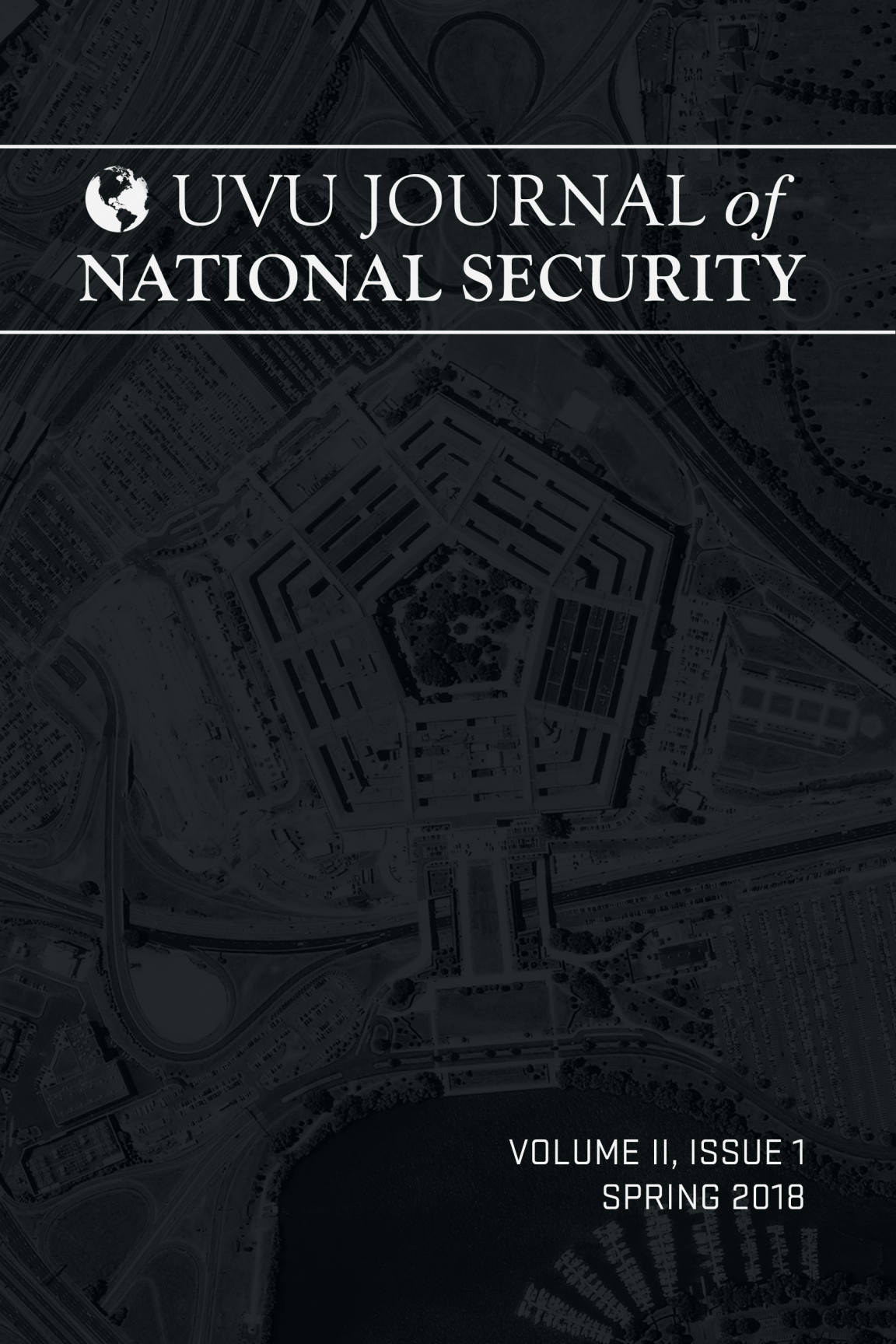

UVU JOURNAL *of* NATIONAL SECURITY

VOLUME II, ISSUE 1
SPRING 2018

UVU JOURNAL *of* NATIONAL SECURITY

VOLUME II
ISSUE 1
SPRING 2018

UVU JOURNAL *of*
NATIONAL SECURITY

ISSN 2576-1595

Center for National Security Studies
Utah Valley University
800 West University Parkway
Orem, UT 84058

www.uvu.edu/nss/journal.html

UVU JOURNAL *of*
NATIONAL SECURITY

The *UVU Journal of National Security* is Utah's first student-edited academic journal focused on national security issues. The *JNS* is published twice annually—in April and December—and is supported by the Center for National Security Studies (CNSS) at Utah Valley University (UVU). The *JNS* publishes timely, insightful articles on critical national security matters, including topics relating to foreign affairs, intelligence, homeland security, terrorism, and national defense. The *JNS* accepts articles from UVU students, alumni, faculty, staff, and administration. Submissions should be sent to the *JNS* Editor-in-Chief at nationalsecurity@uvu.edu.

The Center for National Security Studies

The CNSS at UVU was established in January 2016. The Center is the first of its kind in the State of Utah. The CNSS is a nonpartisan academic institution for the instruction, analysis, and discussion of the issues related to the field of U.S. national security. The mission of the CNSS is twofold: to promote an interdisciplinary academic environment on campus that critically examines both the theoretical and practical aspects of national security policy and practice; and to assist students in preparing for public and private sector national security careers through acquisition of subject matter expertise, analytical skills, and practical experience. The CNSS aims to provide students with the knowledge, skills, and opportunities needed to succeed in the growing national security sector.

Utah Valley University

UVU is a teaching institution that provides opportunity, promotes student success, and meets regional educational needs. UVU builds on a foundation of substantive scholarly and creative work to foster engaged learning. The university prepares professionally competent people of integrity who, as lifelong learners and leaders, serve as stewards of a globally interdependent community.

UVU JOURNAL *of*
NATIONAL SECURITY

VOLUME II SPRING 2018 ISSUE 1

CONTENTS

A Note from the Editor-in-Chief

Savannah Mork

Each semester we put together this *Journal*, we think we have a clear, easy path to publication. To Professor Deb Thornton, who sup ports that idealism and makes everything possible when it does not work out like we plan, a million thanks. This Journal would truly not be possible without the hours of hard work and devotion put forth by her and her English class each semester.

To my staff—Joee, Emma, Ryan, Joseph, Jonathan, and Clark—thank you for keeping everything on for keeping everything on track and answering my countless emails and texts to check on the same problem four times. To Professor Ryan Vogel, whose dedication to this Journal and his students truly knows no bounds, thank you. You make everything we do possible.

While this Journal is still quite young, I am proud of how it has grown in terms of topics covered and the amount of submissions we receive. The students of Utah Valley University are quite exceptional both in their scholarship and their dedication to bettering themselves and those around them. I am honored to have attended this unive rsity and to have been a part of such a wonderful program. It has been a true privilege to lead this edition of the Journal. I look forward to seeing how both this *Journal* and the Center for National Security Studies grows.

Savannah Mork

Editor-in-Chief

Journal of National Security

Foreword: The Changing Landscape of National Security

Dean David McEntire
College of Health and Public Service at UVU

If it seems as if the world is more complicated and uncertain today as compared to the past, there is a logical reason for that. It is true! National security threats abound and they seem to be expanding and changing on an almost-daily basis.

Of course, we still face the traditional risk of interstate conflict and ongoing concerns about the proliferation of nuclear weapons. However, we are not certain if Iran will continue to justify the acquisition of nuclear weapons for religious purposes or if individuals like Kim Jong-un will actually use them against the United States or others (and not just threaten to use them) to advance his agenda for power and national self-interest.

But, there are many new risks emanating from other sources. China and Russia have sophisticated cyberwarfare programs, and the latter country was recently accused of political assassination through poisoning and trying to influence or meddle in national elections through social media.

ISIS appears to be on the run and has lost both influence and territory. Nevertheless, new terrorist organizations form frequently and all types of attacks continue to occur in the Middle East, Africa, Europe, the United States and elsewhere.

Added to these issues are international disagreements over a border wall, tariffs, and challenges presented by well-organized drug cartels. There are domestic problems rising from deranged individuals who use automatic weapons to kill individuals in Las Vegas or detonate bombs in Texas. Even issues like the Ebola outbreak, riots based on

racial/social/economic relations, and false emergency warnings in Hawaii are causing us to rethink the very notion of national security itself.

Fortunately, this outstanding student-run journal is tackling these important issues. Therefore, I endorse the articles in this volume and commend the authors for helping us learn more about national security. Because the national security landscape continues to shift in dramatic ways, we must find ways to improve our professional obligations in these areas.

Sincerely,

David A. McEntire, PhD

Dean, College of Health and Public Service

The World According to Vladimir Putin

Robert M. Jorgensen
Frederick H. White

Recently, top White House advisor H.R. McMaster called Russia's interference in elections throughout the world, including the United States, "insidious" and openly condemned the Kremlin for meddling in the democratic process of sovereign nations.[1] Similarly, the investigation led by special counsel Robert Mueller has already indicted former national security advisor Michael Flynn, and Mueller's team continues to question key individuals within President Donald Trump's administration about coordination of efforts with Russian representatives. Less than a year ago, it was not uniformly accepted that the Russians had interfered in US elections or that Donald Trump had benefited from this alleged cyber campaign against presidential candidate Hillary Clinton. Also, with several Senate and Congressional investigations underway, much of what we think we know now about Russian interference in US and European elections might change in due course. Therefore, in our introduction to this issue of the *UVU Journal of National Security*, we will provide some perspective on why such actions by the Russians might seem justified, and we will concentrate on President of the Russian Federation Vladimir Putin's worldview and his possible reasoning for conducting a covert cyberwar with the West.

From the outset we must acknowledge Vladimir Putin's publicly stated political goals. He has outlined his worldview in presentations

[1] *McMaster Says U.S. Must Reveal "Insidious" Russian Meddling to Prevent Further Attacks*, Radio Free Europe/Radio Liberty (Jan. 3, 2018, 8:00 PM), https://www.rferl.org/a/mcmaster-russia-election-meddling-insidious-implausible-deniability/28953524.html.

domestically and abroad, and they have been covered by western media, offering few surprises for those who have been listening.[2] One 2013 speech at an international conference with German Chancellor Angela Merkel and other world leaders in attendance continues to circulate on the internet (with English subtitles) with the provocative title "Vladimir Putin Exposes the NWO." This presentation by Putin challenges the American and European Union (EU) approach to geopolitics, leaving no doubt that Russia intends to operate as a counterbalance in the world.[3] Putin's political decisions in his third presidency aim to create economic, social, and political instability for the US and the EU; to sow discord between the US, EU and their former allies; to reestablish "spheres of influence" (boundaries that approximate the old Cold War spheres of influence); and to (re)gain recognition for Russia as a significant international power.[4] With these guiding principles, Russia's recent activities in Syria and Ukraine might be put into proper context from the Kremlin's perspective.

So, how did we get to this point? A brief review of recent history provides context for the Kremlin's present position. In 2005, Putin began to retreat from his earlier agreements with western leaders after the Orange Revolution in Ukraine undermined a pro-Kremlin candidate, Viktor Yanukovych, in favor of Viktor Yushchenko, a pro-West candidate for president. That same year, Putin created an international sensation when he claimed that the breakup of the USSR was the worst geopolitical tragedy of the twentieth century. This statement was followed by a Kremlin-sanctioned, official nostalgia for key elements

[2] Miriam Elder, *Vladimir Putin Warns Foreigners Not to Intervene in Russian Politics*, Guardian (Dec. 12, 2012, 8:36 AM), https://www.theguardian.com/world/2012/dec/12/vladimir-putin-foreigners-russian-politics; Molly K. McKew, *Putin's Real Long Game. The World Order We Know Is Already Over, and Russia Is Moving Fast to Grab the Advantage. Can Trump Figure Out the New War in Time to Win It?* Politico (Jan. 1, 2017), https://www.politico.com/magazine/story/2017/01/putins-real-long-game-214589; Evan Osnos, David Remnick, and Joshua Yaffa, *Trump, Putin, and the New Cold War*, The New Yorker (Mar. 6, 2017), https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war.

[3] *Vladimir Putin Exposes the NWO Part 1*, https://www.youtube.com/watch?v=ENh5-srKfHA; *Vladimir Putin Exposes the NOW Part 2*, https://www.youtube.com/watch?v=7sEVRGE2_Vw; *Vladimir Putin Exposes the NOW Part 3*, https://www.youtube.com/watch?v=P6htXKMUKEs.

[4] Probably the most convincing argument to support this assertion is made by Fiona Hill and Clifford G. Gaddy in Mr. Putin: Operative in the Kremlin, New and Expanded (Brookings Institute Press 2015).

of Imperial and Soviet Russia's past that would soon be depicted in Russian movie theaters and on state-controlled television. Putin was turning inward and reverting to the discourse of his own childhood—that the West is the natural enemy of Russia.

As early as 2007, Putin suggested that US and EU political hegemony was a danger to non-western civilizations. He advocated for what would eventually be called a multipolar world that would be guided by the historical past and geopolitics rather than neo-liberal ideals supporting human rights and free markets. Putin's approach was meant to appeal not only to his own Russian political base but to conservatives, alt-right types and neo-fascists in the US and EU.[5] When Hillary Clinton became the US Secretary of State in 2009, there was a much-ballyhooed "Russian reset" that was to drastically improve relations between the two countries. Not unexpectedly, the situation deteriorated rather rapidly as the Russians bristled at Clinton's support for "regime change" in countries that Russia considered to be within its sphere of influence.[6]

The issue of regime change became particularly personal for Putin when Russian citizens first protested legislative elections in 2011 and then in greater numbers took to the streets when Putin won his third presidential election in 2012. To Western observers, it was rather surprising that "Russia without Putin" was loudly voiced in the streets of Moscow.[7] In a planned "Million Man March," crowds reached sizes not seen since the political protests of the 1990s that encouraged the end of the Soviet Union. At this point Putin reacted with force and 30 individuals were arrested and charged after incidents in Bolotnaya Square. This crackdown had a chilling effect on the political protests and brought a quick decline in public dissent.[8] From the Kremlin's

[5] Franklin Foer, *It's Putin's World. How the Russian President Became the Ideological Hero of Nationalists Everywhere*, Atlantic (March 2017), https://www.theatlantic.com/magazine/archive/2017/03/its-putins-world/513848/.

[6] As examples, Color Revolutions in former Soviet republics, Arab Spring, Overthrow of Muammar Gaddafi's regime, and stated desire to depose Syrian President Bashar al-Assad.

[7] Ellen Barry, *Rally Defying Putin's Party Draws Tens of Thousands*, New York Times (Dec. 10, 2011), http://www.nytimes.com/2011/12/11/world/europe/thousands-protest-in-moscow-russia-in-defiance-of-putin.html; Tom Parfitt, *Anti-Putin Protesters March through Moscow*, Guardian (Feb. 4, 2012, 10:48 AM), https://www.theguardian.com/world/2012/feb/04/anti-putin-protests-moscow-russia.

[8] Ellen Barry and Michael Schwirtz, *Arrests and Violence at Overflowing Rally in*

perspective, the protests of 2011–2013 had been organized by Hillary Clinton and the Central Intelligence Agency (CIA), using hybrid tactics that were intended to lead to regime change in Russia.[9] The belief that Clinton was among those trying to unseat Putin would inform much of Russia's actions during the US presidential elections.

More importantly, as Putin annexed Crimea in 2014, he believed that he could rely on oil and gas extraction to support his efforts. He also turned away from the Russian middle class and cultural elite who had come out onto the streets and shouted, "Russia without Putin." He would appeal to a much larger section of the population with a brand of Russian nationalism that was anti-American, opposed to the "fascism" in Ukraine, and appealed to a particular type of Russian Orthodox conservatism—shown by campaigns against the all-female rock band (and political agitators) Pussy Riot and in attacks on gay rights activists.[10]

In defiance of the West, Vladimir Putin annexed Crimea and began covert military actions in Eastern Ukraine. The US and the EU seemed to be caught off guard by such bold strategic moves, but Putin was responding to a perceived expansion of the EU and the countries of the North Atlantic Treaty Organization (NATO) into Ukraine. Not only was Ukraine within the Kremlin's claimed sphere of influence,

Moscow, New York Times (May 6, 2012), http://www.nytimes.com/2012/05/07/world/europe/at-moscow-rally-arrests-and-violence.html; Irina Borogan and Andrei Soldatov, *What Force (and Forces) Can the Kremlin Use Against the Opposition?* OpenDemocracy (11 June 2012), https://www.opendemocracy.net/od-russia/irina-borogan-andrei-soldatov/what-force-and-forces-can-kremlin-use-against-opposition; Samuel A. Greene, Moscow in Movement: Power and Opposition in Putin's Russia (Stanford University Press 2014); Mischa Gabowitsch, Protests in Putin's Russia (Polity Press 2017).

[9] David M. Herszenhorn and Ellen Barry, *Putin Contends Clinton Incited Unrest Over Vote*, New York Times (Dec. 8, 2011), http://www.nytimes.com/2011/12/09/world/europe/putin-accuses-clinton-of-instigating-russian-protests.html; Miriam Elder, *Vladimir Putin Accuses Hillary Clinton of Encouraging Russian Protests*, Guardian (Dec. 8, 2011, 5:46 AM), https://www.theguardian.com/world/2011/dec/08/vladimir-putin-hillary-clinton-russia; Michael Crowley and Julia Ioffe, *Why Putin Hates Hillary: Behind the Allegations of a Russian Hack of the DNC is the Kremlin Leader's Fury at Clinton for Challenging the Fairness of Russian Elections*, Politico (July 25, 2016, 6:20 PM), https://www.politico.com/story/2016/07/clinton-putin-226153.

[10] Karen Dawisha, Putin's Kleptocracy. Who Owns Russia? 318 (Simon & Schuster 2014).

but the country was the historic homeland of the Slavic nation, and it was inconceivable that Kiev would side with the West. Russia's military tactics and effectiveness in a new type of hybrid warfare (including cyber attacks and more) reversed expectations, given the performance of these same forces during an earlier conflict in Georgia.[11]

The conflict had centered on two "breakaway provinces" that were officially part of Georgia but had separate, unrecognized governments. Abkhazia and South Ossetia have been supported by Russia. In August 2008, Georgian President Mikhail Saakashvili sent troops into South Ossetia to deal with separatists, and Russia responded militarily. Although Russia won the actual battles, the feeling was that they had lost control of the information space and had been defeated in the new cyber-media arena. For example, President Saakashvili made a direct plea to the US via a live feed on CNN. As a result, Putin called for even greater military reform than the changes that had already been accomplished.[12]

Under the leadership of Defense Minister Sergei Shoigu and Chief of the Russian General Staff Valerii Gerasimov, the Russian military was (re)organized for twenty-first-century hybrid warfare to encompass military, technological, media, political, and intelligence tactics that destabilize an enemy at minimal cost. According to what has become known as the "Gerasimov Doctrine," the Russian military will strive to fight future wars with a four-to-one ratio of non-military to military measures in order to shape the political and social landscapes of adversaries through subversion, espionage, propaganda, and cyberattacks.[13] This reorganized approach to warfare by the Russian military was on full display in Ukraine. Maria Snegovaya of the Institute for the Study of War called the approach "reflexive control," which "causes a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situa-

[11] Matthew Rojansky and Michael Kofman, *A Closer Look at Russia's "Hybrid War,"* Kennan Cable 7 (Apr. 14, 2015), https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.

[12] Dmitry Gorenburg, *The Russian Military under Sergei Shoigu: Will the Reform Continue?* PONARS Eurasia Policy Memo No. 253 (June 2013), http://www.ponarseurasia.org/memo/russian-military-under-sergei-shoigu-will-reform-continue; ***See also*** Hill and Gaddy, Operative in the Kremlin, *supra* note 4 at 385–97.

[13] Andrew Monaghan, *Putin's Way of War. The "War" in Russia's "Hybrid Warfare,"* 45 Parameters 65–74 (2015–2016).

tion decisively."[14] In 2014, when President Yanukovych fled Ukraine following prolonged protests in Kiev, Putin perceived once again in these protests the regime change tactics of the US and felt that he might be the next target. As a result, we might argue that Putin's decision to resort to military action in Ukraine and to interfere in US elections was retaliation for the threat enacted on his own presidency and that of the Ukrainian President—an equal response to a perceived threat to Russian sovereignty.

As a recently published report on Russia for the Committee on Foreign Relations argued, Putin's regime views the late twentieth century and early twenty-first century as a period that produced repeated attempts by the West to undermine and humiliate Russia. Such a viewpoint allows Putin to represent himself as the leader of a nation at war: "This narrative repeatedly flogs core themes like enemy encirclement, conspiracy, and struggle, and portrays the United States, NATO, and Europe as conspiring to encircle Russia and make it subservient to the West."[15] Within this context of war, Putin's attacks on the US and EU can be justified internally.

Significantly, western intelligence agencies have compiled extensive evidence regarding Kremlin interference in several semi-consolidated and consolidated democracies. In addition to the aforementioned involvement with Georgia and Ukraine, the US Senate's Committee on Foreign Relations has identified Russian action in Montenegro, The Netherlands, Serbia, Bulgaria, Hungary, Latvia, Lithuania, Estonia, Norway, Denmark, Finland, Germany, Sweden, the United Kingdom, France, Spain, and Italy.[16] The techniques have ranged from sustained social media campaigns to simple handbooks on suggesting effective methods for influencing elections. Bulgarian security services intercepted a 30-page dossier destined for the country's Socialist Party.[17]

[14] Maria Snegovaya, *"Reflexive Control": Putin's Hybrid Warfare in Ukraine Is Straight out of the Soviet Playbook*, Business Insider (Sept. 22, 2015, 6:42 AM), http://www.businessinsider.com/reflexive-control-putins-hybrid-warfare-in-ukraine-is-straight-out-of-the-soviet-playbook-2015-9.

[15] A Minority Staff Report for the Use of the Committee on Foreign Relations of the United States Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Homeland Security Digital Library (Jan. 10, 2018), https://www.hsdl.org/?abstract&did=806949, 13.

[16] *Id.* at 99–137.

[17] Joe Parkinson and Georgi Kantchev, *Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections*, Wall Street Journal (Mar. 23, 2017, 11:19 AM),

The dossier contained strategies on how to influence elections by "planting fake news and exaggerating poll data." A number of allegations have been made regarding Russian influence affecting the Brexit referendum, and Facebook has been working with the Parliament of the United Kingdom to investigate the use of social media to sway opinions.

Perhaps the most notable chapter of Putin's prolonged campaign of interfering with sovereign state elections is the 2016 presidential election in the US. The first major public indication of Russian support for the Trump campaign came in December 2015. In a press conference, Putin referred to Trump as the absolute leader in the Republican primary race and noted he was "a very bright and talented man."[18] Putin continued by adding, "He says that he wants to move to another level of relations, to a deeper level of relations with Russia. How can we not welcome that? Of course we welcome it."[19]

Putin's public statement came after the Federal Bureau of Investigation (FBI) had already detected Russian cyber-espionage activities targeting the Democratic National Committee (DNC). In September of 2015, the FBI contacted the DNC to report that the bureau had been monitoring Russian activity within DNC computers. The group, codenamed APT29, The Dukes, and Cozy Bear by various security researchers and government agencies, had been associated with the Russian intelligence agency, the Federal Security Service or FSB (present-day KGB).[20] The DNC did not take any publicly known action at that time to address the threat. In June and July 2016, more than 19,000 emails were published on DCLeaks, a site that is believed to be an outlet for Cozy Bear to disseminate stolen documents.[21] The emails cover a period from January 2015 to May 2016 and reveal many of the inner workings of the DNC.

https://www.wsj.com/articles/how-does-russia-meddle-in-elections-look-at-bulgaria-1490282352.

[18] Nick Grass, *Putin: Trump "A Very Bright and Talented Man,"* Politico (Dec. 17, 2015, 2:36 PM), https://www.politico.eu/article/putin-trump-a-very-bright-and-talented-man-republican-presidential-candidate/.

[19] *Id.*

[20] Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, Crowdstrike (June 15, 2016), https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[21] Michael Kan, *US Officially Blames Russian Government for Election-Related Hacking*, PCWorld (Oct. 7, 2016, 1:15 PM), https://www.pcworld.com/article/3129447/us-officially-blames-russian-government-for-election-related-hacking.html.

Another group, one associated with Russian intelligence's GRU bureau, launched a massive phishing attack against Hillary Clinton's campaign staff. Phishing attacks consist of assuming a false identity and sending email messages to solicit information from unsuspecting targets. Often, these messages purport to be from a service and are actually an attempt to trick the target into entering credentials into a decoy website. The credentials are used to access the target's real accounts. In March 2016, the group implicated in this attack, codenamed APT28 or Fancy Bear, successfully phished John Podesta, the chairman of Clinton's presidential campaign. In this case, APT29 allegedly sent out hundreds of emails to those associated with Clinton's campaign in an attempt to compromise accounts. Podesta received an email that indicated his personal Gmail account had been compromised. An aide forwarded the email to the IT support group for confirmation. The response to Podesta stated it was a "legitimate email" and that he should "change his password immediately."[22] The response contained a typographical error and should have read, "illegitimate email." When Podesta clicked on the link to change his password, he was redirected to a site controlled by Fancy Bear. By supplying his credentials, Podesta gave Fancy Bear complete access to his personal Gmail account, and approximately 20,000 pages of emails were stolen and subsequently released through WikiLeaks, another potential partner (cut-out) of the Russian FSB.

US intelligence services also identified breaches of the Republican National Committee (RNC) systems during this same time. These breaches were also attributed to the same Russian actors; however, the information stolen was not posted on DCLeaks or WikiLeaks. This supports the theory that Russian intelligence was seeking to damage Clinton alone.[23] It is possible to hypothesize that Putin most likely desired to damage Clinton's presidency (she was the projected winner of the US elections) as Putin's own third presidency had been marred by protests organized by the CIA (as Putin believed). At this point, it is still unclear whether Kremlin activities were also meant to influence

[22] *Hackers Apparently Fooled Clinton Official with Bogus Email*, Associated Press (Oct. 29, 2016, 10:04 AM), https://www.news24.com/World/News/hackers-apparently-fooled-clinton-official-with-bogus-email-20161029.

[23] David E. Sanger and Scott Shane, *Russian Hackers Acted to Aid Trump, U.S. Says*, New York Times (Dec. 9, 2016), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html.

the elections for candidate Trump or were simply intended to significantly damage a Clinton presidency from the outset.

Originally, a hacker named Guccifer 2.0 admitted responsibility for a number of these hacks. Though he claimed to be Romanian, he struggled to use grammatically correct Romanian when he was interviewed. Likewise, there was substantial evidence that Guccifer 2.0 used a Russian-language VPN service. Based on this and other evidence, the Department of Homeland Security issued a statement saying the Guccifer 2.0's actions were "consistent with the methods and motivations of Russian-directed efforts."[24]

In January 2017, the Office of the Director of National Intelligence (DNI) released a report titled "Assessing Russian Activities and Intentions in Recent US Elections." The report revealed that the three major US intelligence agencies had all concluded that Russia interfered in the 2016 Presidential Election. Specifically, the FBI, CIA, and NSA stated:

> We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, to denigrate Secretary Clinton, and to harm her electability and potential presidency. We further assess that Putin and the Russian Government developed a clear preference for President-elect Trump.[25]

The assessment describes additional actions attributed to Russian intelligence to undermine the 2016 presidential election, including extended social media campaigns that were meant to sway public opinion, cyber-espionage against US political organizations, and public disclosure of breached data. The report also implicates the popular website and television news channel RT (sponsored by the Kremlin) as a primary source of anti-Clinton propaganda.

In the months since the DNI report was released, additional de-

---

[24] *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, Homeland Security (Oct. 7, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

[25] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ii (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

tails have emerged about the scope of Russian social media influence. Facebook has admitted that almost one-third of the US population was exposed to material posted by Russian troll farms.[26] Facebook, the owner of Instagram, also claimed that the Russia-based Internet Research Agency was responsible for more than 120,000 Instagram posts.[27] Specifically, these posts have been centered on divisive issues and have been designed to evoke strong reactions.

The focus of this introduction is not to litigate Russian influence in the 2016 US presidential election. Mueller's investigation will soon make this possible. The point is to understand Putin's worldview and to offer strategies for interpreting future Russian actions. In 2005, President Putin declared that the collapse of the Soviet Union had been the greatest geopolitical catastrophe of the twentieth century. Although these comments may have been partially directed at Western critics who had noted Putin's shift toward an authoritarian government, they also reflected an officially sanctioned nostalgia for the Soviet Era, practically an official invitation to re-remember the best qualities of the Soviet Union—a wistfulness that would continue to grow over time. Just as significant, Putin's comments were made two days before a verdict was expected for the Russian oligarch Mikhail Khodarkovskii, who had just endured a show trial in which he had been accused (and would be convicted) of fraud as head of Yukos, one of the largest Russian oil companies to emerge from the privatization of state assets during the presidency of Boris Yeltsin. Only two years previous, Khodarkovskii and fellow oligarch Roman Abramovich had been hailed in Russia for their business acumen.[28] At odds were Putin, with his return to authoritarianism via a rehabilitation of the Soviet past, and a business elite who had emerged from the lawless 1990s, wealthy but vulnerable to legal prosecution. This lawless period had been devoid of strong

[26] Elizabeth Weise, *Russian Trolls Had Huge Presence on Social Media*, USA Today (Oct. 31, 2017), https://www.pressreader.com/usa/usa-today-us-edition/20171031/281711204909010.

[27] Sheera Frenkel, *For Russian "Trolls," Instagram's Pictures Can Spread Wider Than Words*, New York Times (Dec. 17, 2017), https://www.nytimes.com/2017/12/17/technology/instagram-russian-trolls.html.

[28] For example, Valerii Butaev's article in *Komsomol'skaia Pravda* extols the acquisition of Abramovich's oil company Sibneft by Khodarkovskii's company Yukos for three billion dollars. Valerii Butaev, *Khodarkovskii i Abramovich v odnoi uprazhke*, Komsomol'skaia Pravda (Apr. 23, 2003, 2:28 AM), http://www.kp.ru/daily/23019/3283/.

central leadership and moral fortitude, but now Putin was offering social and economic stability in the place of personal freedom. In Putin's speech, economic stability was intertwined with a sense of Soviet morality that had been lacking in the years between the fall of the Soviet Union and the establishment of Putin's law-and-order society.[29]

By 2007, Russians were invited by Kremlin backers to reassess Putin's new national unity that relied heavily on sanitized memories of a Soviet past that enjoyed first-world status as an oppositional force to US and EU political hegemony. Russia was perceived as "stronger" when it opposed the West and "weaker" when it was trying to gain acceptance into the World Trade Organization and other Western economic and political organizations. Putin and Russia would no longer seek acceptance by the West. Russia would attempt to return to its Soviet past, when Soviet soldiers changed the tide of the Second World War at Stalingrad, and Soviet scientists and cosmonauts were the first to conquer space.

In Putin's reanimation of the Soviet past, he seemed to favor the strong leadership of Stalin (while avoiding associations with the cult of personality), but within the context of the perceived abundance of the Soviet 1970s, thus confusing the details of the Soviet legacy, selectively choosing the "best" elements of the Joseph Stalin and Leonid Brezhnev eras, while clearly avoiding Nikita Khrushchev's liberal *thaw*. As evidence of Putin's official strategy, Kremlin-sponsored youth camps at Lake Seliger were organized in 2005 to contour the ideology of Russian national unity, in imitation of Soviet-style youth organizations that once supported Communist doctrine. That same year, pro-Kremlin Gazprom Media took over the influential newspaper *Izvestiia*, which soon after strongly supported the government's line.

In 2006, two harsh critics of the president died in mysterious ways: the journalist and human rights activist Anna Politkovskaya was killed in an elevator outside of her apartment in Moscow, and former Russian secret service agent and journalist Alexander Litvinenko was poisoned in London with radioactive polonium-210. The media control strategy also advanced in that same year when the newspaper *Kommersant* was bought by steel magnate Alisher Usmanov, an oligarch

[29] Vladimir Putin, *Annual Address to the Federal Assembly of the Russian Federation*, President of Russia (Apr. 25, 2005, 8:31 PM), available in English at http://en.kremlin.ru/events/president/transcripts/22931.

with close ties to the Russian government. By 2008, some 90 percent of Russian media was directly or indirectly controlled by the Kremlin.[30]

With Putin's internal control of the media and his own populace largely solidified, the political protests of 2011–2013 were not only a surprise, but in Putin's mind were most certainly organized and executed by foreign operatives. With such perceived threats to Putin's presidency and to Russian sovereignty, the reorganization of the Soviet military according to the Gerasimov Doctrine might be understood as a legitimate reaction to a significant external threat. Putin made clear in March 2014 that Russia was willing to cooperate with the West in the future, but only on its own terms. Russia would not become a Western-style democracy as many had hoped; Russia would not belittle itself to become part of any economic or strategic alliances; Russia would not become a part of Europe. Russia would always be Russia.[31]

Within the contexts cited in this chapter, cyber attacks, interference in elections, and other covert actions might be defensible by Putin within the new, but unclear, rules of twenty-first-century military and political engagement. In fact, the Gerasimov Doctrine openly states that Russia will shape the political and social landscape of the adversary through subversion, espionage, propaganda, and cyberattacks—military and political actions that were meant to check western aggression (perceived or real) against Russia.

[30] Allen C. Lynch, Vladimir Putin and Russian Statecraft 78 (Potomac Books 2011).

[31] Hill and Gaddy, Operative in the Kremlin, *supra* note 4 at 262–63.

Understanding FISA: A Deconstruction of America's Foreign Intelligence Gathering Law

Samuel Elzinga

Introduction

The Foreign Intelligence Surveillance Act, better known as FISA,[1] has dominated many conversations pertaining to national security and constitutional rights. The legislation was the result of numerous senate hearings on the US government's abuses of domestic surveillance techniques during the Richard Nixon Era and was implemented to help preserve the ethical and legal gathering of intelligence.[2] Since its introduction into public law in 1978, FISA and its role in American intelligence gathering has changed with the addition of new amendments to the original bill. Even throughout the gradual additions of amendments, the Foreign Intelligence Surveillance Act's purpose has remained the same: to establish procedures for the United States government's collection of foreign intelligence.

The Act and some of its provisions have come under fire in recent years, particularly following information leaks from former intelligence officer Edward Snowden, which sparked a national discussion about FISA and its role in protecting Americans from foreign threats. Despite conflicting public opinion, FISA remains a part of US law, with a new reauthorization of its key provisions signed by President Donald Trump on January 19th of this year. Regardless of FISA's controversial

[1] 50. U.S.C. 1801 § et seq.

[2] James G. McAdams III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, Federal Law Enforcement Training Center Online (2007), https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf.

nature, it is absolutely imperative to understand its provisions and how it both safeguards the American public and the security of our nation.

Background

FISA was the culmination of two extensive investigations conducted by select Senate Committees, the first of which was concerning President Nixon and his use of federal resources to spy on political opponents.[3] On June 17, 1972, five men were apprehended breaking into the Democratic National Convention headquarters located in the Watergate complex. When asked about the break-ins by a *Washington Post* reporter, US Attorney Earl Silbert said the burglars were "professionals with a 'clandestine' purpose."[4] The five men would later be charged with "felonious burglary and with possession of implements of crime," but their motivation was still unknown at the time.[5] The FBI began a vigorous investigation into the matter and began to question the Nixon Campaign, who just won reelection in a landslide victory.

In July of 1973, the FBI later discovered a connection between the cash carried by the five men during the break-in and a slush fund[6] used by President Richard Nixon's Committee for the Re-Election of the President, otherwise known as the CRP.[7] The Senate Select Committee on Presidential Campaign Activities was conducting its own investigation of the matter, and evidence quickly began piling up against the president.[8] It was later discovered that Nixon recorded many of his conversations, and the Supreme Court required him to release the tapes.[9] After the tapes revealed Nixon was attempting to cover up the break-in, articles of impeachment were introduced in the

[3] Lamar Waldron, Watergate: The Hidden History: Nixon, The Mafia, and the CIA 531 (Counterpoint 2013).
[4] Alfred E. Lewis, *5 Held in Plot to Bug Democrats' Office Here*, Washington Post (June 18, 1972), http://www.washingtonpost.com/wp-dyn/content/article/2002/05/31/AR2005111001227.html.
[5] *Id.*
[6] The term slush fund is defined by Merriam-Webster as "an unregulated fund often used for illicit purposes." *Slush fund*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/slush%20fund.
[7] David Hosansky, Eyewitness to Watergate 37 (Congressional Quarterly Inc. 2006).
[8] *Id.* at 117.
[9] United States V. Nixon, 418 U.S. 683 (1974).

House, which ultimately prompted President Nixon to resign.[10, 11] While the Nixon investigation and ultimate impeachment were key steps towards establishing regulated intelligence-gathering procedures, the Church Committee regarding the CIA's use of illegal wiretapping would ultimately be the force driving behind the creation of FISA.

On January 21, 1975, Senator John Pastore of Rhode Island introduced a resolution to discover "the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government."[12] After a near-unanimous vote, the United States Select Committee to Study Governmental Operations with Respect to Intelligence Agencies was established. The select committee was formed as a broader, more in-depth investigation to work in complement with President Gerald Ford's Rockefeller Commission, which was designed to "determine whether any domestic CIA activities exceeded the Agency's statutory authority" to spy on Americans.[13] Shortly after its passage, Senator Frank Church of Idaho became chairman and dubbed it the Church Committee.

From January 27, 1975, to April 29, 1976, the Church Committee published 14 documents: one interim report, seven volumes of public hearings, and six books. These documents covered a wide range of intelligence-related topics, but most importantly, uncovered blatant Fourth Amendment violations by agencies within the intelligence community.[14] While the investigation was underway, Senator Church appeared on *Meet the Press* for an interview concerning the investigation. Without giving away any compromising details, Senator Church candidly warned viewers that

> If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine

[10] James M. Naughton, *A Historic Charge*, New York Times (July 28, 1974), https://www.nytimes.com/1974/07/28/archives/a-historic-charge-two-more-article.html.
[11] James M. Naughton, *New Accusation*, New York Times (July 30, 1974), http://www.nytimes.com/1974/07/30/archives/new-accusation-nixon-is-charged-with-failure-to-uphold-nations-laws.html.
[12] S. Res. 21, 94th Cong. (1975).
[13] Exec. Order No. 11, 828, 40 Fed. Reg. 1219 (Jan. 4, 1975).
[14] S. Rep. No. 67-522, (1975), *see also* note 21.

> together in resistance to the government, no matter how privately it was done, is within the reach of the government to know.[15]

The Church Committee filed its final report eight months later, and after the release of their documents to the public, it became evident some law was required to both preserve the Fourth Amendment and the ethical intelligence collection conducted by the United States intelligence community.

In the aftermath of the Watergate Scandal and the revelations in the Church Committee's reports, lawmakers needed to develop a "comprehensive statutory procedure"[16] to ensure unethical intelligence gathering practices were put to a stop in the United States. Pressure was not only coming from the legislative and executive branches to find a solution, but the judicial as well. After the 1972 Supreme Court Case *United States v. United States District Court*, which overruled previous intelligence gathering procedures, the Court urged Congress to "provide a judicially-manageable standard applicable to electronic surveillances conducted for national security purposes"[17] Their request was finally heard in 1978 with the introduction of the Foreign Intelligence Surveillance Act.

Provisions of FISA

The goal of FISA at the time was simple, it was meant to "establish a statutory procedure that permits the government to conduct electronic surveillance."[18] The Act accomplishes this by establishing strict requirements for collecting foreign intelligence within the United States, laying out a strict application process for warrants, and establishing a specific court to review these applications. Though FISA's powers today have expanded beyond the original bill, the procedure to collect intelligence remains the same.

For electronic intelligence to be gathered from a target under FISA, a rigorous application process is required. First, a federal agent

[15] Frank Church, *The Intelligence Gathering Debate*, NBC Universal Archives (1975), https://www.youtube.com/watch?v=YAG1N4a84Dk.
[16] Scott J Glick, FISA's *Significant Purpose Requirement and the Government's Ability to Protect National Security*, 1 Harvard NSJ 88–111 (2010), http://harvardnsj.org/wp-content/uploads/2015/01/Vol.1_Glick_Final.pdf.
[17] McAdams, *supra* note 2, at 2.
[18] Glick, *supra* note 16.

needs to make the actual application, which requires the approval of the Attorney General. For the Attorney General to approve any application, it must include the following information in the application found in Section 104 of the Act: (1) the identity of the officer making the application, (2) the approval of the Attorney General to make the application, (3) the identity or the description of the target of the surveillance, (4) a statement of facts that lead the applicant to believe the target is an agent of the foreign power[19] and the facilities[20] named in the application are being used or about to be used by the target, (5) a statement of proposed minimization procedures,[21] (6) a detailed description of the type of information intended to be gathered and the type of activities subjected to the surveillance, (7) certification from a national security official appointed by the US president that certifies the purpose of the surveillance is to gather foreign intelligence and that the intelligence cannot be obtained by normal investigation techniques, (8) a statement of the means by which the surveillance will happen and whether physical entry is required to begin the surveillance process, (9) a statement of facts with all the previous applications involving the target or specific facilities in the application along with a statement explaining why another application is needed, (10) a statement saying how long the surveillance will take place, and (11) minimization procedures for any other electronic or physical devices being

[19] The term "agent of a foreign power" has two definitions in the Act. The first definition categorizes agents of a foreign as anyone who is not a United States citizen that acts in the United States as an officer or employee of a foreign power or acts on behalf of a foreign power who engages in clandestine within the United States. The second definition categorizes agents of a foreign power as anyone who knowingly engages in clandestine intelligence gathering for a foreign power which violate criminal statutes in the United States, knowingly engages in international terrorism or sabotage on behalf of a foreign power, or knowingly aides and abets anyone described by the act as an "agent of a foreign power." *See* 50 U.S.C. § 1801 (b) for clarification.

[20] An example of a facility would be a cell phone.

[21] To generalize, minimization procedures are specific procedures adopted for each particular investigation by the Attorney General minimize the "acquisition and retention, and prohibit the dissemination of nonpublicly available information concerning unconsenting United States citizens." The Attorney General adopts these minimization procedures and is required to report them to the House Permanent Select Committee on Intelligence at least 30 days prior to their effective date. *See* 50 U.S.C. § 1801(h) and 50 U.S.C. § 1802(a)(2) for clarification.

surveilled.[22] If the Attorney General finds all of these criteria are met, the application is then sent to the Foreign Intelligence Surveillance Court, otherwise known as FISC.

Due to its secretive proceedings and its role in the FISA warrant application process, FISC is a little-known judicial institution that is often far removed from the public eye. All documents handled by the court are top secret and are only released to the public after being heavily redacted, and the hearings themselves are closed to the public. The judges serving on the FISC are responsible for the final approval of the electronic surveillance, which then permits the surveillance requested in the warrant. The Chief Justice of the Supreme Court appoints seven district court judges to serve on the FISC; they "have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States."[23] In the event that a FISA application is denied, a special appellate court hears the application appeals. This appellate court is known as the Foreign Intelligence Surveillance Court of Review. The judges serving on the Court of Review are appointed by the Chief Justice of the Supreme Court and serve for a period of seven years.[24] According to subsection "c" of section 103 of FISA, "Proceedings under this Act shall be conducted as expeditiously as possible," meaning the judges serving on the court could hear FISA applications every day of the year, at any time of the day.[25] Due to the sensitive material contained in the FISA warrant applications, the proceedings of the court are kept secret, with security measures taken by the Chief Justice, Attorney General, and Director of Central Intelligence.[26]

For a FISA warrant application to be approved by the court, the judge reviewing the application must look to ensure certain criteria are met.[27] The judge must find that (1) the President has authorized the Attorney General to approve FISA applications, (2) the application is made by a federal officer and approved by the Attorney General, (3) there is probable cause the target of the surveillance is an agent of a foreign power, (4) the proposed minimization procedures meet the

[22] 50 U.S.C. § 1804 (a) (1982).
[23] 50 U.S.C §1803(a) (1982).
[24] 50 U.S.C § 1803(d) (1982).
[25] 50 U.S.C § 1803(c) (1982).
[26] *Id.*
[27] 50 U.S.C § 1805(a) (1982).

definition of minimization procedures under Section 101(h), and finally, (5) the application has all the statements and certifications required in section 104 of the Act. If these conditions are in fact met, "the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance."[28] The FISA warrant is then approved for either 90 days or until the electronic surveillance is completed, whichever comes first.[29] In the event that the desired intelligence is not gathered in the 90 days, an extension may be granted for up to one year by a FISA judge if he or she believes that the desired intelligence will be gathered in that time, that the agent complied with the proper minimization procedures, and that no intelligence concerning unconsenting American citizens has been "acquired, retained, or disseminated."[30]

There is only one way to bypass this thorough application process. In Section 105 of the Act, the Attorney General can issue an emergency FISA order so long as a FISC judge is informed of the emergency order by the Attorney General.[31] The emergency application is then required to be seen by a FISC judge within 24 hours.[32] The emergency application is then reviewed by the judge, and the application follows the same approval process as any other application.[33] If the application is denied, no evidence gathered during that time can be disclosed or used in a trial when prosecuting individuals. Since its passage into law, however, FISA's powers have gradually increased to encompass more forms of surveillance and have provided federal agents more leniency with their applications.

Expansion of Powers under FISA

The first amendment that expanded FISA's power came in 1994 with the Counterintelligence and Security Enhancements Act, which extended FISA to allow physical searches for foreign intelligence purposes.[34] In 1998 came the Intelligence Authorization Act for Fiscal Year

[28] *Id.*
[29] 50 U.S.C § 1805(d) (1982).
[30] 50 U.S.C § 1805 (d)(3) (1982).
[31] 50 U.S.C §1805 (e)(2) (1982).
[32] *Id.*
[33] *Id.*
[34] 50 U.S.C § 1822 (2012).

1999, which authorized the use of pen registers[35] and similar devices in foreign intelligence gathering and terrorism activities.[36] The Intelligence Authorization Act for Fiscal Year 2000 expanded the definition of an agent of a foreign power to include anyone who "knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power."[37] The Intelligence Authorization for Fiscal Year 2001 allowed the Attorney General to request the authorization for the electronic surveillance of a US citizen if they were deemed to be an agent of a foreign power as described under 50 U.S.C § 1801 (b)(2). The amendment also allowed the surveillance target's past activities to be taken into account when determining probable cause. These power expansions under FISA were gradual and took place over several years, but after the 9/11 attacks, FISA's power, role in the government, and access to people's personal information was greatly expanded.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, known by its more notable short name, the USA PATRIOT Act, was the first FISA amendment issued after 9/11. It was introduced in the House just six weeks after the attacks and was the largest amendment to FISA at the time. To summarize the 347-page document in a single sentence, professor of legal research Michael T. McCarthy states that the PATRIOT Act "grants additional wiretapping and surveillance authority to law enforcement and intelligence agencies, adds financial disclosure and reporting requirements to combat terrorist funding, and gives greater authority to the Attorney General to detain and deport aliens suspected of having terrorist ties."[38] Many provisions in the PATRIOT Act were supposed to "sunset"[39] in 2005, but were reauthorized in 2005.[40]

[35] A pen register is a device or process used to trace outgoing signals from a specific phone to their destination. The pen register merely does not provide any information on the data transmitted between the devices; it merely produces a list of the phone numbers accessed.
[36] 50 U.S.C § 1842.
[37] 50 U.S.C § 1801 (b)(2).
[38] Michael T. McCarthy, *USA Patriot Act*, 39 Harv. J. on Legis. 435, 454 (2002).
[39] A "sunset" is a specific time mentioned in a bill when the policies enacted will no longer be in effect. Removing the sunset clause means the policies enacted in the PATRIOT Act have no specific end time.
[40] USA PATRIOT Improvement and Reauthorization Act of 2005: Conference

The largest overhaul of the bill came in 2008 with the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. In this amendment, title VII of FISA is heavily amended, allowing the Attorney General and the Director of National Intelligence to authorize "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[41] To ensure that this new expansion of FISA is not abused in any way, the Act stipulates that all intelligence gathering must be conducted "in a manner consistent with the Fourth Amendment to the Constitution of the US."[42]

Controversy Concerning FISA

Even though great effort has been made to ensure intelligence gathering procedures in the United States are kept ethical and regulated with heavy oversight, FISA's procedures remain controversial and attract criticism from the American public. The first time the Act and its amendments came under great public scrutiny was during the passage of the PATRIOT Act. The act was pushed through Congress very quickly with little time to read the bill itself. This caught the attention of the ACLU, who claims the Act violates the Constitution by restricting the Fourth and First Amendments.[43] Even with these claims, there have been few Supreme Court cases questioning the constitutionality of FISA. There have been three notable court cases concerning FISA's constitutionality. In two cases, FISA's authority was left unquestioned, but one case, ruled on by the FISC Court of Review, limited some of FISA's power in relation to the US president's, stating,

> [A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.[44]

Report (to accompany H.R. 3199), Congress.gov (2005), https://www.congress.gov/congressional-report/109th-congress/house-report/333/1?overview=closed.

[41] 50 U.S.C § 1881(a) (2012).

[42] 50 U.S.C § 1881(b)(5) (2012).

[43] *Surveillance Under the USA/PATRIOT Act,* American Civil Liberties Union, https://www.aclu.org/other/surveillance-under-usapatriot-act.

[44] *In Re: Sealed Case,* 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

FISA's constitutionality is not its only controversy. In 2013, former NSA contractor Edward Snowden revealed the NSA was collecting phone records from millions of Americans.[45] Along with this revelation, Snowden also released thousands of classified documents, which some called the most important leak in the history of the United States.[46] To those in the intelligence community, however, the leak was absolutely disastrous. It showed how the United States gathered vital intelligence that helps to protect Americans. General Michael Hayden, the former Director of the CIA, weighed in, calling Snowden, "an incredibly naïve, hopelessly narcissistic and insufferably self-important defector."[47] Since the leaks, Snowden has lived in Russia as an exile, with no hopes of returning to the United States.

Another criticism of FISA is the Foreign Intelligence Surveillance Court. Some scholars cite the Court as a rubber stamp court and a mere formality in the FISA application process.[48] Of the 34,000 FISA applications filed by the government, fewer than 20 have been denied, giving the Court a near 100% rate of approval.[49] Since this revelation in 2013, Congress sought to create reform in the Court by introducing reform bills, though they never saw a vote.[50]

FISA was at the center of a more recent, more troubling, issue. On February 2, of this year, House telligence Committee Chairman Devin Nunes released a memorandum titled "Foreign Intelligence Surveillance Act Abuses at the Department of Justice and the Federal Bureau of Investigation." The memo, as the title suggests, brought to light

[45] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily,* The Guardian (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[46] Daniel Ellsberg, *Edward Snowden, Saving Us From the United Stasi of America.* The Guardian (June 10, 2013), https://www.theguardian.com/commentisfree/2013/jun/10/edward-snowden-united-stasi-america.
[47] Jason Murdock, *Edward Snowden is a "Naïve, Narcissistic and Insufferably Self-Important Defector", Claims Former NSA Boss*, International Business Times (Feb 24, 2016), http://www.ibtimes.co.uk/edward-snowden-naive-narcissistic-insufferably-self-important-defector-claims-former-nsa-1545685.
[48] Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?,* 66 Stan. L. Rev. Online 125 (2014), https://www.stanfordlawreview.org/online/is-the-foreign-intelligence-surveillance-court-really-a-rubber-stamp/..
[49] *Id.*
[50] Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. (2013).

serious abuses of FISA in order to collect intelligence on a perceived agent of a foreign power. Some suspect political motivation behind the misconduct affecting the FISA process, but the memo does not necessarily confirm these allegations. Ultimately, this memo was not as big a story as many made it out to be and did not directly hurt national security interests. It did, however, destroy much of the confidence Americans had in the United States' intelligence gathering practices, which could have potential ramifications in the future.

Conclusion

FISA and its provisions have changed to meet the security threats faced by the United States as they have appeared. The additions of new law and the expansion of FISA powers has been controversial, causing many provisions in the Act and its amendments to come under public scrutiny, prompting lawmakers to take a closer look at the Act. FISA currently sits at a rather worrisome intersection between national security and personal privacy. National security is a top priority, especially in an age where the world stage is constantly changing at a very rapid pace. It is vital for the United States government to protect its interests in this era of uncertainty, justifying its need to surveille potentially harmful foreign agents of states who wish to do America harm. However, the rights of private citizens must be respected, and agencies that are gathering intelligence are required to respect citizens' privacy when conducting their surveillance.

In FISA, the minimization procedures mentioned in Section 101 provide some reassurance that their personal information will not be collected by the United States, but if a citizen desires to find out what minimization procedures various intelligence agencies have adopted, they will be met with disappointment. Current minimization procedures adopted by the Attorney General and intelligence agencies are not publicly available and are only available once they are no longer deemed top secret, meaning a current, meticulous analysis of how the government protects American privacy rights is unavailable. However, if minimization procedures were removed and not replaced, the intelligence community could theoretically spy on any person regardless of their actual threat level to the United States. This dilemma is very concerning, and it seems as though no progress has been made to finding a solution.

There is no simple answer to the best methods of intelligence-gathering regulation. The United States has a right to protect itself from foreign threats coordinating outside of and operating within its borders. However, the government has no business surveilling law-abiding Americans. These are some of the reasons that FISA was established. Removing the law would take intelligence-gathering regulations back to the laws of the 1970s, which would result in a nearly immediate and unavoidable constitutional crisis between the American public and the intelligence community. FISA, regardless of how controversial it may be, is an integral part of American Intelligence Law that must remain current with the issues facing American intelligence agencies. It not only aims to protect American citizens from political surveillance and abuse but ensures that American sovereignty is protected. The Foreign Intelligence Surveillance Act is here to stay, and the procedures it outlines will remain at the core of American foreign intelligence-gathering practices.

When Weapons Cross the Sea: The Long Connection Between Colonel Gaddafi and the Provisional IRA

Monica English

The Provisional Irish Republican Army (pIRA) led a violent paramilitary campaign in Great Britain and Northern Ireland from 1969 until 1997. The destruction and carnage of this campaign was escalated through the donation of money and arms from Colonel Muammar Gaddafi, dictator of Libya.[1] In this essay, I will outline the connection between the pIRA and Colonel Gaddafi of Libya, place the moments of connection between these organizations within the greater events in each country, show how common animosity for Great Britain and other post-colonial powers lead the pIRA and Gaddafi to be natural allies, present the depth and the breadth of the goods that flowed into the pIRA's hands, and highlight the impact these goods have had on their destructive capacity.

At 27, Muammar Gaddafi came to power in September 1969 following a bloodless coup that ousted the current King Idris;[2] 1969 also marked the year in which the pIRA came into existence following the split of the Irish Republican Army (IRA). The origins of the IRA can be traced to Catholic nationalism in the early 1900s. IRA members were considered terrorists in many circles because of their violent tactics used to oppose British rule in Ireland. In 1969, the IRA splintered

[1] Guy Arnold, author of *The Maverick State* (*see* note 2), says that there are "600 ways of spelling Gaddafi's name." While I might challenge the number being that high, I have spent a frustrating number of time searching for documents which use at least a dozen different spellings. I choose to use the spelling Gaddafi unless I am quoting a source and then I will retain the original spelling.

[2] Guy Arnold, The Maverick State: Gaddafi and the New World Order 2 (Cassell 1997).

into two groups, the Original IRA, which opposed violence, and the pIRA, which believed in continuing an armed struggle against the British.[3] While the Original IRA was to completely disband three years later, the pIRA would continue actively opposing British presence in Northern Ireland for another three and a half decades. Gaddafi and the pIRA both chafed at the British presence in their homelands and in many ways were natural allies.

Gaddafi's anti-imperialist, anti-Western views developed early in life. His boyhood hero was Omar Mukhtar, the Libyan who led the 1920s resistance against Italy's brutal colonization of Libya. He also idolized Egypt's Gamel Abdel Nasser, who led the overthrow of the Egyptian monarchy and later wrested control of the Suez Canal away from Britain.

Following the 1969 coup, Gaddafi was appointed chairman of the Revolutionary Command Council, which was the prime governing instrument of the new government. Gaddafi immediately set about ridding Libya of all possible colonial influences by insisting that the US and Great Britain vacate their military bases and driving out most of the Italians who had settled in Libya during times of colonization.[4] Gaddafi quickly developed three broad political principles: first, to curtail Western involvement in Libya; second, to move towards Arab unity, and third, to oppose Israel.[5]

The pIRA in Northern Ireland did not have the luxury of demanding a withdrawal of British influence from their homeland. The 1969 faction split that saw the birth of the pIRA came at a time when conflict between the Catholic/Nationalist/Republican (CNR) community and the Protestant/Unionist/Loyalist (PUL) was heating up. The CNR community, after being inspired by the successful nonviolent human rights movements in India and the United States, organized marches to bring illumination to the discrimination being suffered by their community. The main complaints were against gerrymandering, housing discrimination and employment discrimination. The first civil rights march took place in 1968 and participants were batoned by

[3] David McKittrick and David McVea, Making Sense of the Troubles: A History of the Northern Ireland Conflict 254 (Viking 2012).
[4] Arnold, *supra* note 2, at 1-3.
[5] McKittrick and McVea, *supra* note 3.

police resulting in 77 injured civilians.[6] Riots broke out regularly; residents of Londonderry put up barricades and denied police entry into "Free Derry." Five hundred British troops were sent to Northern Ireland, where they were deployed to the streets of Belfast and Derry. Among other heavy-handed tactics, they deployed over 1,000 canisters of CS gas (tear gas) in residential areas.[7]

In 1971, the British enacted the policy of internment which gave the army the power to arrest and detain people without reason or trial. In the first two days of internment, 342 people, all Catholic/Republican, were arrested and taken to makeshift camps. Internment lasted for the next four years, during which close to 1,981 people were detained, all but 107 of whom were Catholic/Republican. Membership in the pIRA mushroomed as anger over unexplained arrests continued while the pIRA's shooting and bombing offensive against Great Britain and British players in Northern Ireland began.[8] At this point in history, the pIRA's access to weapons was mostly limited to WWII-era devices, a range of handguns, and a variety of firearms smuggled in from sympathetic sources in the United States. Explosives were made of rudimentary materials, usually fertilizer bombs. As the conflict escalated, the need for more modern weaponry increased.

Because of their strong anti-imperialist stance and strategy of armed struggle against the British Government, the pIRA sought other militant separatist groups with similar views. They made connections with groups such as Basque Euskadi Ta Askatasuna (ETA) in Spain, the Palestinian Liberation Organization (PLO), and Front de Libération de la Bretagne (FLB) in France. In February of 1974, there was a strong enough relationship between ETA, FLB, and the pIRA that together, they signed the Charter of Brest.[9] The Charter stated they were "aware of the universal character of imperialism and the extreme gravity of the situation in their countries by the continuance of the resulting colonial system, solemnly declare the need for a union between the

[6] Martin Melaugh, *The Civil Rights Campaign: A Chronology of Main Events,* CAIN, http://cain.ulst.ac.uk/events/crights/chron.htm.

[7] Ed Moloney, A Secret History of the IRA 356 (Penguin 2007).

[8] Martin Melaugh, *Internment: A Chronology of the Main Events*, CAIN, http://cain.ulst.ac.uk/events/intern/chron.htm.

[9] Michael McKinley, *Of "Alien Influences": Accounting and Discounting for the International Contacts of the Provisional Irish Republican Army*, 11 Journal of Conflict Studies 7, 7–35 (1991).

oppressed peoples of Europe."[10] It would be the Front de Libération de la Bretagne, a militant separatist group in France, that first connected the pIRA with the Libyan regime of Gaddafi in 1972.[11]

Gaddafi gained respect for the pIRA after seeing Joe Cahill, a prominement leader of the pIRA, at a press conference in Belfast during the internment swoops. Cahill had been instrumental in the founding of the pIRA even though Cahill, as a top member of the pIRA, was high on the list of wanted men, he managed to slip into the conference, speak in front of the international press corps, and slip out without capture. The audacity of that appearance boosted the morale of the pIRA and garnered the interest of Libyan officials.[12]

Gaddafi knew very little about the political situation in Northern Ireland or the campaign of the pIRA. He knew they were dissidents who targeted the British, but he did not have an understanding of the complex relationships among the people within Northern Ireland itself. Gaddafi had begun funding groups he considered anti-imperialist around the globe. His goal in supporting the pIRA was less about Northern Ireland and more about challenging and harming Britain for its colonial actions of the past and its imperialist actions of the current time.[13]

Wealth acquired from oil gave Gaddafi the ability to fund movements around the globe that he considered anti-imperialist. At the time Gaddafi came to power, Libya supplied more than 25 percent of Western Europe's oil and was the world's fifth-largest oil-producing country.[14] In 1970, less than a year after Gaddafi's rise to power, the government put pressures on the oil companies to accept higher taxes. Negotiations were fierce, and most of the cards were in Libya's hands. On the first anniversary of the coup in the middle of negotiations, Gaddafi announced, "The people who have lived for 5,000 years without petroleum are also able to live without petroleum for decades in

[10] Devashree Gupta, *The Role of Licit and Illicit Transnational Networks During the Troubles*, University Press Scholarship Online, doi:10.7228/manchester/9781784995287.003.0006.
[11] *Id.*
[12] Sean Boyne, Gunrunners: The Covert Arms Trail to Ireland 146-47 (OBrien 2006).
[13] Louise Richardson, *Terrorists as transnational actors,* 11 Terrorism and Political Violence, 209, 209-19 (1999), doi:10.1080/09546559908427541.
[14] Arnold, *supra* note 2, at 43.

order to achieve their legitimate rights."[15] In addition to negotiating new deals with oil producers, Libya also nationalized foreign oil importing and marketing organizations. The influx of wealth from the oil industry gave Gaddafi resources and power to support revolutionary movements he saw worthy.

On June 11, 1972, Gaddafi made his first public declaration of support for the pIRA on Libyan Radio. During a celebration marking the anniversary of the evacuation of the United States from the Wheelus military base in Tripoli, Gaddafi said:

> We support the revolutionaries of Ireland who oppose Britain and who are motivated by nationalism and religion. The Libyan Arab Republic has stood by the revolutionaries of Ireland. It maintains strong links with the Irish revolutionaries. There are arms and there is support for the revolutionaries of Ireland. . . . We have decided to move to the offensive. We have decided to fight Britain in her own home. We have decided to create a problem for Britain and to drive a thorn in her side so as to make life difficult for Britain. . . . She will pay a double price. She will pay dearly. We will give her two blows for one received.[16]

In 1972, members of the pIRA's Army Council met representatives of the Libyan Foreign Ministry in Poland. At this meeting, it was suggested that the pIRA send representatives to Tripoli, where they would receive semi-diplomatic status. Eddie O'Donnell, who was known as Mister Eddie to his Libyan handlers, was the first envoy for the pIRA. Mister Eddie was housed in an opulent Italianesque villa in Tripoli's embassy district, given a generous weekly wage, and provided with every luxury imaginable.[17]

The next three years saw more than $3.5 million make its way from Libya, through City of London Banks, to the pIRA's treasuries.[18] It is quite likely that several arms shipments made their way from Libya to Northern Ireland during this time, although only two shipments are verifiable. The first was a small number of rocket launchers

[15] *Id.* at 42.
[16] United Kingdom, *Qadhafi and Irish Terrorism.* Foreign and Commonwealth Office, 1, 1-2 (1986), http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=476387.
[17] Moloney, *supra* note 7, at 9–10.
[18] *Id.*

flown in on a small aircraft, and the second was five tons of arms transported by sea.[19, 20]

Gaddafi offered a large shipment of arms to the pIRA with the stipulation that they had to arrange for the transport themselves. A contact in the illicit arms trade, Gunther Leinhauser, owned a 298-ton coaster called the *Claudia*, which they procured for the operation.[21] The *Claudia* was loaded during nighttime hours in Tripoli harbor by members of the Libyan armed forces.[22] The cargo included 243 revolvers, 247 AKM rifles, 24,000 rounds of ammunition, 97 anti-tank mines, 500 grenades, 48 pounds of high explosives, and 660 pounds of gelignite (blasting gelatin).[23]

The *Claudia* made its way from Tripoli to the coast of Ireland. Just before reaching the Irish coast on March 28, 1973, the *Claudia* was intercepted by Irish naval personnel. The Irishmen aboard, including Joe Cahill, were arrested and taken into custody. The *Claudia* was taken to a naval base in Cork harbor, where soldiers unloaded the cargo, examined the weaponry, and drew up an inventory. As soon as the process was complete, the skipper and crew were allowed to sail away on the *Claudia*. It is suspected that the reason Leinhauser and his crew were not detained is that they were part of a sting operation, cooperating with Irish officials.[24]

On December 9, 1973, Edward Heath, Prime Minister of Great Britain; Liam Cosgrove, the Taoiseach[25] of Ireland; and representatives from political parties from both sides of the political divide joined to sign into law the first attempt at power sharing within the Executive branch of Northern Ireland. The implementation of the power-sharing executive drew ire from much of the Unionist community.[26] A general strike was called by Ulster Worker's Council, a Unionist organization that was opposed to the sharing of power with Irish Nationalists and the proposed role for the Republic of Ireland in governing Northern

[19] Exposure: Gaddafi and the IRA (PBS 2011).
[20] Boyne, *supra* note 12, at 432.
[21] *Id.* at 144.
[22] *Id.* at 149.
[23] *Id.* at 433.
[24] *Id.* at 151.
[25] Elected leader of Ireland.
[26] Dr Martin Melaugh, *Ulster Workers' Council Strike - Summary of Main Events*, CAIN, http://cain.ulst.ac.uk/events/uwc/sum.htm.

Ireland. The strike lasted for two weeks and brought on power outages due to striking workers in electricity-generating plants. This lack of power shut down factories and brought industries crucial to Northern Ireland's economy to a standstill. Road blocks were set up to keep workers from their places of employment through inconvenience and intimidation. Under this economic, political, and social pressure, the Stormont executive was abolished, and Great Britain imposed direct rule on Northern Ireland.[27]

Gaddafi expressed admiration for the strike organized by the Ulster Worker's Council. Clearly he did not understand that the Unionists of the Ulster Worker's Council and the Republicans of the pIRA were on opposing sides. Gaddafi then invited members of the Ulster Defense Association (UDA), a unionist paramilitary, to Libya to discuss providing them with arms.[28] There is no evidence of arms provided, but the UDA did have a chance to plead their case as foes of the pIRA. This conflicting narrative of the conflict in Northern Ireland muddied the waters for Gaddafi on the Irish issue.[29] Whether the cause was the loss of weapons aboard the *Claudia* or the visit by the UDA (or another reason that has not come to light), the relationship with Gaddafi cooled for the next several years. Gaddafi went so far as to state in a *Newsweek* interview in 1976 that he had "finished with the IRA" and that his relations with London and Dublin were improving.[30]

The pIRA prisoners garnered international headlines during hunger strikes in 1981. The "Troubles," a euphemistic term for the political violence of the day, were in full swing in the 1970s. From 1972 until 1976, all prisoners convicted of "Troubles"-related crimes were given special political status in prison. Having political status allowed the prisoners to wear their own clothes instead of the prison uniforms, receive extra visits, and be housed with fellow paramilitary prisoners. This status was removed in 1976 and sparked a variety of protests in the prison population over the next six years. The culmination of these protests was a series of hunger strikes in 1981 that ended in the starvation deaths of ten prisoners.

The starvation deaths during the hunger strikes were covered by

[27] McKittrick and McVea, *supra* note 3, at 103.
[28] Boyne, *supra* note 12, at 282.
[29] United Kingdom, *supra* note 16, at 3.
[30] Arnold, *supra* note 2, at 110.

news outlets worldwide. Even though Gaddafi and the pIRA had not been in contact since the mid-1970s, he became aware of the hunger strikes due to the extensive news coverage of the events, and his interest was once again piqued. In 1981, Gaddafi wrote a letter to the UN Secretary General, Dr. Kurt Waldheim, urging the UN to intervene. He compared the deaths to ancient sacrifice and accused Great Britain of lacking humanity. He said that the hunger strikes were a "very painful human tragedy, a tragedy that should have shocked the conscience of the entire world." He went on to say, "These men should be granted a political status in view of the fact that they are indeed fighting for a just and sacred cause, the freedom of their nation, which is one of the world's smallest, but which still has its place under the sun, free as God created it."[31]

Relations between Libya and Great Britain took a significant turn for the worse three years later in 1984, when Gaddafi started employing the tactic of assassinating Libya's exiles in foreign countries. Early in 1984, a series of bombs attacks occurred in London and Manchester neighborhoods that housed communities of Libyan exiles. These were widely suspected of being orchestrated by Gaddafi's regime although Libya strongly denied involvement.[32] These acts of aggression led to demonstrations outside the Libyan's People's Bureau (Libyan Embassy) in London. During one of these demonstrations on April 17, automatic gunfire from one of the embassy's windows hit and killed a 25-year-old constable who had been policing the anti-Gaddafi protests.[33] British police placed the embassy under a state of siege; in retaliation, Libyan police and demonstrators surrounded the British Embassy in Tripoli.[34] The siege continued for 11 days. Negotiations brought Great Britain to cut off all diplomatic ties with Libya, after which the 30 Libyans within the embassy were driven to the airport and put on a flight back

[31] Ed Carty, *Gaddafi Urged UN Chief to Halt Hunger Strike,* Irish Examiner (Dec. 30, 2011), http://www.irishexaminer.com/ireland/gaddafi-urged-un-chief-to-halt-hunger-strike-178541.html.
[32] Yehudit Ronen, *Libya's Conflict with Britain: Analysis of a Diplomatic Rupture,* 42 Middle Eastern Studies 271, 273 (2006), doi:10.1080/00263200500417645, 273.
[33] United Kingdom, *supra* note 16, at 5.
[34] R. and Special to the New York Times, *Libyans Permit Britons to Leave Tripoli Embassy*, The New York Times (Apr. 18, 1984), http://www.nytimes.com/1984/04/19/world/libyans-permit-britons-to-leave-tripoli-embassy.html?pagewanted=all.

to Libya, and British Embassy workers were expelled from Tripoli.[35]

According to the Libyans, the incident was a terrorist attack. On the day that Great Britain broke off diplomatic relations with Libya, an official broadcast from The Voice of the Arab Homeland said:

> The people's committee will form an alliance with the secret IRA in view of the fact that it champions the cause of liberating Ireland and liberating the Irish nation from the tyranny of British colonialism. The people's committee will open branches for the secret IRA in all Libyan towns, and if Britain tries to use any means to pressurize and oppress Libyan Arabs, the revolutionary committee will enable the IRA to do whatever it wishes in Britain and retaliate twice as strongly.[36]

Around this time, Gaddafi started to once again provide arms and money to the IRA. There is a frustrating lack of consensus about many of the facts surrounding the connections between Gaddafi and the pIRA in the 1980s. What can be ascertained is that at least four shipments of arms successfully made it from Libya to Northern Ireland. The first brought seven tons of arms, the second ten tons, the third 14 tons, and the fourth a much larger shipment of 105 tons.[37] Each of these shipments happened in basically the same way: the skipper, Adrian Hopkins, would sail to Malta, where the pIRA crew would be waiting. They made their way to a predetermined point out at sea where they would meet a Libyan vessel, whose crew would transfer the cargo to the pIRA vessel.[38]

The largest shipment of arms was planned for October 1987. This shipment would be as large as all four previous shipments combined and as such would require a different protocol. In mid-October, a 50-year-old Panamanian vessel, *MV Eksund,* was loaded with arms by Libyan soldiers using a crane under the watchful eyes of top pIRA operatives. The ship was loaded in the dark of night on the docks of Tripoli. A massive 150 tons of cargo were brought on board. The haul included 1,000 AKM rifles, 10 heavy machine guns, 600 hand grenades, 50 tons of ammunition, several rocket launchers and rockets, mortars,

[35] Moloney, *supra* note 7, at 13.
[36] United Kingdom, *supra* note 16, at 5.
[37] Boyne, *supra* note 12, at 273.
[38] Moloney, *supra* note 7, at 19.

20 surface-to-air missiles, and more than two tons of Semtex explosives.[39] This shipment, unlike the four before, would not make it into the hands of the pIRA.

Two weeks into her journey, the *MV Eksund's* steering mechanism failed. Repairs were hastily attempted, but the Eksund drifted into French Territorial waters in the Bay of Biscay.[40] The boat was spotted, surrounded, and boarded by French customs men. Within hours, the news broke and sent shockwaves through Ireland and Britain. This shipment and the knowledge that successful shipments had already made their way into the hands of the pIRA were devastating blows to the government and security forces of Ireland and Britain.[41]

The capture of the *MV Eksund* seemingly ended the connection between the pIRA and Gaddafi, but the destruction using the weapons that had been transferred would continue to wreak havoc for the next 30 years. According to a report by the Northern Ireland Affairs Committee of the House of Commons, "There is no doubt that the weapons, funding, training and explosives that Colonel Gaddafi provided to the Provisional IRA over the course of 25 years both extended and exacerbated the Northern Ireland 'Troubles' and caused enormous human suffering."[42] Another UK government report states, "The supply of Semtex greatly enhanced, with deadly effects, the Provisional IRA's bombing campaign from the late 1980s."[43]

From the 1980s onward, almost every bomb attack the pIRA carried out incorporated Libyan Semtex, an odorless explosive that does not explode even when exposed to a naked flame. Semtex, when used with a detonator, can produce a blast many times more powerful than a fertilizer-based explosive and increases destructive capacity exponentially. Some of the most well-known bomb attacks that incorporated Libyan Semtex are the 1983 Harrod's bombing, which utilized a car

[39] *Id.* at 436.
[40] *Id.* at 4.
[41] *Eksund Arms Find: Statement,* Houses of the Oireachtas 374 (Nov. 5, 1987), http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/ takes/dail1987110500004?opendocument.
[42] Great Britain, *HM Government Support for UK victims of IRA Attacks That Used Gaddafi-Supplied Semtex and Weapons: Government Response to the Committee's Fourth Report of Session 2016-17,* www.parliament.uk (Sep. 14, 2017), https://publications.parliament.uk/pa/cm201719/cmselect/cmniaf/331/33102.htm.
[43] *Id.*

bomb outside Harrod's department store during Christmas shopping season, killing six, injuring 75, and doing extensive damage; the 1984 Brighton Hotel Bomb, where Prime Minister Margaret Thatcher and her cabinet were staying during a Conservative Party conference, five were killed; the 1987 Enniskillen bombing in which eleven mourners were killed at a memorial service; the 1993 Baltic Exchange bomb in 1993, which killed three, injured 91, and caused more than a billion dollars in damage; the 1996 Manchester bomb, at 3,300 pounds, the largest bomb to explode in Great Britain since WWII, which did not kill anyone but did cause $917 million in damage.[44, 45, 46, 47]

When each of these bombings occurred, many assumed the only actors were the pIRA of Northern Ireland and Great Britain. In each of these devastating explosions there was another strategy also in play. Gifts of Libyan Semtex, as well as arms and funds, were presented by Gaddafi with the express purpose to harm Great Britain; that purpose was actualized.

The long connection between Gaddafi from Libya and the pIRA highlights one transnational connection between international terrorist actors. The collaboration, transfer of arms, and gifts of funds drastically changed the Northern Ireland conflict. While it is common for scholars and journalists to simplify this conflict into a straightforward standoff between the pIRA and Great Britain, the Libyan connection creates a more complex narrative and challenges scholars to consider transnational connections in other conflicts around the globe.

---

[44] *IRA's City of London Bomb Aimed for Financial Impact*, The Christian Science Monitor (Apr. 27, 1993), https://www.csmonitor.com/1993/0427/27082.html.
[45] *BBC ON THIS DAY | 12 | 1984: Tory Cabinet in Brighton Bomb Blast*, BBC News (Oct. 12, 1984), http://news.bbc.co.uk/onthisday/hi/dates/stories/october/12/newsid_2531000/2531583.stm.
[46] David Cutler and London Editorial Reference Unit, *Timeline - Worst IRA Bomb Attacks on Mainland Britain*, Reuters (May 16, 2011), https://uk.reuters.com/article/uk-britain-security-bombings/timeline-worst-ira-bomb-attacks-on-mainland-britain-idUKTRE74F31Q20110516.
[47] Adam Taylor, *Analysis | Two Bombings in Manchester, 21 Years Apart, Show The Changing Nature of Terrorism*, The Washington Post (May 23, 2017), https://www.washingtonpost.com/news/worldviews/wp/2017/05/23/two-bombings-in-manchester-21-years-apart-show-the-changing-nature-of-terrorism/?utm_term=.0f503691b03c.

The Cultural Effects of ISIS

Quinn McCloskey

On September 11, 2001, tragedy struck in the United States. A terrorist group known as Al-Qaeda carried out simultaneous attacks across the east coast, killing thousands, wounding thousands more, and shocking an entire country. This tragic event and the extended war that followed had a significant impact on many aspects of the culture of the United States. There were major changes in US law regarding international security and federal surveillance powers, new considerations by voters and candidates in the political arena during presidential elections, a rise in Islamophobia in the US affecting Muslim Americans, and a clear shift in the subjects of popular entertainment media such as movies, TV shows, and video games.

In more recent years, a new terrorist threat has emerged. An Al-Qaeda splinter group known as the Islamic State in Iraq and Syria, or ISIS, has drawn global attention with attacks being carried out in their name all around the world. ISIS has never carried out an attack of the same scale as those carried out by Al-Qaeda on September 11th, but they have expanded so rapidly with highly successful recruiting and the occupation of a large amount of territory that they have prompted a response from the US military. There is no doubt that ISIS has had an impact on the countries that they have occupied and those who have taken in a large number of refugees from occupied territories, but have they had an effect on US culture, and if so, has it been the same level of change that was caused by Al-Qaeda? To compare these two groups and their influence we will first look at the changes made to US law in response to each.

Policy Response

In direct response to the September 11th attacks, Congress enacted the USA PATRIOT Act,[1] which was signed into law by US President George W. Bush on October 26, 2001.[2] In his speech given during the signing, the President referenced both the September 11th attacks and the anthrax attacks on postal facilities, stating that the purpose of the act was that "terrorists must be pursued, they must be defeated, and they must be brought to justice."[3]

More specifically, the USA PATRIOT Act made four changes to the laws governing our law enforcement organizations: permission for counterterrorism investigations to use methods that were already in use by other law enforcement agencies; vast improvements in information sharing requirements between agencies; an update of warrant procedures; and increased penalties for those involved in terrorism.[4]

Although this is a fairly broad generalization of the content of the act, these general permissions were initially a broadly accepted reaction to the attacks on September 11th, but over the next several years they became the center of a great deal of controversy. Privacy concerns and fear of overreaching governmental access to information eventually led to many additional protections for US citizens being added in the USA PATRIOT Improvement and Reauthorization Act of 2005,[5] but the original permissions given in the Act still remain a major part of counterterrorism efforts in the US.

A much more controversial reaction to the September 11th attacks was revealed in a *New York Times* article released on December 16, 2005. The article, titled "Bush Lets U.S. Spy on Callers Without Courts," exposed a secret presidential order that allowed the National Security Agency to conduct limited wiretapping operations on United States

---

[1] USA PATRIOT is an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."
[2] Office of the Press Secretary, *President Signs Anti-Terrorism Bill,* White House, https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011026-5.html.
[3] *Id.*
[4] *The USA PATRIOT Act: Preserving Life and Liberty*, Justice Dept., https://www.justice.gov/archive/ll/highlights.htm.
[5] F. James Sensenbrenner, *H.R.3199–USA PATRIOT Improvement and Reauthorization Act of 2005*, 109th Cong. (Mar. 9, 2006).

citizens without the need to obtain a warrant.[6] Regardless of the outrage that this caused, the exposure eventually led to the passing of the FISA Amendments Act of 2008, which both legalized and regulated many of the activities that were conducted in the previous years.[7]

These are two major examples among many that have been legislated in reaction to the war with Al-Qaeda, and they are also controversies that have been a persistent topic of conflict between the rights of the public and the power of the federal government. So what major legal changes have we seen since the US committed to combating ISIS in late 2014 that can be seen as a reaction to the new threat?

The most direct comparison is the creation of the USA Freedom Act that was signed on June 3, 2015,[8] an act that was a direct response to the expiration of multiple parts of the USA PATRIOT Act, which had expired the day before. The act restored most of the provisions of those expired parts, with a few adjustments. The majority of the changes that were made were done for the sake of civil liberties, creating limits found in new controls and reporting requirements for federal surveillance operations.[9] This suggests that, although ISIS can easily be seen as a more dangerous organization in terms of scope and wealth, the parties concerned with the creation of this act do not consider ISIS to have the same level of influence and communication presence in the domestic United States that Al-Qaeda possessed during the creation of the USA PATRIOT Act.

There was at least one extension of federal surveillance power that was given as a result of the Freedom Act. Section 701 of Title VII in the Freedom Act allows surveillance to continue on non-US-citizen targets believed to be involved in terrorist activity to continue for a period of 72 hours after they are believed to have entered U.S. territory, instead of requiring all surveillance to stop until a warrant is issued.[10] This change indicates that, although ISIS may not be considered to have the same existing physical presence in the United States as

[6] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, New York Times (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

7 H.R. 6304: FISA Amendments Act of 2008, 110th Cong. (July 9, 2008).

[8] H.R. 2048: USA FREEDOM Act of 2015, 114th Cong. (June 3, 2015).

[9] USA Freedom Act, House Judiciary Committee, https://judiciary.house.gov/issue/usa-freedom-act/.

[10] H.R. 2048: USA FREEDOM Act of 2015, 114th Cong. (June 3, 2015).

Al-Qaeda, there is a greater worry that ISIS will attempt to insert their agents into the United States in the coming years.

This is the only major extension of US domestic law that seems to be directly related to the conflict with ISIS. However, there was a small but important change made in regards to international law. In the article titled "How the War Against ISIS Changed International Law," Michael P. Scharf, the Dean and Director of the Frederick K.Cox International Law Center, explains the background and reasoning for UN Security Council Resolution 2249, which was seen as the legal permission to commence attacks on ISIS in Syria.[11] In the article, Scharf explains that the change will likely be a permanent result of this Resolution: "that use of force in self-defense is now permissible against 'nonstate actors' such as terrorists when the territorial state is unable to suppress the threat that they pose."[12]

Although UN Security Council Resolution 1386, adopted on December 20, 2001,[13] essentially granted the same permission for the War in Afghanistan, there was consistent criticism and debate over whether it should have passed because it violated the sovereignty of the Afghan government, which did not give permission to the United States to use force in their territory. This reasoning initially prevented Resolution 2249 from being adopted, as Syria similarly refused to grant permission for use of force in their territory. However, following the attacks conducted by ISIS around the globe, the Resolution passed, which essentially legalized the use of self-defense against non-state actors in another country if the host country cannot or will not act.[14]

Although it has been less than three years since the US became involved in the war with ISIS, we can see that they have already had an impact on our legal system, but since they are perceived to be a different kind of threat, the reaction has happened in different areas. The attacks on September 11th caused a domestic panic and a reaction in the federal system, but since the ISIS threat is seen as being primarily located outside US territory, the reaction has been almost exclusively related to international law.

---

[11] Michael Scharf, *ISIS Has Changed International Law*, The Conversation (Apr. 28, 2017), http://theconversation.com/isis-has-changed-international-law-56781.
[12] *Id.*
[13] Res. 1386, Security Council Report (2001).
[14] Scharf, *supra* at note 11.

Political Reactions

The changes in the law and the reasons for those changes have been clear, but along with these changes came a new platform for US presidential candidates to use to try and win the minds of their potential voters. Although the exact reasons for the success or failure of any US presidential election are largely left to speculation, there can be no doubt that the aftermath of 9/11 was a consistent part of voter considerations in the following elections.

Immediately after 9/11 it was clear that US citizens from both major political parties were united in our fight against terrorism and the Al-Qaeda threat. According to Gallup polls, President George W. Bush reached a 90% approval rating immediately after the attacks on September 11th,[15] reinforcing the notion that the American public fully supported the decisions to go to war in Afghanistan. However, after the war in Iraq began in 2003, the president saw a sharp decline in public support, which put his potential reelection in the following year at risk.[16]

An article written by Christopher Preble, the director of foreign policy studies at the Cato Institute, suggests that regardless of all the negative attention that President Bush's war in Iraq had brought down on him, he still managed to use this counterterrorism sentiment and "convinced a majority of voters that the war in Iraq was directly tied to the war on terrorism.[17] Meanwhile, Senator Kerry's campaign failed to detail how his strategy, both in Iraq and on terrorism more generally, would constitute a vast improvement over the current state of affairs."[18] Even though President Bush had clearly lost popularity, the American public still decided that his stance on terrorism was desirable enough to overshadow his faults.

Another Gallup poll conducted in 2006 demonstrated the divide of opinions about the Iraq war that existed among the Democratic and Republican parties, with 68% of Republicans stating that they still had at least a somewhat favorable view of the war in Iraq, and a staggering

---

[15] *Presidential Approval Ratings–George W. Bush*, Gallup, http://www.gallup.com/poll/116500/presidential-approval-ratings-george-bush.aspx.
[16] *Id.*
[17] Christopher A. Preble, *Iraq and the Election of 2004*, Cato (Nov. 26, 2004), https://www.cato.org/publications/commentary/iraq-election-2004.
[18] *Id.*

88% of Democrats expressing an unfavorable view of the war.[19] In the 2008 elections, the soon-to-be President Barack Obama used these strong sentiments to his advantage.

Instead of maintaining the idea that the war in Iraq was part of the global war on terror as President George W. Bush had, President Obama separated the two, stating that the US resources in Afghanistan were central to the war on terror and the fight against terrorism was still a priority, but the war in Iraq was not central to that idea, and that our troops should be removed from Iraq.[20] In doing this, President Obama still managed to use the strong anti-terrorism sentiment as President Bush had, while simultaneously managing to appeal to the strong Democratic sentiments against the Iraq war to help secure his vote into the presidency.

Election 2016

It is clear that terrorism remains a central subject in the political arena, but has ISIS had any effect on the viewpoints of politicians and the American public, or has the platform used by candidates remained the same? By 2016 ISIS was a clear enemy of the United States and was seen as a threat to the safety of many. Because of this danger that ISIS posed, and the continuing public support for the fight against terrorism, both of the candidates expressed similar stances on the need to defeat ISIS.

However, in some ways Hillary Clinton's stance differs from previous approaches. In the war against Al-Qaeda, the US took primary responsibility for most military aggression to combat the threat. During Hillary Clinton's campaign, however, she stated that the groups that are more directly threatened by the territorial expansion of ISIS should play a more significant role in the fight to defeat ISIS, and that the United States should provide more supportive roles and focus on preventing recruitment into ISIS.[21] Were this stance successful, it would

[19] *Republicans and Democrats Disagree on Iraq War, but Support Troops*, Gallup (Sept. 28, 2006), http://www.gallup.com/poll/24760/republicans-democrats-disagree-iraq-war-support-troops.aspx/

[20] Helene Cooper, Shan Carter, Jonathan Ellis, Farhana Hossain, and Alan McLean, *On the Issues: Iraq and Afghanistan*, New York Times (May 23, 2012), https://www.nytimes.com/elections/2008/president/issues/iraq.html

[21] *Where Hillary Clinton and Donald Trump Stand on Foreign-Policy Issues*, WSJ, http://graphics.wsj.com/elections/2016/donald-trump-hillary-clinton-on-foreign-policy/.

reflect the earlier mentioned effect that ISIS had on the system of law, that the situation requires a more international effort and less of a direct change from the United States.

However, President Trump had a considerably more aggressive and direct approach to the ISIS threat, from speeches during which he stated that he would "bomb the shit out of 'em,"[22] to statements about bringing back waterboarding as a way to help combat ISIS.[23] These views are essentially the same reactions toward terrorism that the attacks on 9/11 initially brought forth, and though their stances on ISIS were not the primary subject of the election in 2016, that Trump managed to secure the presidency with these types of proposals indicates that the ISIS threat did not trigger any sort of change to the approach of successful presidential candidates, and that the only change they brought to the political arena was the reignition of the same aggression towards counterterrorism from the voters that was initially brought to light in 2001.

Although ISIS has clearly warranted a reaction in both policy and politics, it seems that the only unique differing factor between the reaction to ISIS and the reaction to Al-Qaeda is the shift in approach from a primarily unilateral to a multilateral approach. Hopefully those who make future choices regarding international policies will take advantage of this improved international cooperation to strengthen ties with our allies and create a silver lining from this new threat.

Social Implications

The reaction of American politicians is a viable way to determine the effects of Al-Qaeda and ISIS on US culture, but the reaction of the people themselves is a much more accurate indicator. Unfortunately, one reaction that we have seen is an increase in Islamophobic aggression. In each of the five years prior to the attacks in 2001, the FBI reported an average of around 27 hate crimes directed towards Muslims.[24] Then in 2001 there was a dramatic spike in aggression toward Muslim Americans, with 481 reported hate crimes directed at Muslim Americans.[25] Although in the years following September 11, 2001, the

[22] (Nov. 12, 2015), https://www.youtube.com/watch?v=k2XW c8MZC-4.
[23] (Feb. 10, 2016), https://www.youtube.com/watch?v=4LLimz0d05E.
[24] UCR Publications, Hate Crime Statistics 1996–2001, (May 9, 2012), https://ucr.fbi.gov/ucr-publications# Hate.
[25] *Id.*

attacks dropped back down, there were still at least 100 more hate crimes reported in each year following 2001 than the average hate crime reported prior to 2001.[26]

In addition to the increase in hate crimes as a response to the attacks on September 11, many Muslim Americans have also experienced problems rising from the general distrust for Muslims that has occurred since the attacks. In an extensive survey conducted by the Pew Research Center ten years after the attacks, Muslim Americans were asked how their lives had changed since 9/11.[27] In the survey, a majority of the Muslims participants stated that their lives had become more difficult since 2001, with many of them experiencing an increase in others acting suspicious of them, incidents of offensive name-calling, or being profiled by airport security.[28]

However, one more positive aspect that has arisen from the increased attention that was drawn toward the Muslim community was a dramatic increase in enrollment toward Arabic language studies in American Universities.[29] A report released by the Modern Language Association shows that from 2002 to 2006 there was a 126.5% increase in enrollment into Arabic language study programs, and a continued 46.3% increase from 2006 to 2009, a much greater increase than any of the other top ten languages being taught at universities.[30] Although this rise in interest may be primarily due to the career opportunities that have arisen within the government and other internationally focused organizations in the post-9/11 era, this increased interest will hopefully increase the education and tolerance of the remainder of the American public toward the Muslim community to some degree.

With the emergence of ISIS, there came a second spike in hate crimes toward Muslim Americans. The FBI UCR report for 2015

---

[26] *Id.*

[27] *Muslim Americans: No Signs of Growth in Alienation or Support for Extremism*, Pew (Aug. 29, 2011), http://www.people-press.org/2011/08/30/muslim-americans-no-signs-of-growth-in-alienation-or-support-for-extremism/.

[28] *Id.*

[29] *Arabic Language Studies Booming in the US,* ICEF Monitor (Dec. 1, 2014), http://monitor.icef.com/2014/12/arabic-language-studies-booming-us/.

[30] Nelly Furman, David Goldberg, and Natalia Lusin, *Enrollments in Languages Other Than English in United States Institutions of Higher Education,* MLA 2009 (Dec. 2010), https://apps.mla.org/pdf/2009_enrollment_survey.pdf.

recorded nearly double the amount of anti-Muslim hate crimes as those recorded in 2014, with 307 separate incidents.[31] Although this is not the same level of increase that was seen after the 9/11 attacks, it is still unfortunate that portions of the American community continue to link Islamic extremists to Muslims living in our country.

However, this increase in hate crimes toward Muslims may not be linked to ISIS in any way. A *New York Times* article published on September 17, 2016, suggests that this increase may actually be a result of blatantly derogatory remarks made during the presidential elections.[32] These remarks could have simply encouraged and emboldened those who already held some degree of disdain toward the Muslim community to act out, regardless of whether or not they actually saw ISIS as a legitimate threat.

The reaction of the American people to the emergence of the threat of ISIS seems to be even less noticeable than that of the politicians and policy makers. However, a comparison of cultural changes would not be complete without taking a look at the most obvious and internationally recognized presentation of American culture: our entertainment media.

Mass Media Influence

Since the attacks in 2001, we have seen a major shift in the media. Video games and movies have both seen a rise in subjects that are either directly related to terrorism, or related to topics that arose from our reaction to the attacks in 2001, such as privacy concerns and overreaching government authority.

The most obvious and most well-known example of this is the *Call of Duty* video game franchise. The first *Call of Duty* game was released in October, 2003,[33] one of the more popular games in a new genre known as the "military shooter."[34] In the book *Playing War: Military Video Games After 9/11*, Matthew Payne offers a possible explanation

---

[31] *Victims*, FBI (October 20, 2016), https://ucr.fbi.gov/hate-crime/2015/topic-pages/victims_final.

32 Eric Lichtblau, *Hate Crimes Against American Muslims Most Since Post-9/11 Era*, New York Times (Sept. 17, 2016), https://www.nytimes.com/2016/09/18/us/politics/hate-crimes-american-muslims-rise.html.

[33] CALL OF DUTY, http://microsites.ign.com/call-of-duty-a-short-history/.

[34] Matthew Thomas Payne, Playing War: Military Video Games after 9/11. (New York University Press, 2016).

to the rise in popularity of this genre.[35] One of the primary reasons, Payne posits, is reflective of a national feeling of anxiety and helplessness that was brought forth as a result of the attacks on September 11th, and these games allow a release from these feelings by allowing the players to become a participant and a hero who is directly involved in the conflict.[36]

After multiple installations to the *Call of Duty* franchise that were set in both the World War II era and the modern era, Activision released *Call of Duty: Modern Warfare 2* in 2010.[37] This addition to the series drew a large amount of media attention after it was discovered that one of the missions during the single player campaign required the player to shoot down innocent civilians at a Russian airport while infiltrating a terrorist organization as an undercover agent.[38] This naturally sparked a great deal of outrage in the US, no doubt because of the fear that still remained from the 9/11 attacks and because not only did it depict a terrorist attack, but it had the player actively participate in committing the attack.[39]

Apart from the military shooter genre, there have also been many games released that had a plot centered around the ideas of freedom of information and excessive government powers. One of the most well known of these is the video game *Mirror's Edge*, a game that takes place in a futuristic "utopian" society where crime is nearly non-existent, but the government monitors all communications.[40] Senior producer Owen O'Brien stated in an interview that "one of the core questions that the game asks you is, how much of your personal freedom are you willing to give up for a comfortable life?"[41] This is a fairly obvious reference to the ongoing debates about the struggle between privacy and security that the USA PATRIOT Act had sparked in the public arena over the last several years.

[35] *Id.*
[36] *Id.*
[37] CALL OF DUTY, *supra* at note 33.
[38] N. Hohl, *Why No Russian Is The Most Controversial Video Game Level Ever*, Opshead (Mar. 16, 2016), http://opshead.com/article/619/why-no-russian-is-the-most-controversial-video-game-level-ever.
[39] *Id.*
[40] Mirror's Edge, https://en.wikipedia.org/wiki/Mirror%27s_Edge.
[41] Christian Nutt, *Living on the Edge: DICE's Owen O'Brien Speaks,* Gamasutra (June 6, 2008), http://www.gamasutra.com/view/feature/132081/living_on_the_edge_dices_owen_.php?page=4.

Compared to this influence that the war against Al-Qaeda and the aftermath in the following years has on the video game community, the conflict with ISIS seems to have almost no effect at all. Major military shooter franchises have steered away from any obvious relation to modern conflicts since 2014. The only game that specifically labels ISIS as the antagonists is a simple, $7 game with the bare bones of a storyline called *IS Defense*.[42] Although the game has received positive reviews, it hardly compares to the massive franchises that stemmed from the war against Al-Qaeda.

However, this lack of interest in using the fight against ISIS as a theme in video games could prove to be detrimental in the near future as, unlike Al-Qaeda, ISIS has attempted to use the video game market as a recruiting tool. ISIS has already created a modified version of the popular *Grand Theft Auto* series that keeps the major features of the original game but adds the ability for the character to use ISIS fighting tactics such as roadside bombs and beheadings.[43] The large influence the video game scene has on the perspective of young people needs to be considered, and a counter-narrative should be provided to combat this potential recruiting tool.

The reaction of the American movie industry is much more telling of the cultural effects. This industry, which tends to make political statements considerably more often, has had several releases related to the attacks in 2001 and the following wars. Films have been made about different points of view from nearly every stage of the conflict.

There were multiple films made about the events on September 11th themselves, which tended to avoid any sort of political agenda. One of the more well-known films that falls into this category is *United 93*, which tells the true story of the passengers onboard one of airliners that was hijacked who managed to fight back and force the plane to crash before reaching its intended target.[44]

A much greater number of films have been made about the wars

[42] Will, *New Video Game Has You Defend Europe from ISIS Invasion*. FUNKER 530 (Apr. 18, 2016), https://www.funker530.com/new-video-game-has-you-defend-europe-from-isis-invasion/.

[43] Matthew Hall, *"This Is Our Call of Duty": How ISIS Is Using Video Games*, SALON (Nov. 1, 2014), http://www.salon.com/2014/11/01/this_is_our_call_of_duty_how_isis_is_using_video_games/.

[44] Paul Greengrass, *United 93* (Universal Pictures 2006).

that followed the events in 2001. One example of this is the film *Lone Survivor*, which is based on the true story of a failed SEAL team mission during which three members of the team were killed while only one managed to make it home alive.[45] This film and the book that it is based on address some of the moral issues that American soldiers were faced with in regards to the Rules of Engagement that the soldiers were required to follow during their time in Afghanistan.

Though many of the films mentioned have political messages, they all generally lean toward a positive view of the military. However, as with video games, there are many films that were made as critiques to the government surveillance programs and as warnings about the dangers of giving the government too much power.

One of the most blatant examples of this is the film *Eagle Eye*. The 2008 film starring Shia LaBeouf and Michelle Monaghan is an action thriller in which the primary antagonist is a super-computer created by the government that has access to every digital device and infrastructure system in the United States.[46] Though this over-the-top film does not have much more to the message besides "government surveillance is bad," the fact that it was popular shows that the American people still likely saw the government as the "bad guy" in terms of their security and privacy during the decade of the USA PATRIOT Act.

Though there have been many highly regarded international films made regarding the ISIS conflict and the refugee crisis that has occurred as a result of the ISIS expansion, these films have unfortunately not drawn much attention back in the United States. However, unlike in the video game scene, there is at least one major film that is reportedly in production in the US that directly relates to the conflict with ISIS. It is going to be a film adaptation of the *Rolling Stone* article "The Anarchists vs. The Islamic State,"[47] a "real-life story of a group of US radicals, volunteers and outcasts who have teamed up with Kurdish militia the People's Protection Units to fight Isis in Syria, with the ultimate aim of establishing an anarchist collective in the region."[48] Based

[45] Peter Berg, *Lone Survivor* (Universal Pictures 2013).
[46] D.J. Caruso, *Eagle Eye* (Paramount 2008).
[47] Seth Harp, *The Anarchists vs. the Islamic State*, Rolling Stone (Feb. 14, 2017), http://www.rollingstone.com/politics/features/american-anarchists-ypg-kurdish-militia-syria-isis-islamic-state-w466069.
[48] Gwilym Mumford, *Jake Gyllenhaal to Play Anarchist Joining the Fight Against Isis*. Guardian (Mar. 24, 2017), https://www.theguardian.com/film/2017/mar/24/

on this synopsis, the story will not be the heroic soldier story that we have seen in so many other films since 9/11, but it will still likely show ISIS as the clear antagonists, and if it is well received, it could usher in a new generation of films centered around counterterrorism.

Whether or not this film succeeds will likely be an important factor in the years to come, as ISIS has already proven their abilities to use videos and short films to make their ideals appealing to various crowds. ISIS has demonstrated that they know how to make their lifestyle appealing, with videos being released on Youtube that essentially make it appear as though they are living the life of an action hero. We may not see any clear influence in our films and shows as we did with Al-Qaeda, but it can certainly be argued that we should, or ISIS may end up gaining the admiration of those who could have otherwise known what kind of organization ISIS is before it is too late.

As it has only been a few years since the beginning of the conflict with ISIS, and most of the films referencing 9/11 and the war in Afghanistan were released many years later, it is still possible that we will see an increase in films related to ISIS or whatever events may follow our current war; but based on the limited impact that ISIS has had on other domestic issues and popular media, this seems unlikely.

Even in less structured entertainment media such as Youtube videos and comedy sketches, Al-Qaeda maintains their influence over ISIS. Though there have been plenty of examples of ISIS-related humor, such as the controversial BBC sketch about the "Real Housewives of ISIS," a parody of the popular American TV series that poked fun at ISIS ideals with some rather offensive humor,[49] it is still overshadowed by humor related to Osama Bin Laden and Al Qaeda. A clear example of this is the sketch comedy video released by Key & Peele on Youtube titled *Al-Qaeda Meeting*.[50] This video, which now has over 10 million views, was released in December 2014, well after the American public was made aware of the ISIS threat, and still uses the Al-Qaeda organization as a subject of their comedy. Whether or not it would have been

jake-gyllenhaal-daniel-espinosa-isis-syria-film-drama.

[49] Samuel Osborne, *BBC's The Real Housewives of Isis Comedy Sketch Divides Public Opinion*, Independent (Jan. 5, 2017), http://www.independent.co.uk/news/media/tv-radio/bbc-the-real-housewives-of-isis-sketch-islamic-state-revolting-comedy-controversy-opinion-reaction-a7510581.html.

[50] C., (Dec. 11, 2014), https://www.youtube.com/watch?v=IHfiMoJUDVQ.

more popular if it focused on ISIS instead of Al-Qaeda is up for debate, but it is a clear indication that even after more than a decade and the emergence of a new, and arguably more powerful terrorist threat, the US public may never see ISIS as the same level of adversary as they see Al-Qaeda.

Conclusion

Overall the primary reason for the perception of ISIS seems to be the lack of the same feeling of danger on our own soil that was caused by the 9/11 attacks. If this is true then ISIS could potentially obtain the same level of influence that Al-Qaeda managed if they successfully conduct a large-scale attack inside US territory, but hopefully the lessons we have learned since 2001 will prevent that from happening, and hopefully, with our improved international cooperation we will be able to more efficiently defeat ISIS abroad so their influence is lost on the international level as well.

In the end it can be concluded that, in terms of the feelings of the American people, and according to the politicians and lawmakers, ISIS is not the influential group that Al-Qaeda once was. We are at war with ISIS, and because of this the group will continue to have some impact on our lives. Because of adjustments to our governmental counterterrorism tools, we will hopefully move toward becoming more educated and tolerant toward Muslims, and experience a normal shift toward new enemies in popular entertainment. It seems unlikely that the impact of ISIS will reach anywhere near the culture-changing influence created by Al-Qaeda in the post 9/11 era.

An Anonymous Solution to Terrorism

Andre Jones

Introduction and Thesis

All over the world, people are interconnected through the internet. Space that was once used for filing cabinets and shelves is now server rooms for thousands of terabytes of digital information and data storage. While companies and organizations seek ways to utilize social media and internet technology, others will use it for terror. The proliferation of cyberterrorism has caused the Pentagon, corporations, and institutions of higher learning to create Cybersecurity graduate degrees and programs to combat this new strain of warfare. Because companies' and nations' entire infrastructure relies on the security of their databases and online information, a new type of soldier is bred: the cyber soldier. Today, the experts of cyberwarfare are a valuable commodity with which US government agencies have a love/hate relationship. But what does the government have to gain by working with these experts? Terrorists around the world have begun to recruit hundreds and thousands via the internet and social media. US counterterrorism experts struggle to put a permanent stop on the spread of the violent extremists' online presence. While the need for better counterterrorism initiatives still exists, the budget for expensive new programs does not. In this paper I will evaluate who cyber vigilantes such as those linked with Anonymous are, how the US government and private sectors are adapting to cyber warfare, and possibilities for government recruitment and cooperation with these hackers in combating online terrorism and recruitment.

Anonymous

The actors of cyber warfare do not fall into the dichotomy of state actors and terrorists. Countering violent extremism does not stop at government agencies, and neither does the desire to fight international terrorist groups, ISIS being the foremost among them. For a moment, let us take a look at a third-party actor in the fight against ISIS, the hacktivists who call themselves Anonymous. Merriam-Webster has three definitions for the word *anonymous: 1)* of unknown authorship or origin, 2) not named or identified, or 3) lacking individuality, distinction, or recognizability.[1] Combined with the political motivation for anarchic social change, this definition describes the manner of operation exercised by Anonymous.

In the 2005 film *V For Vendetta*, the anarchist freedom fighter named *V* saves a girl from the British secret police, prompting the girl to ask who he was. After he says he is a man in a mask, she acknowledges that she can see that, wherewith he replies, "Of course you can, I'm not questioning your powers of observation, I'm merely remarking upon the paradox of asking a masked man who he is."[2] Trying to understand the internet vigilantes known (or unknown) as Anonymous is like asking a masked man who he is because no one knows who they are, thus the collective name: Anonymous. They are an international network of hackers whose purpose is internet activism and anti-cyber surveillance. This group has no organization and no leadership, with "a very loose and decentralized command structure that operates on ideas rather than directives."[3]

To better grasp who Anonymous is, it is critical to understand who hacktivists are and how their culture that has cultivated the last decade. "Hacktivism" is described as using computers and networks to promote a political agenda, which can span from hacking to promoting social change to cyberterrorism.[4] Like the pirate code, the hackers'

[1] *Anonymous*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/anonymous.

[2] V for Vendetta, dir. James McTeigue, The Wachowski Brothers (Virtual Studios 2005).

[3] Brian B. Kelly, *Investing in a Centralized Cybersecurity Infrastructure: Why Hacktivism Can and Should Influence Cybersecurity Reform.* 92 Boston Univ L.R. 1664–711 (2009), http://www.bu.edu/law/journals-archive/bulr/volume92n4/documents/KELLY.pdf.

[4] Adam Shepherd, *What Is Hacktivism?* ITpro (Jan. 2, 2018), http://www.itpro.

rules of governance guide their actions.[5] This code includes tenets that hackers should naturally distrust authority and promote free access of information.The first hackers originated from MIT in the 1960s, where hacking first appeared as pranks between students.[6] Hacktivism is a combination of these principles with a political focus of raising the public's awareness of various issues. If you want to understand the felonious zeitgeist of hacktivists, this incognito collective is a good place to start.

Though Anonymous does not have an organization per say, they do have a homepage. They describe themselves as "an internet gathering," whereas others have referred to them as a "cyber lynch-mob"[7] or even digital Robin Hoods.[8] The beginnings of Anonymous start on the darker side of the web, a chat website called 4chan. Here, people who logged on to comment without a username, were automatically assigned "anonymous." Eventually this led to the idea that as a group of online hackers, they could influence others through movements for political means. Anonymous' hacktivism began with protests against the Church of Scientology, where 7,000 in 100 cities worldwide gathered to protest the church.[9, 10] Wearing "Guy Fawkes"[11] masks, these protesters sparked the start of the political movement of Anonymous. In the years

co.uk/hacking/30203/what-is-hacktivism.

[5] Manushag N. Powell, British Pirates in Print and Performance 140 (Palgrave Macmillan 2015).

[6] Erik Brunvard, *A Little Bit of Hacker History* University of Utah (Oct. 15, 1996, 13:40), https://www.cs.utah.edu/~elb/folklore/afs-paper/node3.html

[7] E. Gabriella Coleman, *Anonymous: From the Lulz to Collective Action,* Mediacommons (Apr. 6, 2011), http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action.

[8] Adam Carter, *From Anonymous to Shuttered Websites, the Evolution of Online Protest,* CBC News (Mar. 15, 2013), http://www.cbc.ca/news/canada/story/2012/03/15/f-online-protest.html.

[9] John Cook, *After an Embarrassing String of High-Profile Defection and Leaked Videos, Scientology Is Under Attack from a Faceless Cabal of Online Activists. Has America's Most Controversial Religion Finally Met its Match?* http://www.xenu-directory.net/news/20080317-radar.html (Mar. 17, 2008).

[10] Carlos Moncada, *Organizers Tout Scientology Protest, Plan Another,* Tampa Tribune (Feb. 12, 2008), http://www.tbo.com/news/breaking-news/2008/feb/12/organizers-tout-scientology-protest-plan-another-ar-154044/.

[11] Guy Fawkes was a Catholic dissident who helped plan the failed Gunpowder Plot of 1605 in whichFawkes and others attempted to assassinate the protestant King James by detonating barrels of gunpowder beneath the British Parliament, http://www.history.com/news/guy-fawkes-day-a-brief-history.

following, Anonymous would be responsible for cyber-attacks on Paypal, which resulted in the loss of 3.7 million dollars,[12] and Sony, where more than 100 million accounts were compromised.[13]

Anonymous' history is a mixed grab bag of illegal and legal activities, each event receiving a different title beginning with "Operation." US National Security agencies began to take notice of Anonymous during their Operation Tunisia during the Arab Spring revolutions. Distributed Denial of Service attacks (DDoS) hit Tunisian government websites, including that of the Prime Minister.[14] In addition to taking down websites, the hacktivists helped to provide internet connectivity for the Tunisian people to share videos about the uprising.[15]

#OpCharlieHebdo

In January of 2015, two brothers shot their way into the offices of the French cartoonist newspaper *Charlie Hebdo*. The day of the attack, the two burst into the wrong address asking, "Where is *Charlie Hebdo*?" and upon realizing it was the wrong place, fired a bullet into the door and left.[16] The terrorists accosted one of the cartoonists named Rey and forced her to let them inside with her keycode. Before asking her anything else, they sprayed the reception desk with bullets, killing a maintenance worker, then they proceeded to the second floor. There they entered the editorial meeting of 15 people and began shooting each of them at point blank range in the head. Before leaving, they identified themselves as part of Al-Qaida in the Arabian Peninsula.[17]

[12] Sandra Laville, *Anonymous Cyber-Attacks Cost PayPal £3.5m, Court Told*, Guardian (Nov. 22, 2012), https://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court. Note: The £3.5m was converted to US dollars using the currency rate of 1,07255 (rate at time of the publication of this article).

[13] *Sony Caught Up in Cyber War with Indignant Hackers,* Charleston Gazette-Mail (May 30, 2011), https://www.wvgazettemail.com/business/sony-caught-up-in-cyber-war-with-indignant-hackers/article_c3608737-b665-5c58-9e97-ff3a26528ac3.html.

[14] Parmy Olson, We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency 141–145 (Little, Brown 2012).

[15] Yasmine Ryan, *Anonymous and the Arab Uprisings* Al Jazeera. (May 19, 2011), http://www.aljazeera.com/news/middleeast/2011/05/201151917634659824.html.

[16] Soren Seelow, *Attentat à "Charlie Hebdo": "Vous Allez Payer car vous avez Insulté le Prophète,"* Le Monde (Jan. 8, 2015), http://www.lemonde.fr/societe/article/2015/01/08/vous-allez-payer-car-vous-avez-insulte-le-prophete_4551820_3224.html.

[17] Holly Watt, *Terrorists Shouted They Were from Al Qaeda in the Yemen before Charlie Hebdo Attack*, Daily Telegraph (Jan. 7, 2015), http://www.telegraph.co.uk/news/

The attack resulted in 12 deaths and 11 injuries. According to the Israeli news agency Haaretz, the terrorists acquired assault rifles, sub machine guns, shotguns, and rocket launchers for the attack through the Brussels black market.[18]

These were French citizens who murdered all those people. But how does ISIS play a role in their recruitment? Growing up, the brothers were virtually orphaned multiple times after their mother committed suicide; afterward, they later became involved with French gangs, then radical extremism.[19, 20] Cherif and Said Kouachi were French citizens who had been arrested before for terrorist activities and who had trained with Al-Qaida operatives in Yemen for three years leading up to 2015.[21] After the cover of the *Charlie Hebdo* magazine depicting Muhammad was published in 2011, early Al-Qaida members loyal to Abu Musab al-Zarqawi had tried shutting down the satirical publication through firebombing of their office and hacking their home website.[22] An article from the *UK Guardian* about the firebombing investigates potential terrorist ties between the 2011 vandalism and cyberthreats to the Charlie Hebdo massacre in 2015. The *Guardian* article states, "Charlie Hebdo's website also appeared to have been hacked to show images of Mecca."[23] The main video from the article showed the director Charb (Stephane

worldnews/europe/france/11330636/Terrorists-shouted-they-were-from-al-Qaeda-in-the-Yemen-before-Charlie-Hebdo-attack.html.

[18] Shlomo Papirblat, *Belgian Arms Dealer Confesses to Supplying Paris Attackers,* Haaretz (Jan. 14, 2015), http://www.haaretz.com/news/world/1.637034.

[19] Andrew Higgins and Maia De La Baume, *Two Brothers Suspected in Killings Were Known to French Intelligence Services* New York Times (Jan. 8, 2015) https://www.nytimes.com/2015/01/08/world/two-brothers-suspected-in-killings-were-known-to-french-intelligence-services.html?_r=1.

[20] Lamiat Sabin, *Charlie Hebdo: What Do We Know about Suspects Said and Cherif Kouachi Who Allegedly Shot 12 People Dead?* Independent (Jan. 8, 2015), http://www.independent.co.uk/news/world/europe/charlie-hebdo-profile-of-suspected-killers-said-and-cherif-kouachi-who-shot-12-people-dead-9964153.html.

[21] Julian E. Barnes, Adam Entous, and Devlin Barrett, *U.S. Shared Intelligence with French about Paris Brothers' Yemen Trip,* Wall Street Journal (Jan. 9, 2015), https://www.wsj.com/articles/u-s-shared-intelligence-with-french-about-paris-brothers-yemen-trip-1420844151.

[22] James Boxel, *Firebomb Attack on Satirical French Magazine*, Financial Times (Nov. 2, 2011), https://www.ft.com/content/75f87b24-0541-11e1-a3d1-00144feabdc0.

[23] Angelique Chrisafis, *French Government Defends Magazine Firebombed over Muhammad Cartoon*, Guardian (Nov. 2, 2011), https://www.theguardian.com/world/2011/nov/02/charlie-hebdo-magazine-muhammad-cartoon.

Charbonnier) talking about how the staff was "just doing its job as usual." It was shocking to realize that this man in a 2011 interview on cyber threats would later be shown as one of the 12 killed during the 2015 terrorist attack on the newspaper. Finding French websites that show connections between the two attacks was a challenge. One in particular stuck out, a press release from a French news site called *20 Minutes*. The report said French authorities discovered Jihadist flags and Molotov cocktails in the abandoned getaway car.[24] Connecting the firebombing and the terrorists shows the augury of cyberterrorism leading up to the 2015 attack.

In the days following the attack, Anonymous' videos began to flood the internet with the message, "We are declaring war against you, the terrorists."[25] Anonymous wrote messages across many websites; one of the messages (from a social media website called Pastebin in this case) was "freedom of expression has suffered inhuman assault . . . and it is our duty to react."[26] At the time, few noticed this declaration of war from Anonymous, either because they did not think the hacktivists would be able to make a difference, or that they had little understanding of who they were.

The Anonymous Twitter account OpParis announced its social media-driven campaign against ISIS soon after the attacks, beginning with an all-out online attack that had been urged on by thousands of Parisians. According to CBS, Anonymous reported "20,000 Twitter accounts of ISIS" were taken down, followed by the hashtags *#OpParis* and *#TangoDown*.[27] This issue, like a two-sided coin, has ups and downs. While Anonymous does hinder ISIS's ability to recruit and get its

[24] *Attaque à "Charlie Hebdo": Drapeaux djihadistes et cocktails Molotov dans la voiture abandonnée . . . Les deux suspects repérés à Villers-Côtterets . . .* , 20 Minutes (Aug. 1, 2015), http://www.20minutes.fr/societe/1512431-20150108-attaque-charlie-hebdo-drapeaux-djihadistes-cocktails-molotov-voiture-abandonnee-deux-suspects-reperes-villers-cotterets.

[25] Keely Lockhart, *"Hacktivist" Group Anonymous Says It Will Avenge Charlie Hebdo Attacks by Shutting Down Jihadist Websites*, Daily Telegraph (Jan. 9, 2015), http://www.telegraph.co.uk/news/worldnews/europe/france/11335676/Hacktivists-Anonymous-says-it-will-avenge-Charlie-Hebdo-attacks-by-shutting-down-jihadist-websites.html.

[26] *Id.*

[27] Brian Mastroianni, *Anonymous vs. ISIS: Who Has the Upper Hand in Social Media War?* CBS News (Nov. 24, 2015), http://www.cbsnews.com/news/anonymous-vs-isis-social-media-war/.

propaganda out there through Twitter, it may hamper the intelligence communities from being able to track down the source of the Twitter accounts. We have only hit the tip of the iceberg when it comes to terrorist social media activity; there is still Facebook, Telegram, and even Tinder.[28]

US Cyber Capabilities

Among those involved in counterterrorism, many say that terrorists are the most adaptive threat on the planet. When people hear the word *intuitive*, they usually think of LinkedIn or Elon Musk. We can look at a shoe and think of comfort; terrorists look at a shoe and think of a makeshift bomb. Unless we step up and become more entrepreneurial in our approaches to counterterrorism, groups like ISIS will continue to threaten innocent people.

Not only did ISIS find and train operatives who were native Frenchmen, they also employed cyberterrorism tactics to shut down *Charlie Hebdo*'s website. After dealing with Al-Qaida tactics for nearly 15 years, counterterrorism specialists realized that they were seeing the emergence of a new breed of terrorist. Scott J. White, director of computing and security technology at Drexel University, illuminated a reason why ISIS is a different threat: "What is interesting is that this group of young extremists who are part of ISIS, or ISIL, is that they are young and computer savvy and are using social media incredibly effectively."[29] To combat these millennial cyber terrorists, the Pentagon, US corporations, and higher education institutions will have to take on the mantle of training the next generation of cyber warriors.

Before examining whether there is a possible relationship between these cyber vigilantes and the government, we need to understand where the United States stands on cybersecurity. In 2014, the US Secretary of Defense announced a new plan to triple the department's cybersecurity force, starting with 1,000 agents and 1,000 analysts before 2016.[30] Many programs exist within the military to train new

[28] Nathan McAlone, *ISIS Is Even Recruiting on Dating Websites*, Business Insider (May 17, 2016), http://www.businessinsider.com/isis-is-even-recruiting-on-dating-websites-2016-5.

[29] *Id.* at note 26.

[30] Dune Lawrence, *The U.S. Government Wants 6,000 New "Cyberwarriors" by 2016*, Bloomberg (Apr. 15, 2014), https://www.bloomberg.com/news/articles/2014-04-15/the-u-dot-s-dot-government-wants-6-000-new-cyberwarriors-by-2016.

cyber cadets, including the Army Cyber Institute and the US Marine Corps's cybersecurity division. Currently, the Pentagon's efforts are focused on providing funding to students through scholarships, the largest program being the CyberCorps founded in 2000. Not only does this improve our cyber posture, but it helps provide sufficient pay to keep people happy. Sometimes people need to be paid more if their work consists of being locked up in a room, forbidden to tell people about what they do, while they are preventing security breaches. Millennials today are one of our best solutions to protecting US interests and companies from cyberterrorism and the ones who will bring a strong vision of how to best implement cybersecurity in the future for both civilian and military institutions. To this end, and to improve the United States' cyber posture, the military command Cybercom was created in 2009 and elevated to the unified combatant command it is today: Cyber Command.[31]

Universities across the nation have begun funding the next generation of cybersecurity graduates who will oversee the United States future cyber capabilities. A press release from Utah Valley University on March 14, 2017, stated that they would begin offering a Master of Science degree in Cybersecurity starting fall of 2017.[32] The director of the program, Robert Jorgensen, said, "This workforce solution was funded by a grant by the US Department of Labor's Employment and Training Administration," evidence that the Pentagon was successful in funding its new armada of cyber cadets through higher education.[33]

Students are heavily involved in the cyber warfare discussions as well. The *Deseret News* reported on a student-led event at the same university titled Pizza and Politics: Russia and Cyber Warfare, which discussed the diplomatic stress happening between the United States and Russia with the controversy over the "Russian hacking" of the

[31] Jim Garamone and Lisa Ferdinando, *DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command*, U.S. Department of Defense (Aug. 18, 2017), https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/.
[32] Layton Shumway, *UVU Cybersecurity Students Take Second Place at Regional Competition*, Utah Valley University (Mar. 14, 2017), http://blogs.uvu.edu/newsroom/2017/03/14/uvu-cybersecurity-students-take-second-place-at-regional-competition/.
[33] Robert Jorgensen, *Program Director, Cybersecurity Career Pathways Program*, Utah Valley University (2017), http://www.uvu.edu/ist/cybersecurity/.

2016 US presidential election.[34] Students at the event asked questions about the technology used in these hacks and the extent of the danger of the attacks.[35] During the event, the questions about "who did it" were answered, resolving that this technology was created by a nation state, rather than by non-state actors such as ISIS. However, experts have begun to ask what will prevent technology like this from falling into the hands of terrorists. These are some of the reasons that the Department of Defense is increasing the number of cybersecurity programs and scholarship funding.

Not only will the next generation of cybersecurity analysts be cultivated within higher education institutions such as Utah Valley University, but through corporations and businesses as well. In March of 2017, I spoke with cyber experts from the private and public sectors at the 2017 Cybersecurity conference hosted by the US Chamber of Commerce and the Salt Lake Chamber at the University of Utah. At these conferences, cyber analysts discuss challenges to effective cybersecurity and how to entice more companies to hire their firms. By hiring them, the companies basically ask them to hack into their database to see how much information they can steal and how much havoc they could wreak.

I interviewed intelligence officials and analysts about the possibility of new programs engaging with pro-government hackers to combat online terrorism and recruiting. One analyst I spoke with hacked a well-known travel company's database and easily obtained the company's top 20 executives' accounts and passwords, which came as a shock when the analyst presented each person his or her personal passwords. Imagining what this type of weapon would be used for in terrorists' hands is a frightening realization. This is not just a computer nerd hobby; this is the next form of security and warfare in the modern world.

My first interview was with Todd Neilson, the president and co-founder of Secuvant, a firm that helps businesses build cybersecurity

[34] Ryan Morgan, *What a UVU Panel Said about Difficulty of Tying Hacking to Russia*, Deseret News (Apr. 11, 2017), https://www.deseretnews.com/article/865677632/Cybersecurity-expert-explains-difficulty-attributing-hacking-to-Russian-government.html.

[35] Lincoln Op't Hof, *Putin, Cybersecurity Analyzed by White and Jorgensen*, UVU Review (Apr. 19, 2017), http://www.uvureview.com/recent/news/putin-cybersecurity-analyzed-by-white-and-jorgenson/.

infrastructure.[36] I asked him what he thought of Anonymous and if there were a possibility for vigilante-government collaboration against terrorism. He replied,

> There is a national stigma that Anonymous still exists at full capacity, when in fact they have splintered into smaller groups such as LulzSec and Lizard squad. The problem with having a leaderless organization like theirs is that any high school kid can do something stupid and claim he was working for Anonymous."

I asked what he thought about offering incentives to third-party hackers for information leading to the apprehension or death of terrorists and their propaganda efforts, and he said there were three major issues that the government would have to overcome. 1) The guarding of information: providing data to help the government causes businesses and individuals to ask "what's in it for me," resulting in the loss of cooperation. 2) The legal perspective: shareholders do not want to release information to the government in most cases. For example, in order to determine where and who is committing cyber-crimes, you need access to the data that was taken or affected. 3) The cultural issue: most of the time when a virus or phishing attack happens to a company, it is due to an employee clicking on a malicious email—which could have been avoided with proper training. However, the media has a culture of reporting that the company was "hacked," which can be misleading.

A survey was done by The Ponemon Institute in 2010 revealing that of a simple random sample of 50 large US companies that suffered cyberattacks, $5.9 million dollars was the median annual damage from these cyberattacks."[37, 38] A study by Norton Antivirus reported boiling cyber threats down to an individual level; accounting for time lost and direct damage done, the costs to private citizens around the world were

[36] Interview with Todd Neilson, president and co-founder of Secuvant (Mar. 23, 2017).

[37] Ponemon Institute, *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies 1*, Arcsight (2011), http://www.arcsight.com/collateral/whitepapers /2011_Cost_of_Cyber_Crime_Study_August.pdf (defining the fifty "large" companies being those with more than 700 enterprise seats).

[38] *Operation Ghost Click: International Cyber Ring That Infected Millions of Computers Dismantled*, FBI (Nov. 9, 2011), http://www.fbi.gov/news/stories/2011/november/mal ware_110911/malware_110911.

close to $388 billion. McAfee did a similar survey and claimed damage to the global economy reached $445 billion.[39, 40] That is more money than nine of the top ten billionaires in 2016, excluding Bill Gates, who tops out at 75 billion.[41] Because big money and online data are so interconnected, we have reached a threshold as a nation where companies and people are at risk of cybercrime and even cyberterrorism.

Cybersecurity Solutions in the Future

After meeting with the CEO of Secuvant, I sat next to John Bauer, a former NSA agent (name has been changed at the request of the interviewee). After 14 years of working for the NSA, he was contracted to work for a cybersecurity consulting group. I asked Bauer what, if any, opportunities exist to collaborate with hacktivists when it comes to fighting terrorism? "When it happens, it's almost always a one-way relationship," John said, "and as for recruitment, the NSA focuses on top talent from accredited sources. Anonymous has people who do this only as a hobby. There is a difference between hobby hacktivists and trained government employees where this is all they do, hours on end, every day."[42] After this interview, I wondered if the past relationship between the US government and Anonymous would render any efforts to collaborate impossible.

Yet, Anonymous continues to act as a force against terrorism. In November 2015, following the Charlie Hebdo attack, ISIS terrorized Paris again. Suicide bombers and armed ISIS members carried out six different attacks in one night. In total, 130 people were killed and 368 people injured, making this the deadliest attack in the European Union since 2004 (the train bombings in Spain). Days afterward Anonymous stepped up their campaigns, again declaring war on the Islamic State. However, the vigilante response to this ISIS attack was much greater

[39] *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*, SYMANTEC (Sept. 7, 2011), http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 ($274 billion of $388 billion lost was because of "time lost due to [the victims'] cybercrime experiences")

[40] *Cyber Crime Costs Global Economy $445 Billion a Year: Report*, REUTERS (June 9, 2014), http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609.

[41] Rebecca Lee, *Meet the World's Richest People of 2016*, CBS NEWS (Mar. 1, 2016), https://www.cbsnews.com/news/2016-forbes-magazine-world-billionaires-richest-bill-gates/.

[42] Interview with former NSA Analyst (23 March, 2017).

this time. Infamous hackers with names such as The Jester and Ghost Security Group joined the fight against the Islamic State. These hacktivists' tactics included shutting down social media sites, pretending to be recruits to gain information on the Dark Web, and even providing the US government with intelligence. Considering these groups were primarily an Anarchist/Free Speech collective in their ideology, it was an interesting development to see them team up with a government entity, let alone the United States government.

Ghost Security Group, a volunteer "cyber-crime fighting vigilante" organization and offshoot of Anonymous, provided "screenshots of internal communications about an impending attack in Tunisia" to Michael S. Smith, COO of the defense contractor Kronos Advisory.[43] He reported that the information provided did help break up the terrorist cell before the attack happened.[44] Ghost Security Group used to brandish the Guy Fawkes masks, revealing their Anonymous roots. However, since their efforts have caught the eyes of people in high places, namely the former director of the Central Intelligence Agency, General David Petraeus, they have shed the masks and connections to Anonymous. Possibly becoming the first of its kind, this small group and its efforts to run the Islamic State off the internet may turn into a professional cyber-consultancy.

During an interview with Fox News, Smith complimented Anonymous, "They certainly have people there with remarkable skill sets."[45] We have a group of masked, unidentified people, fighting a subterranean war on terrorism who have found purpose in hacking terrorists. Is Anonymous' Internet war against terrorism effective? According to one known member of Anonymous, it is fulfilling the purpose of pushing back. Anonymous member @MadSci3ntis5t (as known on Twitter) told research associate E. T. Brooking with the Council on Foreign Relations, "How much do I think the internet war matters? I

[43] E. T. Brooking, *Anonymous vs. the Islamic State*, FP, https://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/.
[44] Reuters, *Hacking Group Anonymous Disables Thousands of Pro-ISIS Twitter Accounts and Taking Militant Websites Offline,* Daily Mail (Nov. 18, 2015), http://www.dailymail.co.uk/news/article-3323597/Activist-hackers-battle-Islamic-State-cyberspace.html.
[45] Fox and Friends, *How Anonymous' Attack on ISIS Is Counterproductive*, Fox News (Nov. 23, 2015), http://video.foxnews.com/v/4627918228001/?playlist_id=930909787001#sp=show-clips

think it's important because they need to know people aren't gonna put up with that crap!"[46]

The final interview I had during the cybersecurity conference was with Supervisory Special Agent of the FBI, James Lamadrid. I asked him if the FBI seeks to work alongside cyber vigilantes such as Anonymous against terrorism. "Hackers are highly valuable and we definitely want them on our side," commented Lamadrid. "Of course, we would vet them to see if they have any prior illegal activity that would prevent them from working with us."[47] Agent Lamadrid said during a panel that day that he was over the FBI's Salt Lake City Cyber Task Force and said that the agency has a total of six cybersecurity offices, Utah being one of them.

Clearly, the NSA and FBI have different criteria for hiring hackers. One hacker, however, seemed like a perfect candidate for either program, if you could convince him to formally join: The Jester, a "computer vigilante" known for hacking "anti-American, jihadist, and homophobic websites."[48] This former military contractor with US Special Operations Command (SOC) used a cyber weapon he created called XerXes, an advanced automated virus that performed denial of service attacks on targeted jihadist websites, the Taliban being his first victim.[49] The Jester's WordPress blog has a picture of Captain America on the front, shamelessly indicating that he is an American hacktivist. As an antagonist to Anonymous, he has repeatedly tried to shut down Julian Assange's WikiLeaks, claiming it "endanger[s] the lives of our [US] troops, 'other assets' & foreign relations."[50] The Jester was able to hack certain hacktivists who worked alongside WikiLeaks by creating a QR code for his Twitter account that had an embedded code that scanned phones for associated Twitter accounts. I would be surprised if the government has not already asked him to work with intelligence

[46] *Id.* at note 44.

[47] Interview with James Lamadrid, FBI Special Agent (23 March, 2017).

[48] Nancy Houser, *The Reality of Hacking Islamic Extremist Websites,* Digital Journal (Mar. 9, 2015), http://www.digitaljournal.com/internet/the-reality-of-hacking-islamic-extremist-websites/article/427486.

[49] Ashlee Vance, *WikiLeaks Struggles to Stay Online After Attacks,*" New York Times, (Dec. 3, 2010), http://www.nytimes.com/2010/12/04/world/europe/04domain.html.

[50] Anthony M. Freed, *The Jester Hits WikiLeaks Site With XerXeS DoS Attack,* Infosec Island (Nov. 29, 2010), http://www.infosecisland.com/blogview/9865-The-Jester-Hits-WikiLeaks-Site-With-XerXeS-DoS-Attack.html.

agencies (such as Treadstone 71, a known cyber-defense contractor he has worked with before)[51] to tackle terrorism on a cyber front.

The US government has had its ups and downs with Anonymous and other groups in the past, but the argument stands that the hackers would be a powerful ally against terrorism. Over the last 16 years of fighting terrorism, some of the most critical intelligence we have received is through Arab citizens who felt comfortable providing the government key intelligence to thwart terrorist attacks.[52, 53] Citizen-intelligence gathering, whether through hacktivist collectives who find purpose through taking down terrorist websites or graduate students at Utah Valley University researching new ways of combating cyberterrorism, can be a valuable resource to the government.

Uniting the World Against Cyberterrorism Online

Major world powers such as the United States and Russia have begun to indulge in cyberwarfare. If this is to be the new mode for warfare in the future, the issue of preventing terrorists from employing the same tactics remains. Viable options still exist to enlist vetted hackers to become government employees or to offer incentives for cyber vigilantes to provide useful information to US intelligence.

First, one needs to define terrorism and cybercrime. The US Code of Federal Regulations (US CFR) defines terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[54] However, there is no universal definition of terrorism due to its emotional and political charge. There are some overlapping principles in most definitions, including threats of violence against innocent people, the presence of a political goal, and non-state actors as the offenders. This does not

[51] *Hacktivist "The Jester" Draws Crowd at Hacker Halted,* Infosec Island (Oct. 31, 2011), http://www.infosecisland.com/blogview/17784-Hacktivist-The-Jester-Draws-Crowd-at-Hacker-Halted.html.

[52] Paul Mueller and Steele Steele, *Fighting Terrorism with Our Best Asset–Our Citizens*, The Hill (Dec. 30, 2015), http://thehill.com/blogs/congress-blog/civil-rights/264143-fighting-terrorism-with-our-best-asset-our-citizens.

[53] Anthony Cotton, *Private Citizens Getting Help in Fight Against Terrorism*, Denver Post (Nov. 15, 2011), http://www.denverpost.com/2011/11/15/private-citizens-getting-help-in-fight-against-terrorism/.

[54] 28 C.F.R., Section 0.85. https://www.fbi.gov/file-repository/stats-services-publications-terror_98.pdf.

include violence used in wartime or peacetime "by a nation state against another nation state regardless of legality or illegality that are carried out by properly uniformed forces or legal combatants of such nation states."[55]

Understanding the definition of cybercrime is also an important factor in differentiating between terrorists and cyberterrorists. According to Norton AntiVirus' lengthy and detailed explanation on their website, cybercrime is "a crime that has some kind of computer or cyber aspect to it."[56] After searching for a more detailed definition, I had to acknowledge Norton because almost all other definitions simply said that cybercrime is a computer-related crime that involves a computer and a network.[57] Some more substantive subject matter can be found regarding the types of networks used to commit crimes, which include "internet (networks including but not limited to chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)," while high-profile cyber cases include hacking, theft (copyright infringement), illegal mass-surveillance, public releases of sensitive material, and child pornography.[58]

To combine these definitions into "cyberterrorism," we can examine what it is, what it looks like today, and what it could cause in the future. *Digital Crime and Digital Terrorism* defines cyberterrorism by separating it from cybercrime: "Cyber terrorism is a component of information warfare, but information warfare is not . . . cyber terrorism. For this reason, it is necessary to define these topics as separate entities."[59] Beyond the usual cybercrimes of our day in the form of pesky email scams that fill our inboxes, terrorists have used the same tools to recruit fellow extremists and terrorize the public with videos of beheadings and murders. These are just a few examples of the differences between cyberterrorism and cybercrime.

[55] Defense Threat Reduction Agency, *Terrorism: Concepts, Causes, and Conflict Resolution*, U.S. Air Force (Jan. 14, 2002), http://edocs.nps.edu/dodpubs/org/DTRA/.

[56] *What Is a Cybercrime?* Norton by Symantec, https://us.norton.com/cybercrime-definition.

[57] Robert Moore, Cybercrime: Investigating High-Technology Computer Crime (Routledge 2005).

[58] Debarati Halder and K. Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations (IGI Global 2012).

[59] Robert Taylor, Eric Fritsch, Tory Caeti, Kall Loper, and John Liederbach, Digital Crime and Digital Terrorism 19 (Prentice Hall 2011) (2006).

After September 11, 2001, the Department of Defense through the US Strategic Command (USSTRATCOM) was tasked with creating a joint task force to combat cyberterrorism called Global Network Operations (GNO), which was technologically integrated into all of the Department of Defense's networks and systems, including all its connected agencies and services. Despite the department's best defensive attempts, Russian hackers in August 2015 seized the Joint Chiefs of Staff's email system, which was used by nearly 3,500 military and civil personnel.[60] A few months earlier FBI Director James Comey had stated, "We are picking up signs of increasing interest," when asked about terrorists employing cyberterrorist tactics.[61]

During the cybersecurity conference I mentioned earlier, FBI Agent Lamadrid stated during a panel that terrorist cyberattacks were unsophisticated but effective, further driving home the message that cyberterrorism, if not prevented, could end disastrously.[62]

During the fourth season of the television series *24*, terrorist leader Habib Marwan uses cyberterrorism to initiate forced meltdowns of over 100 nuclear power plants across the United States. Penny Hitchin with Nuclear Engineering International reports on the validity of these kinds of plots: "Five years ago Iran's nuclear complex was breached by a computer virus. Stuxnet, a sophisticated and complex piece of malware that targeted operation of Iran's uranium enrichment centrifuges, was the first cyber-weapon to be publicly disclosed."[63] She then reports on two more incidents: the first was a failed attack on North Korea's nuclear program, where the virus only worked if directly entered into the system from inside the complex, and the second was an attempted email phishing scheme that hit 3,500 employees at Korea Hydro & Nuclear Power Company, which company denied any operations were compromised.[64]

[60] David Martin, *Russian Hack Almost Brought the U.S. Military to Its Knees*, CBS News (Dec. 15, 2016), http://www.cbsnews.com/news/russian-hack-almost-brought-the-u-s-military-to-its-knees/.

[61] Damian Paletta, *FBI Director Sees Increasing Terrorist Interest in Cyberattacks Against U.S.*, The Wall Street Journal (July 22, 2015), https://www.wsj.com/articles/fbi-director-sees-increasing-terrorist-interest-in-cyberattacks-against-u-s-1437619297.

[62] Lamadrid, *supra* note 47.

[63] Penny Hitchin, *Cyber Attacks on the Nuclear Industry*, Nuclear Engineering International (Sept. 15, 2015), http://www.neimagazine.com/features/featurecyber-attacks-on-the-nuclear-industry-4671329/.

[64] *Id.*

Director general Yukiya Amano of the International Atomic Energy Agency (IAEA) spoke at the first International Conference on Computer Security, warning, "Last year alone, there were cases of random malware-based attacks at nuclear power plants, and of such facilities being specifically targeted."[65] All a terrorist cell would need is to acquire the virus program and be granted access to a US nuclear power facility, allowing them the ability to wreak havoc on a monstrous scale. Unlike the terrorists in *24*, the counter argument is that no one to date who has the credentials to enter a nuclear power plant in the US has ever been reported. But, as Hitchin mentioned above, used as an email attachment or download, all ISIS would need is for one employee to open a malicious email to breach the system.

Conclusion

Recruiting and hiring efforts need to be offered to hackers who qualify, and the possibilities are endless when it comes to offering incentives to groups such as Anonymous or GhostSec for providing information that leads to the capture or death of ISIS members. Both hacker groups have employed effective tactics such as posing as recruits to gain information and suppressing terrorist-owned social media recruitment accounts, sometimes even terminating accounts. Gabriella Coleman, a scholar on hacker culture, said

> People go into these forums and try to cull intelligence data themselves. . . . We see this quite a bit in the hunt for pedophilia, Anonymous and other non-Anonymous people are essentially hunting these people out. I think this is a development that will stay with us as citizens—this citizen intelligence-gathering. They are able to send this information to the FBI, and stuff like that. It's unknown whether or not this is fruitful, but it's obviously helpful to have this flow train of more eyes out there. It could be potentially beneficial.

Coleman also notes that private citizens who attack terrorist groups are opening a new front in the arena of digital conflict: "That being said, this wave of civilian-led digital attacks on a force like ISIS marks

[65] Yukiya Amano, *IAEA Director General's Speech at International Conference on Nuclear Security: Commitments and Actions*, IAEA News Center (Dec. 5, 2016), https://www.iaea.org/newscenter/statements/speech-at-international-conference-on-nuclear-security-commitments-and-actions.

a new development fighting terrorism, just as ISIS's use of social media propaganda marked a new development in waging it."[66]

To determine the fruitfulness of this "citizen intelligence-gathering," more studies such as the one you just read must be done. Ultimately, future cybersecurity efforts will be shaped by many factors, including new ideas such as working with hackers to fight online terrorism. For this cause, it would be beneficial if we offer the public opportunities to help fight terrorism, even if it is just through awareness. Additionally, more government resources should be devoted to cyberterrorism prevention. Of course, Congress would rather consider more cost-effective options such as international coordination on locating and helping troubled and potentially extremist youth to have better education and opportunities or encouragement for communities and businesses to work together on finding ways to raise awareness on cyberterrorism. Providing incentives and government job opportunities through a US cyber warfare initiative can equate to more pro-government volunteer hackers getting involved in the fight. So, permit me, then, to offer the most auspicious of alternatives: that we work with hackers to bring down ISIS and future online terrorism.

[66] *Id.* at 26.

Contributors

David McEntire is the Dean of the College of Health and Public Service at Utah Valley University. He has had a long career in National Security, including teaching FEMA employees about how to properly respond to terrorist attacks. He has authored five books and has written several academic articles on international disasters, response and community preparedness, homeland security and emergency mangagment theory. He recieved a Bachelors degree from Brigham Young University, and a Masters and PhD from the University of Denver. Dean McEntire recieved the 2010 B. Wayne Blanchard Award for Academic Excellence in Emergency Managment in Higher Education.

Robert M. Jorgensen joined the faculty of Utah Valley University in 2013 after a 20-year professional career along the Wasatch Front. He is the Program Director for UVU's Cybersecurity programs, including the new Master of Science in Cybersecurity, which was launched in fall 2017. Robert is a frequent presenter and panelist at conferences ranging from the Governor's Utah Economic Summit to cybersecurity conferences such as BSidesSLC and Derbycon. He is active in the local cybersecurity community as the CSX Liaison for the Utah Chapter of ISACA, the President of the Salt Lake City Chapter of (ISC)2, and a member of the board of directors of UtahSec.

Frederick H. White is the Associate Vice President of Engaged Learning at Utah Valley University and professor in the Department of Languages and Cultures. He is a leading specialist on the Russian writer Leonid Andreev and has published in Russian Modernism, psychology and literature in the Russian fin de siècle, the economics of culture, and post-Soviet cinema.

Samuel Elzinga is a freshman at Utah Valley University, majoring in Political Science and minoring in Constitutional Studies. He is very involved in clubs on campus and currently serves in the leadership of

College Republicans and Young Americans for Liberty. He is also currently interning in Congressman Chris Stewart's district office. Samuel plans to attend law school and hopes to build a career in privacy and national security law.

Monica English is a senior in Utah Valley University's Integrated Studies program. her areas of emphasis are Peace and Justice Studies and Religious Studies. She is also pursuing a minor in Gender Studies. Monica currently serves as the Vice President of UVU's Peace and Justice Club and is also a student fellow for the Ethics Center on campus. Monica has presented papers at several conferences, including the J. Bonner Ritchie Dialogue for Peace Symposium, the European Horizons Western Regional Conference, the Writing for Social Change Conference and the Wheatley Institute Religion in the Public Sphere Conference. Monica's current research interests are women in peace building; the intersection of religion and gender and the post-conflict aspects of Northern Ireland. Monica is co-writing a paper on the intersection of religion and sexuality with Dr. Debjani Chakravarty. Monica is preparing to return to Northern Ireland in June of 2018 to interview members of the Northern Ireland Women's Coalition about their role in peacebuilding in the 90s.

Quinn McCloskey is a graduate of Utah Valley University who holds a bachelors degree in Criminal Justice and a minor in National Security Studies. Before attending UVU, he served six years in the U.S. Air Force as a Cryptologic Language Analyst. He now plans to use his experience and degree to pursue a career in federal law enforcement.

Andre Jones is graduating as a senior from UVU in Political Science with a focus on Russian and National Security. He is the founder of the *Journal of National Security* and served as its first editor-in-chief. Prior to his senior year, Andre interned in Washington DC in the office of the President Pro Tempore of the Senate working on national security and defense issues. He hopes to establish himself as a subject matter expert of security ties with Russia and one day work in the Pentagon on US national security and foreign policy. Andre was recently accepted to Masters programs at Georgetown and American University, among others.


UVU
CENTER for
NATIONAL SECURITY
STUDIES
UTAH VALLEY UNIVERSITY