one example of community engagement efforts and the development of key partnerships to counter extremism by the Los Angeles Police Department ("LAPD"). Recognizing that communities from which radicalization and recruitment takes place are best positioned to prevent it, the LAPD has partnered with the Muslim Public Affairs Council ("MPAC") to collaborate with government, public and private organizations, and faith-based organizations, in this effort. [71]

MPAC operates the "countering violent extremism" ("CVE") initiative *Safe Spaces*. Safe Spaces attempts to increase resilience to violent extremism in Muslim-American communities by helping families and communities engage in dialogue about difficult topics, including threats of radicalization and recruitment. Safe Spaces also helps communities form "crisis inquiry teams" to help identify individuals at risk of engaging in radicalization and recruitment with the goal of helping them turn away from such extremism."[72]

Other strategies and organizations similar to Safe Spaces are being developed across the United States and other western states. These organizations establish "innovative public-private partnerships that increase mutual trust, build capacities, strengthen resilience, and then develop and evaluate community-delivered prevention and

[68] Gartenstein-Ross & Grossman, *supra* note 34, at 59.

[69] CBS News, *supra* note 1.

[70] Weyers, *supra* note 16.

[71] Barrett, *supra* note 14, at 31.

[72] Stevan Weine, *How to stop ISIS from recruiting Americans*, CNN (Sept. 11, 2014, 6:24 PM), http://www.cnn.com/2014/09/11/opinion/weine-isis-recruitment/index.html.

intervention activities."[73] Building partnerships, particularly with communities most vulnerable to ISIS and extremist recruitment efforts, will help otherwise marginalized people and groups become more integrated into society, thus providing stronger group identity and a voice that can be heard, rather than suppressed. Having such a voice and group identity will reduce a person or group's desire to seek satisfactory identity within extremist movements and reduce discrimination and hostility against the West that can ultimately lead to joining ISIS.

To effectively counter ISIS radicalization and recruitment efforts, we must also provide a strong anti-ISIS narrative. To develop such a narrative, messages of those posting about their difficulties living under ISIS rule, those who have defected from ISIS, and especially the messages provided by moderate Muslim leaders who have denounced ISIS narratives and actions, must be used. The anti-ISIS narrative must then be spread by all means necessary and directed towards those most vulnerable to ISIS recruitment and radicalization efforts.

Life for unmarried women has been depicted as very difficult. One female member of ISIS described life as a single woman as being very difficult, as women are not even allowed to go outside without a chaperone, making tasks like going to the store quite difficult.[74] Also, western female migrants in particular are often subjected to mistreatment and discrimination from locals and "may even be denied access to essential goods and services on the basis of their foreign status."[75] Some ISIS women have also talked about the devastation of living in a warzone, such as being hit by bombs and air strikes and losing husbands and friends to fighting.[76] These types of stories, particularly when they come from those who support ISIS, should be utilized in the anti-ISIS narrative, as these messages of difficulty and hardship could serve to decrease the effectiveness of ISIS propaganda messages.[77]

[73] *Id.*

[74] Hoyle et al., *supra* note 17, at 23.

[75] *Id.* at 25.

[76] Hoyle et al., *supra* note 17, at 26–27.

[77] *Id.* at 25.

There are several people from the West who have defected from ISIS.[78] "In September 2007, the late Abu Yahya al Libi, a senior member of the al-Qaeda Sharia Committee, offered the U.S. a six-step plan to defeat al-Qaeda. At the top of his list of advice was to amplify the cases of 'backtrackers'—or ex-jihadists who had renounced armed action."[79] This tactic of utilizing the messages of those who have defected from the movement can be effective in combating ISIS because such messages refute and disprove ISIS's propaganda narratives.

Dr. Maha Hosain Aziz magnified the need to use defectors, and possibly celebrities, in anti-ISIS propaganda.[80] She suggested that if a potential recruit is already experiencing alienation from society and government, then government-released anti-ISIS media may prove ineffective. Using ISIS defectors and even celebrities as spokespeople for anti-ISIS propaganda can be very effective—especially considering potential recruits may feel a stronger connection to these people, and their messages may deeply resonate, especially with teenagers.[81] Defectors can also be a source of information and provide answers to the questions of why people join ISIS, what prompted them to defect, how much they were paid, what training was like, who are key leaders in the organization, and how the group operates—information that can be used against ISIS.[82]

Perhaps the most important part of developing an anti-ISIS narrative is encouraging and spreading messages provided by moderate Muslim leaders. Recently, Sheikh Ahmed al-Tayeb of Cairo's al-Ahzar University stated that "a historical misreading of the Koran has led to intolerant interpretations of Islam," and he called for a "radical reform of religious teaching to tackle the spread of Islamic extremism."[83] Another Muslim leader, Sheikh Abdallah Bin Bayyah—a leader of the Forum for Promoting Peace in Muslim Societies—helped bring together 250 Islamic scholars "to promote a unified

[78] Aziz, *supra* note 7.

[79] Susan Sim, *Countering Violent Extremism: Leveraging Terrorist Dropouts to Counter Violent Extremism in Southeast Asia*, QATAR INTL ACAD. FOR SEC. STUDIES 7–8 (Jan. 2013), http://soufangroup.com/wp-content/uploads/2013/12/CVE-PHASE-II-VOL.-II-Final-Feb-13.pdf.

[80] Aziz, *supra* note 7.

[81] *Id.*

[82] *Id.*

[83] *Al-Azhar top cleric calls for religious teaching reform*, BBC NEWS (Feb. 23, 2015), http://www.bbc.com/news/world-middle-east-31580130.

peaceful response to the current violence, issuing a Fatwa in response to [ISIS]."[84] Messages from such authorities can help refute the extremist ideologies being spread by radical leaders, such as those who contributed to the radicalization and recruitment of Adam Gadahn, and properly educate people about the doctrines of Islam.

Anti-ISIS narratives provided by those who post about difficulties living under ISIS rule, ISIS defectors, and moderate Muslim leaders must be widely publicized and targeted toward those most vulnerable to pro-ISIS propaganda. To do this, we must utilize the same tactics as ISIS supporters and recruiters. The internet, being a key component in modern radicalization, must also be "a key battleground in pushing back against [recruitment efforts]."[85]

ISIS has become very proficient at utilizing social media to radicalize and recruit because it has proven to be effective. Governments, community organizations, schools, and—as previously suggested—defectors and celebrities must take part in posting anti-ISIS narratives. This is the best way to reach young people in modern society, who happen to be the biggest targets of ISIS recruitment and radicalization efforts.

In reality, community engagement efforts and efforts directed toward developing and effectively spreading anti-ISIS narratives will not be 100 percent effective in preventing ISIS recruitment and radicalization. But, there are several people who have defected from ISIS, people who have been stopped in their attempt to join ISIS, as well as people who have disengaged in the radicalization process. These people need to be engaged and reintegrated into society. One way to do this is through the development of exit programs.

Vidhya Ramalingam and Henry Tuck, of the Institute for Strategic Diologue, suggested that "[e]xit programmes are one of the most important and effective ways to have an impact on existing movements. They work with individuals to leave behind extremist ideologies, groups and movements. They attempt to change both the belief structures of individuals (deradicalisation) as well as the

[84] *Global Terrorism Index 2014: Measuring and Understanding the Impact of Terrorism*, INST. FOR ECON. & PEACE 3 (2014), http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf.

[85] Hoyle et al., *supra* note 17, at 38.

behavioural aspects (disengagement).”[86] Governments need to work with agencies at all levels to engage communities to help create exit programs for those who have either left violent extremist movements, or those who have been stopped in their attempt to join or engage in violent conflict.[87]

Conclusion

Blocked desires, frustration, desire for satisfactory group identity, group discrimination, and poor opportunities to improve one’s situation in societal structure can all eventually spiral into creating or inspiring one to join a violent conflict. In the case of the ISIS conflict, community engagement efforts, the development and effective spreading of anti-ISIS narratives, and the creation of exit programs can help marginalized people and groups become integrated into society to develop a positive identity, provide a voice and recognition within society, and ultimately be effective at thwarting ISIS recruitment and radicalization efforts in the West.

[86] Vidhya Ramalingam & Henry Tuck, *The Need for Exit Programmes*, INST. FOR STRATEGIC DIALOGUE 4 (Sept. 2015), http://www.strategicdialogue.org/ISD_EXIT_Report__September2015.pdf

[87] *Id.*

Tracking the Wolf: Lone Wolf Terrorism and Detection

Alexandre Rodde

Introduction

"The system was flawed obviously. When seventeen people die, it means the system is flawed. That is why we need to learn from what happened," stated Manuel Valls,[1] the French Prime Minister, talking about the three attacks in Paris last January. On January 7th, at 11:30, Said and Cherif Kouachi opened fire at Charlie Hebdo's headquarters, killing twelve people, including two police officers. Two days after, while the French Raid and GIGN, both elite police units, were surrounding the brothers in Dammartin-en-Goele, another shooting started in Paris. Amedy Coulibaly, a repeated offender who met Cherif Kouachi in prison, was taking hostages in a kosher grocery shop. A simultaneous assault led to the death of the three terrorists, after the death of a total of innocent seventeen people.[2]

"No one helped him. There's not a larger conspiracy at all." said Christopher Combs,[3] when talking at a press conference after Larry McQuilliams was shot by the police after his attempted attack in Austin, Texas. McQuilliams, on November 28, 2014, shot more than a hundred rounds into a building in downtown Austin and then tried to burn the Mexican Consulate before being shot by APD Sergeant Adam Johnson eleven minutes after the beginning of the attack. Wearing a tactical jacket, McQuilliams also had a map of thirty-four potential

[1] *Attentats : "Quand il y a 17 morts, c'est qu'il y a eu des failles" déplore Valls* ["Seventeen deaths are are a proof of a flawed system"], LE PARISIEN (Jan. 10, 2015, 6:45 PM), http://www.leparisien.fr/faits-divers/attentats-quand-il-y-a-17-morts-c-est-qu-il-y-a-eu-des-failles-deplore-valls-10-01-2015-4434869.php.

[2] *Chronologie : 3 jours d'attentats terroristes sur la France* [Three days of terrorist attacks in France], L'OBS (Jan. 10, 2015, 10:11 AM), http://tempsreel.nouvelobs.com/charlie-hebdo/20150110.OBS9671/charlie-hebdo-chronologie-3-jours-d-attentats-terroristes-sur-la-france.html.

[3] Jim Vertuno, *Larry McQuilliams, Shooter in Austin, Had Extremist Views: Police*, HUFFINGTON POST (Dec. 1, 2014), http://www.huffingtonpost.com/2014/12/01/larry-mcquilliams-austin-shooter-extremist_n_6251928.html.

targets and IEDs[4].

"If you can kill a disbelieving American or European—especially the spiteful and filthy French—or an Australian, or a Canadian, or any other disbeliever from the disbelievers waging war, including the citizens of the countries that entered into a coalition against the Islamic State . . . kill him in any manner or way however it may be," said Abu Mohammad al-Adnani,[5] the ISIS spokesman in a message released on the Internet in September 2014. This online message was mentioned by investigators in both the Michael Zehaf-Bibeau[6] and Zale Thompson investigations. On October 22 2014, Michael Zehaf-Bibeau killed a Canadian soldier and was killed when entering the parliament in Ottawa. On October 23, Zale Thompson attacked a police officer with a hand axe before being shot.[7]

These four attacks, leading to deaths and injuries in three different countries, share common elements. All four were conducted by lonely individuals with a vague political and/or religious objective, and cheap, relatively easily obtained means. Diverging from the classic form of political or religious group terrorism, they are examples of a new brand of terrorists: the lone wolves.

In order to understand what this new threat is, the first section of this paper will start by establishing a definition of the term lone wolf, and then move to an historic study of the phenomenon. Using both these elements it will try to draft a general profile of the lone wolf.

Once understood and known, the second part of this paper will try to understand where, when, and how we can attempt to detect and stop the future attacks, both looking at lone wolves who are U.S. citizens and also foreign lone wolves.

[4] Greg Botelho, *Man who shot at consulate, federal courthouse Austin police HQ, killed* CNN (Nov. 28, 2014), http://www.cnn.com/2014/11/28/us/texas-austin-shooting/.

[5] Helen Davidson, *Isis instructs followers to kill Australian and other "disbelievers"*, GUARDIAN (Sept. 23, 2014), http://www.theguardian.com/world/2014/sep/23/islamic-state-followers-urged-to-launch-attacks-against-australians.

[6] *Michael Zehaf Bibeau: 5 facts*, HEAVY (Oct. 22, 2014), http://heavy.com/news/2014/10/michael-zehaf-bibeau-ottawa-parliament-shooting-terro-attack/.

[7] Chris Pleasance, *Hatchel wielding Muslim radical who attack rookie cops spent months visiting jihadist websites and stalked officers for hours*, DAILY MAIL (Nov. 4, 2014), http://www.dailymail.co.uk/news/article-2820584/Hatchet-wielding-Muslim-radical-attacked-rookie-New-York-cops-spent-months-visiting-jihadist-websites-stalked-officers-hours.html.

The last part of this paper will examine new and various challenges in terms of sharing of intelligence between agencies and nations, the importance of social media and a possible active approach to this issue.

Knowing the Wolf

Terrorism is a hard term to define. The American legal definition, as stated under 18 U.S.C. § 2331, reads:

> [I]nternational terrorism means:
> (**A)** involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
> **(B)** appear to be intended
> **(i)** to intimidate or coerce a civilian population;
> **(ii)** to influence the policy of a government by intimidation or coercion; or
> **(iii)** to affect the conduct of a government by mass destruction, assassination, or kidnapping[.][8]

The definition of domestic terrorism is also given in the same statute:

> [D]omestic terrorism means activities that—
> **(A)** involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
> **(B)** appear to be intended—
> **(i)** to intimidate or coerce a civilian population;
> **(ii)** to influence the policy of a government by intimidation or coercion; or
> **(iii)** to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
> **(C)** occur primarily within the territorial jurisdiction of

[8] 18 U.S.C. § 2331 (2012).

the United States.[9]

Both these definitions are partially exact when talking about lone wolf terrorism. But the difference between terrorism and lone wolf terrorism is not a legal one. In fact, lone wolf terrorists and network terrorists share the same means, results, and sometimes beliefs. An accurate definition of lone wolf can be found in Burton and Stewart's article "The Lone wolf Disconnect."[10] The authors insist first on the distinction between a lone wolf and a sleeper operative. Contrary to the lone wolf, the sleeper operative is linked to an organization, infiltrated in the target group or society, and remains dormant until the attack order is given by its organization.[11] Burton and Stewart explain that the lone wolf differs because he is "a standalone operative who by his very nature is embedded in the targeted society and is capable of self-activation at any time."[12] Therefore "a lone wolf is a person who acts on his or her own without order from— or even connection to—an organization."[13] A variant of the phenomenon has also been defined: the "lone pack."[14] This term, which may look like an oxymoron, can be considered a new variation of the lone wolf. But then what differentiates a lone pack from a terrorist group? First the lone pack is just two individuals, whereas the terrorist group can gather more terrorists. Moreover, the lone pack shares with the lone wolf that it is acting on its own without instruction from a larger terrorist group.[15] From these definitions, it is important to differentiate between lone wolf terrorists and individuals acting for private gain or revenge.[16] Lone wolf actions, like those of any terrorist, are fueled by political beliefs. Consequently, they have to be

[9] *Id.*

[10] Fred Burton & Scott Stewart, *The Lone Wolf Disconnect*, SECURITY WEEKLY (Jan. 30, 2008), https://www.stratfor.com/weekly/lone_wolf_disconnect.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Raffaello Pantucci, *A Typology of Lone Wolves*, ICSR (Mar. 2011), http://icsr.info/wp-content/uploads/2012/10/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf.

[15] *Id.*

[16] "Solo actor terrorism and the mythology of the lone wolf" in "Lone Wolves: myths or reality?" P. Jackson and G.Gable.

considered first and foremost as terrorists.[17]

Historic Study of the Phenomenon

Contrary to common belief, and as to the mainstream media description, lone wolf terrorism is far from being a new phenomenon. In his book about lone wolf terrorism,[18] Ramon Spaaij linked the phenomenon to nineteenth century European anarchist thinkers promoting the idea of "propaganda by deed" against the existing social order. If some attacks happened, hoping to be the first step of a global revolution, they are hardly comparable to the modern form of lone wolf terrorism. The first example of "modern" lone wolf terrorism seems to be the murder of Medgar Evers by Byron de la Beckwith for his involvement with the National Association for the Advancement of Colored People in 1957 in Mississippi.[19] Arrested again in 1973, de la Beckwith was carrying a bomb in Louisiana. This attack would be the starting point for the major trend in lone wolf terrorism during the second half of the twentieth century: white supremacist lone wolf terrorism.[20] Enticed by the concept of leaderless resistance,[21] white supremacist leaders made attacks "the duty of every patriot to make the tyrant's life miserable."[22] The concept, and a new vocabulary, was popularized by white supremacists Tom Metzger and Alex Curtis, the first one even redacting "Law for the Lone Wolf" in the nineties.[23] With the popularization of the concept appears a wider variety of

[17] Burton and Steward also separates lone wolf from what they call "lone nuts" defined as "mentally individuals acting for other reason." Burton & Stewart, *supra* note 10.

[18] *See generally* Ramon Spaaij, UNDERSTANDING LONE WOLF TERRORISM: GLOBAL PATTERNS, MOTIVATIONS AND PREVENTION, Springer Brief in Criminology, 2012.

[19] *Id.* at 24.

[20] Even the term "lone wolf" is reportedly an invention of Thomas Metzger who founded White Aryan Resistance in the seventies. He used the term for the first time in the nineties, in his *Laws of the Lone Wolf.*

[21] Defined as a social resistance strategy in small or individual cell go against an established power. This concept was popularized in white supremacist by Louis Beam.

[22] Louis Beam, *Leaderless Resistance*, (Feb. 1992), http://www.louisbeam.com/leaderless.htm.

[23] Tom Metzger, *Laws for the Lone Wolf*, RESIST, http://www.resist.com/Articles/literature/LawsForTheLoneWolfByTomMetzger.htm.

ideology in lone wolf cases: nationalism, animal rights, anti-abortionist, and Islamism.[24] With the increased accessibility of the Internet, the lone wolf ideology and propaganda praised by gurus and violent leaders started being shared and broadcast to more potential lone wolves. Internet propaganda became a place of self-radicalization, and a huge source of information for lone wolves, both on the ideological side and the practical way to commit attacks.[25] The Tsarnaev brothers,[26] as the Kouachi brothers and Amedy Coulibaly[27] used the Internet to learn about their violent ideology but also to advocate their ideas, and in the case of Coulibaly to explain his actions. Moreover, when the phenomenon migrated from anarchist Europe to twentieth century America, it continued in both regions to expand to new areas like Australia or the Middle East. But who are these lone wolves?

Profile of the Lone Wolf Terrorist

1. Ideology and Motivations

As discussed before, nowadays lone wolves are of various ideological movements. If right wing extremist and Islamists are the main source of lone wolves, nearly every violent school of thought has been mentioned. [28] However, in most cases, and as described by white supremacist Tom Metzger, "[n]o matter what the ideology many modern lone wolves most likely have been involved with, in most successful cases their ideology is kept secret, some even taking it to

[24] Spaaij, *supra* note 18 at 12.

[25] *Id.* at 56–58.

[26] Tamerlan and Dzhokhar Tsarnaev detonated two bombs at the end of the Boston marathon, killing three people on April 15, 2013.

[27] According to new facts in the French investigation, Coulibaly may have been an operative of ISIS acting under command. Text messages and emails discovered by the French police may have been sent by a third man in charge of the attack. However, his journey remains an interesting example of radicalization and therefore useful to our study of the lone wolf profile. Elise Vincent, Attentats de Paris : les messages du commanditaire au tueur de l'Hyper Cacher, LE MONDE (Nov. 7, 2015), http://www.lemonde.fr/police-justice/article/2015/11/07/attentats-de-paris-les-messages-du-commanditaire-au-tueur-de-l-hyper-cacher_4805099_1653578.html.

[28] Spaaij, *supra* note 18 at 12.

the grave."[29] Larry McQuilliams is the perfect example of this. Whilst his past affiliations with Christian extremist group Phineas Priesthood[30] and the fact that he attacked the Austin Mexican Consulate made him close to right wing extremism, nothing truly explains his motivations or the timing of his attack.[31] Anders Breivik is another lone wolf mixing various extremist ideologies[32] in order to justify or explain his killing of seventy-seven persons in Norway in July 2011.[33] Most of the political background of the current lone wolves comes from easy to understand, Manichean propaganda online. While less politically informed and trained than the first lone wolves, the current lone wolves are killing more people.[34]

2. Social Background

Lone wolves, like others terrorists, come from various social backgrounds. If recent cases like the Kouachi brothers[35] or Mohammed Merah come from low-income families in crime-riddled French suburbs the opposite can also be found.[36] Theodore Kaczinzky was born in a middle class family and was able to be hired as an assistant professor as the University of Berkeley.[37] More than social backgrounds or academics, lone wolves seems to first be lonely

[29] Tom Metzger, *Begin With Lone Wolves*, RESIST, http://www.resist.com/Articles/literature/BeginWithLoneWolvesByTomMetzger.html.

[30] Chase Hoffberger, *Shooter Had Hate in His Heart*, AUSTIN CHRONICLE (Dec. 5, 2014), http://www.austinchronicle.com/news/2014-12-05/shooter-had-hate-in-his-heart/.

[31] *Id.*

[32] Mostly xenophobic, anti-communist, and "counterjihad" as seen on the manifesto he broadcast on the Internet.

[33] Asne Seirstad & Sarah Death, Anders Breivik massacre/ Norway's worst nightmare, GUARDIAN, http://www.theguardian.com/world/2015/feb/22/anders-breivik-massacre-one-of-us-anne-seierstad.

[34] Spaaij, *supra* note 18, at 59–61.

[35] *Qui sont les frères Kouachi ?* [Who are the Kouachi brothers?], LE DAUPHINE (Jan. 9, 2015), http://www.ledauphine.com/france-monde/2015/01/09/qui-sont-les-freres-kouachi.

[36] Emiline Cazi, *Merah: l'enfance d'un terrorist* [Merah: childhood of a terrorist], LE MONDE (June 12, 2012), http://www.lemonde.fr/a-la-une/article/2012/06/12/merah-l-enfance-d-un-terroriste_1717066_3208.html.

[37] Nicknamed the Unabomber, Kaczinsky killed three people using bombs sent in the mail.

individuals, sometimes with mental health problems.[38] However, most of them share the common feature of having a criminal record. Following a complex criminal path, most of them have been arrested, and sometimes convicted.[39] Sometimes, as for Amedy Coulibaly, they developed their violent ideology in prison, while serving time for a lesser offense.[40] As put in evidence since the beginning of this paper, nearly every lone wolf has been male, most of them young.[41]

3. Radicalization and the Use of the Internet

If, in older cases of lone wolf attacks, most of the offenders were tangentially linked to a violent organization,[42] which was the main path to their radicalization, it is not the case nowadays. Due to the mainstream access to online content, most of the future lone wolves are now radicalized on the Internet. As explained by Gabriel Weimman in his article on the use of the Internet by terrorists,[43] most violent ideologists are aware of the tremendous advantages offered by Internet: huge audiences, anonymity, little or no regulation, and a multimedia environment. It can help to meet like-minded individuals and self study ideology, terrorist methods, and propaganda. David Copeland[44] had downloaded *The Terrorist Handbook* and *How to Make Bombs* in a cybercafé.[45] Another example can be found with Anders Breivik who wrote *2083: A European Declaration of Independence*, a 1,518 pages manifesto,[46] explaining his actions. Besides, both for propaganda reason and by some misplaced "pride" more and more lone wolves maintain social media profiles.[47] They use it to promote their ideas, show support to violent ideology and share propaganda. They are also sometimes contacted by other people

[38] Spaaij, *supra* note 18, at 16–20.

[39] *Id.*

[40] By being the cellmate of Djamel Behgal, *see also* note 65. Cédric Mathiot, *Amedy Coulibaly et son mentor Djamel Beghal auraient été voisins de cellule en 2005*, LIBERATION (Jan. 16, 2015), http://www.liberation.fr/societe/2015/01/16/amedy-coulibaly-et-son-mentor-djamel-beghal-auraient-ete-voisins-de-cellule-en-2005_1181425.

[41] Spaaij, *supra* note 18, at 16–20.

[42] As an example Byron de la Beckwith had links to the Ku Klux Klan.

[43] Gabriel Weimann, *How Modern Terrorism Uses the Internet*, U.S. INST. OF PEACE (Mar. 2004), at 3, www.usip.org/sites/default/files/sr116.pdf.

[44] The London Nail Bomber was arrested after thirteen days of bombing in 1999.

[45] Spaaij, *supra* note 18, at 57.

[46] The manifesto was send to contact hours before the attacks.

[47] Including Dzhokhar Tsarnaev and Anders Breivik.

sharing the same idea, or directly by an operative of terrorist groups.[48]

4. Logistics and Means

It has been shown that lone wolves, as group-based terrorists, want to "intimidate or coerce a civilian population," "influence the policy of a government by intimidation or coercion," and "affect the conduct of a government."[49] How do they try to reach theses goals? In his article, Peter Phillips explained that lone wolves prefer assassination, armed attack, bombing and hostage taking.[50] Most of theses offenses require weapons in order to be conducted. Ramon Spaaij[51] stated that firearms are predominantly used, especially in the United States.[52] Interestingly, the weapons used differ between lone wolves and group-based terrorists.[53] Whilst the media likes to depict lone wolves as professional bombers, most of them have only basic to average knowledge and skill in bomb making.[54]

All these elements, part of the lone wolf profile, are also opportunities to track him, detect him, and stop him before he commits his attack.

Tracking the Wolf

Lone wolves are, by definition, lonely individuals, acting on their own, and without obvious motive. Consequently the usual ways to detect them and collect intelligence on them are not the solution. In this part, the paper will examine two types of lone wolf terrorist: the homegrown terrorist and the "international" lone wolf terrorist. It is possible, using intelligence on the usual signs of radicalization, violent

[48] This possibility making them operatives from a terrorist group, it won't be studied here.

[49] 18 U.S.C. § 2331.

[50] Peter J. Phillips, *Lone Wolf Terrorism*, 17 PEACE ECON., PEACE SCI. & PEACE POL'Y 1, 24 (2011).

[51] Spaaij, *supra* note 18, at 72.

[52] Around 70% of them, *Id.*

[53] *Id.*

[54] "[M]anufacturing a potent improvised explosive device is technically demanding, especially for the lonely individual with no prior experience in bomb making."; "There may be a disconnect between intention and capability with regard to which weapon(s) a lone wolf terrorists seeks to use." *Id.*

behavior, and preparation of an attack, to detect and prevent the attack from occurring. The multiplication on these "red flags" would allow the intelligence community to detect prospective lone wolves.

Homegrown Lone Wolf

1. Criminal Record and Inmate Record

As shown earlier, most lone wolves have a criminal past, and therefore a criminal record.[55] Most of the attacks necessitate preparation and sometimes training, but also a radicalization of thought.[56] Similar to the mass murderer, the lone wolf has to build his radicalization and will to commit criminal acts. It is frequent that the lone wolf was condemned before for lesser acts, most of them including a political aspect. Examples such as vandalism to classic targets of terrorism,[57] acts of violence during political demonstrations, threats both in person or online and criminal hate speech can be hints of a lone wolf in the making. Therefore it will be interesting to create a federal database of felons convicted for "anti social" felonies and crimes, accessible only to law enforcement and the intelligence community. The objective of this database would be to work as a tool for the intelligence community, fueled by both law enforcement information and intelligence community information. As explained earlier, this database is not, in itself, an answer to the lone wolf problem but could be used as a basis in the search for homegrown lone wolves, gathering information about convicted felons with violent political inclination. Furthermore, the gathering of this information is already available and not protected by any privacy law, necessitating only classification. Then what would be the answer for the lone wolf with non-political convictions?

Amedy Coulibaly is a good example of a lone wolf with a violent past, who came to terrorism late in his criminal life. Raised in the Grande Borne project in Grigny, Coulibaly followed a classic criminal path until he was convicted in 2004 for a bank robbery in

[55] Spaaij, *supra* note 18, at 47–61.

[56] This assertion is becoming less true, with the examples of Zale Thompson and Michael Zehaf-Bibeau, who just ran amok and had very little equipment.

[57] Examples of classic targets: police officers, soldiers, abortion clinics or personnel, equal rights association members, government buildings, etc.

Orleans, to six years in prison.[58] Jailed in Fleury Merogis,[59] he met Djamel Beghal, who would become his mentor.[60] After their release both men met often for training and religious discussion.[61] Beghal was convicted again in France,[62] and Coulibaly died during his attack in Paris.[63] This story shows why prisons have to be considered when collecting intelligence on possible lone wolf terrorists.

Prisons are schools of crime, as stated by many inmates.[64] But they are also places of radicalization. As described in Mark Hamm's article[65] on Kevin Lamar James, even if only a small percentage of prison radicalized inmates act on their beliefs, an important number of terrorist plots starts in prison cells.[66] However it is important to note that prison gangs are not terrorist groups and provide their members with a violent ideology, not with a criminal network on the outside.[67] Hamm explains that, looking for an identity, inmates join religious groups during incarceration. These groups act like gangs, and are hierarchical entities with a set of rules and a common identity.[68] Similarly to Hamm's recommendation, creating a database of

[58] Stéphane Sellami, *Quand Amedy Coulibaly braquait des discothèques parisiennes*, LE PARISIEN (Jan. 30, 2015, 8:31 AM), http://www.leparisien.fr/charlie-hebdo/quand-amedy-coulibaly-braquait-des-discotheques-parisiennes-30-01-2015-4491721.php.

[59] Located in France, it is the biggest prison in Europe with more than 3500 inmates.

[60] Convicted multiple times for act of terrorism Beghal, a French Algerian national, is a former member of the Groupe Islamique Armé (Armed Islamic Group).

[61] Mathiot, *supra* note 42.

[62] Patricia Touranchean, L'aveu de Djamel Beghal incrimine le réseau Ben Laden [The confession of Beghal incriminates the Ben Laden network], LIBÉRATION (Oct. 3, 2001, 1:09 AM), http://www.liberation.fr/evenement/2001/10/03/l-aveu-de-djamel-beghal-incrimine-le-reseau-ben-laden_379155.

[63] L'OBS, *supra* note 2.

[64] "La prison, c'est la putain de meilleure école de la criminalité" ["Prison is the fucking best school for criminals"] said Amedy Coulibaly when interviewed about his time in Fleury Merogis. *La prison, "mon école du crime" : le témoignage d'Amedy Coulibaly en détention*, RTBF (Jan. 13, 2015, 4:07 PM), http://www.rtbf.be/info/medias/detail_la-prison-mon-ecole-du-crime-le-temoignage-d-amedy-coulibaly-en-detention-video?id=8766969.

[65] Mark S. Hamm, *Prison Radicalization: Assessing the Threat in US Correctional Institute*, Nat'l Justice Inst. (Oct. 2008) http://www.nij.gov/journals/261/pages/prisoner-radicalization.aspx.

[66] Kevin James Lamar is responsible for the 2005 Los Angeles Bomb Plot.

[67] Hamm, *supra* note 72.

[68] *Id.*

members of these various prison gangs, with a focus on those with political beliefs, appears to be a good way to prevent attacks. Once again, the sole membership to one of the gangs does not make you a potential lone wolf, but it is another red flag. This prison database already exists and does not require any authorization for law enforcement and the intelligence community to be accessed. After classification and being linked to the criminal record database, it can be used as a powerful tool to detect lone wolves in the making.

2. Link to Violent Ideology

If the potential lone wolf can first encounter his violent ideology in prison, this was not always the case. To find individuals who do not have a criminal record and did not spend anytime in prison, the authorities have to look at more signs to detect potential offenders.

Every lone wolf terrorist, by definition, has violent political beliefs. Most of the lone wolves were radicalized during their twenties, and only a few seem to have been radicalized during their childhood. Therefore if the intelligence community was able to monitor the sources of radicalization, it should be able to detect in a more accurate manner any potential threat. However, most of the information that should be collected in this part is protected by the 4th Amendment and will necessitate the use of the Foreign Intelligence Surveillance Act (FISA) or the implementation of new policies. Others can be from open source databases.

a. Open Source Information

This is the easiest way because it does not require a warrant or a court order. Fortunately open sources are multiplying, especially online. One of the weaknesses of the lone wolf is that, he is neither trained nor willing to be anonymous, contrary to the group-based terrorists. Because of his strong political beliefs, he often strongly broadcasts them. With the rising popularity of social media, some of the individuals discussed here shared their support for extremists groups or ideas.[69] Being public, and with absolutely no expectation of

[69] Amedy Coulibaly sharing videos and “liking” Islamist content on Facebook, or Timothy McVeigh sending letter to local newspapers and distributing flyers.

privacy, content is easily collectable. By following the public profile of individuals advocating, “liking” and sharing violent propaganda, the intelligence community should be able to add a new sign to the database and to link it to the previous information. These are rare occurrences but seem to have become more common and should be considered. Furthermore, previous ways to detect these individuals have to be used too, by surveying violent groups and leaders of these groups, and violent religious propagandists. If the modern lone wolf is less likely to be an associate of these groups than twenty years ago, these methods can still be useful.

b. Electronic Surveillance

As explained earlier, most modern lone wolves encounter their violent ideology online.[70] This method provides easy access, anonymity and possible immunity for demonstration of hatred like threat or insult. Most violent ideologists understood that early on, and chose to broadcast their political thought using the web. That is why electronic surveillance has to be a priority in the hunt for lone wolves nowadays. This paper, being focused on detection, will discuss mostly prospective surveillance policies.

Lone wolves, by their very nature, are hard to detect. They act alone, and therefore do not have reason to communicate with others. They often are the only person aware of their incoming attack. Consequently detecting them is far more challenging than it is for group-based terrorists. Warrant based surveillance, as possible under the Wiretap Act[71] and the Pen Register Statute[72] are not adequate in this case because they require too much in terms of probable cause to be efficient, especially with the lack of signs usually left by lone wolves. The Foreign Intelligence Surveillance Act (“FISA”) could be a solution but in the case of homegrown lone wolves, the target is more likely to be an American citizen and is not a member of a terrorist group by definition.[73] So, what could be the solution?

[70] Spaaij, *supra* note 18, at 56–58; Weimann, *supra* note 45 at 3.

[71] 18 U.S.C. §§ 2510–2522 (2012).

[72] 18 U.S.C. §§ 3121–3127 (2012).

[73] 50 U.S.C § 1801 (2012).

Detecting a lone wolf is truly challenging, and also crucial because of the damage he is able to do. Then it may be necessary to reduce the burden of probable cause in these cases. As seen previously, one major U.S. statute has already taken lone wolves in account: FISA. In 2004, the "Lone Wolf Amendment" was included, authorizing surveillance on non-U.S. persons, engaged "in international terrorism or activities in preparation" and without connection to a foreign power or a terrorist group.[74] While this text is one of the first attempts to fix the problem created by lone wolves, it is not sufficient. FISA is now able to stop what could be called an "international lone wolf" but is still helpless against a homegrown, domestic terrorist, such as Timothy McVeigh. Two options are therefore possible.

The first one, easier to implement, is a FISA amendment. The FISA "Lone Wolf Amendment" should expand to anyone other than a U.S. person planning to engage in domestic terrorism or activities in preparation. This provision will allow surveillance under FISA of domestic terrorism by a non-U.S. person. However, in the case of a homegrown lone wolf terrorist, FISA is once again inadequate.

The second option, more invasive in term of privacy, would be a system similar to the Terrorist Surveillance Program ("TSP"). If the TSP, still hardly understood, was described by the Bush administration as only aimed at international calls, some of the content obtained seems to be purely domestic.[75] By doing this, the TSP was going against the 4th Amendment of the Constitution of the United States, protecting citizens "against unreasonable searches and seizures."[76] As stated in *Illinois v. McArthur*, the Fourth Amendment's "central requirement is one of reasonableness."[77] Assistant Attorney General William Moshella made this argument, while defending the TSP.[78] The idea of a warrantless surveillance program is a controversial one,

[74] 50 U.S.C § 1801(b)(1)(C).

[75] James Risen & Eric Lichtblau, Spying Program Snared U.S. Calls, N.Y. TIMES (Dec. 21, 2005), http://www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html.

[76] U.S. CONST. amend. IV.

[77] 531 U.S. 326, 330 (2001) (citing *Texas v. Brown*, 460 U.S. 730, 739 (1983)).

[78] Letter from William Moshella, Assistant Attorney Gen., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et al. (Dec. 22, 2005) http://www.justice.gov/ag/readingroom/surveillance6.pdf.

but may be the only efficient way to prevent homegrown lone wolf attacks. In fact, the modern homegrown lone wolf does not send emails to his cell to prepare for the attack, does not attend secret meetings in mosques and is not a member of any violent group subsequently defeating most of the usual means of surveillance.[79] Then a possible waiver could be considered for the electronic surveillance of a U.S. person suspected of being a potential lone wolf. This surveillance, based on an assessment, would have to allow the gathering of both content and non-content information, but also to be as brief as possible to protect the privacy of the suspect.[80]

Additionally, it may be useful to expand the third party data use. By using selectors in search engines, it could be possible to ask service providers to report suspicious Internet searches. Internet searches are done without expectation of privacy, the request being sent to a third party; therefore it can also be a source of "red flags" for the intelligence community.

3. Logistics of an Attack

On his *iter criminis,*[81] the lone wolf terrorist has left marks to follow, as seen previously. At this point, he is now planning to act, and therefore needs equipment. As described by Ramon Spaaij, firearms and explosives are the most common used means during lone wolf attacks.[82] Buying and selling of firearms being already regulated, protected by the 2nd Amendment and defended by numerous associations, limiting or monitoring their sales more would be difficult in the United States. However, monitoring of explosives and components of explosives, which are able to trigger huge damage and death, can be expanded.[83] Then, dangerous or sensitive literature can also be considered as a way to detect lone wolves in the making.

a. Weapons and explosives

[79] Most of them are on the edge of such groups, like Paul Ross Evan with the Army of God or the Kouachi brothers with AQAP.

[80] A fifteen day period, renewable if evidence of a probable terrorist plan is found, could be a possibility.

[81] "Criminal path" in Latin, constituted of five steps: criminal thought, criminal resolution, preparatory acts, beginning of execution, and execution of the crime.

[82] Spaaij, *supra* note 18, at 72–73.

[83] The bomb built by Timothy McVeigh claimed 168 lives in Oklahoma in April 1995.

The first element to consider here is the 2nd Amendment of the Constitution stating, "the right of the people to keep and bear Arms, shall not be infringed."[84] Despite the multiplication of background checks and procedures preceding the purchase of firearms, the idea of monitoring weapons in the United States is illusory. Furthermore, the number of weapons in circulation added to secondary market makes it an unpractical way to detect potential lone wolves in America.

Explosives and their components are different. Restrictions already exist on the purchase of ready-to-use explosives, like dynamite, but their components are easier to obtain. One solution would be to use a method similar to those used to prevent the manufacturing of synthetic drugs. This system would necessitate multiple steps to be implemented. First, a committee of experts would have to draft a list of explosive components and the quantities in which they can be dangerous. Then, the use of an ID will be made mandatory in order to buy such components. If the buyer tries to buy too much of or too often a component, the purchase would be refused and a report would be drafted. This system would be a huge asset for the intelligence community given that it provides probable cause for more complete surveillance and prevents the rise of anonymous, dangerous, and repeat bomb makers.

b. Literature

The question of monitoring the purchase or exchange of "subversive" literature is a delicate one. It is a known fact that some pieces of literature, both fictional or not, have been commonly mentioned in lone wolf attack investigations (e.g., books like *The Turner Diaries* or *The Anarchist Cookbook).*[85] It is hard to determine the impact of the books on potential lone wolves. If *The Turner Diaries* promotes hate speech, racism, and rebellion against the federal government, it is first a fictional book. Similarly, the bomb recipes described in *The Anarchist Cookbook* are part of a book and not dangerous per se. Besides, both books are protected under the 1st Amendment of the Constitution assuring the American people that "Congress shall make no law . . . abridging the freedom of speech."[86] The idea of registering the name of every buyer of these books will be

[84] U.S. CONST. amend. II.

[85] The Turner Diaries by William Pierce Luther (1978), under the pen name Andrew MacDonald describes a fictional violent revolution leading to a race war. The book was quoted as an influence by Timothy McVeigh.

[86] U.S. CONST. amend. I.

infringement of a constitutional right and should not be attempted. However, a remaining solution could be, on the basis of fighting copyright infringement, to put trackers on some of the pirated versions on the Internet in order to get some information on their sharing. Still, this option is very close to being unconstitutional, and is far from being the best option.

"International" Lone Wolf

Most of the lone wolves studied here are citizens of the country they attacked, members of the society they harmed.[87] But the recent development of lone wolf terrorism shows that because the propaganda can be broadcast internationally on the Internet, lone wolves are able to create international links. Therefore the intelligence community should use the marks left in this situation to detect potential lone wolves, adding a new red flag to the detection process. The "international" lone wolf as described here can be either a U.S. person or not. The possibility of surveillance, as explained earlier, is therefore different between one and the other. For the convenience of not repeating which was written previously, the paper will not make the difference again. However, the type of surveillance described here is applicable to a non-U.S. person under FISA but not applicable to any U.S. person in the current state of the legislation.

Travel in "Danger Zones"

If radicalization often starts on the Internet, some of the lone wolves in the making then decide to travel abroad to either meet with the propaganda broadcaster and fall deeper into radicalization or to be trained by him. A line has to be drawn here between lone wolves and operatives of a terrorist group. Here, this line is becoming thinner. More and more European lone wolves[88] travel to the "danger zones" to

[87] Spaaij, *supra* note 18, at 67–68.

[88] Such as Mohamed Merah in Afghanistan and the Kouachi brothers in Yemen. Céline Lussato, *Mohamed Merah s'est-il formé lors de ses voyages à l'étranger ?*, L'OBS (Mar. 28, 2012, 12:14 PM), http://tempsreel.nouvelobs.com/monde/20120328.OBS4777/mohamed-merah-s-est-il-forme-lors-de-ses-voyages-a-l-etranger.html; *Kouachi brothers had weapons training in Yemen*, AL JAZEERA (Jan. 11, 2015, 10:50 AM), http://america.aljazeera.com/articles/2015/1/11/kouachi-france.html.

meet with religious fanatics or to get weapons training.[89] This situation is more likely to occur with Islamic lone wolves traveling to the Middle East. Without becoming members of a terrorist group, they have established contact with religious fanatics and have received either religious or political indoctrination or training. Then the lone wolf comes back to his home country or society and plans an attack without instruction or support from the terrorist group. By having contact with a terrorist group, the "international" lone wolf is giving more opportunities to the intelligence community to detect him.

The freedom of movement is protected by the U.S. Constitution under the Privileges and Immunities Clause.[90] However, the protection of the territory allows restrictions on entering and leaving the country. The number of illegal immigrants in the United States being so high, it is nearly impossible to control who is entering and who is leaving the country.[91] That is why focusing on travelers using airplanes is a better option.

The first step of the surveillance should be to determine what countries or regions can be considered as having terrorist strongholds. The intelligence community, with the help of the State Department, should establish a list of these areas and keep it updated. Then, the intelligence community should keep travel logs of travelers going to these places, using those as another red flag. Other elements have to be considered (time of year, length of the trip, number of people traveling) in order to determine the trip's objective. This system is not infringing the freedom of movement because it is only applied to people flying to "danger zones." It is still possible for them to travel "under the radar," using different means of transportation. This additional red flag would be a great help to detect lone wolves serious enough to travel abroad on behalf of their violent beliefs.

[89] Approximately 2000 went to Syria and Iraq, including 930 French citizens. Between 20 and 30% came back. Renaud de Chazournes, *Que faire des djihadistes de retour dans leur pays ?* [How to handle the returning jihadists?], MYEUROP (Oct. 2, 2014, 6:59 PM), http://fr.myeurop.info/2014/10/02/djihadistes-retour-europe-danger-14222.

[90] U.S. Const. art. IV, § 2, cl. 1.

[91] Around 11 million people estimated in 2012. Jens M. Korgstad & Jeffrey S. Passel, *5 facts about illegal immigration in the U.S.*, PEW RESEARCH CENTER (Nov. 19, 2015), http://www.pewresearch.org/fact-tank/2014/11/18/5-facts-about-illegal-immigration-in-the-u-s/.

Contact with Terrorist Groups

The “international” lone wolf can be international in two different ways. As described in the paper, he can travel to a “danger zone” to meet violent ideologists or members of a terrorist group, but he can also contact these members through the Internet. Knowing this, the intelligence community can use it to detect yet another new red flag.

The paper previously discussed the interest of the criminal and inmate records to detect lone wolves. These documents sometimes list known associates of the suspect. It can be a first step to notice connections with a terrorist group. This goal can be reached by using conventional means of surveillance under the Wiretap Act,[92] the Pen Register Act,[93] or the Stored Communications Act.[94] More interestingly, “international” lone wolves are more likely to be non-U.S. persons, allowing FISA surveillance orders against them. Furthermore, the main advantage of the lone wolf terrorist, his ability to stay unnoticed and self-sufficient, disappears when he has contact with a known group. By using the already existing surveillance of suspected members and associates of terrorist groups in the United States, it could be possible to detect lone wolves in the making, looking for advice, propaganda, or training. According to the degree of relation between lone wolf to be and group-based terrorist, it may even be possible to stop both of them on charges others than terrorism, for acts committed in preparation of a future attack.[95]

Connecting the Dots

“Much post-attack recrimination has focused on failures of ‘communication and information sharing’ among the CIA, the FBI and the National Security Agency, and on a lack of effective analysis—in common parlance, an inability ‘to connect the dots,’” says Robert Bryant.[96]

Throughout this paper, proof has been shown that collecting

[92] 18 U.S.C. 2510–2522.

[93] 18 U.S.C. 3121–3127.

[94] 18 U.S.C. 2701–2712.

[95] Hate speech, threats, arms dealing, the possibilities are numerous.

[96] Robert Bryant, *America Needs More Spies*, ECONOMIST (July 10, 2003), http://www.economist.com/node/1907776.

intelligence has been the way to detect potential threats. However, collection without classification has no significance. Every red flag, every mark left by a lone wolf is pointless by itself. But looking at the big picture is the solution to detect and avoid risk in these cases. This is why data mining is extremely important in detecting dangerous individuals.[97] Patterns, probable risk, and accumulation of red flags can be found using data mining. The "international" lone wolf is communicating more than the homegrown domestic lone wolf, and is therefore leaving more tracks to follow. But both of them are probable offenders, identifiable if the needed dots have been collected. It is a two-phase system and neither can be taken lightly.[98] As Bryant wrote it in his article, a good dot connecting system is useless without helpful dots.[99] Detection requires the intelligence community to prepare and to adapt its efforts to a new and changing threat as the lone wolf.

Fighting the Wolf

Lone wolf terrorism is a growing threat for the United States and the world, as shown by the figures for the last forty years.[100] During its existence, the phenomenon has evolved and diversified its form. Consequently, the intelligence community must adapt its

[97] "Data mining uses mathematical algorithms to construct statistical models that estimate the value of an unobserved variable—for example, the probability that an individual will engage in illegal activity. Data mining is best understood as an iterative process consisting of two separate stages: machine learning, where algorithms are applied against known and probabilistic inference, where the models built from algorithms are applied against unknown data to make predictions." U.S. DEP'T OF HOMELAND SECURITY, DATA MINING: TECHNOLOGY AND POLICY: 2008 REPORT TO CONGRESS 31–32 (2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.

[98] Concerning the Kouachi brothers, "Even if you give France a bit of a break," said one former senior United States counterterrorism official, who spoke on the condition of anonymity to avoid antagonizing an ally, "given what we know, and what the French knew then, these guys should have been high on any list. Especially since they seemed to have all the warning signs: travel to the region, a prison record, a social media profile. What more did they need?" Katrin Bennhold & Eric Schmitt, *Gaps in France's Surveillance Are Clear; Solution Aren't*, N.Y. TIMES (Feb. 17, 2005), http://www.nytimes.com/2015/02/18/world/gaps-in-surveillance-are-clear-solutions-arent.html.

[99] "There certainly was a lack of dot-connecting before September 11th, but more important was the fact that the blizzard of information available for analysis was of such poor quality. There were too few useful dots." Bryant, *supra* note 110.

[100] Spaaij, *supra* note 18, at 32.

intelligence collecting and detection methods in order to fight efficiently this rise of political violence. To do so, it is crucial to notice and understand new developments in the concept of lone wolf terrorism.

Sharing Intelligence

Said and Cherif Kouachi, the gunmen responsible for the Charlie Hebdo killings, were not just known by the French DGSI,[101] but were also on the Terrorist Identities Datamart Environment and then on the "no-fly list" because they were considered "potential lone wolves."[102] What triggered their name to be added on the list was their trip to Yemen on an attempted trip to Iraq, information that was later transmitted to the French authorities.[103]

Surprisingly, despite the international aspect of the Kouachi brothers's profiles, their surveillance was not given more priority than others purely domestic. This lack of perceptiveness from the French intelligence services, as shown by Jacques Follorou, is a good example of the damage that can be done when information sharing is not done properly.[104] First, sharing of information was poorly done between French law enforcement and the French intelligence community, which both had files on the Kouachi brothers.[105] Then other issues with the sharing of information occurred inside the French intelligence community itself. French intelligence services are mainly composed of two administrations: the DGSE, in charge of the external security, and the DGSI, in charge of internal security. Sharing of information and coordination of surveillance was nearly non-existent.[106] At the international level, the information of Said Kouachi being trained in

[101] Direction Générale de la Sécurité Intérieure (General Directorate for Internal Security), the French internal intelligence agency.

[102] Maurin Picard, *Les Frères Kouachi étaient connus de Washington* [Kouachi Brothers were known figures by the U.S. intelligence community], LE FIGARO (Jan. 9 2015, 10:16 PM), http://www.lefigaro.fr/international/2015/01/09/01003-20150109ARTFIG00303-les-freres-kouachi-etaient-connus-de-washington.php.

[103] *Id.*

[104] Jacques Follorou, Les attentats en France : la myopie des services de renseignement [The near-sightedness of the intelligence services], LE MONDE (Jan. 11, 2015, 7:56 AM), http://www.lemonde.fr/police-justice/article/2015/01/10/les-attentats-en-france-la-myopie-des-services-de-renseignement_4553283_1653578.html.

[105] *Id.*

[106] Bennhold & Schmitt, *supra* note 112.

Yemen by AQAP, was transmitted from Yemen to the United States then to France.[107] However, an emphasis should have been made on the probable dangerousness of such an individual, and may have prevented the January attack.

Sharing intelligence with another nation is not an easy task, due to defiance existing between countries, and the difficulties related to privacy rights under different legal systems. Notwithstanding, a clear and simple common chart of the potential danger of a specific lone wolf to be would be an amazing tool for intelligence services all over the world. Moreover, mutual assistance agreements should be drafted between long-term allies within the Western world, especially with the increasing flow of population between these countries.

Social Media as a Source of Intelligence

Social media is everywhere nowadays. It is a powerful and easy way to promote and broadcast ideas, as seen during the Arab Spring. Yet it is also a way for violent propaganda to be spread openly and should be used more by the intelligence community as an open source of information.

Djohar[108] Tsarnaev, currently on trial for the Boston Marathon Bombing, owned a VK account,[109] a Twitter account,[110] and an Instagram account.[111] On VK, he described his view of the world as "Islam." On Twitter, he wrote "I will die young" a year before the attack, then "Ain't no love in the heart of the city, stay safe people" during the attack.[112] But his Instagram account, deleted but partially recovered by the investigator from the FBI, offered a better view of his

[107] Picard, *supra* note 116.

[108] Djohar or Dzhokhar or Johar are used according to the English translation from the Chechen.

[109] VK is a Russian version of Facebook.

[110] Alexander A. Santos, *'I Will Die Young': The Eerie Subtext of Dzhokhar Tsarnaev on Social Media*, WIRE (Apr. 19, 2013, 4:47 PM), http://www.thewire.com/national/2013/04/dzhokhar-tsarnaev-social-media-accounts/64400/.

[111] Michael Walsh, *Boston Marathon bombing: Investigators uncovering data from suspect Dzhokar Tsarnaev's deleted Instagram account*, N.Y. DAILY NEWS (Apr. 27, 2013, 3:29 PM), http://www.nydailynews.com/news/national/dzhokhar-tsarnaev-deleted-instagram-partly-uncovered-article-1.1329087.

[112] Santos, *supra* note 125.

ideology. Djohar liked pictures of Shamil Basayev, responsible for terror strikes in Russia, associated with hash tags as such "#FreeChechenia, #Jihad, #Jannah, #ALLAH, #Jesus, and #God."[113] These clues were available and visible to everyone and should have been noticed and studied by the intelligence community.

Considering the flow of information on the Internet to be huge would be an understatement. It is not possible for anyone to notice and analyze every "like" given to a white supremacist group, every #jihad posted on Twitter, or every dastardly comment on an antiabortion website. However, the intelligence community should enhance its effort to detect such expressions of hatred and use it as a potential red flag. The use of third party data is essential in doing so. However, it is essential to remember that violent expression is very common on the Internet and should not be considered extensively as a sign of a probable lone wolf. The information war cannot be lost on the social media without putting at risk of radicalization numerous teenagers and young adults.

Active Approach to Detection

Though this paper advocates a prospective approach, most of the detection methods previously discussed are retrospective. The lone wolf has to act first, and the intelligence community has to notice it and then decide if it is a sign of potential dangerousness or not. Nevertheless, an active approach, even if more complicated and riskier than a reactive one, could be extremely fruitful when collecting intelligence.

1. Possibility of Infiltration for Intelligence Purposes

As explained earlier, the lone wolf, despite his appellation, has some social contact with other individuals sharing his religious or political beliefs. These contacts can take place in real life or online. The "recruiters" of such ideologies, often calling for chaos and violent action, are looking for young and easy-to-radicalize followers. For this reason, infiltrating agents for counter intelligence purposes could be an effective solution to detect lone wolves in the making.

Since COINTELPRO, infiltration of political organizations is seen as an illegal practice and as an abuse of power by the federal

[113] Walsh, *supra* note 126.

government.[114] It is true that, under J. Edgar Hoover's orders, excesses were common and some political organizations were investigated for political reasons more than for national security reasons.[115] However, having an agent inside such groups would be an invaluable asset for the intelligence community. This undisclosed participation, regulated by the Executive Order 12333, would have to follow a strict procedure to prevent any influence of the organization by the infiltrating agent. Most of the information of this subject in the FBI Domestic Investigations and Operations Guide ("DIOG") being classified, it is hard to determine what are the possibilities offered by these methods.[116]

A variation on this option would be to conduct such operations on the Internet. Pro Jihad Facebook groups are looking for followers and readers to keep posting related content. White supremacist forums are looking for administrators and moderators. By having an FBI agent filling these roles, it would be very easy to obtain information and to detect violent ideologists and potential lone wolves.

Infiltrating a group, either in real life or on the Internet, is a difficult and costly operation, but the amount and quality of intelligence collected could be so tremendous that it should be considered by the intelligence community.

2. Creation of a Network of Contacts in a "Known Community"

Infiltrating an agent takes time, money, an "in," and is a risky procedure. Still, the same information could be collected at the same level by creating a network of "associates" in a community known to be "hosting" terrorists. The community can be a neighborhood, a mosque, an Internet forum, a social group, and other types of social gathering places. In the case of the Kouachi brothers, both of them

[114] *COINTELPRO*, FED. BUREAU OF INVESTIGATION, http://vault.fbi.gov/cointel-pro (explaining the FBI's counter intelligence program).

[115] *See generally* Paul Wolf, COINTELPRO: The Untold Story (2001).

[116] FBI Domestic Investigations and Operations Guide, FED. BUREAU OF INVESTIGATION, https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version/.

frequented the Addawa Mosque, on Tanger Street in Paris.[117] If most of the others believers from this mosque were shocked to discover that they shared prayers with violent killers, it may have been possible that some of them had noticed something which could have been useful to the French intelligence community. Without inside information, the intelligence community is blind on an intelligence-collecting front.

Creating a link with people living in communities known to be a hub for lone wolves is primordial. As described in the FBI DIOG,[118] creating liaisons "with the general public, private entities and with local, state, federal, tribal and foreign government agencies for the purpose of building partnership" is recommended.[119] Seemingly it is not possible or advisable for the intelligence community to survey every chemical manufacturer, every gun seller, and every religious or political rally in the United States. Having a trusted relationship with members of these entities, with the common purpose to avoid violence, is a way of collecting intelligence. Moreover, this allows the intelligence community to avoid costs and risks related to their agent. That is why trip wires should be favored, enabling an empowerment of the community against lone predators living among them.

Conclusion

Intelligence is the key to detect terrorists and to prevent attacks. Noticing red flags, connecting them, and detecting individuals is a necessary mission for the intelligence community. Lone wolves, as described by this paper, present a challenge unknown and unprecedented. Citizens of countries all over the world, radicalized to a violent ideology, are launching attacks to trigger terror. Moreover, the Internet has created a hub for violent ideologies to be broadcast. By knowing and understanding the people and mechanisms involved,

[117] Benoît Zagdoun, *Dans l'ancienne mosquée des frères Kouachi, on condamne l'attaque contre "Charlie Hebdo"* [Kouachi brothers' ex-mosque is condemning their action], FRANCETVINFO (Jan. 10, 2015, 5:56 AM), http://www.francetvinfo.fr/faits-divers/attaque-au-siege-de-charlie-hebdo/dans-l-ancienne-mosquee-des-freres-kouachi-on-condamne-l-attaque-contre-charlie-hebdo_792791.html#xtor=AL-79-%5Barticle%5D.

[118] FED. BUREAU OF INVESTIGATION, *supra* note 131.

[119] FED. BUREAU OF INVESTIGATION, FBI DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, 2011 version, at 187.

it is possible for the intelligence community to detect and prevent such tragedies. However, the lone wolf is an evolving threat, from homegrown white supremacist loner to weapons-trained Islamic lone packs, lone wolves in the making are various and changing. But while facing this threat, and continuing to find new ways to efficiently prevent death and terror, it is important to remember to protect the liberties of the people threatened.

Fighting Terrorism Online

Brett Maxfield

"Arguably, the use of the Internet to radicalize and recruit homegrown terrorists is the single most important and dangerous novelty since the terrorist attacks of September 11, 2001."
[1]

Introduction

This policy paper makes to two recommendations to the U.S. government: (1) The government needs to aggressively take down terrorist websites by spearheading a definition of terrorism which can be universally accepted and does not provide First Amendment protection, and (2) the government needs to directly engage those who are at risk of online radicalization by training specialized agents who can effectively and persuasively articulate counterterrorist narratives on websites which are protected by the First Amendment.

In 2012 the Bipartisan Political Center ("BPC") Homeland Security Project released a report entitled *Countering Online Radicalization in America*. This report analyzes online radicalization, especially as it pertains to the United States, and makes specific recommendations for combating online radicalization in two specific categories: (1) reducing the supply in which the BPC recommends the U.S. government does not take down terrorist websites domestically and (2) reducing demand in which the BPC recommends that the U.S. government does not directly engage in trying to steer the at risk away from radicalization.[2] These two recommendations are actually simply stated maintaining the status quo. Currently the United States has no proactive policy such as the two advocated by this paper, but in each of these categories, the BPC does articulate compelling arguments for the need for government to take action to address the causes and conditions which lead to online radicalization and makes numerous recommendations in each category in order to combat its effects. However, the sum of all the excellent recommendations in each

[1] Bipartisan Policy Center, *Countering Online Radicalization in America*, HOMELAND SEC. PROJECT 47 (Dec. 2012), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20_Online%20Radicalization%20Report.pdf.

[2] *Id.* at 8.

category seem to fall short of what is the required course of action suggested by the analysis in each category. This paper analyzes the BPC's work and suggests two much stronger policy measures as recommendations based on the BPC's own analysis and original analysis. These two policy recommendations, which this author makes respectfully to the BCP report, this author believes to be more consistent with the BCP's own analysis of the causes and conditions underlying its recommendations.

Reducing the Supply—The Government Needs to Aggressively Take Down Terrorist Websites by Spearheading a Definition of Terrorism which Can Be Universally Accepted and Does Not Provide First Amendment Protection

The BPC's report states that: "For reasons ranging from the political to the practical, approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable."[3]

When explaining how online radicalism works, the BPC's report states that there are "six processes and dynamics that explain online radicalism"[4] The first two of these processes are:

(1) the online process in which individuals are "immersed in extremist content for extended periods of time" and which "increases support for suicide operations and other, often excessively brutal, terrorist tactics."[5]

(2) the online process in which individuals view "the powerful and (often) emotionally arousing videos from conflict zones" which depict "alleged incidents of torture, rape, and other atrocities by Western troops" which "can induce a sense of moral outrage" and trigger "mobilization into violent action."[6]

[3] *Id.* at 8. However, the report does make one recommend that modifies that view: "Government needs to retain its capability for aggressive takedowns of foreign-based websites but only use it when doing so is absolutely essential to stop a terrorist attack and/or prevent the loss of life." *Id.*

[4] *Id.* at 17.

[5] Bipartisan Policy Center, *supra* note 1, at 18.

[6] *Id.*

There is a logical disconnect here between the first two causes of online radicalism identified by the BPC and the recommendation of the BCP in the report to abstain from attempting to reducing supply, except in very limited circumstances, and only abroad. The BPC's blanket "reasons ranging from the political to the practical" definitely fall short of a satisfactory explanation.[7] The BPC fails to make a convincing case for its conclusion that "approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable" in light of its identification of the six most compelling reasons for online radicalization, especially the two quoted above.

Logic dictates that if terrorist websites are up with violent content with the purpose of causing radicalization or videos intended to induce a sense of moral outrage with the purpose of triggering mobilization into violent action, the government should target such website as soon as identified and aggressively take them down regardless of their country of origin.

The Analogy of Cancer[8]

If one knows that they have a serious, life-threatening cancer, they would be a fool to say to the doctor, "yes, you have identified the source of the cancer and it is operable, but I will just wait to for you to biopsy the most malignant growths as they become terminal." One would expect this person to die of cancer if the doctor followed their suggestion. Terrorism is a cancer on this earth, and the BPC has done a good job of identifying one of its primary sources of origin, but like the person above, the BPC seems to be too lax when it comes to suggesting an effective treatment to be rid of a very serious and deadly problem.[9] Logic dictates that one should get rid of cancer as soon as

[7] *Id.* at 8.

[8] This cancer analogy is my own analysis. However, I am not the first to think of the parallels. *See*, *e.g.*, *Mixing Memory*, BLOGSPOT (Dec. 31, 2005), http://mixingmemory.blogspot.com/2005/12/terrorism-is-like-cancer.html; *see also* Sefer Yilmaz, *An Analogy Between Cancer Cells and Terrorist* Organizations, 9 INT'L J. OF MGMT. ECON. & BUS. 347 (2013).

[9] There are some who disagree that online radicalization is a serious problem: "an ongoing research project funded by the Economic and Social Research Council found that much of the jihadist web presence was about 'preaching to the choir'. While the internet provides a convenient platform for activists to renew their commitment and reach out to like-minded individuals elsewhere, it is largely ineffective when it comes to drawing in new recruits. From the extremists'

possible and not let it spread uncontrollably. Thus, the government should target such websites as soon as they are identified and aggressively take them down regardless of their country of origin.

The CIA Does Not Need Terrorist Websites to Stay Up[10]

The report argues that aggressive take downs, even if limited to foreign, extremely toxic websites, such as those of al Qaeda, may cause more harm than good because the CIA can use these types of websites to monitor the activities and intentions of terrorists, and the removal of them would prohibit the CIA from being able to stop terrorist plots. There is some merit to this argument perhaps when it comes to groups that have managed to grow into worldwide networks such al Qaeda, once they are established and have many potential terrorist plots currently in play, but the BCP does not explain why this view has merit when it comes to a deeper analysis. Its logic does not seem to apply to terrorist start-up groups at all. Even in the case of groups like al Qaeda the balancing of the ability to gather intelligence needs to be balanced against the risk of the websites being used to recruit and grow the organization and devise new plots that might not have been hatched otherwise. The CIA and other, similar intelligence-gathering groups were able to gather information about terrorist groups before the Internet and can still do so if the government takes down those dangerous sources of intelligence.

perspective, the internet's failure to provide face-to-face human interaction nullifies many of its advantages. According to the social movement theorist Quintan Wiktorowicz, exceptionally 'risky' behaviours, such as engaging in violence or crime, always require social networks in order for the perceived cost/ benefit calculation to tip in their favour. Involvement in violence needs to be preceded by a prolonged process of 'socialisation' in which perceptions of self-interest diminish and the value of group loyalties and personal ties increase. This corresponds with the thrust of the argument made by the American academic Marc Sageman, who contends that, '[f]or the type of allegiance that the jihad demands, there is no evidence that the internet is persuasive enough by itself'." *Countering Online Radicalisation: A Strategy for Action*, INT'L CTR. FOR STUDY OF RADICALIZATION & POLITICAL VIOLENCE 13 (2009), https://cst.org.uk/docs/countering_online_radicalisation1.pdf.

[10] In formulating this section, this paper took into consideration the views expressed by: Bruce Hoffman, *Al Qaeda, Trends In Terrorism And Future Potentialities: An Assessment,* RAND (2003); Saxby Chambliss, *We Have Not Correctly Framed the Debate on Intelligence Reform,* U.S. ARMY WAR COLL. Q., 2005; JONATHAN MATUSITZ, TERRORISM AND COMMUNICATION: A CRITICAL INTRODUCTION (2013).

Given that terrorists are intelligent people, often very intelligent, and they are aware that agencies like the CIA are constantly attempting to infiltrate their organizations and obtain information about their intentions, tactics, plots, etc., a logical terrorist group would limit the use of its websites for the purposes of propaganda and radicalization. They would be very careful not to disclose any information which could be used by its enemies against its goals and only share misinformation when it comes to its true intentions, tactics, plots, etc. Thus, there is more value in cutting off the ability of terrorists to use these sites to radicalize than there is in using them to gather valuable information about how to defeat them. The BPC's report does not address this important argument. The DOD, a much better funded organization than the CIA which has its own intelligence gathering and counter terrorist strategies, thinks the opposite of the BPC.[11] Thus, the argument that terrorist websites should be left unmolested so that the CIA can use them to gather information, based on all the open source information available which this author has been able to gather, is an unsatisfactory argument when it comes to establishing such an important policy about national and international security. The argument that government should target such website as soon as identified and aggressively take them down regardless of their country of origin so that terrorist will not be able to easily radicalize within the United States and abroad seems to be more important for the reasons argued above than an argument that the CIA can use these website to gather important information.

There is one rationale for the CIA to keep up terrorist websites, but it is pure speculation and not founded on any real evidence. In theory, the government has the technical capacity and resources to

[11] "The most powerful objection to shutting down violent extremist websites is that valuable sources of tactical and strategic intelligence will be destroyed. In 2008, The Washington Post reported that the Central Intelligence Agency (CIA) strongly opposed the Pentagon's plans to take down the three al Qaeda forums, arguing that the benefits would be short-term disruption at best. One of its officials told the Post: [We] understood that intelligence would be lost, and it was; that relationships with cooperating intelligence services would be damaged, and they were; and that the terrorists would migrate to other sites, and they did. Contrary to popular imagination, therefore, the applicability and effectiveness of aggressive takedowns is limited, and their negative effects can be profound. The lesson is clear: While the U.S. government needs to retain its capability for carrying out cyber-attacks, it should only be used when doing so is absolutely essential to stop a terrorist attack and/ or prevent the loss of life." Bipartisan Policy Center, *supra* note 1, at 26.

hack into the webcams and microphones on people's computers and spy on them.[12] If it were true that the CIA was willing to do this in the name of national security on those only who are visiting terrorist websites, it would make sense to keep up these websites so that the government could record potential terrorists who visit the websites without them knowing and get very high value information to counter terrorism. This could outweigh the dangers of leaving these sites unmolested. This argument is the only rationale which would seem to justify keeping up the terrorist sites. Also, the possibility of such spying, not specifically from government agencies, has actually become the sole purpose and product of software companies like Stop Being Watched and other companies that offer similar anti-spying products for PCs. There is going to be a tipping point, and entertaining such an idea is no longer going to be considered on the fringe of serious policy discourse. Prior to Edward Snowden, the idea that the NSA was collecting and storing all the types of information that now has been revealed would have been considered fringe and not taken seriously in most policy discussions within academia.

Of course, there might be top-secret reasons which might make the CIA argument better than the one presented by this paper, but if such reasons exist, they are not available or not argued by the BPC. The U.S. public is not very enthusiastic about public policies that have "trust us, do not worry" as their primary justification. Nevertheless, due to the nature of national security issues, this may be the only rationale the intelligence community can give because the true rationale is classified. If this is the case here, when it comes to allowing terrorist websites to stay up unmolested, this paper might be wrong in advocating that government should target such website as soon as identified and aggressively take them down, but the other BCP

[12] *See*, *e.g.*, Spencer Ackerman, *CIA Chief: We'll Spy on You Through Your Dishwasher*, WIRED (Mar. 15, 2012), http://www.wired.com/2012/03/petraeus-tv-remote/; Spencer Ackerman*, Senators to investigate NSA role in GCHQ 'Optic Nerve' webcam spying,* Guardian (Feb. 28, 2014), http://www.theguardian.com/world/2014/feb/28/nsa-gchq-webcam-spy-program-senate-investigation; *Is the Government Spying On You Through Your Own Computer's Webcam Or Microphone?*, WASHINGTONSBLOG (June 24, 2013), http://www.washingtonsblog.com/2013/06/is-the-government-spying-on-you-through-your-own-webcam-or-microphone.html. There are hundreds of these types of articles on the web. Ironically, the justification for this type of spying in the novel *1984* and almost every futuristic "big brother" type conspiracy theory is almost always terrorism.

recommendations regarding reducing the supply of radicalization seem to contradict this, for taken as a whole, they advocate the private sector to neutralize terrorist websites. Thus, although in one section of their report they argue that the government should not target these websites and take them down because the CIA needs them to stay up, later sections seem to argue that it is better if the private sector takes them down, which undermines the argument that the CIA needs these websites.[13]

Foreign vs. Domestic Internet[14] and the Dark Web[15]

United States law makes a distinction between foreign and domestic on many fronts, but terrorist organizations do not. When people browse the web, the vast majority are overwhelmingly unaware and unconcerned with the country of origin of the content. The First Amendment is a constitutionally protected right of U.S. citizens, but it is not an absolute right and does not override all national security interests. Furthermore, U.S.-based terrorist content can radicalize people outside of the United States just as easily as in the United

[13] "Other ways of limiting the supply of violent extremist content rely on the cooperation of the private sector, especially Silicon Valley–based Internet companies like Google, Facebook, Twitter, and Paltalk, the platforms of which have been used by violent extremists and terrorists. Since 2008, lawmakers such as Senator Joe Lieberman (I-Conn.) have repeatedly urged these companies to take down content that supports terrorism and criticized them for failing to do so more vigorously." Bipartisan Policy Center, *supra* note 1, at 27.

[14] In formulating this section, this paper took into consideration the views expressed in the following articles: Philip Sohmen, *Taming the Dragon: China's Efforts to Regulate the Internet,* 1 STAN. J. OF E. ASIAN AFFAIRS 17 (2001), http://web.stanford.edu/group/sjeaa/journal1/china1.pdf; Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. TIMES (Apr. 23, 2006), http://www.d.umn.edu/~jford/phil3242/Google%27s%20China%20Problem%20%28and%20China%27s%20Google%20Problem%29%20-%20New%20York%20Times.pdf; Rebecca MacKinnon, *Flatter world and thicker walls? Blogs, censorship and civic discourse in China*, 134 SPRINGER SCIENCE BUS. MEDIA 31 (Aug. 9, 2007), http://www.jstor.org/stable/27698209?seq=1#page_scan_tab_contents.

[15] Nathan Chandler, *How the Deep Web Works*, HOW STUFF WORKS (Dec. 23, 2013), http://computer.howstuffworks.com/internet/basics/how-the-deep-web-works.htm.

States. The BPC report recommends taking down foreign-based websites but not any U.S.-based websites. This paper advocates the government should target all such websites as soon as identified and aggressively take them down regardless of their country of origin. This is especially true of what is known as the Dark Web, which is not known to most of the general public, caters to those who are on the fringes of society and are more likely to engage in criminality. The BCP report argues that it is too difficult for the government to effectively monitor and take down terrorist websites.[16] However, as the recent take down of the Silk Road[17] by the FBI and other Dark Web drug trafficking sites show, the government has the ability to effectively monitor all of the web, including the Dark Web, if it wishes to do so.[18]

Free Speech vs. National Security in the Face of a New Clear and Present Danger[19]

The report references a First Amendment test which a website must meet for it to be taken down in the United States .[20] This test is

[16] "For reasons ranging from the political to the practical, approaches that are aimed at reducing the supply of violent extremist content on the Internet are neither feasible nor desirable." Bipartisan Policy Center, *supra* note 1, at 8.

[17] The Silkroad was a Dark Web site which used Bitcoin to facilitate anonymous black market transactions, primarily for illegal drugs.

[18] Hsinchun Chen, *Sentiment and affect analysis of Dark Web forums: Measuring radicalization on the internet*, IEEE 109 (2008), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4565038&tag=1; Andy Greenburg, *Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains*, Wired (Nov. 7, 2014), http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.

[19] The phrase "clear and present danger" comes from Justice Oliver Wendell Holmes, Jr. in the case of Schenck v. United States, which is not the current law controlling free speech issues related to the advocacy of violence. Schenck v. United States, 249 U.S. 47, 52 (1919). The controlling law is generally the case Brandenburg v. Ohio, which states that "the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action." Brandenburg v. Ohio, 395 U.S. 444, 447 (1969). Nevertheless, the phrase is still regularly used in a colloquial sense to describe the law controlling free speech issues related to the advocacy of violence. The new clear and present danger for the purpose of this paper is online radicalization and the new global phenomena of global terrorism in general.

[20] Bipartisan Policy Center, *supra* note 1, at 24.

difficult to overcome. The test has three major elements: (1) there must be a direct, credible threat (2) against an individual, organization, or institution, which (3) must incite imminent lawlessness or meet the test for harassment (which is a less rigorous standard than inciting imminent lawlessness).[21]

This test references the Anti-Defamation League's ("ADL") *Combating Extremism in Cyberspace: The Legal Issues Affecting Internet Hate Speech* as its authority, but it is not accurately summarizing the ADL article which articulates many cases where there are easier tests to meet the requirements to avoid First Amendment protection.[22] The Anti-Defamation League's article continues: "[g]enerally defined as declarations of 'intention to inflict punishment, loss, or pain on another, or to injure another by the commission of some unlawful act,' true threats receive no First Amendment protection. *US v. Watts*, 394 U.S. 707 (1969), *R.A.V. v. St. Paul*, 505 U.S. 377 (1992)."[23] However, the caveat of being "true threats" makes this a moving target in most cases since it is very difficult to prove that a threat is true when made, usually only once it has been carried out, does one know for certain that it was a true threat.[24]

In *United States v. Rahman*, the Second Circuit Court of Appeals reviewed the conviction of Ahmad Ali Rahman, an Islamic cleric convicted for masterminding the 1993 attack on the World Trade Center in New York.[25] While Rahman was not involved in the detailed planning of the attacks, he engaged in public talks calling on his followers to make war against the United States and to take action to further Jihad. The question before the Court was whether Rahman could be prosecuted for knowingly engaging in terrorism.[26] The Court found that Rahman's speech constituted seditious conspiracy and therefore had no protection at all.[27] Although one might question if

[21] *Id.*

[22] *Combating Extremism in Cyberspace: The Legal Issues Affecting Internet Hate Speech*, ANTI-DEFAMATION LEAGUE 3–8 (2000), http://archive.adl.org/civil_rights/newcyber.pdf.

[23] *Id.* at 4.

[24] Kathleen Ann Ruane, *Freedom of Speech and Press: Exceptions to the First Amendment*, CONG. RESEARCH SERV. (Sept. 8, 2014), http://fas.org/sgp/crs/misc/95-815.pdf .

[25] 189 F.3d 88, 103 (2d Cir. 1999).

[26] *Id.*

[27] *Id.* at 114.

Rahman would have been convicted if all that had happened was communications about fighting the government, it is important to note that Rahman's talking was worthy of a twenty-year sentence.

In *United States v. Al- Timimi*, a jury convicted Ali Al-Timimi, a cleric at the Dar al-Arqam Center in Falls Church, VA, for inciting terrorism against the United States.[28] Al-Timimi's conviction centered on advice he gave to eight followers at a secret meeting on the night of September 16, 2001. During that meeting, Al-Timimi claimed that the September 11 attacks were justified.[29] He asked his followers to leave the United States and fight in Afghanistan with the Taliban and al Qaeda.[30] Although Al-Timimi did not actually undertake any overt actions against the United States himself, he was nonetheless convicted for inciting his followers to wage war against the United States. The government indicted and convicted him for conspiracy to make war against the United States even though he did not undertake overt acts to accomplish the conspiracy. The Court found that his speech was a direct cause of his followers' crimes. The jury convicted him of incitement to terrorist activity on the grounds of conspiracy based on his speech.

These two cases and many referenced in the ADL report illustrate that the government has the ability to take down terrorist websites in theory without offending the protection of the First Amendment. However, these cases are exceptions to the Brandenburg test. Each case is narrowly tailored according to facts that were investigated alongside the speech in question, making the speech an issue from a law enforcement standpoint. But the BCP report does not advocate that the government take down websites that meet the test it articulates. This paper argues that the government should be aggressive when it comes to fighting violent extremists online even if it means coming up against the First Amendment.

The Need for A New Test—A Universal Definition of Terrorism

[28] Milton Viorst, *The Education of Ali Al-Timimi,* ATLANTIC 1 (June 2006), http://www.theatlantic.com/magazine/archive/2006/06/the-education-of-ali-al-timimi/304884/.

[29] *Profile: Ali Al-Timimi*, IVESTIGATIVE PROJECT ON TERRORISM, http://www.investigativeproject.org/profile/104 (last visited Jan. 23, 2016).

[30] *Id.*

There are so many different definitions of terrorism as described by Gus Martin in *Terrorism and Homeland Security* and Louise Richardson in *What Terrorists Want: Understanding the Enemy, Containing the Threat* that there is an ambiguity to its meaning, making the definition of terrorism very subjective. Thus, the phrase, "one man's freedom fighter is another man's terrorist."[31] This subjectivity results in an equivalent terrorist definition of that once used by the Supreme Court for obscenity, "I know it when I see it." The problem with this type of subjectivity is that it effectively makes terrorism an impossible term to define in an effective way across agency jurisdictions, states, and nations. To quote Richardson in an interview she gave on November 11, 2006:

> Let me preface my remarks by saying what I mean when I use the term terrorism. One of the things I used to do when I used to teach a course on terrorism in the nineties was have my students collect usages of the term terrorism. Because the term has always been used so loosely that it comes to lose all meaning. So we used to collect references in the New York Times to currency speculation as economic terrorism, domestic violence as domestic terrorism, prank telephone calls as telephone terrorism, and so on. And so I'd like to rein in this definition, and by terrorism I simply mean the deliberate targeting of non-combatants for a political purpose . . . I go through a more complicated seven-point articulation of what I take to be the seven crucial characteristics of the term terrorism, but . . . I'll spare you that and simply say, 'The deliberate targeting of civilians for political purpose.' So it's the means that are used and not the ends that are pursued and not the political context in which the act takes place that determines whether or not, in my view, a group is a terrorist group.[32]

[31] LOUISE RICHARDSON, WHAT TERRORISTS WANT: UNDERSTANDING THE ENEMY, CONTAINING THE THREAT 6–10 (2006); Gus Martin, Terrorism and Homeland Security 12–13, 16–17, 112 (2011). *See also* Boaz Ganor, *Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter?*, IDC HERZLIYA (Jan. 1, 2010), http://www.ict.org.il/Article.aspx?ID=1123.

[32] Louise Richardson, *Address at World Affairs Council of Northern California*, FORA.TV (Nov. 11, 2006), http://fora.tv/fora/fora_transcript_pdf.php?cid=376.

One development which would greatly help in the evolution of the First Amendment law regarding the government's ability to take down terrorist websites would be the establishment of a definition of terrorism which can be universally agreed to by U.S. law enforcement and internationally by entities such as the UN and NATO. This paper suggests a definition of terrorism consisting of three elements:[33] 1) politically motivated,[34] 2) violent acts, or plans in furtherance of such

[33] In creating a definition of terrorism one may ask if the three elements of terrorism (alienated individual, legitimizing ideology, and enabling environment) should be taken into account, along with the seven characteristics of terrorism, as articulated by Louise Richardson in *What Terrorists Want: Understanding the Enemy, Containing the Threat*, and also the four components of the phenomenon of terrorism (social, economic, political, and religious conditions and philosophies) which must be contextualize to specific existing and particular times and places in light of the issues of revenge, renown or reaction should be incorporated into such a definition. *Id.* at 41–44, 80–81, 88–94, 128–129. Can terrorism, which can be discussed as a species of political violence or a strategy adopted by groups with widely differing goals and constituencies, be boiled down to a simple and usable definition? The question is answered by the question itself. Complexity must be logically reduced to its most basic elements for it to be easily used and practical. Making the definition of terrorism a complex matter does not serve the interests of anyone but the terrorist themselves. Thus, this paper attempts to make a useful and universal definition. However, this author also acknowledges that the definition proposed in this paper is substantively equivalent to the definition proposed by Boaz Ganor in numerous articles and books.

[34] This element distinguishes the remaining two the elements. Violence against civilians if not politically motivated is tragic and can be called murder or an act of insanity by a deranged person or persons. However, violence against a civilian or civilians can be motivated by passion, criminal intent, such as in a case of a bank robbery, or other motivations, but when looked at as politically motivated, then it becomes a military tactic which the perpetrators always believe to be a just cause. This is because terrorist are rational actors. By making a political motive the first element of the definition of terrorism, there is a chance to take the term out of the obscurity of relativism, which usually circles around arguments of whether a cause is just or not, and establishes as an a priori presumption that all causes subject to its meaning are presumed just causes, not that anyone would universally agree to the justness of any particular cause subject to the term, but that the perpetrators of terrorism always do feel their cause is just and are rational actors. Thus, making political motivation the first element of terrorism, makes the just/ unjust cause element of many definitions of terrorism irrelevant. All politics are presumed just for the purpose of this definition. As Boaz Ganor has argued, the goal is to make violence against civilians an unacceptable tactic of war and remove any element of whether a cause is just or not. In this understanding of politic motivation, religion can also often but not always be taken to be political. Islamic extremists seeking to establish a theocracy would be considered political by this definition, but the

acts of violence or advocating violence,[35] 3) against civilians or which would likely harm civilians.[36] If these elements were met, the First

Thuggees of India or Thugs who saw their violence against civilians as an act of worship to Mother Kali, were acting out of a desire to show supreme devotion to their deity without any political aim, and thus would not be considered terrorists by the definition advocated in this paper. Religion can be political but it can also be non-political. The same goes for the issues of revenge, renown or reaction. This element is the most difficult to deal with when it comes to overcoming the First Amendment objection to taking a website down, as discussed below.

[35] This element is the most fundamental and almost universally accepted as an element of all other definitions of terrorism. However, some definitions of terrorism would allow for acts which are not violent in the way the word is meant in this definition, say prank phone calls, the destruction of property, vandalism, or the hacking of websites or other technology. This definition of terrorism does not include these examples as what it means by violence. The result of violence would also be included in this definition even if it was not intended, if the other two elements are present, but the absence of violence would not exclude the terrorism if it was intended although not achieved.

[36] By civilians, this paper does not mean non combatants, which one might define as inactive military, police, or other types of law enforcement or government armed forces. Civilians here means non-military, non-law enforcement, ordinary citizens. It does not included government officials of any type but would include low-level government employees such as secretaries, clerks, post officers, etc. The reason for this narrow definition of civilian is that groups engaged in terrorism are usually rational actors who believe they have a just "war" against governments. The use of violence against civilians is a tactic they employ because they believe it will bring more attention to their cause or cause the government to rethink a policy they take issue with, in a way which furthers their aims. No group engages in terrorism because they think it will make their group or cause less effective. The goal of this definition of terrorism is to make civilians a protected class which will make rational actors not want to target due to the logical conclusion that it will not further their cause to due so, in a cost/benefit analysis. Although the current thinking of counterterrorism seems to be that the most high value targets for terrorists moving forward will be the targeting of children and contemplate that terrorists will target children for sexual exploitation to be streamed online. I argue that this is because the murdering of children is somehow seen as less morally repugnant then the sexual exploitation of children below. This moral repugnancy would in the current world mindset not help further any cause as a tactic, whereas the murdering of children still may. By building a consensus around civilians as sacred in the way that the sexual innocence of children is currently taken to be sacred, it is believed by this author that groups would avoid targeting civilians as targets because it would no longer further their causes, just like sexually exploiting children online would not further any political cause. Ironically, the First Amendment exclusion to protecting the sexual exploitation of children is contingent on there being no political value to it. One may ask why civilians should be granted this sacred status and not noncombatants? Noncombatants are political actors and terrorism is driven by political motives. Noncombatants assume a risk when taking their roles in the world which civilians do not, which is especially true in the case of military or law enforcement. This is not to

Amendment protection to such websites would be overcome. This paper argues this test should replace the above referenced test consisting of three elements: (1) There must be a direct, credible threat (2) against an individual, organization, or institution, which (3) must incite imminent lawlessness.[37]

Most websites exposing views to large amounts of extremist content or videos posted with the purpose to incite violence against the United States would be found to be terrorist websites under this new test and not protected by the First Amendment. Currently, most of these websites which are the cause of online radicalization are not protected by the First Amendment, but might not be taken down if the government agency involved uses the test articulated by the BCP report. Because under that test it is hard to evaluate if there is a "credible" threat or a minor threat, only established terrorists are credible. Their threats are not sufficiently focused on specific individuals, organizations, or institutions; just U.S. civilians at large, and they do not call for imminent violent action, but allow those they radicalize to take their time in plotting and executing their violence against civilians. None of these websites would be protected under the new test, for they are politically motivated and advocate violence towards civilians.

The Child Pornography and Obscenity Analogy—We Should Be Able To Label and Target Terrorism Just As We Can Label and Target Child Pornography and Obscenity So the Government Can Take It Down

Law is not static. It changes over time to reflect the values of society. The U.S. Constitution is a static articulation of law, but its interpretation has changed dramatically since it was written, especially in the last 100 years. Today the promotion of terrorism is not protected

say that violence targeted against noncombatants should be punished less—perhaps it should be punished even more—but for sake of limiting a definition of terrorism so that it can be a tool to combat terrorism, this paper excludes noncombatants from it. The purpose here of this definition is primarily to make it easy to take down terrorist websites, but it excludes noncombatants for the sake of the broader goal of establishing a universal definition which might limit the scope of terrorism and serve as a tool to deter it terrorism both domestically and internationally.

[37] *Brandenberg*, 395 U.S. at 447.

activity under the U.S. Constitution as interpreted under the First Amendment. But there is no clear rule or test to label and go after terrorism with specificity, due to the obscured definition. It is only addressed on a case-by-case basis, which caters to maintaining a subjective understanding of its meaning. Rather, as illustrated by the legal analysis of the ADL,[38] there are many different tests that allow the government to go after terrorist websites without offending the First Amendment. This is because the importance of terrorism in our society is relatively new. September 11, 2001 marked its true birth in the U.S. societal consciousness. Islamic radicals take a very long view of history. They plan for there to be many more acts of terrorism as big as or bigger than those of 9/11 over the next 100 to 1000 years in the United States. It may take a few more big terrorist attacks on U.S. soil to change the current interpretation of the First Amendment, but if one desires to end terrorism, whether abroad or domestically, one must be able to label and target it. Currently, this targeting is hard—if not almost impossible—to do consistently and objectively.

None but child pornographers themselves dispute the right of the government to aggressively take down child pornography sites, whether domestic or international. Why such resistance to the government aggressively taking down terrorist websites intended to radicalize violent extremism against U.S. civilians? Who should object but the terrorists themselves? One can easily argue that terrorism is at least as bad as child pornography if not in fact much worse. Of course not all obscenity is child pornography, but all child pornography is obscenity and no obscenity is protected under the First Amendment.

If one takes the arguments for the causes of radicalization in the BPC's report and the recommendations that the BPC suggests and replaces the idea of radicalization with child pornography, less people would agree with BPC's report. Society has had a long time to think about obscenity and child pornography relative to terrorism. Even though all three have been with us since the dawn of human history, terrorism has only recently come on the scene in U.S. social consciousness in a major way. The understanding of the First Amendment has been modified over time to protect more and more of what once considered obscenity and yet has still managed not to protect obscenity, especially not child pornography. Thus, this trend

[38] Bipartisan Policy Center, *supra* note 1, at 24; Anti-Defamation League, *supra* note 24, at 3–8.

toward celebrating the First Amendment's protection of free speech does have some clearly defined limits. The definition of obscenity has evolved over time, making it more limited, but also more objective.[39] The same can happen with the definition of terrorism.

In 1964, Supreme Court Justice Potter Stewart defined obscenity in *Jacobellis v. Ohio*[40] as "I know it when I see it,"[41] which could equally be said about the definition of terrorism today. This expression has become one of the most famous phrases in the entire history of the Supreme Court for its lack helpfulness in defining obscenity in an object manner. In 1868, the English case *Regina v. Hicklin*[42] defined obscenity as depravity and corruption in "those whose minds are open to such immoral influences."[43]

In 1957, *Roth v. United States*[44] defined obscenity as a "dominant theme taken as a whole" which appeals to "prurient interest" in the eyes of an "average person, applying contemporary community standards."[45] This was again changed in *Memoirs v. Massachusetts*,[46] to three elements: (1) patently offensive, (2) appealing to prurient interest, and (3) of no redeeming social value.[47]

Then came *Miller v. California*,[48] changing it to: (1) The average person, applying local community standards, looking at the work in its entirety, must find that it appeals to the prurient interest, (2) The work must describe or depict, in an obviously offensive way,

[39] *See* MARJORIE HEINS, NOT IN FRONT OF THE CHILDREN: 'INDECENCY,' CENSORSHIP, AND THE INNOCENCE OF YOUTH 360 (2d ed., 2001); Louis Henkin, *Morals and the Constitution: The Sin of Obscenity*, 63 COLUM. L. REV. 393, 414 (1963); Harry Kalven, Jr., *The Metaphysics of the Law of Obscenity,* SUPREME COURT REV. 1, 1–45 (1960); Robert F. Goldman, *Put Another Log on the Fire, There's a Chill on the Internet: The Effect of Applying Current Anti-Obscenity Laws to Online Communications,* 29 GA. L. REV. 1075 (1995).

[40] 378 U.S. 184, 197 (1964).

[41] *Id.*

[42] L.R. 2 Q.B. 360 (1868).

[43] *Id.*

[44] 354 U.S. 476, 489 (1957).

[45] *Id.*

[46] 383 U.S. 413, 418 (1966).

[47] *Id.*

[48] 413 U.S. 15, 15 (1973).

sexual conduct, or excretory functions, and (3) The work as a whole must lack "serious literary, artistic, political, or scientific values."[49]

As illustrated by the above chronicling, the understanding of the First Amendment has changed over time when it comes to obscenity from a vague, subjective definition to an objective definition which makes obscenity easy to label and target by government, especially in the case of child pornography. The definition of terrorism and its relationship to the First Amendment also needs to evolve so as not to protect terrorist extremism or radicalization efforts but allow government to easily label and target terrorism and thus protect the Homeland. The BCP makes suggestions that seem to protect online terrorist extremism and radicalization efforts when it would never make such suggestions to protect obscenity. Terrorism is a matter at least equally as abhorrent as and more insidious than child pornography. Child pornography is a felony which potentially can bring a life sentence in prison,[50] but the type of terrorist websites which are contemplated by the BCP are arguably acts of treason punishable by death under U.S. law if engaged in by U.S. citizens.[51]

Recommendations

This paper suggests that the BPC should change its recommendation to leave domestic terrorist websites unmolested and its limited recommendation regarding taking down foreign websites with the following: the government needs to aggressively take down terrorist websites by spearheading a definition of terrorism which can be universally accepted and does not provide First Amendment protection.

[49] *Miller*, 413 U.S. at 23 (citing Kois v. Wisconsin, 408 U.S. 229, 230 (1972)).

[50] 18 U.S.C. §§ 2251–2260 (2008).

[51] U.S. CONST. art. III, § 3, cl. 1. "Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989)." 18 U.S.C. § 2339B(a)(1) (2012).

The United States has the ability to spearhead the effort to establish a universally accepted definition of terrorism so it can label and target terrorism just as it does child pornography and obscenity. And, if terrorist websites are up with violent content with the purpose of causing radicalization or videos intended to induce a sense of moral outrage with the purpose of triggering mobilization into violent action, the government has the ability target such websites as soon as identified and aggressively take them down regardless of their country of origin.

As stated above, this paper suggests a definition of terrorism consisting of three elements: (1) politically motivated, (2) violent acts or plans in furtherance of such acts of violence or advocating violence, (3) against civilians or which would likely harm civilians.

A simpler version of the same three elements can be articulated like this: terrorism is political violence against civilians. These three elements can easily be placed into language consistent with the test against obscenity articulated in *Miller*.[52]

There is of course a major legal problem here in that what otherwise would be obscenity is not obscenity if politically significant. In other words, having a serious political purpose protects what otherwise not be protected under the First Amendment, and yet no amount of sophistry of political purpose will protect child pornography from not being found obscene. This paper suggests that political purpose not be a saving clause but an element denying First Amendment protection. This is counterintuitive to the logic of First Amendment jurisprudence that especially protects political speech. This paper recommends an exception to First Amendment protection in which a political purpose is an essential element for exclusion. This is an uphill battle, but because the political purpose prohibition is not narrow, only political purposes coupled with a violent intent toward civilians, or in other words, only political purposes of a terrorist nature are to be excluded. But no such reform can happen without a universally accepted definition of terrorism as a basis from which to begin a debate about reform in this area of law and public policy.

Implementation of New Recommendations

Terrorism is going to be a long-term problem for our nation to address. It may take years before Congress and the courts fully address

[52] *Miller*, 413 U.S. at 23 (citing Kois v. Wisconsin, 408 U.S. 229, 230 (1972)).

a balanced and functional regime of laws and procedures to take down terrorist websites such as those contemplated above. However, in the meantime, the executive branch has the ability to act under current law in various ways to take down terrorist websites via various agencies if they meet the test consisting of three elements: (1) there must be a direct, credible threat (2) against an individual, organization, or institution, which (3) must incite imminent lawlessness. Executive agencies have the privilege and responsibility of playing the judge of what constitutes these elements when it comes to evaluating the facts of a specific case, knowing that it could be years or never at all before an Article III judge reviews their decisions. They should be aggressive on the side of taking down potentially dangerous site with a high potential of radicalization. If nothing else, the CIA can be employed to neutralize terrorist websites abroad. If the United States truly wants to end terrorism, it should and must do everything in its power to reduce the supply of terrorists by ending the ability of terrorists to use the Internet to radicalize anyone nationally and internationally.

The BPC's other four of the "six processes and dynamics that explain online radicalization" can also be neutralized by targeting and aggressively taking down all websites which intend or could be construed to be able to radicalize. This paper agrees with the BPC in that the United States should not establish nationwide filtering systems. If the government takes down terrorist websites, there is no need for nationwide filtering systems that can perhaps interfere with non-terrorists websites by accident. This paper also agrees with all the other recommendations made by the BPC's report on supply.

Reducing Demand—The Government Needs to Directly Engage Those Who Are At Risk of Online Radicalization by Training Specialized Agents Who Can Effectively and Persuasively Articulate Counter Terrorist Narratives On Websites Which Are Protected by the First Amendment

The BPC's report acknowledges that: "Much needs to be done to activate a virtual marketplace in which extremism, terrorism, and other bad ideas are drowned out by pluralism, democracy, and the peaceful means through which good ideas can be advanced."[53] However, the report recommends that the federal government should

[53] Bipartisan Policy Center, *supra* note 1, at 8.

only play a limited role in bringing this marketplace about and primarily rely on the private and not-for-profit sectors to address the need. There is nothing wrong with the specific proactive recommendations made by the report encouraging the rise of nongovernmental counter-extremist voices in cyberspace, but they do not go far enough. This paper does find fault with the report's recommendation that the Government does not attempt to fill this void. The report has an excellent analysis of the need for activism to steer people "at risk" away from radicalization, articulating a very strong three point argument for why this reduction of demand cannot be left to chance or "the free market of ideas" due to: (1) an enthusiasm gap, (2) a pluralism gap, and (3) a skills gap.[54] However, the report argues that government is not able to close any of these gaps directly due to laws and political conventions that prevent government from interfering with the domestic political discourse.[55]

The report justifies this position by citing in the Smith-Mundt Act of 1948,[56] "which restricts the domestic dissemination of information"[57] and an article by Josh Rogin, *Much ado about State Department 'propaganda'* in Foreign Policy from May 23, 2012.[58] This paper does not find these arguments sufficient to justify a policy of governmental inaction or limited action (to only influencing nongovernmental actors to fill the void) in light of the BPC's analysis of the need and the nongovernmental alternatives that might fill the

[54] *Id.* at 32.

[55] "The capacity of government to close these gaps and—in doing so—activate a fully functioning marketplace of ideas is limited due to laws and political conventions that prevent the U.S. government from interfering in the domestic political discourse. This does not mean, however, that the government's hands are tied completely. As will be shown, the federal government can play a positive role in creating an environment in which civic actors feel empowered to challenge violent extremist and terrorist propaganda. It can also spread information, facilitate the exchange of experiences and best practices, and bring together different stakeholders, such as private business and community groups, who can take positive action." *Id.* at 32.

[56] *Id.* at 51. "The most frequently cited example is the Smith-Mundt Act of 1948, which restricts the domestic dissemination of information—produced typically by the State Department and the Department of Defense—that is aimed at foreign audiences. *See* Josh Rogin, *Much ado about State Department 'propaganda'*, FOREIGN POLICY (May 23, 2012), http://foreignpolicy.com/2012/05/23/much-ado-about-state-department-propaganda/".

[57] *Id.*

[58] Rogin, *supra* note 70.

gaps with the encouragement of the government. Rather, this paper recommends that the government needs to directly engage those who are at risk of online radicalization by training specialized agents who can effectively and persuasively articulate counter terrorist narratives on websites which are protected by the First Amendment.[59]

The Enthusiasm, Pluralism, and Skills Gaps[60]

The BPC has articulated strong arguments for the need to fill a void when it comes to steering people "at risk" away from radicalization, but these very arguments are also the reasons why the private sector is insufficient to meet the needs, regardless of how much governmental encouragement is given to potential nongovernmental actors who may play a role in the solution. The primary role of government is to provide public good which no free market can give society efficiently, such as roads, police, fire fighting, utilities, and standing armies for national security. As the BPC has convincingly

[59] Although the US has not engaged in this counter terrorism tactic to date, the UK has been engaged until very recently, "But in 2010, the new Conservative government declared . . . the program, known as 'Prevent,' a failure . . . The emphasis has shifted to tough action - promises to strip British jihadis of their passports and stop radical preachers from speaking in public or using social media. Having undertaken the 'most significant domestic program by any Western country to foster a moderate version of Islam and prevent radicalization,' said James Brandon, former head of research at the anti-extremism Quilliam Foundation, 'the UK has effectively given up trying to stop jihadists from being created.'" Michael Holden, *Why Britain is still losing its fight against radicalization*, REUTERS (Oct. 13, 2014), http://www.reuters.com/article/us-mideast-crisis-britain-radicalisation-idUSKCN0I20ET20141013.

[60] "In the U.S. tradition, the rationale that underlies freedom of speech is the notion of a marketplace of ideas, in which truth prevails as long as good and bad ideas are allowed to compete. Bad ideas—even falsehoods—will eventually be crowded out, while the truth will emerge as stronger and more robust, having been tested in a free, fair, and—sometimes—fierce contest . . . At first glance, the Internet seems to have made this marketplace more effective. Prior to its creation, not everyone had the opportunity to participate in the trade of ideas. Access to the mass media was expensive and controlled by gatekeepers—journalists, editors, and proprietors—who had a tendency to filter out cranks, extremists, and conspiracy theorists. The Internet turned the situation on its head: It gave everyone access, reduced the cost of publishing to virtually zero, and eliminated the reliance on journalistic middlemen. Even so, the rise of the Internet has created its own share of distortions and market failures." Bipartisan Policy Center, *supra* note 1, at 31.

shown, such a need exists online and in the realm of social media, when it comes to fighting terrorism by trying to win the hearts and minds of those “at risk” of radicalization. Yet, the BPC recommends that government only encourage nongovernmental actors to fill the gaps.

Enthusiasm[61]

When it comes to the enthusiasm of terrorists to engage online and in social media to radicalize, there is a need to counter this enthusiasm with a superior enthusiasm working worldwide, seven days a week, twenty-four hours a day. This is a tall order. There is no financial incentive to such a mission. If the U.S. government had left putting a man on the moon to the private sector, only encouraging the private sector to do so rather than creating NASA, it may have taken much longer for the mission to be accomplished. There was much more enthusiasm for putting a man on the moon back then in both the general public and private sector than there is today to try and curb terrorism by steering people “at risk” away from radicalization.

Pluralism[62]

As the BPC has explained, pluralism does not exist when it comes to the type of sites which have the potential to radicalize. Assuming that there are private sector parties willing and able to engage, it is reasonable to assume that these parties, even if they did

[61] “The enthusiasm gap: Instead of having extremist views drowned out by opposing views, the Internet has amplified extremists’ voices. Whether on YouTube, blogging platforms, or in newspaper comment sections, the cranks, extremists, and conspiracy theorists now seem to be everywhere, and—rather than being crowded out by moderates—they are the ones doing the crowding out. Their enthusiasm, energy, and excitement is unmatched by the political mainstream: According to experts like psychologist John Suler, this allows them to dominate discussions and it conveys the impression that they are the majority.” *Id*. at 32.

[62] “The pluralism gap: Far from creating more—and more vigorous—debate, the Internet has created ever-smaller ghettos for ideas and discourses, which, in turn, have reduced the number of spaces in which extremist and/ or controversial ideas are openly contested. The best examples are extremist forums, which have thousands of users arguing about tactics and strategy but who rarely challenge each others’ assumptions. These forums serve as echo chambers, in which extremist attitudes are hardened, not challenged. In the words of Mark Potok of the Southern Poverty Law Center, ‘There is no real exchange of ideas on whitepower.com.’” *Id*.

exist, would come from a pluralistic—if not ultra-pluralistic—point of view with the goal of spreading the ethos of pluralism. How well will ultra-pluralistic preachers be received in the closed-minded "ghettos" of terrorist chat rooms? They will not be well received. They will be kicked out or ignored.

Skills[63]

To be effective in curbing radicalization by trying to steer away people "at risk" from extremism, the actors must have rare and hard-to-acquire skills. They must know how to sympathize with fringe, anti-social, dark, hateful beliefs and attitudes of extremists and to establish a rapport, trust, a meeting of the minds that penetrates the heart, over time, perhaps years or decades. Not many in the private sector possess the needed skills in divergent fields such as psychology, political science, ethics, law, Islam, and technology[64] and have the ability to

[63] "The skills gap: Young people are said to be digital natives who feel comfortable using information technology, but they often lack the skills to evaluate and contextualize online content—whether because some parents are intimidated by the online environment and take a hands-off approach or because schools are not teaching analytical skills sufficiently. The capacity of government to close these gaps and—in doing so—activate a fully functioning marketplace of ideas is limited due to laws and political conventions that prevent the U.S. government from interfering in the domestic political discourse. This does not mean, however, that the government's hands are tied completely. As will be shown, the federal government can play a positive role in creating an environment in which civic actors feel empowered to challenge violent extremist and terrorist propaganda. It can also spread information, facilitate the exchange of experiences and best practices, and bring together different stakeholders, such as private business and community groups, who can take positive action." *Id.*

[64] The amount of cross fields is hard to define, for example, "Touch points: A classic service design method that will help me identify and pinpoint exact moments when radicalization hits the final trigger towards recruitment. Those triggers can then be studied further for a comprehensive analysis. Study of user journeys will help me to achieve this particular method. Once I have established touch points, I can redesign those and test it on selected group of civilians and record reactions. It can also be helpful in de-radicalization processes… Ethnographic… a research strategy… called snowball sampling to establish the behaviors of subjects and determine if they are vulnerable to radicalization process, or on the other hand, susceptible enough for de-radicalization. Psychographics can also be embedded in this tactic for generating better results." Krisha Patel, *Using Design Research to disrupt Online and Social Media Terrorist Recruitment*, (May 2014) http://www.academia.edu/7332652/Using_Design_Research_to_disrupt_Online_and_Social_Media_Terrorist_Recruitment.

speak several languages to turn others away from radicalism. There is no market for people for the needed combination of skills. How many people in the general public or private sector could walk off the street and command a space shuttle mission to the International Space Station and back without any specialized government training? Imagine that someone suggested that national defense in the form of the operation of the Armed Forces be left to untrained non governmental actors? This would be too foolish to even contemplate, yet for a fraction of every dollar spent on the Armed Forces to combat terrorism, one could form an army of pluralistic persuaders to engage people "at risk" and reduce terrorism at its source.[65] The argument that it is too hard for the government to do this is not viable. However, that there is no political will for such a solution currently is true.

The Smith-Mundt Act of 1948

According to a RT.com report entitled *US ends ban on 'domestic propaganda'*, "The Smith-Mundt Act has ensured for decades that government-made media intended for foreign audiences doesn't end up on radio networks broadcast within the US. An amendment tagged onto the National Defense Authorization Act removed that prohibition this year [2013], however, and as of earlier this month those news stories meant for nations abroad can now be heard easily by American ears."[66] In a related article by the Business Insider titled *The NDAA Legalizes The Use Of Propaganda On The US Public*:

[65] "In fiscal year 2012, the United States spent $17.25 billion on counter-terrorism." Drew Desilver, *U.S. spends over $16 billion annually on counter-terrorism*, PEW RESEARCH CTR. (Sept. 11, 2013), http://www.pewresearch.org/fact-tank/2013/09/11/u-s-spends-over-16-billion-annually-on-counter-terrorism/; "The fiscal 2013 cost of national security comes to more than $1.3 trillion . . . ." David Cay Johnston, *The true cost of national security*, COLUM. JOURRNALISM REV. (Jan. 31, 2013), http://www.cjr.org/united_states_project/the_true_cost_of_national_secu.php?page=all#sthash.pcAAkkcu.dpuf.

[66] "Until earlier this month, a longstanding federal law made it illegal for the US Department of State to share domestically the internally-authored news stories sent to American-operated outlets broadcasting around the globe. All of that changed effective July 2 [2013], when the Broadcasting Board of Governors (BBG) was given permission to let US households tune-in to hear the type of programming that has previously only been allowed in outside nations." *US ends ban on 'domestic propaganda'*, RT (July 15, 2013, 6:32 PM), https://www.rt.com/usa/smith-mundt-domestic-propaganda-121/.

> Lt. Col. Daniel Davis . . . dedicated a section of his report to Information Operations (IO) and states that after Desert Storm the military wanted to transform IO 'into a core military competency on a par with air, ground, maritime and special operations.' Davis defines IO as 'the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.' IO are primarily used to target foreign audiences, but Davis cites numerous senior leaders who want to (in the words of Colonel Richard B. Leap) 'protect a key friendly center of gravity, to wit US national will' by repealing the Smith-Mundt Act to allow the direct deployment of these tactics on the American public.[67]

This move to allow propaganda on U.S. citizens on U.S. soil was not the case when the BPC report was published. When it comes to the counterterrorist policy advocated by this paper this is a good thing, but it does raise concerns about how much national security issues can and are diminishing our civil liberties. But, as the Foreign Policy article cited by the BPC states, "the update for Smith-Mundt was intended to recognize that U.S. public diplomacy needs to compete on the Internet and through satellite channels and therefore the law preventing this information from being available to U.S. citizens was simply obsolete."[68]

Conclusion

In spite of the potential danger of the erosion of civil liberties, (1) the government needs to aggressively take down terrorist websites by spearheading a definition of terrorism which can be universally accepted and does not provide First Amendment protection, and (2) the government needs to directly engage those who are at risk of online radicalization by training specialized agents who can effectively

[67] Michael Kelley, *The NDAA Legalizes The Use Of Propaganda On The US Public*, BUS. INSIDER (May 21, 2012, 5:11 PM), http://www.businessinsider.com/ndaa-legalizes-propaganda-2012-5#ixzz3JqUzi3bX.

[68] Rogin, *supra* note 70.

and persuasively articulate counter terrorist narratives on websites which are protected by the First Amendment.

It is an unhappy and unfortunate reality that terrorism has caused Americans to give up some of their civil liberties in exchange for greater peace of mind to counter terrorism since 9/11. This tide will not recede anytime soon, if ever. The trend worldwide is for less privacy, more intrusive government. The two recommendations of this paper will further this trend towards "Big Bother" fears, in exchange for greater peace of mind regarding our ability to prevent another 9/11 from happening. Some may argue that the very recommendations being made by this paper are a victory for terrorists, especially Islamic terrorists that find the American way of life as one of its primary justifications for their violence. The threat of terrorism and the need for the government to take actions to counter those threats, often at the expense of civil liberties, makes the duty of citizens to care about the character of those they elect and allow to serve in government of utmost importance.

There Is No Second Cold War: Despite Record Low Sea-Ice Levels There Is No Race for the Arctic

Jeff Janaro

Introduction—Consequences of U.S. Ratification of UNCLOS Amid Growing Tensions With Russia

In the twenty-first century, many experts believe that climate change, technological advances, and an increasingly connected global market for resources may unlock the considerable economic potential of the Arctic region. The Arctic is defined in statute (15 U.S.C. § 4111) as all United States and foreign territory north of the Arctic Circle and all United States territory north and west of the boundary formed by the Porcupine, Yukon, and Kuskokwim rivers; all contiguous seas, including the Arctic Ocean and the Beaufort, Bering, and Chukchi Seas; and the Aleutian Chain.[1]

The melting of Arctic sea ice to record lows in recent years has prompted many nations, principally those with Arctic Ocean coastlines ("Arctic states"), the United States, Canada, Russia, Norway, and Denmark (Greenland), to reassess their commitments and interests in the vast and formidable Arctic.

> Many forecast Arctic summers will be free of ice in a matter of decades, potentially opening the region up to hundreds of billions of dollars in investment, including energy production, shipping, and fishing. The thaw will also pose new security demands as greater human activity induces states to increase their military and constabulary presence. While most experts dismiss the prospects for armed aggression in the Arctic, some defense analysts and

[1] R. J. Paupp Jr., *U.S. Coast Guard Artic Strategy*, U.S. COAST GUARD HEADQUARTERS 11 (May 10, 2013), http://www.uscg.mil/seniorleadership/DOCS/CG_Arctic_Strategy.pdf.

> academics assert that territorial disputes and a competition for resources have primed the Arctic for a second Cold War.[2]

This paper will examine the existing international legal framework governing the Arctic. Then, the actions of the United States and Russia within the existing legal framework will be analyzed to determine if there is any merit to the claims that the Arctic is a region on the brink of a "Second Cold War." Finally, the 1982 United Nations Convention on the Law of the Sea ("UNCLOS") will be studied, with specific attention paid to the national security consequences to the United States if it decides to ratify the Convention. Again, this matter will be analyzed as related to United States and Russian relations in the Arctic.

This study concludes that the Arctic is not an area of a burgeoning "Second Cold War" between the United States and Russia, as some would suggest. Rather, despite strong rhetoric, Russia has been a cooperative partner in the region, demonstrating the Arctic is an area where the United States and Russia can develop trust and strengthen their relationship despite disagreements in other parts of the world. Secondarily, an argument against ratification of UNCLOS will be made primarily on the grounds that the U.S. cedes too much sovereignty to the United Nations without gaining any national security protections that do not already exist outside of UNCLOS.

The Existing Arctic Legal Framework

The Law of the Sea is applicable in the marine Arctic as it is in any other ocean. Numerous international treaties are applicable in the marine Arctic, but one comprehensive, region-specific agreement for the region does not exist.[3] The Arctic is primarily governed by soft law (not legally binding) arrangements. Arctic coastal states have sovereignty, sovereign rights, and jurisdiction to explore and exploit oil and gas on their continental shelves, though the status of the Arctic

[2] *The Emerging Arctic: Risks and Opportunities*, COUNCIL ON FOREIGN RELATIONS, http://www.cfr.org/arctic/emerging-arctic/p32620#!/ (last visited Jan. 18, 2017).

[3] *The Arctic Ocean Review: Phase I Report* 2009-2011, ARTIC COUNCIL PROTECTION OF THE ARTIC MARINE ENVIRONMENT WORKING GROUP 828 (2011), https://oaarchive.arcticcouncil.org/bitstream/handle/11374/1623/AOR_Phase_I_Report_to_Ministers_2011.pdf?sequence=1&isAllowed=y.

states' continental shelves are currently unknown.[4] Legally binding international treaties to explicitly manage the Arctic have remained elusive because of the Arctic states' insistence on maintaining their sovereignty and sovereign rights.

"To date, only a package of international soft law mechanisms coordinates the states in regards to each state's treatment of the Arctic area."[5] These soft law mechanisms include, but are not limited to, UNCLOS, the Ilulissat Declaration, the Arctic Council, and the newly formed Arctic Coast Guard Forum ("ACGF"). Many other subject-specific treaties are in place between individual countries that regulate fishery conservation, commercial shipping, and management of Arctic waterways, but this paper will focus on the four primary international soft law mechanisms specified above because they are generally applied to the region and provide the greatest insight into the future of Arctic cooperation. UNCLOS is the most comprehensive legal framework governing the world's oceans, and many scholars look to UNCLOS as the path of least resistance to Arctic cooperation.[6] However, there are several problems that arise from this viewpoint that will be addressed in detail below.

1982 United Nations Convention on the Law of the Sea

UNCLOS governs nearly every aspect of maritime law, including sovereignty limits, navigation, seabed mining, and environmental protection of the world's oceans.[7] It also provides a legal framework for resolving ocean-related disputes.[8] On November 16, 1994, the UNCLOS entered into force, but not for the United States, who decided not to ratify the instrument. Despite more than ten years of intense negotiations that culminated in the final Convention, the United States chose not to participate in UNCLOS in the early 1980's because of provisions dealing with deep seabed mineral resources beyond national jurisdiction. After a 1994 agreement that

[4] Kristin Noelle Casper, Student Article, *Oil and Gas Development in the Arctic: Softening of Ice Demands Hardening of International Law*, 49 NAT. RESOURCES J. 825, 835–36 (2009).

[5] *Id.* at 836-37.

[6] *See*, *e.g.*, Mark Jarashow et al., Note, *UNCLOS and the Arctic: The Path of Least Resistance*, 30 FORDHAM INT'L L. J. 1587, 1589 (2007).

[7] United Nations Convention on the Law of the Sea, Dec.10, 1982, 1833 U.N.T.S. 397 [hereinafter U.N. Convention on the Law of the Sea].

[8] *Id.* art. 279–99.

amended parts of UNCLOS dealing with deep seabed mineral resources, the UNCLOS, Annexes and Agreement package was formally submitted to the U.S. Senate on October 7, 1994, for advice and consent to accession and ratification.[9] However, the Senate took no action.

Each of the succeeding administrations, up to and including the Obama Administration, have expressed the desire to ratify UNCLOS.[10] In 2009, President George W. Bush addressed the utility of UNCLOS in the United States Arctic Policy directive,[11] saying "[t]he Senate should act favorably on U.S. accession to [UNCLOS] promptly, to protect and advance U.S. interests, including with respect to the Arctic."[12] Despite decades of executive intent to see the United States join the Convention, the requisite political will has not been there to push ratification.[13] In the interim, the United States has adhered to most UNCLOS provisions anyway; as most of the Convention is customary international law.[14] Specific articles within the Convention, in particular those with national security ramifications, will be discussed in greater detail in Section II.

Ilulissat Declaration: May 28, 2008

The Ilulissat Declaration, adopted by all Arctic states in 2008, is an agreement between the five Arctic states stating the existing legal framework for the Arctic under UNCLOS and other subject specific

[9] *See* U.N. Convention on the Law of the Sea, Oct. 7, 1994, S. Treaty Doc. 103–39 (1994).

[10] John B. Bellinger, *Should the United States Ratify the UN Law of the Sea?* COUNCIL ON FOREIGN RELATIONS (Nov. 11, 2014), http://www.cfr.org/treaties-and-agreements/should-united-states-ratify-un-law-sea/p31828.

[11] *See* Directive on Arctic Region Policy, 45 Weekly Comp. Pres. Doc. 47, 49 (Jan. 9, 2009), http://www.gpoaccess.gov/wcomp/search.html (suggesting that the U.S. Senate act favorably on the U.S. accession to UNCLOS).

[12] *Id.*

[13] Eugene H. Buck, Cong. Research Serv., RL32185, U.N. Convention on the Law of the Sea: Living Resources Provisions (Jan. 18, 2011)., fas.org/sgp/**crs**/row/RL32185.pdf.

[14] *See* Peter A. Buxbaum, *U.S. Administration Pushes UNCLOS*, ISN (Aug. 24, 2007), http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?ots591=4888CAA0-B3DB-1461-98B9-E20E7B9C13D4&lng=en&id=53665 ("US policy since the Reagan administration has held that UNCLOS reflects customary international law and asserted navigational rights based on the treaty's provisions.").

treaties governing the region are adequate, that Arctic nations should seek peaceful resolutions to boundary disputes, and that the Arctic states should not pursue one comprehensive Arctic agreement.[15] Specifically, the Declaration says:

> [T]he law of the sea provides for important rights and obligations concerning the delineation of the outer limits of the continental shelf, the protection of the marine environment, including ice-covered areas, freedom of navigation, marine scientific research, and other uses of the sea. We remain committed to this legal framework and to the orderly settlement of any possible overlapping claims.[16]

Arctic Council

The Arctic Council was established in 1996 as a high level intergovernmental forum for coordination among the Arctic states and indigenous Arctic populations. Its focus has historically been sustainable development and environmental protection. "It is a 'soft law' body that serves an advisory function, but the organization—which includes the United States and Russia as active participants—has successfully raised the profile of Arctic issues and facilitated a science-based, depoliticized approach to developing environmental policy for the region."[17] The Council has worked extensively on Arctic offshore oil and gas activities, maritime shipping, and natural resource protection.[18]

The Arctic Council occupies a critical role in developing policy and best practices for the region. Despite not making "hard law," the Council has made important contributions in developing unity of effort amongst Arctic states. Because of the substantial political obstacles a potential comprehensive Arctic Treaty would have to overcome, the Arctic Council has great potential to play an increasingly important

[15] *Illulissat Declaration*, ARCTIC OCEAN CONFERENCE (May 27–29, 2009), http://www.oceanlaw.org/downloads/arctic/Ilulissat_Declaration.pdf.

[16] *Id.*

[17] Michael A. Becker, *Russia and the Arctic: Opportunities for Engagement Within the Existing Legal Framework*, 25 AM. U. INT'L L. REV. 225, 234 (2010) (citing Oran R. Young, *Whither the Arctic? Conflict or Cooperation in the Circumpolar North*, 45 POLAR REC 73, 79 (2009)).

[18] *Id.* at 234–35.

role in its effort to improve Arctic governance by promoting the harmonization of national laws and regulations, a strategy that may be more effective than the promotion of one comprehensive "Arctic Treaty." At the same time, the Arctic Council can seek to ensure that international institutions in a position to effect widespread reforms, like the International Maritime Organization and other international bodies are "well informed about conditions prevailing in the Arctic."[19]

Practical ways to expand the influence and legitimacy of the Arctic Council are:

> [i]nclusion of more entities [because of the significant impact environmental changes in the Arctic have around the world. Greater inclusion in the Arctic Council would have two main benefits.] First, the expertise of outside entities can contribute to productive responses to environmental challenges. Second, a more widespread consensus on activities and governance in the Arctic will serve to increase the legitimacy of actions taken in the Arctic.[20]

Arctic Coast Guard Forum

The most recent development in the realm of Arctic governance is in the form of the ACGF, which was started in November 2015.[21] The ACGF includes coast guards or similar agencies from Canada, Denmark, Finland, Iceland, Norway, Sweden, Russia, and the United States.[22] The forum complements the Arctic Council, which provides a forum for high-level diplomatic cooperation on Arctic issues, by focusing on operational and national security issues that the Arctic Council is prohibited from discussing.

The ACGF leverages collective resources to coordinate communications, operational plans, and on-the-water activity.[23] In many ways, this new forum is a very practical resource for

[19] *Id.* at 234 (citing Oran R. Young, *Whither the Arctic? Conflict or Cooperation in the Circumpolar North*, 45 POLAR REC. 73, 81 (2009)).

[20] Michael T. Geiselhart, Note, *The Course Forward for Arctic Governance*, 13 WASH. U. GLOBAL STUD. L. REV. 155, 176 (2014).

[21] Ronald A. Labrec, *U.S. Coast Guard Unveils a New Model for Cooperation on Top of the World*, CFR (Nov. 2, 2015), http://blogs.cfr.org/davidson/2015/11/02/u-s-coast-guard-unveils-a-new-model-for-cooperation-on-top-of-the-world/.

[22] *Id.*

[23] *Id.*

coordinating multi-national disaster response and search and rescue effort in the region. Importantly, the forum's emphasis on cooperation promotes United States' desire to keep the region free from conflict, and is a way for the United States and Russia to facilitate constructive Arctic national security discussions that are non-confrontational.

Although the ACGF has been existence for only one month, it represents a promising arena for Arctic-specific national security concerns to be discussed amongst the Arctic states. "Despite concerns with Russian actions in Europe and the Middle East, and the pending claims of Arctic seabed by member nations, the ACGF allows a dialogue with Russia on common issues even while relations are strained elsewhere."[24]

A New Cold War? Russian Arctic Presence

Russian officials have made bold claims about the importance of the Arctic to their nation's future. Recent economic slowdown might be preventing a Russian Arctic from being an immediate threat, however it does not diminish the need for a proactive United States response and policy regarding United States-Russian relations in the Arctic. In the United States, three schools of thought have congealed around Russian relations in the Arctic. First, because of territory disputes and the potential to capture vast natural resources, the Arctic is the battleground of the "Second Cold War," and the likely beginning of the "Race for the Arctic." Second, despite disagreements in other parts of the world, Russia has been a cooperative international partner in the Arctic and reports of tensions between the two powers are overstated. Lastly, though Russia currently poses no threat to the United States in the Arctic, as their economy rebounds and Arctic resources continually become more accessible, a Russian threat in the Arctic will be more tangible.

The Russian Arctic encompasses nearly the entire northern coast of Eurasia and 50% of the total Arctic coastline, includes Russia's strategic nuclear fleet, and accounts for about 20% of Russia's GDP and 22% of its exports.[25] Russia is an Arctic superpower and it perceives its Arctic region as a key development driver of the

[24] *Id.*

[25] Linda Edison Flake, *Russia's Security Intentions in a Melting Arctic*, 6 MIL. & STRATEGIC AFFAIRS 99, 105 (Mar. 2014), http://www.inss.org.il/uploadImages/systemfiles/MASA6-1Eng%20(4)_Flake.pdf.

country in the twenty-first century. Russia's interests in the Arctic have been largely driven by the promise of lucrative hydrocarbon resources beneath the Arctic Ocean, a perception promoted by Russia's state-owned energy giants, as well as by the development of a new Arctic-shipping route, the Northern Sea Route ("NSR").[26]

Despite initial optimism, less than a year after Vladimir Putin returned to the Kremlin following contested Russian parliamentary elections and the largest domestic demonstrations of his tenure, it was apparent that Russia was returning to its historic Soviet course of state-centric Arctic development, including an over-reliance on natural and mineral resources, as well as military modernization and mobilization of its strategic nuclear deterrent.[27] "Russia has substantially revitalized its military mobilization and modernization programs in the Arctic[,]" yet it remains unclear what Russia's actual intentions are in the Arctic.[28]

At President Putin's request in March 2015, the Russian military launched an unannounced exercise that involved more than 45,000 Russian forces, fifteen submarines, and forty-one warships and practiced full combat readiness in the Arctic.[29] Between 2013 and 2014, there was a three-fold increase in air incursions over the Baltic region, the North Sea, and the Atlantic Ocean.[30] Tensions between Russia and NATO aligned countries does not show sign of easing, as a Russian ground attack aircraft was shot down on November 24, 2015 by Turkish forces near the Turkey-Syrian border.[31]

[26] Pavel K. Baev, *Russia's Arctic Aspirations*, ARCTIC SECURITY MATTERS 51 (June 2015), http://www.iss.europa.eu/uploads/media/Report_24_Arctic_matters.pdf.

[27] Atle Staalesen, *Governor: Putin is good for the Arctic*, BARENTS OBSERVER (Mar. 6, 2012), http://barentsobserver.com/en/articles/governor-putin-good-arctic.

[28] Heather A. Conley & Caroline Rohloff, *The New Ice Curtain: Russia's Strategic Reach to the Arctic*, Center for Strategic and International Studies, IX (Aug. 2015), http://csis.org/files/publication/150826_Conley_NewIceCurtain_Web.pdf.

[29] Thomas Grove, *Russia starts nationwide show of force*, REUTERS (Mar. 16, 2015), http://reuters.com/article/2015/03/16/us-russia-military-exercises-idUSKBN0MC0JO20150316.

[30] Ott Ummelas*, NATO Jets Intercept Russian Fighter Plane over Baltic Sea*, BLOOMBERG (Nov. 17, 2014), http://www.bloomberg.com/news/articles/2014-11-17/nato-jets-scrambled-to-intercept-russian-plane-over-baltic-sea.

[31] Caroline Mortimer, *Turkey shoots down Russian plane: Physicists say both official accounts are scientifically impossible*, INDEPENDENT (Nov. 28, 2015), http://www.independent.co.uk/news/science/turkey-shoots-down-russian-plane-astrophysicists-say-both-official-accounts-are-partially-a6752741.html.

However, Russia's military buildup and recent incursions may not be a sign of an imminent aggressive policy change in the Arctic. Over the last few years, Russia's economic development in the Arctic has substantially slowed. Prior to the Russian incursion into Ukraine in 2014, significant natural gas finds had been postponed. In 2014, Transneft, Russia's state-owned pipeline monopoly, announced that it will likely have to delay the launch of two new oil pipelines in Siberia,[32] and other international energy companies have departed the Russian Arctic and postponed their development activities.[33]

Russian nationalistic rhetoric abounds as part of its Arctic narrative. Deputy Prime Minister Dmitry Rogozin, who chairs Russia's new Arctic Commission and who foreshadowed "serious economic collisions in the twenty-first century" in the Arctic, has stated, "[i]t is our territory, it is our shelf, and we'll provide its security. And we will make money there . . . . They [the West] will put us on a sanctions list—but tanks do not need visas."[34] Other outlandish statements from Rogozin include calling the 1867 sale of Alaska by Russia a "betrayal of Russian power status,"[35] and his recent reference to the Arctic as "Russia's Mecca" raises concern over Russia's Arctic intentions.[36] Yet despite this rhetoric and several military training exercises in the Arctic, Russia's actions in the Arctic have thus far been cooperative and comparable to the conduct of other states with a presence in the region. Specifically, on continental shelf

[32] Olesya Astakhova, *Russia's Transneft says sanctions may delay oil pipelines launch*, REUTERS (Sept. 16, 2014), http://www.reuters.com/article/2014/09/16/us-russia-transneft-sanctions-idUSKBN0HB1G520140916.

[33] Mikael Holter, *Exxon, Rosneft Scrap Arctic Deals as Russia Sanctions Bite*, BLOOMBERG (Dec. 1, 2014, 4:22 AM), http://www.bloomberg.com/news/articles/2014-12-01/exxon-rosneft-scrap-arctic-contracts-as-russia-sanctions-bite.

[34] Lucy Clarke-Billings, *Russia begins huge surprise air force drill on same day as NATO starts Arctic training*, INDEPENDENT (May 27, 2015), http://www.independent.co.uk/news/world/russia-begins-huge-surprise-air-force-drill-on-same-day-as-nato-start-arctic-training-10275692.html.

[35] Trude Pettersen, *Controversial politician to head Arctic commission*, BARENTS OBSERVER (Feb. 6, 2015), http://barentsobserver.com/en/security/2015/02/controversial-politican-head-arctic-commission-06-02.

[36] Ishaan Tharoor, *The Arctic is Russia's Mecca, says top Moscow official*, WASH. POST (Apr. 20, 2015), http://www.washingtonpost.com/blogs/worldviews/wp/2015/04/20/the-arctic-is-russias-mecca-says-top-moscow-official/.

issues, environmental, and fishery issues, Russia has thus far been a cooperative partner at the Arctic Council and elsewhere in peacefully resolving disputes.[37]

The aforementioned NSR, which has historically been an emerged national transportation route of the Russian Federation,[38] allows passage from the Atlantic to the Pacific via the shortest route along the Northern coast of Siberia, reducing transport time from China to Europe by at least twelve days compared to the traditional Suez Canal route.[39] Though some scholars say Russia's use of the NSR may run afoul of international law to the extent it continues to impose burdensome requirements on prospective commercial shipping interests, the Northern Sea Route Administration says that navigation of the NSR will be performed according to the commonly accepted principles and norms of the international law, international agreements of the Russian Federation, NSR Russian Federal Law, other Federal Laws, and other regulatory legal documents.[40] Further, "Russia's position on this particular issue is generally consistent with that of Canada, the only other similarly-situated state (and not a state that is frequently associated with lapses in adherence to rule of law principles)."[41] While the NSR is an area for potential dispute, just as elsewhere within the Arctic where Russian rhetoric has been strong but their actions indicate a willingness to cooperate with the international community, this dispute will likely be resolved amicably.

United States Arctic Presence

It is widely accepted as fact that the United States does not have sufficient Naval and Coast Guard assets to operate in the Arctic.[42] Coast Guard officials and others have long warned that the United States government does not have the equipment or infrastructure

[37] *See* Becker, *supra* note 17, at 249–50.

[38] *NSR General Description Area*, NORTHERN SEA ROUTE INFO. OFFICE http://www.arctic-lio.com/nsr_generalareadescription (last visited Jan. 17, 2016) [hereinafter *NSR*].

[39] *Russian PM Orders Plan to Increase Northern Sea Route by 20 Times*, RT.COM (June 9, 2015, 10:47 PM), https://www.rt.com/business/265756-northern-sea-route-medvedev/.

[40] *NSR*, *supra* note 37.

[41] Becker, *supra* note 17**, at 249–50.**

[42] Max Cacas, *Coast Guard Prepares as Arctic Heats Up*, SIGNAL MAGAZINE (June 2012), http://www.afcea.org/content/?q=coast-guard-prepares-arctic-heats.

needed to respond to emergencies, enforce the United States' exclusive economic zone, or achieve other national objectives in a more heavily traversed Arctic.[43] The Coast Guard's Arctic Strategy describes the operational challenges in the region to include vast distances, extreme weather, and limited infrastructure.[44] The closest United States deep-water port to Barrow, Alaska, the main population center, is more than 1100 miles away in Dutch Harbor, and there are only two small commercial airports in the United States Arctic at Barrow and Deadhorse, Alaska.[45] Other challenges include poor radio propagation, partial satellite coverage, geomagnetic interference with navigation equipment, and limited cellular networks.[46]

In a September 2015 visit to Alaska, President Obama noted the need for more assets in the Arctic region and spoke of fast-tracking the construction of a new Coast Guard icebreaker.[47] The White House announcement compared Russia's forty-one current and eleven planned icebreakers to the two operational polar icebreakers of the United States.[48] A 2011 study of Coast Guard ice breaking requirements found the service requires approximately six new icebreakers to meet U.S. needs for polar access.[49]

Additional shortfalls in the areas of command and control and vessel tracking will also limit the ability of the United States to provide maritime safety, security, and environmental protection in the region.[50] The Obama administration's National Strategy for the Arctic Region recognizes this when it states that it will "develop, maintain, and exercise the capacity to execute Federal responsibilities in our

[43] *Id.*

[44] *See* R. J. Paupp Jr., *U.S. Coast Guard Artic Strategy*, U.S. COAST GUARD HEADQUARTERS (May 10, 2013), http://www.uscg.mil/seniorleadership/DOCS/CG_Arctic_Strategy.pdf.

[45] Labrec, *supra* note 21.

[46] U.S. Coast Guard, Arctic Strategy 14 (2013), http://www.uscg.mil/seniorleadership/DOCS/CG_Arctic_Strategy.pdf.

[47] Julie Hirschfeld Davis, *Obama to Call for More Icebreakers in Arctic as U.S. Seeks Foothold*, N.Y. TIMES (Sept. 1, 2015), http://www.nytimes.com/2015/09/02/us/politics/obama-to-call-for-more-icebreakers-in-arctic-as-us-seeks-foothold.html?_r=0.

[48] *Id.*

[49] Stew Magnuson, *Sticker Shock: $1 Billion for New Icebreaker*, NAT'L DEF. MAGAZINE (June 2013), http://www.nationaldefensemagazine.org/archive/2013/June/Pages/StickerShock$1BillionforNewIcebreaker.aspx.

[50] Paupp, *supra* note 44, at 24–25, 31.

Arctic waters, airspace, and coastal regions."[51]

The End of a Cold War Mentality

Despite tensions with Russia in Eastern Europe and Russia's aggressive Arctic rhetoric, there is no emerging "Second Cold War" with Russia. The United States and Russia have cooperated in the Arctic, and the region presents an opportunity for both nations to interact and negotiate in an international forum. The global attention being brought to the region on account of sea ice decline is driving certain scholars and pundits to exaggerate tensions between the Arctic states, particularly the United States and Russia, claiming tensions in the Arctic are heating up.[52] This can likely be somewhat attributed to the average age of Representatives (fifty-seven) and Senators (sixty-two) in Congress, who would be old enough to have been influenced by their parents and media at the height of the Cold War, when Mutually Assured Destruction (MAD) was the prevailing policy between the two ideologically opposed nations.[53]

In addition to Russia's cooperative presence in the Arctic, there are also other significant reasons why there is no looming threat of a second Cold War: "the absence of a global ideological dimension to the conflict; the prevalence of tension in the post-Soviet space versus in other regions; and the much greater relative power of non-Western states (China, India, Brazil and others) that have, so far, refused to take sides."[54] Perhaps most importantly, there is a profound difference in interpersonal relations between the two nations. Russians and Americans enjoy travel privileges between the two nations, are able to interact freely with one another, and most seek to find common ground

[51] *Id.* at 6.

[52] *See, e.g.*, Julia L. Gourley, *Keeping Things Cool in the Arctic*, INST. OF THE NORTH, http://www.institutenorth.org/assets/images/uploads/articles/Keeping_Things_Cool_in_the_Arctic_By_Julia_L._Gourley_United_States_Senior_Arctic_Official_U.S._Department_of_State.pdf.

[53] Jennifer E. Manning, Cong. Research. Serv., R42964, *Members of the 113th Congress: A Profile* 2 (Nov. 24, 2014), www.senate.gov/CRSReports/crs-publish.cfm?pid=&0BL R\C?.

[54] Matthew Rojansky & Rachel S. Salzman, *Debunked: Why There Won't Be Another Cold War*, NAT'L INTEREST (Mar. 20, 2015), http://nationalinterest.org/feature/debunked-why-there-wont-be-another-cold-war-12450.

on issues through mutually respectful dialogue, as noted in both nations participation in forum such as the Arctic Council and ACGF.[55]

The United States and UNCLOS

The United States should not ratify UNCLOS at least until a comprehensive study of its extended continental shelf is completed. And then, should the United States choose to ratify the Convention, there should be no mistaking that it is not to preserve navigation rights or sovereignty claims to our continental shelf. Rather, it would be exclusively for the benefit of cooperation with the international community and any benefits derived therefrom. The main reasons why ratification of UNCLOS is not necessary, at least not at present, is because (1) unlike other treaties the United States is party to, Articles 309 and 310 of UNCLOS expressly forbid a nation to accept some of the provisions of the Convention while excluding others,[56] (2) the United States does not need the Convention to claim our extended continental shelf, nor for boundary dispute settlement purposes as all must abide by customary international law of the sea regardless of accession to UNCLOS, (3) accession would be financially reckless considering the United States does not know the value of the resources of its extended continental shelf that would provide the basis for the amount of royalties required to be paid to the International Seabed Authority under Article 82, and (4) the United States' freedom of navigation rights and law enforcement authority are not protected by UNCLOS; rather UNCLOS puts into writing what is already universally accepted as international law of the sea.[57] Navigation rights of the United States are better protected by the Navy's continued practice of conducting Freedom of Navigation Operations (FONOPS) around the globe.

Most of the arguments for ratification are based on industry or sector-specific concerns. For example, the oil and gas industry would prefer to have all extended continental shelf claims resolved through

[55] *Id.*

[56] U.N. Convention on the Law of the Sea, *supra* note 7, art. 309, 310.

[57] *The Law of the Sea Convention* (Treaty Doc. 103-39) *Before the S. Foreign Relations Comm., 112th Cong.*
(2012) (statement of Steven Groves, Bernard and Barbara Lomas Fellow, The Heritage Found.),
http://www.heritage.org/research/testimony/2012/06/the-law-of-the-sea-convention-treaty-doc-103-39.

UNCLOS so they would not have as much risk exposure when investing in the region.[58] Similarly, the United States Navy and Coast Guard both are concerned about freedom of navigation issues that they feel would be resolved through UNCLOS.[59] While each of these concerns are valid unto themselves, they are not reason enough for lawmakers to ratify the Convention when viewed in totality of UNCLOS and what accession to the Convention would mean for the United States economy, natural resource protection, sovereignty, military power, and national security.

Articles 309 and 310: UNCLOS is an All or Nothing Proposition

A treaty is a compromise between nations. By nature, a party to a treaty gives up something and gains something else in return. As with comprehensive legislation, there are often provisions of a treaty that are uncontroversial and attractive, while other provisions are controversial and divisive. UNCLOS is no exception. "However, unlike most other treaties, the terms of UNCLOS prevent the United States from exempting itself from its more controversial provisions."[60] Specifically, Article 309 states "No reservations or exceptions may be made to this Convention unless expressly permitted by other articles of this Convention,"[61] thereby forbidding the United States to disregard provisions that do not comport with the U.S. Constitution or long-standing U.S. law and policy.[62] Similarly, Article 310 says although states can make statements, inter alia, about the harmonization of their nation's laws with the treaty, they can only do so "provided that such declarations or statements do not purport to exclude or to modify the legal effect of the provisions of this Convention in their application to that State."[63] So, unlike the vast majority of treaties entered into by the United States, UNCLOS expressly forbids any modification or

[58] Holter, *supra* note 33.

[59] U.S. Coast Guard, *supra* note 46, at 27.

[60] Groves, *supra* note 57.

[61] U.N. Convention on the Law of the Sea, *supra* note 7, art. 309.

[62] *United Nations Convention on the Law of the Sea: 103-39, Hearing Before the S. Comm. on Foreign Relations,* 112th Cong, (testimony of Steven Groves, Senior Research Fellow at the Margaret Thatcher Center for Freedom), http://www.heritage.org/research/testimony/2012/06/the-law-of-the-sea-convention-treaty-doc-103-39.

[63] U.N. Convention on the Law of the Sea, *supra* note 7, art. 310.

declaration to only agree to part of the treaty.

Seabed and Extended Continental Shelf Claims

The Arctic is a region with vast natural resources and several coastal nations all in relatively close proximity. It is very natural and probable that there will be disputes over access to these resources and boundary lines. This is no different than many other places on earth, and should not be over-dramatized because of the exotic and distant location of the Arctic. What is important is how the international community chooses to resolve these matters. The United States government has made it clear through the U.S Arctic Policy directive that it encourages the "peaceful resolution of disputes in the Arctic region."[64]

The first step in dispute resolution is for the parties to collect and analyze relevant geographic and geomorphologic data to support their boundary claims. Thereafter, the parties should compare those data and try to resolve any differences through negotiations.[65] If the parties cannot settle the differences through negotiations, there is always the option of resorting to third party dispute settlement. The International Court of Justice has dealt with many such cases,[66] and the International Tribunal for the Law of the Sea ("ITLOS") is now also competent to deal with such matters.[67] Notably, the United States does not have to be party to the Convention to submit a claim to the Tribunal, as the Tribunal is open to States Parties to the Convention (i.e., States and international organizations which are parties to the Convention), and also entities other than States Parties, (i.e., States or inter-governmental organizations which are not parties to the Convention)[68] and to state enterprises and private entities "in any case expressly provided for in Part XI or in any case submitted pursuant to

[64] *See* Directive on Arctic Region Policy, *supra* note 11.

[65] Hans Corell, *The Arctic: An Opportunity to Cooperate and Demonstrate Statesmanship*, 42 VAND. J. TRANSNAT'L L. 1065, 1068 (2009).

[66] *See* Dispute Regarding Navigational and Related Rights (Costa Rica v. Nicar.), Judgment I.C.J. 133 (July 13, 2009), http://www.icj-cij.org/docket/files/133/15321.pdf (addressing a dispute between two countries over navigation rights on the San Juan River).

[67] U.N. Convention on the Law of the Sea, *supra* note 7, annex VI.

[68] *The Tribunal*, INT'L TRIBUNAL FOR THE LAW OF THE SEA, ITLOS, https://www.itlos.org/en/the-tribunal/ (last visited Jan. 17, 2016).

any other agreement conferring jurisdiction on the Tribunal which is accepted by all the parties to that case."[69]

Agreeing to UNCLOS would create a system where the country could influence the litigation of seabed claims. Ratifying UNCLOS would give the United States the "right to nominate and participate in the election of judges to ITLOS . . . as well [sic] the right to add names to the lists from which arbitrators are selected."[70] As the situation currently stands, the United States is the only Arctic coastal state without the ability to directly influence the nomination of judges determining international maritime boundary disputes.[71] The incentive of being able to put judges on the bench is not a valid reason for ratification of the Convention, as any judges nominated by the United States would be expected to be impartial and is bound by law of the sea.

Specific claims to nation's extended continental shelf are submitted to the Commission on the Limits of the Continental Shelf. The continental shelf commission lacks transparency that is troubling. In the specific case of Russia's extended continental shelf claims, other nations are not allowed to review the particulars of Russia's submission to the Commission, nor are they allowed to view the particulars of the Commission's recommendations back to Russia.[72] This lack of transparency makes peer review and oversight over the process difficult, if not impossible. Once Russia acts in accordance with the recommendations of the Commission, Russia's actions are final and binding upon the international community, unless of course it is disregarded by a nation not party to UNCLOS, in which case there would again be no need for ratification as most of these boundary disputes need to be recognized and honored by the disputing parties.[73] Again, this is not to say that a coastal state cannot legally make a claim to extend its rights to its outer continental shelf without first being a party to UNCLOS, because it can do so under customary international

[69] U.N. Convention on the Law of the Sea, *supra* note 7, art. 20.

[70] Angelle C. Smith, Note, *Frozen Assets: Ownership of the Arctic Mineral Rights Must be Resolved to Prevent the Really Cold War*, 41 GEO. WASH. INT'L L. REV. 651, 669 (2010).

[71] *Id.*

[72] J. Trent Warner, *One Small Step for a Submersible, One Giant Land Grab for Russiankind: An Evaluation of Russia's Claim to the North Pole under International Law*, 57 NAVAL L. REV. 49, 86 (2009).

[73] U.N. Convention on the Law of the Sea, *supra* note 7, art. 76(8).

law.[74]

Proponents of ratification say such a claim would lack legitimacy because the criteria for determining the outer limits of the shelf would be arbitrary, unilaterally derived, and driven by self-interest, opening the door to excessive claims the world over.[75] But this potential skepticism and international derision of a sovereign country claiming its extended continental shelf has not, to date, negatively affected the United States. The history of cooperation in the Arctic through bilateral agreements between Arctic coastal states proves the need for ratification is unfounded on these grounds. In the 2008 Ilulissat Declaration, the Arctic coastal states committed to "the orderly settlement of any possible overlapping claims." Russia and Norway have already adhered to this promise by peacefully finalizing their long-unresolved maritime boundary in the Barents Sea in 2010.

The United States recognizes that it is important to settle these boundary issues in order to promote its exercise of sovereign rights over natural resources and living marine species in certain areas, and as "critical to [the] national interests in energy security, resource management, and environmental protection."[76] With this in mind, the United States has historically been able to resolve maritime boundary disputes despite not being a party to UNCLOS. Specifically, the United States had a maritime boundary dispute with Russia in the Bering and Chukchi Seas that primarily dealt with "the boundary created by the 1867 Convention ceding Alaska, and whether it had any bearing upon the Beaufort Sea maritime boundary."[77] This dispute was settled by a 1990 agreement between the two countries where Russia agreed to the United States exercising EEZ jurisdiction within an "'Eastern Special Area' [that] lies more than 200 nm from the baseline of the [United States] but less than 200 nm from the baseline of Russia."[78] While Russia's parliament has not yet ratified the

[74] Thomas H. Heidar, *Legal Aspects of Continental Shelf Limits*, in LEGAL AND SCIENTIFIC ASPECTS OF CONTINENTAL SHELF LIMITS 20 (Myron H. Nordquist, John N. Moore & Thomas H. Heidar eds., 2004).

[75] Warner, *supra* note 68, at 98.

[76] *See* Directive on Arctic Region Policy, *supra* note 11.

[77] DONALD R. ROTHWELL, THE POLAR REGIONS AND THE DEVELOPMENT OF INTERNATIONAL LAW 173 (1996).

[78] *Maritime Jurisdiction and Boundaries in the Arctic Region*, DURHAM UNIV. (Aug. 4, 2015), https://www.dur.ac.uk/resources/ibru/resources/Arcticmap04-08-15.pdf.

agreement, the countries have honored the agreement through diplomatic notes.[79] This is an important example of two countries resolving a boundary dispute without relying on arbitration. Additionally, Canada and United States have joined forces in mapping their possible continental shelves in the Arctic and will likely negotiate a maritime boundary agreement in the future.[80]

If the United States can resolve such disputes without ceding sovereignty to do so to the United Nations, the argument that the Convention should be ratified in order to resolve boundary disputes is weak and unconvincing. Russia and the United States continue to abide by the aforementioned 1990 maritime boundary agreement.[81] Because countries are free to claim their outer continental shelf and come to agreements with other nations on their boundaries without being party to UNCLOS, and can submit claims to ITLOS regardless of whether they are party to the Convention or not, the case for ratification is not supported by the need for seabed and extended continental shelf claim resolution.

Article 82—International Seabed Authority Royalties

If the United States joined the convention, it would be required to transfer royalties generated from oil and gas development on the U.S. continental shelf to the International Seabed Authority for distribution to the "developing world."[82] The Authority is empowered to distribute those funds to developing and landlocked nations, including some that are corrupt, undemocratic, or even state sponsors of terrorism.[83] Article 82 of the Convention says "[t]he coastal State shall make payments or contributions in kind in respect of the exploitation of the non-living resources of the continental shelf beyond 200 nautical miles from the baselines from which the breadth of the

[79] *Id.*

[80] Gourley, *supra* note 52.

[81] Rothwell, *supra* note 77, at 176–77.

[82] Steven Groves, *U.N. Convention on the Law of the Sea Erodes U.S. Sovereignty over U.S. Extended Continental Shelf,* HERITAGE FOUNDATION (June 7, 2011), http://www.heritage.org/Research/Reports/2011/06/UN-Convention-on-the-Law-of-the-Sea-Erodes-US-Sovereignty-over-US-Extended-Continental-Shelf [hereinafter Groves, *Continental Shelf*].

[83] *Id.*

territorial sea is measured."[84] These payments are made annually and on the basis of the value of production from the shelf.

Currently, the United States leases tracts of its extended continental shelf to development companies through the Department of Interior. These companies pay the United States government a rate between twelve and eighteen percent of their production.[85] Should the United States ratify UNCLOS and be required to share royalties with the International Seabed Authority, the government could be ceding over half of the royalties derived from the land, as the International Seabed Authority royalty rate is itself seven percent.[86] This is potentially billions of dollars of revenue to developing countries that could otherwise benefit the taxpayers of the United States. Moreover, the United States government already provides sizable contributions to international aid organizations for programs such as vaccination, schooling, and road building which it considers likely to improve conditions in developing countries. UNCLOS does not do this. Rather, it requires states that are able to extract mineral wealth from the seas to compensate those that are not.[87]

By ratifying UNCLOS, the United States would give up a degree of independence over its extended continental shelf and would be ceding vast sovereignty to the United Nations, while committing the United States to financial tributes to the International Seabed Authority without a clear understanding of the associated costs of doing so. Because no definitive study has been made that calculates the United States' potential extended continental shelf or the value of the resources therein, the commitment to pay a tribute per Article 82 of UNCLOS means giving a blank check to the United Nations. No state or actor with any sense of financial stewardship would agree to the terms of such a deal without first having an extensive survey of the value of the lands to be taxed completed.

Freedom of Navigation and Law Enforcement

In 1993, the Department of Defense issued an Ocean Policy Review Paper on "the currency and adequacy of U.S. oceans policy, from the strategic standpoint, to support the national defense

[84] U.N. Convention on the Law of the Sea, *supra* note 7, art. 82.

[85] Groves*, Continental Shelf*, *supra* note 74.

[86] Jeremy Rabkin, *The Law of the Sea Treaty: A Bad Deal for America*, 3 COMPETITIVE ENTERPRISE INST. 1, 6 (2006), http://www.cei.org/pdf/5352.pdf.

[87] *Id.*

strategy."[88] The paper concluded that despite the United States not being party to UNCLOS, national security interests in the oceans have been protected through the application of customary international law.

Two decades after the Department of Defense policy review was published, there is no evidence that supports accession to UNCLOS as essential to the protection of United States' national security interests. Throughout its history, the United States has successfully protected its maritime interests despite not being an UNCLOS member because enjoyment of the convention's navigational provisions is not restricted to UNCLOS members.[89] Those provisions represent widely accepted customary international law, some of which has been recognized as such for centuries. UNCLOS members and nonmembers alike are bound by the convention's navigational provisions.[90]

The convention's articles on navigation on the high seas (Articles 86–115, generally) and passage through territorial waters (Articles 2–32, generally) were copied almost verbatim from the Convention on the High Seas and the Convention on the Territorial Sea and the Contiguous Zone, both of which were adopted in 1958.[91] The United States is party to both conventions, which like UNCLOS, are considered to be codifications of widely accepted customary international law.[92]

Over time, the consistent practice of states following customary international law indicates that the UNCLOS navigational provisions are almost universally accepted. This view is crystallized in the *Restatement of the Law, Third, of the Foreign Relations Law of the United States*, which says "by express or tacit agreement accompanied by consistent practice, the United States, and states generally, have accepted the substantive provisions of the Convention, other than those addressing deep sea-bed mining, as statements of customary law

[88] Groves, *supra* note 57, at 4.

[89] *Id.* at 5.

[90] *Id.*

[91] Steven Groves, *Accession to the U.N. Convention on the Law of the Sea Is Unnecessary to Secure U.S. Navigational Rights and Freedoms*, HERITAGE FOUNDATION (Aug. 24, 2011), http://www.heritage.org/research/reports/2011/08/accession-to-un-convention-law-of-the-sea-is-unnecessary-to-secure-us-navigational-rights-freedoms.

[92] *Id.*

binding upon them apart from the Convention."[93]

In addition to customary international law established over centuries, the United States relies on the U.S. Freedom of Navigation ("FON") Program to protect those rights and freedoms.[94] The FON Program was instituted to challenge attempts by other nations to "extend their domain of the sea beyond that afforded them by international law."[95]

There are additional unfounded law enforcement and national security related concerns about the United States' failure to ratify UNCLOS. Again, UNCLOS merely codifies existing customary international law on these issues as it does others.

> The Convention's provisions on innocent passage are very similar to Article 14 in the 1958 Convention on the Territorial Sea and the Contiguous Zone, to which the United States is a party . . . A ship does not . . . enjoy the right of innocent passage if, in the case of a submarine, it navigates submerged or if, in the case of any ship, it engages in an act in the territorial sea aimed at collecting information to the prejudice of the defense or security of the coastal State, but such activities are not prohibited by the Convention. In this respect, the Convention makes no change in the situation that has existed for many years and under which we operate today.[96]

Referring to Articles 92 and 110 of the Convention, opponents argue that the treaty does not explicitly guarantee a right to board or interdict when evidence of terrorist intentions through WMD is involved.[97] However, as with the freedom of navigation provisions,

[93] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES 5 (AM. LAW INST. 1987).

[94] Grove, *supra* note 29 (citing J. ASHLEY ROACH & ROBERT W. SMITH, UNITED STATES RESPONSES TO EXCESSIVE MARITIME CLAIMS 6 (2d ed.1996)).

[95] Groves, *supra* note 91.

[96] *Accession to the 1982 Law of the Sea Convention and Ratification of the 1994 Agreement Amending Part XI of the Law of the Sea Convention, Hearing Before the S. Comm. on Armed Services*, 108th Cong. (testimony of William Taft).

[97] Marjorie Ann Browne, Cong. Research. Serv., *The U.N. Law of the Sea Convention and the United States: Developments Since October 2003*, at 5 (June 3, 2005), http://issuu.com/forgenerations/docs/unlawofconventions.

despite opponents of ratification being misinformed over existing customary international law, UNCLOS does not protect or solidify any law enforcement rights that are not pre-existing without accession to UNCLOS.

To board and interdict vessels from other countries, either with the consent of the vessel's flag state, or upon the high seas if the vessel is assimilated to be "stateless," are rights enjoyed by all maritime nations whether a party to UNCLOS or not. Testimony from the legal advisor to the Senate Armed Services Committee, though in favor of ratification of UCNLOS, supports the notion that UNCLOS provides the same sovereignty protections for the interdiction and boarding of vessels at sea in the Arctic, just as it does elsewhere. Specifically, he said:

> [T]he Convention recognizes numerous legal bases for taking enforcement action against vessels and aircraft suspected of engaging in proliferation of weapons of mass destruction, for example, exclusive port and coastal State jurisdiction in internal waters and national air space; coastal State jurisdiction in the territorial sea and contiguous zone; exclusive flag State jurisdiction over vessels on the high seas (which the flag State may, either by general agreement in advance or approval in response to a specific request, waive in favor of other States); and universal jurisdiction over stateless vessels. Further, nothing in the Convention impairs the inherent right of individual or collective self-defense (a point which is reaffirmed in the proposed Resolution of Advice and Consent).[98]

His points are well made, however they lead to the contrary conclusion that ratification of UNCLOS does not grant the United States enjoyment of rights not already existing under customary international law.

Accession to UNCLOS simply does not provide any additional protections or benefits to the United States as related to freedom of navigation or law enforcement. Despite the steadfast support of the Navy[99] and Coast Guard[100] for accession to the Convention to

[98] *Id.*

[99] *The Convention on the Law of the Sea*, U.S. NAVY JUDGE ADVOCATE CORPS, http://www.jag.navy.mil/organization/code_10_law_of_the_sea.htm (last visited Jan. 18, 2016).

"preserve" freedom of navigation rights, there is no evidence that indicates accession to the Convention as necessary for such preservation of rights.

CONCLUSION

UNCLOS, along with a wide array of international agreements and organizations, provides the legal framework for the Arctic. While ratification of UNCLOS has peripheral benefits associated with inclusion in an international Convention, there are too many compelling reasons why ratification by the United States is not necessary or prudent when considering the national security interests of the United States. With regards to Russia, ratification of UNCLOS is unnecessary as Russian actions in the region have been aggressive, but cooperative, and fully within customary international law. Ratification of UNCLOS does not guarantee that any state, Russia, the United States, or any other, will always conduct itself in a manner that lives up to international standards.[101] Because of this, the Arctic region should not be considered a battleground for future conflict. Rather, the Arctic should serve as a catalyst and a stepping-stone for greater cooperation and partnership with the Russian government and international community.

While UNCLOS "crystallizes" existing customary international law, no rights the United States enjoys regarding Law of the Sea are granted by ratifying the Convention. UNCLOS does, however, provide a universally recognized baseline to reference when dealing with any maritime issues, Arctic or otherwise. As discussed at length above, many of these issues, from freedom of navigation to the resolution of maritime boundary disputes, are quintessential law of the sea issues to which international policymakers bring a wealth of experience.[102]

It is important, however, that the United States does not get left behind other Arctic states in capability and development of the Arctic region, as the region is ripe with opportunities and resources. In order to bring about the necessary action and achieve results, it is imperative that matters relating to the Arctic be addressed at the highest political level. Rather than taking the "path of least resistance" to Arctic governance, which is ratification of UNCLOS, specific

[100] *U.S. Coast Guard Arctic Strategy*, U.S. COAST GUARD (May, 2013), http://www.uscg.mil/seniorleadership/DOCS/CG_Arctic_Strategy.pdf.

[101] Becker, *supra* note 17, at 235.

[102] *Id.* at 235–36.

actions the United States should take include: (1) continued emphasis and expansion of the Arctic Council, which will keep the United States' environmental and natural resource interests in the forefront of international deliberations, (2) continued United States leadership and participation in the recently founded Arctic Coast Guard Forum, which is designed to address national security interests of the Arctic states that cannot be discussed through the Arctic Council, and (3) continued investment in Arctic capable assets that will enable the United States to safeguard oil and gas investments in the region, provide search and rescue capabilities to handle the expected increase in shipping through the NSR and other areas, and most importantly to continue our practice of conducting FONOPS worldwide.

Arbitrary Actions or Certain Arbitration

Patrick Stewart

Introduction

United States companies are under constant attack from cybercriminals around the world. These cybercriminals run the gamut in sophistication from some kid in his parents' basement, to very sophisticated criminal organizations, to nation states. Attacks can range from Distributed Denial of Service ("DDOS") attacks, theft of customer information, to theft of intellectual property ("IP"). While theft of customer information often makes the headlines, companies can suffer devastating losses due to the theft of their IP. Current estimates put the losses of U.S. companies, due to cyber IP theft, at nearly 100 billion USD annually.[1]

The theft of IP by nation states is, in many ways, similar to the expropriation of companies' foreign investments. In both cases, companies invest millions of dollars into developing the capacity to generate profit, whether through a factory in a foreign state or in a research and development lab on the West Coast. In both cases, when the asset is taken, the ability of the company to profit is diminished or destroyed, and there is a substantial deprivation of value with regards to the asset.

International regimes have been put in place to prevent or mitigate the expropriation of foreign investments around the world. Bilateral Investment Treaties ("BITs") and multinational trade agreements have established forums where wronged investors can take expropriating states to arbitration and recover damages. Historically, the ability of a state to steal the asset of a foreign company was limited to the geographic confines of that state. However, with the ever spreading connectivity of the internet, it is now possible for a state to

[1] *See* Net Losses: Estimating the Global Cost of Cybercrime, CTR. FOR STRATEGIC AND INT'L STUDIES 2 (June 2014); Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Cost $445 Billion Annually*, WASH. POST (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

steal the crown jewels of a company from half the world away through a cyber attack that steals their IP.

While sanctions may be an attractive option for dealing with this problem, sanctions do little, if anything, for the victim of the cybertheft. Therefore, an arbitration regime should be established to allow victim companies to recover the costs of cybercrime directly from the state.[2] These arbitrations could be modeled on those of investor-state arbitrations conducted through the International center for Settlement of Investment Disputes ("ICSID"), the Iran-United States Claims Tribunal, or other arbitration institution. The victim would benefit because they would receive compensation for the loss, and the offending state would agree to arbitration to avoid being subject to sanctions that could ultimately be more costly than the damages awarded by a tribunal.

This paper will begin by providing a brief overview of the some of the problems the United States and companies face when trying to grapple with the problem of cybercrime. Next, the paper will provide a short analysis of the current legal remedies available to victims of state-sponsored cyberattacks. The paper will then describe the system of investor-state arbitration, followed by how the proposed arbitrations system would be conducted. Finally the paper will address possible critiques of the proposal.

The Problem

Stewart Baker—former Assistant Secretary of Policy at the Department of Homeland Security ("DHS") and former General Counsel at the National Security Agency ("NSA")—recently explained the absurdity of the current posture toward cybercrime, by comparing it to how we keep our streets safe.[3] Mr. Baker said that currently, to keep people safe in cyberspace, we ask them to install defenses and pay money every year or every few months to update

[2] This paper will assume that the technology exists to accurately and in a cost effective manner, attribute cybertheft. The government has historically shown its ability to attribute certain cyberattacks. Additionally, even if attribution capabilities are only in their infancy, their capabilities will only improve, allowing this arbitration framework to be used more extensively in the future.

[3] Stewart Baker, Partner at Steptoe & Johnson, ABA Standing Committee on Law and National Security Breakfast Program: Sanctions as a Tool to Combat Cyber Espionage (Dec. 4, 2015).

those defenses to keep them from becoming obsolete.[4] Mr. Baker said that this is analogous to the police chief telling citizens that they will be safe on the streets as long as they wear body armor and buy the body armor upgrades every year.[5] As Mr. Baker rightly noted, such a police chief would not last one day on the job; the police chief must go after criminals, not just instruct citizens on how to protect themselves.[6] In the same way, something must be done to go after state-sponsored cyberthugs.

Those addressing this difficult problem generally approach it from any of three angles: better security, deterrence of attacks, and mitigation of the consequences. Unfortunately there is no way to perfectly secure a company in the cyber domain and, as Mr. Baker said, the onus of security should not be entirely on individuals.[7] Even if there were such a security solution, human error would almost certainly be the chink in the mail that would allow the attackers to penetrate. It is also equally unrealistic to think that companies will go offline or to that attackers will decide, on their own, that stealing is wrong. Mitigation of the consequences of a cyberattack can often be difficult, as it takes on average 229 days to detect a cyberattack,[8] and it is unlikely that the average cybercriminal could begin to repay the damage caused to companies by their attacks.

To go after cyberthugs, we need to be focusing on the second two angles. Individuals may be deterred by stepped-up prosecutions and the prospect of lengthy prison sentences and steep civil penalties and damages awards. Mitigation of consequences may be achieved through insurance, or perhaps even recovering the stolen data. However, companies may not be able to fully mitigate the consequences, and what are lengthy prison sentences to a sovereign state? To deter states from engaging in cyberattacks,[9] the United States must develop and implement adequate deterrent measures.

In fact, this year the United States began doing just that. After the government attributed the cyberattack on Sony Pictures

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] Jeffrey Roman, *Speeding up Breach Detection*, BANK INFO SEC. (Nov. 25, 2014), http://www.bankinfosecurity.com/speeding-up-breach-detection-a-7604/op-1.

[9] In the context of this proposed policy, "cyberattack" means generally what is covered in Executive Order 13,694. This is not a policy meant to curb good old fashioned espionage, but to curb and mitigate the effects of economic espionage and cyberattacks that damage and disadvantage U.S. companies.

Entertainment to North Korea, sanctions were imposed on ten "North Korean officials and three government agencies."[10] Then, on April 1, 2015, President Obama "signed an executive order establishing the first sanctions program to allow the administration to impose penalties on individuals overseas who engage in destructive attacks or commercial espionage in cyberspace."[11] James A. Lewis—Senior Fellow at the Center for Strategic and International Studies—views the new sanctions program as promising, and as a means of combating economic espionage, particularly from China.[12]

But if the goal was to also mitigate cyberattacks and not merely deter them through the imposition of costs, a different approach is needed. While civil suits against individual cybercriminals may not yield much in the way of mitigating the losses of victims, states on the other hand can almost certainly afford to pay. In the world of investor-state arbitration, the *Chorzow Factory* case established the international standard for awards for illegal acts: "that reparation must, as far as possible, wipe out all the consequences of the illegal act and reestablish the situation which would, in all probability, have existed if the act had not been committed."[13] The same approach should be taken when dealing with state-sponsored cyberattacks.

Current Legal Remedies

Companies that are victims of state-sponsored cyber attacks have limited legal remedies. Though the Economic Espionage Act of 1996 makes it a crime to engage or conspire to engage in economic espionage against U.S. companies, the statute provides no private right

[10] Carol Morello & Greg Miller, *U.S. Imposes Sanctions on N. Korea Following Attack on Sony*, WASH. POST, (Jan. 2, 2015) (noting however that "[n]one of the individuals sanctioned . . . is believed to have been directly involved in the hack into Sony.").

[11] Ellen Nakashima, *U.S. Establishes Sanctions Program to Combat Cyberattacks, Cyberspying*, WASH. POST, (Apr. 2, 2015), https://www.washingtonpost.com/world/national-security/us-to-establish-sanctions-program-to-combat-cyberattacks-cyberspying/2015/03/31/7f563474-d7dc-11e4-ba28-f2a685dc7f89_story.html; Executive Order 13,694, 80 Fed. Reg. 18077, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Apr. 1, 2015).

[12] Nakashima, *supra* note 11.

[13] The Factory at Chorzow, Judgment, 1928 P.C.I.J. (ser. A) No. 17, at 89 (Sept. 13).

of action.[14] There are other possible legal remedies but it is not clear that these remedies would be satisfactory to either the United States or the victims themselves.

The Computer Fraud and Abuse Act,[15] and the Wiretap Act,[16] each provide a private right of action to victims of specified cybercrimes. Additionally there are common law torts of trespass and invasion of privacy that would likely apply to the compromise of a company's computer networks.[17] Despite the plethora of cyber attacks on companies by state actors, and the relevant statutes and common law remedies, "no electronic privacy suit has been brought successfully against a foreign sovereign."[18]

The lack of successful suits is likely the result of a combination of three factors. The first relates to the Foreign Sovereign Immunities Act ("FSIA").[19] The second relates to the difficulty of producing evidence attributing the cyberattack to the offending state, beyond the preponderance of the evidence. And finally, the fear of retaliation by the offending state. The first two factors will be addressed here, while the third will be addressed below.

As one scholar has noted, it has been "assumed that foreign governments and their hackers are beyond the reach of American law," and that "sovereign immunity shields foreign states from civil suits for cyberattacks."[20] Generally speaking, the FSIA does shield foreign states from suit in U.S. courts; however, there is an exception for tortious acts or omissions.[21] The number of "tort exception cases involving statutory violations are surprisingly few," and "[n]o court has squarely addressed the issue" of whether the tort exception applies to statutory torts.[22] There is at least one scholar who argues that this exception is intended to include such torts, and that the FSIA does not prohibit suits brought by U.S. companies against foreign states for

[14] *See* Eleanor T. Phillips et. al., *Intellectual Property Crimes*, 52 AM. CRIM. L. REV. 1289, 1292 (2015) (citing Economic Espionage Act of 1996, U.S.C. §§ 1831–1839 (2012)).

[15] 18 U.S.C. § 1030(g) 2012).

[16] 18 U.S.C. § 2520(a) (2012).

[17] *See* Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COLUM. HUMAN RIGHTS. L. REV. 227, 239–41 (2015).

[18] *Id.* at 232.

[19] 28 U.S.C. §§ 1602–11 (2012).

[20] Gilmore, *supra* note 17, at 232.

[21] 28 U.S.C. §1605(a)(5).

[22] Gilmore, *supra* note 17, at 259.

state-sponsored cyberattacks.[23] Nonetheless, this is an unproven area of the law and a company's ability to prevail in such a suit is far from clear.

The second difficulty in bringing cases against foreign states for cyberattacks is the difficulty in producing evidence. In the first instance, the techniques used to definitively prove the origin of the cyberattack may themselves violate U.S. law, exposing the company to civil and criminal liability, as well as tainting the evidence.[24] Many times, the U.S. government is able to utilize its capabilities and identify the actor behind a particular cyberattack, as in the case of the Sony attack, or the indictment of the five Chinese PLA officers.[25] However, the U.S. government would likely rebuff any calls for it to turn over the "proof" that the alleged state was in fact involved in the attack and the methods and processes by which that proof was obtained. There is a big difference between the government merely stating that China was behind a particular attack, and revealing its sources and methods for how it was able to develop the causal chain between the attack and China. Without the government's assistance, and without risking violating the laws themselves, companies will have serious impediments to establishing evidence connecting the state to the attack.

These challenges do not necessarily foreclose the possibility of a company bringing a suit against a state. However, due to the uncertainty of the law and the difficulties associated with establishing the necessary evidence, current legal avenues do not appear promising. Companies need an alternative means of recouping losses due to state-sponsored cyberattacks.

Additionally, victim-initiated suits may not be successful in achieving the government's policy goals. The government has shown a willingness and desire to impose financial costs on states that commit cyberattacks against U.S. companies.[26] While this goal may be achieved if an award is granted to the victim, the government would be in a precarious position if the verdict was for the defendant state. The

[23] *See id.* at 259–67.

[24] *See* Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, Note, 82 GEO. WASH. L. REV. 1229, 1246–49 (2014).

[25] *See* Morello, *supra* note 10; Ellen Nakashima & William Wan, *U.S. Announces First Charges Against Foreign Country in Connection with Cyberspying*, WASH. POST, (May 19, 2014), https://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

[26] *See* Morello, *supra* note 10; Executive Order 13,694, *supra* note 11.

government would be in the position of having to decide whether to impose sanctions against the state it knows (through classified means) is guilty, despite the court verdict for the state, or to capitulate and withhold sanctions. Additionally, even if the victim received what it and the government viewed as a just award, the appeals process could take years, delaying the impact of the eventual award.

Investor-State Arbitration

Since the late 1990s and early 2000s, investor-state arbitrations have become increasingly common.[27] Unlike a suit filed in court, the fundamental principle underlying arbitration is the consent of *both* parties.[28] Investor-state arbitration provisions are contained in many BITs, and the first investor-state arbitration under a BIT occurred in 1987.[29] Additionally, the Iran-United States Claims Tribunal, established in 1981, has resolved over 3900 cases, most of which involved "claims by nationals of one State Party against the other State Party . . . ."[30]

Generally, in investor-state arbitrations, states manifest their consent to arbitrate in a BIT or other investment treaty. Consent can also be manifested in contracts, or even by agreement after the dispute has occurred. The non-state investor manifests consent to arbitrate either by contract or, more commonly, by submitting an arbitration claim.

Arbitration agreements allow the parties to customize the process at the outset. Arbitration agreements will establish what type of disputes will be subject to arbitration, the rules that will govern the arbitration such as ICSID,[31] UNCITRAL,[32] or SCC,[33] whether the

[27] *See* United Nations Conference on Trade and Development, http://unctad.org/en/Pages/DIAE/ISDS.aspx (last visited Dec. 7, 2015).

[28] *See* ANDREA M. STEINGRUBER, CONSENT IN INTERNATIONAL ARBITRATION 5.54 (Oxford University Press 2012).

[29] *See Asian Agricultural Products Ltd v. Sri Lanka*, (registered in 1987) ICSID Case No ARB/87/3; Sachet Singh & Sooraj Sharma, *Investor-State Dispute Settlement Mechanism: The Quest for a Workable Roadmap*, 76 UTRECHT J. OF INT'L & EUR. L. 88, 90 (2013) (noting that "prior to this most of the investment disputes that [were] referred to the international tribunals were either brought in pursuance to contractual agreements by the private parties or were State-to-State arbitrations.").

[30] Iran-United States Claims Tribunal, http://www.iusct.net (last visited Dec. 7, 2015).

[31] International Centre for Settlement of Investment Disputes. *ICSID convention, regulations and rules*. International Centre for Settlement of Investment Disputes (2003),

arbitration will be administered by an institution or whether it will be ad hoc, where the arbitration will take place, and so on. The parties can also stipulate the law that will be applied to the dispute. This customizability allows parties to have more certainty and control over the process and its costs.

Arbitration tribunals can consist of a sole arbitrator agreed to either by both parties or by any other odd number of arbitrators.[34] Often tribunals consist of three arbitrators, one appointed by each party, and a third, the presiding arbitrator, selected by the two party-appointed arbitrators.[35] Under ICSID Rules, the parties can challenge the appointment of an arbitrator on the grounds that the arbitrator manifestly lacks independent judgment.[36] If an arbitrator is found to lack such qualities, the arbitrator is removed and replaced.[37] Other arbitration institutions have similar processes for determining whether an arbitrator is impartial, and if so found, how to replace them.[38]

Awards of ICSID tribunals and the Iran-United States Claims Tribunal are final.[39] Awards may not be appealed and parties may not attempt to have them set aside.[40] The award is enforceable in any state in the case of Iran-United States Claims Tribunal cases, and in any

https://icsid.worldbank.org/ICSID/StaticFiles/basicdoc/CRR_English-final.pdf [hereinafter, ICSID Rules].

[32] U.N. Commission on International Trade Law, Arbitration Rules, *UNCITRAL Rules on Transparency in Treaty-based Investor-State Arbitration*, (2013), https://www.uncitral.org/pdf/english/texts/arbitration/rules-on-transparency/Rules-on-Transparency-E.pdf [hereinafter UNCITRAL Rules].

[33] Arbitration Institute of the Stockholm Chamber of Commerce, *Arbitration Rules* (2010), http://sccinstitute.com/media/40120/arbitrationrules_eng_webbversion.pdf [hereinafter SCC Rules].

[34] ICSID Rules, *supra* note 31, at art. 37.

[35] *See id.* Note that the Iran-United States Claims Tribunal consists of nine arbitrators, three Americans, three Iranians, and three neutrals agreed upon by the State Parties. *See* Declaration of the Government of the Democratic and Popular Republic of Algeria Concerning the Settlement of Claims by the Government of the United States of America and the Government of the Islamic Republic of Iran (Iran-US Claims Rules), art. II (Jan. 19, 1981).

[36] ICSID Rules, *supra* note 31, at arts. 14, 57.

[37] *Id.* at art. 5, Appendix.

[38] *See, e.g.*, UNCITRAL Rules, *supra* note 32, at art. 14; SCC Rules, *supra* note 33, at arts. 15–17.

[39] ICSID Rules, *supra* note 31, at art. 54; Iran-US Claims Rules, *supra* note 35, at art. 4.

[40] ICSID Rules, *supra* note 31, at arts. 54–55; Iran-US Claims Rules, *supra* note 35, at art. 4.

signatory state in the case of ICSID arbitrations.[41] In such states, the award is to be viewed as if it was a final decision from that state's highest court.[42] Arbitration is thus very appealing to investors because there is little threat that an award will be postponed by lengthy appeals and the award can be enforced in various states without the threat of it being set aside.

Additionally, investor-state arbitration can help de-politicizing disputes. In the absence of investor-state arbitration, confrontations regarding investment disputes generally occurred at the state-to-state level.[43] By allowing the disputes to be handled at the investor-state level, as opposed to the state-state level, the disputes were removed from the realm of power politics which has helped create diplomatic stability.[44]

Arbitrating Damages from Cybertheft

The United States should make it a policy to offer states, against whom sanctions relating to a cyberattack are going to be issued, the opportunity to avoid (or mitigate) sanctions by agreeing to arbitrate over damages with the injured party. Such a policy would allow the United States to punish the offending state, while at the same time allowing to the injured party to recoup some, or hopefully all, of their losses. Additionally, calculating the costs inflicted by a particular sanction is an imperfect science and it is quite possible that sanctions will inflict more or less damage on the offending state than the victim suffered. Submitting disputes to arbitration would give both the United States and the offending state certainty as to the outcome. Importantly, this policy would only be applied to destructive cyberattacks or cybertheft that amount to economic espionage. Stealing weapon designs or security clearance documents through cyberattacks should generally *not* be included because that is just "good old fashioned cyber-enabled espionage," a craft in which the

[41] ICSID Rules, *supra* note 31, at art. 55; Iran-US Claims Rules, *supra* note 35, at art. 4.

[42] ICSID Rules, *supra* note 31, at art. 55; Iran–US Claims Rules, *supra* note 35, at art. 4.

[43] *See* Julia Hueckel, *Rebalancing Legitimacy and Sovereignty in International Investment Agreements*, 61 EMORY L.J. 601, 640 (2012).

[44] *See* Sergio Puig, *Emergence & Dynamism in International Organizations: ICSID, Investor-State Arbitration & International Investment Law*, 44 GEO. J. INT'L L. 531–550 (2013).

United States frequently engages.[45] There are easy distinctions between stealing the designs for the F-35 and the designs for the Apple Watch. The distinction would seem to break down with more dual use technologies such as GPS or advanced alloys. While these policy distinctions would be important, they are almost certainly already being made. In order to effectively implement the sanctions program unveiled by the President in April, the administration must be deciding which types of cyberattacks qualify for sanctions, and which are just good old fashioned espionage.[46] Therefore, achieving policy goals through arbitration as opposed to sanctions would not affect the difficult decision of determining which cyberattacks qualify for sanctions or arbitration, and which do not.

Unlike in investor-state arbitration where it is necessary to prove expropriation or other violation of a treaty, in the proposed arbitrations, the injured party would need only prove damages. Though this may at first seem unfair to the offending state, the purpose of the arbitration is not to determine culpability or wrongdoing. Such a process would have been completed by Treasury's Office of Foreign Asset Control ("OFAC") during its consideration of whether to impose sanctions in the first place; OFAC's determination would serve as res judicata. During the OFAC process, the offending state may even have had the opportunity to advocate in its own defense with regards to the matter. Therefore, the sole purpose of the arbitration would be to determine the appropriate damages award.

Such an agreement would not need to serve as an admission of guilt or culpability on the part of the offending state. The arbitration could stipulate as much and the arbitration tribunal could take as stipulated, for the purposes of the arbitration, that the offending state had committed the alleged cyberattack. Because there would be no need to establish attribution or veracity of the evidence (as that stage would have taken place during the OFAC review), there would be no concerns on the part of the United States of needing to share sources and methods or other classified documents.[47]

[45] Ankit Panda, *US CIA's Operations in China Take a Step Back in Wake of OPM Breach*, DIPLOMAT, (Oct. 1, 2015), http://thediplomat.com/2015/10/us-cias-operations-in-china-take-a-step-back-in-wake-of-opm-breach/.

[46] *See* Executive Order 13,694, *supra* note 11; Nakashima, *supra* note 11.

[47] Because the arbitration will be about the cost of the cybercrime, it is likely that most, if not all of the relevant information will lie with the victim itself as opposed to the government. Additionally, merely stating that the government knows that it was State A that breached the victim hardly seems like disclosing sources and methods, especially if similar information would have been made public is the U.S.

The United States would be able to set the parameters of the arbitration. Unlike in investment treaties where the United States must make concessions and engage in a give-and-take, here the United States would have nearly all of the bargaining power. The position of the United States would effectively be that the offending state (or parts thereof) have been found culpable of committing cyberattacks against U.S. companies and therefore the United States is using its authorities to impose costs. Traditionally, these costs would be imposed via sanctions; however, if the offending state and the victim agree, the costs will be determined through arbitration and awarded directly to the victim. In both instances, the goals of the United States are met. Therefore, the offending state would have little to bring to the negotiating table and would have limited bargaining power to set the terms of the arbitration.

The terms of the arbitration agreement could be standardized, or could be customized on an ad hoc basis. The United States would be able to establish what was to be considered when determining the award, such as research and development costs, value of material stolen, damage caused (including to the victim's reputation), and so on. If the United States determined that costs alone will likely be insufficient to achieve its policy goals, the tribunal could be instructed to consider punitive damages as well. Due to the nature of arbitrations, they could be customized in any fashion deemed appropriate.

As with investor-state arbitrations, these arbitrations may have the effect of depoliticizing these disputes. While one of the goals of the policy would be to reduce the number of state-sponsored cyberattacks, it may also make it easier to address the ones that occur. Smaller scale attacks that may not have risen to the level of warranting sanctions could be resolved in such arbitration; and if the offending state refuses, the refusal could provide additional justification for sanctions, or perhaps even for elevated sanctions.

The arbitration agreements should establish ad hoc tribunals. There would be no need for a standing arbitration tribunal as the total number of cases is likely to be very low.[48] Additionally, establishing a standing body can work when the states involved are known *ex ante*; however, in the cases envisioned by this policy, while there may be the

Government had pursued sanctions (or at the least inferences would have been possible).

[48] The Iran-United States Claims Tribunal is a standing tribunal, however it has heard nearly 4,000 cases, many more than would likely be pursued under this policy. *See* Iran-United States Claims Tribunal, *supra* note 30.

usual suspects, the offending state would not be known until after an attack.

This policy would have the additional benefit of adding legitimacy to punishments imposed for state-sponsored cyberattacks. While a state would still be free to protest and maintain its innocence, it would be hard for the state to argue that the punishment was unreasonable. Both sides would be able to present evidence relating to valuation, and the final award would provide certainty to the offending party as to how much they will pay.[49] Additionally, having a tribunal determine damages may provide a measure of transparency to the process of punishing states.

Critiques

There may be those who question such a policy. For one, they may ask why a state would ever agree to arbitrate in such a manner. Others may ask whether it would not be better to enter into bilateral or multilateral treaties, as opposed to ad hoc agreements. Additional concerns may include a scenario where an award is smaller than the United States had hoped for, and whether such a policy can satisfy U.S. policy goals. Finally, there is the concern mentioned above, the company's fear of retaliation from the offending state.

As stated supra, the President has already established a sanctions regime to be employed against states engaging in cyberattacks against U.S. companies.[50] While the United States and its allies are getting ever better at targeting sanctions, sanctions are still rather blunt instruments. The imposition of such sanctions would have serious repercussions that would likely be incalculable (at the outset) for the targeted state. In contrast, under the proposed system, the damage caused by the attack would be determined by the tribunal and the offending state would have certainty as to how much it would pay. This is in stark contrast to sanctions, the effects and duration of which are uncertain and may be enticing to the offending state.

The question may arise of why not enter into formal treaties as opposed to ad hoc agreements. It is unlikely that such treaties would be desirable or successful. As stated earlier, bilateral treaties may be insufficient because it is unknown if the next cyberattack will come from China or from France. Relatedly, even if the government were to

[49] This is as opposed to sanctions where the costs can be impossible to judge at the outset.

[50] *See* Executive Order 13,694, *supra* note 11.

develop a list of "usual suspects" and pursues treaties with them, it may strain relations with those states to essentially say, "we have no faith that you will respect fair play and not steal from our companies to unfairly advantage your own." The only treaty based solution must be a nearly universally adopted agreement. However, it is unclear why the United States, or any other state, would expend political capital to pursue such an agreement. These arbitrations merely allow the United States to achieve its policy goals, while at the same time benefiting the victim; they do not provide the government meaningfully new tools for imposing costs against offending states. Therefore, ad hoc tribunals are a more reasonable solution.

Of real concern would be the scenario where an award is smaller than the United States had hoped for, and the question arises whether such awards can satisfy U.S. policy goals. Some of this concern could be alleviated at the outset by the United States establishing the terms of the arbitration.[51] Even still, unsatisfactory awards may arise. Though less than hoped for, the United States could take the view that arbitration awards are due immediately and therefore placing immediate pressure on the offending state, as opposed to having to wait for the effects of sanctions to have a similar impact.

If the United States was still unsatisfied, they could always resort to imposing sanctions or other diplomatic action. The United States could take the position at the outset that they reserve the sovereign right to impose sanctions even after an award has been paid; however the sanctions would not be implemented until after the award, and the good faith effort on the part of the offending state to arbitrate could be taken into considerations when determining the sanctions.[52] Imposing such sanctions may mean the de facto end of any future arbitration, but the arbitrations should not impact the ability of the United States to exercise its sovereign powers to achieve its policy goals.

Finally, there is the concern about companies fearing to engage in such arbitration for fear of retaliation by the offending state. This is a real concern, but perpetual cowering is not an option; companies need to stand up and assert their rights. And companies would not be going it alone; the United States government would be standing behind them,

[51] However, it would be a delicate balance of crafting terms that would be most likely to satisfy policy goals, while at the same time not completely predetermining the outcome such that the offending state would be dissuaded from arbitrating.

[52] Or in the event that the offending state exhibits bad faith.

ready to levy sanctions or exert other diplomatic pressure should the need arise.

Conclusion

Companies face many threats in the cyber realm, and the limited options in responding to those threats is troubling. While states may nominally commit to not engaging in harmful cyberattacks, the threat of such attacks is always looming. The United States has taken steps to establish consequences for these cyberattacks, but these solutions do nothing to make the victims whole. By adopting a policy of arbitration as a remedy in the first instance, the United States has the opportunity to meet its policy objectives, benefit the victim company, and perhaps provide transparency and added legitimacy to the practice of punishing sovereign states for their illegal acts.

Good For Now, But Not For Later: An Exploration of the Tallinn Manual as an Appropriate Temporary Solution and an Ineffective Permanent Solution to the Lack of International Legal Guidance Existing in the Cyberspace Domain

MIDN Erin N. DeVivies & MIDN Michael G. Harding

Introduction

The Tallinn Manual is a non-binding academic study commissioned by the NATO Cooperative Cyber Defense Center of Excellence ("NATO CCD COE") of how current international laws and treaties apply to cyber warfare. It was written between 2009 and 2012 in response to the 2007 cyber-attacks on the nation of Estonia. The result of the three year, three-hundred-page study was a well thought out set of ninety-five rules which relates regulation in cyberspace to jus ad bellum (right to wage war) and jus in bello (law of war) issues, and addresses some aspects of the omnipresent question of when and how much activity in cyberspace is appropriate.[1]

While the Tallinn Manual is by no means perfect or wide reaching, it manages to provide a set of courses of action for a very limited series of cyber instances, namely "Acts of Aggression" as determined by the U.N. Security Council. One of the most practical aspects of the manual as determined with 20/20 hindsight is its focus on "blacklisting" specific acts rather than attempting to "whitelist" every conceivable circumstance. This is significant because it attempts to establish a culture of civility and responsibility in cyberspace as opposed to a rulebook for the world to follow.

The resulting litmus test that the International Group of Experts ("IGE") drew up in developing the manual was the distinction that a mere inconvenience in cyberspace is not enough to justify a use of

[1] Kristen Eichenser, *Review of The Tallinn Manual on the International Law Applicable to Cyber Warfare*, 108 AM. J. INT'L L. 585, 585 (2014).

force in response under the definition provided by the U.N. Security Council. This is significant in that it clarifies an issue in the global media today regarding the "cyber-attacks" on corporations and the government such as Sony, Lockheed-Martin, and the Office of Personnel Management ("OPM"), and whether said "attacks" rise to the level of requiring a response in order to save face on the world stage. Prior to the publication of the Tallinn Manual, this was not a settled argument, although the small scale of the Sony attacks would likely not have resulted in a physical response, regardless of the findings of this manual.

One of the most valuable results of the Tallinn Manual is that it establishes the concept of "repudiation" in the cyber domain. A nation-state may not knowingly allow its cyber infrastructure to be used in an attack. This is almost identical in concept to the limitations that the international community has placed on the use of a nation's infrastructure to support terrorism. The U.N. Security Council has been very explicit in its denouncement of countries that allow the use of their infrastructure in attacks; indeed the U.N. Charter specifically states that invasion of a country is only justified in the cases of self-defense or humanitarian offenses. The humanitarian clause is very specific in that it states that a country must be unable or unwilling to stop an ongoing event in order for another country to step in and initiate action.[2]

The final and most important conclusion is that certain events should be considered to be an act of force under the U.N. Charter and thus warrant an indeterminate type of response. While the occurrence of physical harm inflicted upon individuals and property has been considered for some time to be a "red line" within the cyber domain, the fact that physical harm is actually specified is an important step forward in creating a common set of agreements for operating in this domain. Similar to the Law of the Sea, whose intent is to attribute blame or to specify methods for determining amount of blame, the Tallinn Manual is a cursory first step into the field of coalescing attribution and normalcy in the cyber domain.

The Tallinn Manual in Cyberspace

Unequivocally, the Tallinn Manual is a remarkable body of work, especially considering the celerity that was applied in its

[2] U.N. Charter art. 51.

creation. To produce such a manual to address the completely unchartered domain that was cyberspace prior to the manual's inception, in just three short years, speaks volumes to the talent and brilliance of the twenty renowned international law scholars and practitioners who drafted it. However, while there is definitely notability in the hasty creation of a governing authority in an ungoverned domain, with haste comes inefficiency and the Tallinn Manual is littered with inefficiency. The Tallinn Manual falls short of comprehensiveness in three major regards: Firstly, the application of the same Just War principles that reign over conventional warfare to the cyberspace domain is fundamentally flawed. While the idea to apply this blanket set of warfare rules to yet another domain is novel and of course, ideal, the unique nature of the cyberspace domain prevents this archaic theory from being completely applicable and in turn, effective. Second, in the flurry to create a regulatory body of work for application in the cyberspace domain, the IGE was not able to conclude upon each issue agreeably. There are numerous instances within the Tallinn Manual where the stated conclusion for a relevant issue is simply that the IGE could not agree. Finally, while the Tallinn Manual does well in addressing cyber activities that rise above the level of a "use of force" or an "armed attack," as defined by the U.N. Charter, the issues surrounding cyber criminality that fall below that threshold are arguably the most relevant ones and the most in need of governance and regulation. While the Tallinn Manual was an excellent temporary solution to the inexistence of governance and regulatory means within cyberspace, a more permanent solution must be considered and drafted.

The cyberspace domain can no longer be regarded as a mere supplement to another larger, more relevant, more excepted warfare domain; rather, cyberspace has grown, inarguably, to affect every other domain, while also standing on its own as a unique and unchartered battlefront. Cyberspace is a fundamentally unique domain and it should be treated as such. As a domain that finds its strength in being so dynamic and innovative, it deserves a dynamic and innovative set of rules to govern it. Otherwise, as it changes and evolves rapidly and unpredictably, it will outgrow any inflexible and archaic bonds and break free of whatever temporary measures have been put forth to govern it. The "bolted-on" solution the Tallinn Manual provides needs to be replaced with a solution that is "baked-in." Cyberspace is completely new, and it needs a completely new set of rules, not just a new application of the same outmoded, albeit venerable, rules that govern the traditional warfare domains.

Evaluating the Tallinn Manual

To revisit the first major shortcoming of the Tallinn Manual in regards to its application as a permanent solution to the ever-so-popular "What are the rules?" question, it is not effective to apply Just War Theory to cyberspace in the same cookie-cutter fashion that it has been applied to traditional warfare domains. The difficulty of attribution and the heightened likelihood of misattribution that the actors in the cyberspace domain thrive off of and leverage consistently make jus ad bellum, the criteria that must be consulted in order to determine the permissibility of engaging in conflict, essentially useless. "The misperception and miscalculation that stem from incomplete information are perhaps the most omnipresent instigators across all forms of conflict."[3] In no other domain prior to cyberspace have individuals possessed the means to compete at the same tactical level that countries do. While its arguable that individuals still do not stand equal with countries at the same level on the cyber battlefront, the degree of accessibility and impact that an individual can have in the greater cyber fight is far more significant than it has been in past warfare situations. In the traditional domains, like air, sea, and ground warfare, in addition to a talented supply of human resources, the kind of copious and expensive physical resources that only countries could produce were necessary pieces for anyone who wished to play the game. However, with cyber, that grandiose financial barrier is essentially diminished and with that fiscal wall bulldozed, the door is opened for a larger pool of nefarious actors making the already existing problem of attribution even more uncertain. Andrea Little Limbago says it best in her article for Endgame, *The Fog of (Cyber) War: The Attribution Problem and Jus ad Bellum*,

> It's time for a framework that builds upon past knowledge while also adapting to the realities of the cyber domain. Too often, decision-making remains relegated to a Cold War framework, such as the frameworks for conventional

[3] Andrea L. Limbago, *The Fog of (Cyber) War: The Attribution Problem and Jus Ad Bellum*, ENDGAME (Jan. 2, 2016), https://www.endgame.com/blog/fog-cyber-war-attribution-problem-and-jus-ad-bellum.

> warfare, mutually assured destruction, and a known adversary. It would be devastating if the complexity of the cyber domain led to misattribution and a response against the wrong adversary – and all of the unintended consequences that would entail.[4]

Simply put, "the digital age amplifies the already complex and opaque circumstances surrounding jus ad bellum."[5]

Secondly, the IGE that is responsible for the creation of the manual, often fail to come to unanimous agreement on key issues within it. As Kristen Eichensehr writes in her *Review of The Tallinn Manual on the International Law Applicable to Cyber Warfare*, "While the rules on which the IGE agreed are very useful in advancing thought and debate about international law regarding cyberwar, more valuable still are the instances in which the *Tallinn Manual* frankly acknowledges disagreement within the IGE."[6] The disagreements among the IGE range across key issues like the constitution of a violation of sovereignty, the permissibility of disabling nefarious malware on a computer existing in an another country, and even issues as fundamental to the manual as to "whether a cyber operation that causes 'extensive negative effects,' but does not 'result in injury, death, damage or destruction,' could constitute an armed attack (p. 56)."[7] While the IGE does provide helpful commentary within the manual regarding majority and minority positions and the support used to arrive at each, the failure to provide unanimous guidance in the only existing legal framework used to govern the cyberspace domain is quite troubling and contributes to the manual's overall ineffectiveness.

Finally, and perhaps most importantly, the Tallinn Manual falls short in addressing the legality of key issues of cyber criminality that fall below the threshold of an "armed attack." While the Tallinn Manual recognizes that the theft of intellectual property and the implications of cyber espionage on both the public and private sectors of the world's nations are currently pivotal issues in cyberspace and will continue to exist as pivotal issues, it does not aim to address them. The day-to-day cyber banter that countries are engaging in and battling against almost always falls below the threshold of an "armed attack."

[4] *Id.*

[5] *Id.*

[6] Eichensehr, *supra* note 1 at 586.

[7] MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 56 (Cambridge University Press, 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual; Eichensehr, *supra* note 1 at 586.

Cyber attacks with physical consequences like Stuxnet are few and far between. Rather, it is acts like the OPM breach and the Sony hack that raise the alarm more frequently and consistently and build the most contention between nations on the cyber battlefront. These are the issues that need to be addressed. These gray zones where countries face non-tangible harm and suffering by virtue of attacks against their businesses or the exfiltration of intelligence materials sensitive to the security and prosperity of their nations are where the greatest threat lies in terms of cyber warfare. No other warfare domain has faced non-tangible threats in the way that the cyberspace domain has, which is why it is fundamentally flawed to apply a framework for legal guidance that fails to champion a unique solution for this unique issue, much less even address it.

Conclusion

Again, the Tallinn Manual is an incredible body of work that was drafted with an impressive sense of urgency by a brilliant pool of talent. The manual served well in providing a temporary solution to the lack of regulatory means and governance in the cyberspace domain, but it is to go too far to settle for the Tallinn Manual as a permanent solution to the extraordinarily unique problems being faced within this realm. After the attacks on Estonia in 2007, the world desperately needed something to stop the flood of uncertainty and non-regulation within cyberspace, and while the Tallinn Manual served valiantly in holding back the first few big waves, it is now 2016 and the seepage is proving to be greater than anticipated. Resultantly, the necessity for a new, more fortified and specific solution grows greater every day.

Contributors

Brittany L. Card
Brittany L. Card is a Master of Arts in Law and Diplomacy student from the Fletcher School of Law and Diplomacy at Tufts University. She is currently a Teaching Assistant at Harvard University and has spent time working with the United Nations Office for the Coordination of Humanitarian Affairs.

John Caton
John Caton is a Master of Public Administration student at the University of Southern California's Sol Price School of Public Policy.

MIDN Erin N. DeVivies
Erin DeVivies is an undergraduate student at the United States Naval Academy in Annapolis, Maryland.

Bradley Dixon
Bradley Dixon is graduate student at Missouri State University pursuing a Master's degree in Global Studies. His academic concentrations are in national security and terrorism while working for the Springfield-Greene County Office of Emergency Management.

Rebekah Glickman-Simon
Rebekah Glickman-Simon is a graduate of Boston University and is currently attending the Tufts University School of Medicine for her Master of Public Health and the Northeastern University School of Law for her Juris Doctor.

MIDN Michael G. Harding
Michael G. Harding is an undergraduate student at the United States Naval Academy in Annapolis, Maryland.

Jeff Janaro
Jeff Janaro is a Juris Doctor candidate at the George Washington University Law School and a Lieutenant Commander in the U.S. Coast Guard. Jeff will graduate in 2017.

LTC Pat Kaune, USA, Army War College Fellow

Pat Kaune is an Army War College Fellow at Syracuse University. He is a graduate of both The Ohio State University and Kansas State University.

Brett Maxfield

Brett Maxfield is a Master of Public Administration student at the University of Southern California's Sol Price School of Public Policy. He also holds a MBA from the University of San Diego, a LLM from the University of San Diego School of Law, a JD from the University of California, Los Angeles, and a BA from the University of California, Berkeley.

Laura McElroy

Laura McElroy is a graduate student at the Fletcher School of Law and Diplomacy at Tufts University and a graduate of the University of Wisconsin. She will graduate from Tufts University in 2017 and is interested in international affairs and human security.

Maida Omerović

Maida Omerović will graduate in 2017 with a Master of Arts in Law and Diplomacy from the Fletcher School of Law and Diplomacy at Tufts University. She has spent several years working as a Program Associate for the Harvard School of Public Health.

Alexandre Rodde

Alexandre Rodde is a recent LLM graduate from the George Washington University Law School where he specialized in National Security Law and Foreign Relations Law.

Patrick Stewart

Patrick Stewart is a Juris Doctor candidate at the George Washington University Law School. He will graduate in 2016 and has previously worked for the Transportation Security Administration and the Department of Homeland Security.