CIRP Journal

Featuring interviews with Former Secretary of the Air Force Debbie Lee James and Author Clint Watts

FALL 2018 VOLUME 3, ISSUE 2

NATIONAL SECURITY

Carnegie Mellon University

CENTER FOR INTERNATIONAL RELATIONS AND POLITICS
In honor of Dr. Kiron Skinner, for her current public service at the US Department of State, directly working on the most important national security issues of our time.
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
</table>
| 7    | Letter from the Publisher and Editor-in-Chief  
*Colin Clarke* |
| 9    | Letter from the Guest Editor  
*Alexandra Pasch* |
| 10   | US Secret Courts: A Primer on Foreign Intelligence Surveillance Courts  
*Alexandra Pasch* |
| 14   | A Loose Pack: Profiles of Lone Wolf Terrorists in the United States  
*Robert Stephens* |
| 19   | State Support for Non-State Armed Groups in Strategic Rivalries: Does It Work?  
*Borge Feliz* |
| 23   | Liberty and Safety: A Quantitative Analysis of Civil Liberties  
*Susanna Seltzer* |
| 28   | Russia, Organized Crime, and Cyber Space  
*Alex Lin* |
| 32   | Organizing Against Terror: The Importance of Institutional Change in Structurally Curbing Transnational Terrorism  
*Rahmon Ross* |
| 37   | Interview with Debbie Lee James, Former Secretary of the Air Force  
*Interviewed by Associate Editor* |
| 44   | Interview with Clint Watts, Author of *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*  
*Interviewed by Associate Editor* |
Publisher and Editor-in-Chief:
Colin Clarke

Founding Editors:
Yong-Gyun Choi
Amanda Kennard
Inyoung Song
Audrey Williams

Guest Editor:
Alexandra Pasch

Associate Editors and Layout, Design, and Production:
Hillary Tanoff
Emily Half

Copyright © 2018 by the Center for International Relations and Politics, Carnegie Mellon University
Porter Hall 223E
5000 Forbes Avenue
Pittsburgh, PA 15213
www.cmu.edu/ir
ISSN: 2328-9295
Dear Reader,

At the Institute for Politics and Strategy (IPS), students have always shown great interest in national security issues. While other issues of the CIRP Journal have focused on refugees, development, and domestic political issues, this fifth iteration of the journal focuses on national security.

Since the CIRP Journal’s founding, IPS and the Center for International Relations and Politics (CIRP) have encouraged students to enter the scholarly world of discussion and examination of issues by contributing to the CIRP Journal. Our fifth journal features the abridged versions of theses by six recently graduated master's students. As the thesis advisor for two of the six alumni featured, I am proud to see their hard work published.

IPS offers students a unique opportunity to obtain an Accelerated Master of Science in International Relations and Politics (IRP/AMP). During their fifth year of study at Carnegie Mellon University, students develop a thesis proposal in the fall semester and submit a completed thesis in the spring semester. Students must defend their thesis in an open forum presentation. From an approved thesis, students submit an abridged version to the CIRP Journal for publishing.

The articles in this journal all relate to national security, yet confront a wide range of issues. While one student focuses on how FISA courts have impacted intelligence surveillance over time, another student dives into the timely topic of the relationship between Russia and cybercrime. Each article adds new and unique perspectives to scholarly discussion on national security.

I would like to thank Debbie Lee James, former Secretary of the Air Force, and Clint Watts, author of Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News, for sitting down with CIRP Journal Associate Editor Hillary Tanoff, to discuss some of the most pressing national security issues of our time for inclusion in the journal. I am sure that both of their visits to campus inspired a new generation to work on vital national security issues, be it in the public sector, private sector, or research in academia.

Sincerely,
Colin P. Clarke
Publisher and Editor-in-Chief
Dear Reader,

The Institute for Politics and Strategy (IPS) at Carnegie Mellon University began a new program in the fall of 2016 – the Accelerated Master of Science in International Relations and Politics (IRP/AMP). The other contributors in this journal, along with myself, served as the inaugural cohort of graduate students.

I chose to pursue the graduate program while spending a semester in Brussels, interning at the US Mission to the European Union in the fall of 2015. Due to the migration crisis stemming from Syria and the subsequent terrorist attacks in Paris in November 2015, my work largely centered around topics in international security. Fascinated by my work and wanting to understand more, I applied for the graduate program.

As a result of our first core course in the master's program, Professor Kiron Skinner's Analytical Social Science and National Security, I became interested in national security law. Due to the course materials and conversations with guests such as Jack Goldsmith, Gen. (ret.) Michael Hayden, and Adm. (ret.) Dennis Blair, I chose to pursue an independent study the following semester with Professor Geoffrey McGovern. My thesis project was heavily influenced by this independent study, which gave me the time to review existing literature, understand the big issues, and focus on a specific topic.

The thesis was by far the most challenging piece of the program. It was difficult to manage a lengthy and substantial project alongside demanding coursework, research assistant roles, and teaching assistant roles. However, the process was significantly aided with great advice and guidance from my thesis advisor – Professor McGovern – who understood my interest in the topic and my goals for the project. As reading through the rest of the journal will make clear, I pursued a slightly different thesis project than the rest of my cohort. Instead of an argument-driven thesis, I wrote a primer on the Foreign Intelligence Surveillance Courts – a gap I found during my independent study. Professor McGovern helped me to organize the project, dividing it into smaller, more manageable pieces, and providing feedback at each step.

Although the thesis project and the overall program were challenging, I believe it was a highly rewarding experience. The program was an excellent opportunity to pursue more focused and specialized work. Most importantly, it revealed to me a legal specialization that I am now interested in pursuing as a career. I look forward to watching the program grow and my peers flourish in their own careers.

Sincerely,
Alexandra Pasch
Guest Editor
American presidents have relied on their Article II powers to dominate the national security domain. Article II refers to a president’s constitutional authority ‘to preserve, protect and defend the Constitution of the United States,’ to justify unitary action of surveillance both for criminal investigations and national security purposes. Consensus on these powers changed with a series of court cases in the early 1970s—United States v. US District Court (Keith), 407 U.S. 297 (1972); United States v. Brown, 484 F.2d 418 (1973); United States v. Butenko, 494 F.2d 593 (1974); Zweibon v. Mitchell, 516 F.2d 594 (1975); and United States v. Ehrlichman, 546 F.2d 910 (1977). Together, these cases mark a significant five-year period of judicial review.

As the courts clarified the surveillance powers and authorities of the president during the 1970s, political developments and corruption scandals ensued under the Nixon administration. Following the Watergate Scandal, two congressional committees—the Church Committee and Pike Committee—convened to investigate the break-in. Considering the extensive surveillance powers of the executive and political corruption surrounding intelligence matters, Congress exercised its power to establish ‘such inferior courts.’

On October 25, 1978, President Carter signed the Foreign Intelligence Surveillance Act (FISA) into law. In his signing statement, President Carter stressed the balance between security and liberty and affirmed that FISA “will remove any doubt about the legality of those surveillances which are conducted to protect our country against espionage and international terrorism.”

The Judges: Selection, Term & Geographic Distribution

FISA established two courts—the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR). FISC consists of eleven federal district court judges and FISCR consists of three federal district or appeals court judges. The Chief Justice of the Supreme Court designates all FISA judges. By statute, judges must be drawn from at least seven of the US judicial circuits, while three of these judges must reside within twenty miles of Washington, DC, to review warrant requests in emergency situations. They serve for a maximum of seven years and cannot serve multiple appointments. FISC judges typically sit for one week at a time on a rotating basis, while FISCR judges meet ad-hoc dependent on appeals. It should be noted that FISC and FISCR judges hold their federal

---

judgeship during their term as a FISA judge, which makes for a highly active workload.²

FISA’s jurisdiction is confined to a specific subject matter: surveillance and data collection for foreign intelligence purposes. FISC has original jurisdiction of this subject matter and serves the trial court function for all surveillance warrant requests, whereas FISCR has appellate jurisdiction and reviews appeals from the government. Essentially, FISCR is a second chance for the government to obtain a warrant.

All FISC and FISCR proceedings are held ex parte – ‘by one party’ – within FISC’s secure facilities in the historic E. Barrett Prettyman United States Courthouse building. Ex parte proceedings, where the government is the only party present, are different from other courts where defendants have the right to challenge their accuser. FISA proceedings are also held in camera- the judge reviews the evidence and conducts the hearing in his/her private chambers. In camera review, which lacks a jury or other public representation, ensures the security of classified material.

Several cases have challenged the constitutionality of FISC’s ex parte, in camera proceedings. The defendants in United States v. Falvey, 540 F. Supp. 1306 (1982) argued that FISC proceedings violated their constitutional right to counsel, their right to be present at proceedings conducted against them, and their right to a public trial. The court held FISC’s ex parte, in camera review process to be constitutional and noted that such review was not unique to the context of foreign intelligence.³ In Global Relief Foundation, Inc. v. O’Neill, 207 F. Supp. 2d 779 (2002), the defendant argued that FISC’s review violated his right to confront witnesses and due process. The court held that ex parte review is constitutional because the government has a compelling state interest concerning national security that outweighs the defendant’s interest in confronting his witness and responding to evidence against him.⁴

Although ex parte, in camera review is the norm, an en banc- before the entire bench or heard by all judges, not just a panel- session is optional and only occurs with exceptional cases that require uniform judgement. FISC sat en banc for In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (2002). This case regarded a request submitted by Attorney General John Ashcroft to allow for greater information sharing between foreign intelligence and criminal investigations. Ashcroft argued for information sharing to identify terrorists potentially living within the United States. Due to these extraordinary circumstances, FISC decided to hear the case en banc.⁵

Warrants and Litigation
To conduct electronic surveillance for foreign intelligence purposes within the United States, the government must first obtain a warrant from FISC. The process begins at the Department of Justice (DOJ). The DOJ reviews requests to conduct electronic surveillance or to conduct physical searches from various agencies. When FISC receives an application, a staff attorney reviews the application to evaluate whether it is complete and meets the legal requirements for warrants obtained under FISA’s jurisdiction. The staff attorney communicates with the agency attorneys to attain more information or to express concerns about the application before

---

⁴ Global Relief Foundation Inc. v. O’NEILL, 207 F. Supp. 2d 779 (N.D. Ill. 2002).
⁵ In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (2002).
writing an analysis to submit to the FISC judge designated for that week.6 The judge then reviews the application and the staff attorney’s analysis to determine the preliminary course of action. This can include approving the application without a hearing, imposing conditions on the approval, deciding a hearing is necessary to grant the application, asking for additional information, or denying the request based on the application. The staff attorney relays the judge’s inclination to the government, who will either provide additional information, make necessary alterations, or submit the final application. When submitting the final application, the government can also request a hearing.

If the application is approved, the judge determines the duration of an order, which depends on both the period necessary to achieve its intended purpose and the target. Generally, a FISA order lasts for a period of ninety days. However, if the target is a foreign power, the duration of the electronic surveillance can be for a period up to one year. If the target is an agent of a foreign power and a non-US person, the duration can be for a period up to 120 days. Therefore, FISA holds a more rigorous standard for electronic surveillance of US persons or when there is a greater probability of incidental collection of US persons.

Aside from FISC’s ex parte, in camera review process, another point of contention is the extremely low rejection rate of warrant requests. From 1979 to 2015, FISC approved 38,365 warrants and only rejected 12— a rejection rate of 0.031 percent.7 However, the annual statistics submitted to Congress by the Attorney General, which resulted in this rejection rate, reflect the final applications. This figure includes applications that were originally rejected due to insufficient evidence or other reasons, but later accepted with more information.

To more accurately report on these statistics, FISC and FISCR modified their categorization of applications. Beginning last year in the annual report to Congress – as mandated by 50 U.S.C. § 1873 – FISC now includes a separate category of ‘order denied in part’ instead of including these applications within the ‘orders modified’ category. The annual report for 2016 indicates 9 applications denied in full, 26 applications denied in part, 339 applications with orders modified, and 1,378 applications granted without modifications.8 Applications that are labeled denied, denied in part, or modified are not approved based on the initial application submitted to FISC. This classification more accurately categorizes warrant requests and shows the frequency of additional evidence required from the government.

**Major Revisions to FISA**

Since 1978, Congress has amended FISA’s jurisdiction, authority, and power. These amendments occurred through fiscal year intelligence authorizations, new legislation, and extensions of sunset provisions. Two major periods of legislative change occurred after the terrorist attacks on 9/11 and the intelligence leaks by Edward Snowden.

On October 26, 2001, President Bush signed The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act). The USA Patriot Act expanded the power of the executive branch, specifically regarding search and surveillance powers of federal law enforcement agencies and the intelligence community. Section 206 authorized FISA to approve warrants for ‘roving’ electronic

---

6 Reggie Walton, Letter from Judge Reggie Walton to Chairman Senator Patrick Leahy, United States Foreign Intelligence Surveillance Court, 29 July 2013.
7 Zak Whittaker, “Here’s How Many US Surveillance Requests were rejected in 2015,” ZD Net, 30 April 2016.
surveillance in any location and with any equipment. Section 208 increased the number of FISC judges from seven to eleven. Section 215 removed the provision which limited the types of records that the government could compel from certain businesses; it expanded the terminology to “any tangible things,” which included “books, records, papers, documents, and other items.”9 Section 218 removed the requirement that the singular purpose of the surveillance was to collect information for foreign intelligence purposes and changed it to a significant purpose. Unlike prior changes to FISA, which occurred through annual intelligence authorizations — ‘must-pass legislation’—the USA Patriot Act was a new piece of legislation. Nonetheless, it quickly passed through Congress before President Bush signed it into law.

A second period of notable change centered around leaked classified information. On June 6, 2013, journalist Glenn Greenwald, published a report about an NSA program involving the collection of telephone records from millions of Americans.10 One day later, The Guardian and The Washington Post reported on the NSA’s Prism Program and soon named Edward Snowden as the source. These leaks dramatically impacted the intelligence community and FISA, as these programs received explicit approval under Section 215 of the USA Patriot Act of 2001 and Section 702 of the FISA Amendments Act of 2008. These revelations and the 2nd Circuit’s ruling in the American Civil Liberties Union v. Clapper 785 F.3d 787 (2015), pressured the Obama Administration to reform surveillance operations under FISA.

On June 2, 2015, President Obama signed The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act (USA Freedom Act). This act banned the bulk collection of data from Americans’ telephone records and Internet metadata and banned the government’s collection pertaining to a specific service provider or a broad geographic region – direct responses to NSA programs leaked by Snowden. However, the USA Freedom Act extended three essential provisions of the USA Patriot Act until December 2019. These included roving wiretaps, lone wolf surveillance authority, and Section 215, which allows the Court to approve warrants to collect tangible items relevant to an investigation instead of a warrant based on probable cause.11 Overall, the USA Freedom Act increased transparency of FISA courts by establishing mandatory disclosure of significant opinions, public reporting for the use of surveillance authority, internal reviews by the Inspectors General, and the addition of amici curiae to provide expert opinion to FISA judges.

**Conclusion**

National security is perhaps the most important responsibility of government. At a time of emerging threats, advances in technology, and unforeseen resilience of enemies, this responsibility is likely also the most challenging. An essential part of this mission is FISA. Yet, FISA Courts operate in shadows, unlike other Article III Courts. Their subject matter jurisdiction, unique rules of procedure, and pivotal role within the intelligence community are often misunderstood and overlooked in studies of national security. As a key institution with significant authority that both enables and restricts the operations of the intelligence community and law enforcement, it is necessary to understand how these courts operate. Though limited by access to classified information, this article attempts to fill a gap in the literature and add to discussions of national security issues.

---


A Loose Pack: Profiles of Lone Wolf Terrorists in the United States

ROBERT STEPHENS

At the end of his second term in office, Barack Obama came under scrutiny for making the claim that “[n]o foreign terrorist organization ha[d] successfully planned and executed an attack on our homeland” over the eight-year term of his presidency.1 Americans were outraged that he would make such a claim after high-profile attacks such as the San Bernardino attacks, the Pulse Nightclub shooting, and others had occurred since his inauguration. Yet the problem lay in semantics. What Obama was referring to, organized group terrorism, had indeed not been prevalent on American soil. What many people were thinking of was “Lone Wolf” terrorism – a term which refers to politically motivated “attacks carried out individually and independently from established terrorist organizations or networks.”2

There was no insinuation made during Obama’s term that terrorism itself was becoming less of an issue. On the contrary, the President’s own Director of Homeland Security Janet Napolitano made it clear that terrorism was still a concern due to the unique challenges lone wolf terrorists present: “[T]hey’re not conspiring. They’re not using phones, the computer networks […] they’re not talking with others any other way that we might get some inkling about what is being planned.”3 Therefore, it is nearly impossible to pre-empt such attacks. Other scholars have gone further to show that, due to the lack of traceable networks, finding what motivates the actors in the first place is a task that proves incredibly difficult for those in the security community.4

This conundrum leaves us with a multitude of questions to be answered- first and foremost, who are the individuals that become Lone Wolf Terrorists in the United States? Because they do not operate as part of a network like formal terrorist organization participants, their behavior can be much harder to identify. Moreover, why do these individuals seek to carry out domestic attacks? While the academic literature goes a long way toward addressing these questions, my project attempts to bring a new perspective that focuses specifically on them. In doing so, I hope to push forward the conversation on this issue and address a major domestic security concern for the United States, especially given the highly varied population that resides here and the ease of access to guns that exists in the United States.

Despite looking at similar points of data from one researcher to the next, what each chooses to

2 Ramon Spaajj, “Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention,” Springer Science & Business Media, 2011, 2. Some also refer to this as “lone actor” terrorism.
3 Ibid, 3.

Robert Stephens received both his bachelor’s degree in Global Studies and International Relations and Politics, and his MS in International Relations and Politics from Carnegie Mellon University. During his time at CMU, he worked on various research projects focusing mainly on Terrorism and Insurgency in the Middle East, and he continues to be interested in this topic. He also worked with student populations in various roles with Student Life and is now serving as Coordinator of Student Outreach and Support for CMU’s Center for Student Diversity and Inclusion.
focus on becomes the basis for much of how they continue to conceptualize Lone Wolf attacks. This causes some to see a clear pattern in what causes Lone Wolf attacks, whereas others see a completely different pattern or see no pattern whatsoever. By scanning the current literature on Lone Wolf attacks, five distinct camps of thought become apparent among those who research such attacks:

1. No profile of Lone Wolves can be created.\(^5\)
2. Lone Wolves are individuals who are socially isolated.\(^6\)
3. Lone Wolves are mentally disturbed individuals.\(^7\)
4. Lone Wolves are just rogue actors who are affiliated with established terrorist organizations.\(^8\)
5. Lone Wolves are becoming more of a problem due to the dissemination of propaganda on the internet.\(^9\)

I contend that a full profile of likely Lone Wolves can be built given all the factors that I listed above, and that these individuals interact with propaganda which implicates a target group as having wronged them in some way. For clarification, this can come in the form of something such as a site which implicates minorities as destroying America, pamphlets which target groups such as the LGBT community as destroying the moral core of America, groups that preach hate such as the Westboro Baptist Church, and everything in-between. Stated formally as hypotheses, here are the predictions put forth from the literature:

- H1: Lone Wolves experience Mental Illness/Mental Disturbance.
- H2: Lone Wolves are individuals who are socially isolated.
- H3: Lone Wolves gain their sole sense of community from affiliation with the ideological communities of currently existing extremist groups.
- H4: Lone Wolves carry out attacks when they are exposed to propaganda that identifies a certain group as having wronged them.

From these hypotheses, I thus formulate my own main hypothesis:

- H5: There is a common factor (or set of factors) from these mentioned that is present in Lone Wolf attacks. It is possible to systematically build a profile of Lone Wolves by testing for the existence of these factors.

In undertaking the task of trying to build a more explanatory profile of Lone Wolf attackers, I will have to work within the realistic restraints set forth by the circumstances of such attacks. I plan on utilizing deep-dive qualitative methodology. I will look to the past to try and establish a model of what the typical traits are that we would expect from Lone Wolves.

---

5 Ibid, 854-870.
Employing a set of case studies, I will have a set list of variables that I believe have partial explanatory power as causal mechanisms for Lone Wolf attacks. I will then delve deeper into the available literature on each individual case and test for the presence of those variables in each of the cases. The variables that I use have been chosen according to what the literature points to as possible or probable push factors in these attacks: mental illness or mental disturbance, social isolation, and latent radical ideology or actual affiliation with a radical organization in the form of significant interactions with a group or its particular ideological framework which encourages an individual to carry out an attack. Finally, I will test each case as well to test if the existence of propaganda can be found in the reasoning stated by the attacker or surmised by law enforcement.

Each of these factors will be coded thusly:

- **Mental Illness/Disturbance:** Mental Illness will be coded if there was a prognosis by a professional or if the actor was taking prescribed medication for a mental affliction.
- **Social Isolation:** This coding criteria will rely heavily on the work of social psychologists who commonly describe Social Isolation as “living alone, having a small social network, infrequent participation in social activities, and feelings of loneliness.” An individual would be considered socially isolated if they are reported to spend most of their time alone and/or have reported experience of bullying/ostracism by others.
- **Radical Ideology/Affiliation:** This will be coded as such if they have claimed a connection with an existing group prior to or while carrying out the attack (i.e., in manifestos, online forums, conversation, etc.), but the affiliation claim must be bi-directional. That is to say, the group that they claim must also reciprocate the affiliation to try and control for individuals who claim certain ideologies to simply draw more attention to themselves.
- **Propaganda:** This factor will be coded in the affirmative if the background investigation after the attack reveals that they interacted with propaganda which identified a target group as having wronged them or their in-group and has a strong ideological bent to it.

I will conduct both a within-case and between-case study utilizing and comparing the above criteria. To make a stronger argument that these criteria are present across cases, I will analyze cases that vary along stated ideological lines, methods used, and targets. I will code each of the factors on a scale which ranks each factor thusly: Non-existent/Weak evidence, Partial/Suggestive evidence, or Clear/Compelling evidence. While this is not a continuous scale (as in, each category is not of equal size and distance apart) I will also represent these categories as 0, 1, and 2 respectively for the purposes of simple visual representation.

In choosing which cases I will utilize for this analysis, there are further constraints on what cases I can use for my analysis. To accurately judge the presence of the variables which I have

---

identified, they will have to be cases with a significant amount of public information available on the backgrounds of the attackers. Furthermore, I want cases that are varied on motivations, targets, and the backgrounds of the actors so that there can be more variance between the cases. This will help to compensate for the fact that, as mentioned earlier, the outcome (that of an attack) will always be affirmative in the cases that I study. This strategy is also in line with the Method of Agreement, a common choice for political science research.

To try and control for the variation on the scale of the cases, I will keep my case selection to cases that have been declared Lone Wolf attacks by the US Department of Defense or other comparable Intelligence/Security bodies (i.e., the CIA, NSA, FBI, etc.). These cases will also have received significant news coverage to ensure that I can find similar resources for all the cases. Finally, the cases all have happened within the last decade so that the difference in means of both the attackers and the coverage is not significantly different between cases.

Keeping with the criteria laid out above, I have identified six appropriate cases for study:
- Dylann Roof and the church shooting in Charleston
- Omar Mateen and the Orlando Pulse Nightclub shooting
- Syed Farook and Tashfeen Malik, who committed the San Bernardino attacks
- Dzhokhar and Tamerlan Tsarnaev, the perpetrators of the Boston Marathon bombings
- James Alex Fields Jr., the man who rammed his car through the crowd in Charlottesville, VA
- Wade Michael Page, who shot and killed six people at a Sikh temple in Oak Creek, Wisconsin

After aggregating the results, I have put them in a table to make them easier to digest between cases as well as within. The results are represented in the table below:

<table>
<thead>
<tr>
<th>Actor</th>
<th>Mental Illness/ Disturbance</th>
<th>Social Isolation</th>
<th>Affiliation</th>
<th>Propaganda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wade Michael Page</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Tashfeen/Syed</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Tsarnaevs</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Dylann Roof</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Omar Mateen</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>James Alex Fields Jr.</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Total (Avg.)</td>
<td>0.667</td>
<td>1.667</td>
<td>1.333</td>
<td>1.167</td>
</tr>
</tbody>
</table>

*These values are representative of the values each actor(s) received in their particular case for each criteria section. 0 represents Non-existent/Weak evidence, 1 represents Partial/Suggestive evidence, and 2 represents Clear/Compelling evidence*
Case Study Results
These results are quite suggestive despite some of the weaknesses of a small study. These results begin to paint a picture of what effects may be at play. The fact that each case contains at least partial/suggestive evidence of Social Isolation leads me to believe that my H3 regarding Social Isolation has some strength, while the preponderance of cases with no evidence at all about mental illness leads me to believe that my H2 regarding Mental Health does not hold up well. As for the other two – Affiliation and Propaganda – there is only an aggregate of suggestive evidence between all the cases that I have presented. There are cases present in both of these categories where no evidence whatsoever was found for the criterion being tested, but one would need to conduct a much larger study with n > 30 to find statistically significant arguments that can be made.

This study aimed to establish a more robust profile of Lone Wolf Terrorists within the United States. By isolating four recurring variables from the research – social isolation, mental illness, previous affiliation with an extremist group, and exposure to propaganda – and testing for their existence in a selection of case studies, the idea was that there would be the interaction of many of these factors across all of the cases sampled. The results reveal that there may not be quite as much variation between individual Lone Wolves as was previously thought. It serves as a starting point for the argument that there are “red flags” which can be observed across all of these cases, especially the lack of significant social interaction that these actors have with their surroundings. Utilizing the findings here, I would argue that an area of the utmost importance is figuring out how to create more social services that provide avenues for social interaction for these at-risk individuals. Doing so would likely be a large undertaking on the part of legislators, but if it could lower the instances of these abhorrent attacks (even more than concerted efforts to target propaganda or networks of which individuals may become a part) then the costs would undoubtedly be worthwhile.
State Support for Non-State Armed Groups in Strategic Rivalries: Does It Work?

BORGE FELIZ

Interstate war has been on the decline for the past several decades. However, intrastate war has not declined as dramatically, and may in fact be increasing in the future. According to Army Captain Sokolovsky Jr., the rising opportunity costs of interstate war mean the use of more proxy forces by states to achieve political goals.1 For its take on the future of war, The Economist’s Special Report indicates that intrastate war has remained relatively common, especially among fragile and failing states, and are relatively long-lasting.2 Given that the future of war will be increasingly tilted towards intrastate conflict and the jockeying among international rivalries today, how does state support for non-state armed groups (NAGs) affect the “power balance” of states in international rivalries? NAGs refer to organized groups that use violence to achieve political goals and are not under the control of a sovereign state’s armed forces.

This article will measure the power balance of the rival state as determined by the ratio of each state’s Composite Index of National Capability (CINC) scores from the Correlates of War (COW) project against support and kinds of support as defined in the Dangerous Companions dataset. The current hypothesis is that support for NAGs can be translated into a power advantage for the supporting state. The goals of this article are two-fold: provide support for the stated hypothesis thus indicating that supporting NAGs is a useful strategy and indicate some environmental factors for when supporting NAGs is a useful strategy.

Research Question and Null Hypothesis

The research question is as follows: for states engaged in strategic rivalries, how does support for non-state armed groups affect their power balance? Power balance here is defined as the ratio of their CINC scores in a given year. The unit of analysis is the “triadid-year”, a number consisting of the target state’s COW ID number, NAG ID number, and potential supporting state’s COW ID number matched with the year. The NAG ID number comes from the Dangerous Companions data set. The null hypothesis would thus be that there is no effect on the ratio of the target state’s and potential supporting state’s CINC scores over time.

Alternative Hypothesis

What can be extrapolated from the relevant literature? States in rivalries are more likely to

---


Borge Feliz graduated with his BS and MS in International Relations and Politics. During his time at CMU he was a member of the fraternity Phi Delta Theta, serving in various positions. He also served as a counselor for Camp Kesem. Borge’s internships include non-profit work, research positions, and congressional work.
support non-state armed groups with whom they share ethnic ties or who can serve a strategic purpose against their rival. In doing so, they hope to affect the power of their rival state. Given the destruction that NAGs are capable of, and with the increased possibility that a NAG’s struggle against their target state can turn into a deadlier and longer-lasting conflict, all areas of power are likely to be affected by state support for non-state armed groups. Treverton and Jones indicate that terrorists and criminal cartels have their power measured by their resources and capabilities. Generalizing, it can be stated that all NAGs can have their power primarily measured by resources and capabilities as well. Thus, states support NAGs not to bolster their own resources but to wear down their opponents. This competing hypothesis represents the “other side of the coin” to my own hypothesis. Whereas I believe the supporting state’s power is augmented and the target state’s power is unaffected, the literature indicates that the target state’s power that is decreased and the supporting state’s power is unaffected.

International Rivalries
In the study of international relations, two major camps have emerged, each with their own separate classification systems and rivalry lists: enduring rivalries as created by Gary Goertz and Paul F. Diehl, and strategic rivalries created by William R. Thompson. Conceptually we think of a rivalry as a relationship between two states in which both use military threats and force with some regularity, as well as one in which both sides formulate foreign policy in competitive terms. Goertz and Diehl construct their enduring rivalry dataset using the levels of conflict between two pairs of states. For them, rivalries refer to competition over a shared good, usually one seen as a zero-sum good for both sides. In the other camp, Thompson constructs his strategic rivalry dataset using a detailed account of perceptions felt by both sides. Because of the often covert-nature of support, strategic rivalries are better suited to the research presented in this article.

Quantitative Methods
After obtaining the excel file containing all the support data from the Dangerous Companions data set, the data was cross-referenced with the list of strategic rivalries given by Thompson and Dreyer’s Handbook of International Rivalries: 1494-2010; the relevant list of strategic rivalries included those that existed from 1945 onwards as the Dangerous Companions data set only includes NAG support starting from 1945. The cross-referenced list produced 87 pairs of states, with 3,886 instances of observations. Then, using COW’s updated CINC scores (version 5, as opposed to the version 4 originally listed in San-Akca’s data), the Ratio of Target State to Potential Supporter State was calculated. For each strategic rivalry pair, the ratio was plotted over time. In some cases, it was clear that a lowered ratio emerged indicating that during support-years it is possible that there was a direct effect of the NAGs on either raising the power of potential supporters or decreasing the power of target states. However, other instances showed fluctuations in the data or an increased ratio.

The results overall are inconclusive. Figure 1 demonstrates the proportions of the results. Inconclusive Ratios account for about 55 percent of the data with Decreasing Ratios accounting for 22.5 percent and Increasing Ratios accounting for 22 percent.

Part of this inconclusiveness has to do with how broad the research question is. By focusing on NAGs, as opposed to the individual kinds of groups, some explanatory power is lost. Furthermore, the inability to analyze the individual kinds of support among the rivalries further dilutes what can be explained. The results indicate the need for more intense and specified studies among the rival dyads. Testing the types of support that may work best to achieve an advantage over a rival state, or any targeted state, will require the construction of a more extensive dataset than the Dangerous Companions dataset. Finally, there are limitations to using CINC scores. CINC scores capture hard power, representing only one aspect of national power. Understanding the power of a state in the international realm requires examining soft power and the ability of the state to effectively channel its resources as it so desires. Doing so may mean modifying the theoretical framework used to examine this research question into one that measures power by outcomes, not necessarily resources or capabilities.

**Qualitative Methods**

The Ethiopia–Eritrea, Somalia–Ethiopia, and Sudan–Eritrea rivalries were chosen for the case studies. These are three cases where 1) both states were targeted by the other (in other words, both supported NAGs against each other) and 2) one state, in bold, emerged as a “winner”. When the “winning” state was targeted they successfully resisted the NAGs and when the state was supporting, effectively did so. The independent variable, support, is present for all cases. Thus, the cases were selected for their variation on the dependent variable. The Sudan-Eritrea rivalry results in a near 400 percent decrease in their CINC ratio over time. The Ethiopia-Eritrea rivalry results in a near 300 percent decrease in their CINC ratio over time. But curiously, the Somalia-Ethiopia rivalry only results in a near 50 percent decrease in their CINC ratio. This variation on the DV, allows the true causal effect to be larger than estimated in this study.

**Analysis**

A clear pattern emerges among these rivalries: the winners systematically supported forces that geographically dispersed the enemy. It was not necessary to provide all kinds of aid to the different NAGs. For example, Eritrea supported groups that kept Ethiopia engaged in the
Ogaden, Afar, and Oromia regions. Ethiopia supported groups in Somalia’s Jubaland, Puntland, and Somaliland regions. Eritrea supported groups in the West, South, and East regions of Khartoum, Sudan. Beyond supporting NAGs operating in distinct locations, the winning states also poured resources into more groups than their opponents. Ethiopia was targeted by a total of thirty-one NAGs, twenty of whom received state support. Eritrea was targeted by nine NAGs, only one of whom received state support. Sudan was targeted by twenty-four NAGs, eleven of whom received state support. And Somalia was targeted by eighteen, nine of whom received state support.

Taken together, geographic diversity and numerical superiority indicates strategic decision-making on the part of the supporting state. If it was simply a matter of numbers, Ethiopia would have been overwhelmed and could not have achieved a victory over Somalia. Likewise, if it was only a matter of geographical diversity, but relative to the size of the state, there’s no way Eritrea could have won a rivalry. The EIJM operated in western Eritrea which is roughly half of the country; the rest of the state is a sliver along the Red Sea.

Conclusion

The country examples observed in this article lend some credence to the idea that supporting NAGs is an effective strategy among rival states. Rival states are more likely to engage in longer-lasting and deadlier conflicts than other dyads. Moreover, the presence of NAGs increases both the intensity and duration of conflicts. Thus, when rival states begin supporting NAGs against their rivals in this more globalized world, the results will be devastating. In many ways, this narrative goes against the thinking that inter-state conflict is at an end. Inter-state conflict is simply taking on a new form, whereby states force others into intra-state conflicts. By creating these, for lack of a better term, internal distractions, rival states can engage on the world stage without being seen as rogue states while still making advances in their strategic interests.

However, given the limitations of this article, several caveats should be added. The study primarily focused on states sharing a border and states that are considered to have lower extractive capacity than their peers. Furthermore, this paper focused on states within strategic rivalries. Given the desire to overcome their rival, or at least prevent a rival victory, states are more likely to divert resources to NAGs in order to achieve this objective.
Liberty and Safety: A Quantitative Analysis of Civil Liberties and Terror in the West

SUSANNA SELTZER

There have been twenty-eight successful attacks perpetrated or claimed by the Islamic State in the West since 2014, and Islamist radicalization has not shown any signs of slowing down.¹ My research question is: what contributes to the increase of Islamist radicalization in the West? To answer this question, this article examines if unequal and unsatisfactory civil and religious liberties of aggrieved minorities in the West makes them susceptible to Islamist radicalization.

I investigate the relationship between metrics of civil and religious freedoms in Western society and the rate at which residents of those Western societies experience Islamist radicalization. The implication of a connection between these trends is that there is an opportunity for precise policy design in preventing radicalization.

**Literature Review**

There is an abundance of literature analyzing the many inputs and outcomes of Islamist radicalization in the Middle East and South Asia. However, because of the vast contextual difference between those regions and the West, that body of work cannot fully answer my question.

There are two perspectives on how to address Islamist radicalization, focused either on the recruiters or the targets, the 'demand' or the 'supply'. My work falls within the supply-side perspective of radicalization, and so this review focuses on that portion of the literature.

While much of the literature examines the choices of the recruiters, others focus on how the grievances of the would-be-recruits fester. Piazza uses quantitative methods to demonstrate a relationship between economic discrimination and domestic terrorism.² His work found that when minority communities are consistently poorer than the average, countries will suffer more domestic terror attacks.³ Ultimately, Piazza suggests that policy makers should integrate the issues of economic discrimination and ethnically-correlated wealth disparities into national security policy. The issue that Piazza leaves unaddressed is how economic

---


³ Ibid.
discrimination is an element of broader socio-political dynamics.

Similar to Piazza, Burgoon looks at the relationship between social welfare policies and both domestic and international terror attacks in Europe. Burgoon provides data to suggest that policies that address social welfare are correlated with low levels of domestic terror. The work of Koopmans contradicts some of Burgoon’s conclusions, by gathering evidence that certain welfare policies contribute to social isolation and block efforts of integration. Poor integration into the community may increase economic discrimination, increasing terrorism, and social isolation may contribute to psychological susceptibility, per Piazza and Horgan. So, it is unclear how social spending as an individual factor impacts radicalization in the West.

Because these explanations for Islamist radicalization in the West are not persuasive, I propose a new theory. I argue that greater civil and religious liberties in Western countries lower the rates of Islamist radicalization. When people feel that their lives and livelihood cannot be improved by the political system in place, they search for a new mode of political expression. Disenfranchised by the democratic process, people may become susceptible to Islamist radicalization, as terror is an alternative way of making a political impact. My research focuses on general societal issues that fuel such disenfranchisement and disillusionment, and these issues go beyond the concerns of economic gain.

Hypotheses
From my proposed theory, I developed two testable hypotheses. They are:

H1: Western countries with a higher level of civil liberties will have lower levels of domestic terrorism.

H2: Western countries with higher levels of religious freedoms will have lower levels of domestic terrorism.

Methods
To test my hypotheses, I developed a database. My dependent variable utilized the data from the Global Terrorism Database (GTD), which provided all of the domestic terror attacks in the West from 1993-2016. I did not utilize data regarding foreign fighters because that data is only available from 2014 onwards. My independent variables, civil liberties and religious freedoms, come from Freedom House and the Religion and State Project.

Civil Liberties Variables
I included thirteen variables related to civil liberties, which cover the years 2003 through 2016. The first resulting variable is the overall freedom status. This is the average of the political rights and civil liberties ratings, which themselves are simplified ratings of political rights and civil liberties scores. These scores are then themselves composites of various ratings of specific liberties available in a given country. The political rights score is an aggregate of a

Liberty and Safety: A Quantitative Analysis of Civil Liberties and Terror in the West

Table 1, Data Summary

<table>
<thead>
<tr>
<th>VARIABLES</th>
<th>Obsv.</th>
<th>Mean</th>
<th>St. Dev</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>936</td>
<td>414.4</td>
<td>236.6</td>
<td>20</td>
<td>840</td>
</tr>
<tr>
<td>Year</td>
<td>936</td>
<td>2.005</td>
<td>6.926</td>
<td>1.993</td>
<td>2.016</td>
</tr>
<tr>
<td>Domestic Terror L1</td>
<td>897</td>
<td>6.651</td>
<td>20.88</td>
<td>0</td>
<td>270</td>
</tr>
<tr>
<td>Freedom House Status</td>
<td>936</td>
<td>1.985</td>
<td>0.121</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Political Rights Rating</td>
<td>936</td>
<td>1.151</td>
<td>0.453</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Civil Liberties Rating</td>
<td>936</td>
<td>1.317</td>
<td>0.584</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Electoral Process</td>
<td>429</td>
<td>11.84</td>
<td>0.480</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Political Pluralism and Participation</td>
<td>429</td>
<td>15.33</td>
<td>0.938</td>
<td>11</td>
<td>16</td>
</tr>
<tr>
<td>Functioning of Government Score</td>
<td>429</td>
<td>10.93</td>
<td>1.326</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>Political Rating Aggregate Score</td>
<td>546</td>
<td>38.11</td>
<td>2.228</td>
<td>30</td>
<td>40</td>
</tr>
<tr>
<td>Freedom of Expression and Belief</td>
<td>429</td>
<td>15.52</td>
<td>0.738</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>Associational and Organizational Rights</td>
<td>429</td>
<td>11.81</td>
<td>0.421</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Rule of Law</td>
<td>429</td>
<td>14.21</td>
<td>1.538</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>Personal Autonomy and Individual Rights</td>
<td>429</td>
<td>14.60</td>
<td>1.202</td>
<td>11</td>
<td>16</td>
</tr>
<tr>
<td>Civil Liberties Aggregate Score</td>
<td>546</td>
<td>56.04</td>
<td>3.486</td>
<td>44</td>
<td>60</td>
</tr>
<tr>
<td>Freedom House Total Aggregate</td>
<td>546</td>
<td>94.14</td>
<td>5.369</td>
<td>75</td>
<td>100</td>
</tr>
<tr>
<td>Official State Religion</td>
<td>814</td>
<td>0.413</td>
<td>0.793</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Official Government Involvement in Religion</td>
<td>814</td>
<td>7.461</td>
<td>2.123</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>Composite measure of religious legislation</td>
<td>814</td>
<td>9.498</td>
<td>3.708</td>
<td>2</td>
<td>17</td>
</tr>
<tr>
<td>Composite measure of religious discrimination against minority religions</td>
<td>814</td>
<td>8.523</td>
<td>7.463</td>
<td>0</td>
<td>30</td>
</tr>
<tr>
<td>Composite measure of religious regulation</td>
<td>814</td>
<td>4.909</td>
<td>3.909</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>GDP per Capita</td>
<td>877</td>
<td>33.068</td>
<td>28.141</td>
<td>1.148</td>
<td>192,989</td>
</tr>
<tr>
<td>GINI Index Score</td>
<td>780</td>
<td>29.38</td>
<td>3.940</td>
<td>20</td>
<td>37.80</td>
</tr>
<tr>
<td>Log Population</td>
<td>897</td>
<td>15.25</td>
<td>2.286</td>
<td>10.13</td>
<td>19.59</td>
</tr>
<tr>
<td>Military Spending</td>
<td>778</td>
<td>1.622</td>
<td>0.751</td>
<td>0.123</td>
<td>5.574</td>
</tr>
<tr>
<td>Human Development Index</td>
<td>827</td>
<td>0.842</td>
<td>0.0583</td>
<td>0.666</td>
<td>0.949</td>
</tr>
<tr>
<td>Muslim Percentage of Pop.</td>
<td>663</td>
<td>1.028</td>
<td>0.0101</td>
<td>1.006</td>
<td>1.043</td>
</tr>
</tbody>
</table>

country’s electoral process, political pluralism, and functioning of government scores. The civil liberties score is an aggregate of a country’s freedom of expression, associational and organizational rights, rule of law, and personal autonomy scores.

Data from the Religion and State Project (RAS) provides detailed variables on religious freedom, from 1990-2014. The official state religion variable indicates if there is a state religion. The official government involvement in religion variable indicates government attitudes toward religion. The composite measure of religious regulation indicates the absence or presence of restriction on religious practices. The measure of religious legislation is determined by the presence or absence of religious laws. The measure of religious discrimination indicates government engagement from no restriction to prohibition. The

---

inclusion of the data from RAS and Freedom House accounts for both general and detailed trends in civil and religious liberties.

The control variables include the Gini coefficient score, Human Development Index score, a log of the population, military spending as a percentage of GDP, and Muslim percentage of population. Summary statistics of all included variables are available in Table 1.

**Results**

A fixed effects analysis is the most common statistical model used in the field to analyze this type of data. Table 2 contains the findings of this regression, which were analyzed as one model. In support of H1 and H2, political rights, rule of law, and freedom of expression all have an inverse relationship with domestic terrorism. This supports my original idea: an inadequate political process pushes people toward radicalization as a means of political expression. If people can express themselves politically, then they feel they can make an impact, be protected, and be themselves. Then, there is no need to seek political solutions outside of the democratic process.

However, not all the significant variables support my working hypotheses. The positive relationship between associational rights and domestic terrorism contradicts H1. This indicates that types of civil liberties affect terrorism differently. Associational rights include freedom of assembly and demonstration. The presence of greater associational rights may mean that civil society movements can more easily influence national politics, and so domestic terror would have greater political influence. However, this is only one rationalization for the relationship between associational rights and domestic terror in the West, requiring further investigation.

Additionally, there is a negative relationship of the composite measure of religious legislation with domestic terrorism, which contradicts H2. This phenomenon requires further investigation by using disaggregated data to examine how specific religious laws interact with the rates of domestic terror in the West.

In summary, higher levels of political rights, rule of law, and freedom of expression indicate lower rates of domestic terrorism in Western countries. Yet, higher levels of associational rights indicate higher levels of domestic terrorism; and lower levels of religious law mean higher levels of domestic terrorism.

**Conclusion**

Radical Islamist attacks have increased in frequency in Europe since the rise of the Islamic State. This increase in terrorist attacks is difficult to stop, as the methods utilized to curtail external attacks are ineffective. So, the desire for preemptive solutions to internal threats has prompted my research question: what factors contribute to the increase of Islamist radicalization in the West?

I originally hypothesized that insufficient civil and religious liberties made people disenfranchised with the democratic political system in the West, pushing them toward Islamist radicalization. To test this idea, I built an original database of domestic terror attacks, and civil and religious liberty metrics in the West. The analysis and evidence in this study suggests that the restrictions of some specific civil liberties, and the expansion of others, do effect how susceptible Western populations are to Islamist radicalization. This information could direct new policies for how Western governments counter Islamist radicalization. Specifically, a domestic
policy structure that is parallel to and works closely with the intelligence community would be a major step in counter-radicalization. Additionally, lawmakers should routinely communicate with minority communities and seek to address their concerns. Such communication will make these communities more connected to the democratic process, which should help to combat disenfranchisement. If such conversations and the outcomes thereof are well-prioritized, these civil liberties task-forces will contribute to the mission of lower Islamist radicalization and fewer domestic terror attacks.

While the analysis in this paper is important to the broader conversation around counter-radicalization, there is room for more analysis. In the future, I would expand the database to include foreign fighters. Moreover, I would disaggregate the information from the compiled religious legislation variable. Additionally, future qualitative case studies would build on the research done so far. Profiles of radicalized individuals may provide new insights, as well as comparative case studies of Western countries. Nevertheless, there are benefits to incorporating domestic politics – civil and religious liberties in particular – into countering Islamist extremism in the West.
In 2007, Estonia was hit with a major systematic cyber-attack. Banks and other portions of government services were effectively shut down. News stations were rendered inoperable and people could not withdraw cash. Someone had launched the first mass DDoS attack against a country. DDoS (Distributed Denial of Service) attacks are launched by large networks of compromised computers in hopes of taking down internet services through sheer volumes of service requests from a host. Sources including Estonian officials immediately pointed towards Russian hackers as the culprit.\footnote{Damien McGuinness, “How a Cyber Attack Transformed Estonia,” BBC News, April 27, 2017, accessed May 05, 2018, http://www.bbc.com/news/39655415.} While the New York Times thought this marked the beginning of an era in cyber warfare, the relationships utilized to conduct the attack have been present in Russia for an extended period of time. The Russian government has demonstrated a repeated pattern of engaging with both criminal elements and private enterprise to create a symbiotic relationship between all three entities.\footnote{Stephen Handelman, “The Russian ‘Mafiya,’” Foreign Affairs, March 01, 1994, 87, accessed May 05, 2018, http://www.jstor.org/stable/20045921.}

This pattern continues with the growth in cyber-crime and the presence of cyber criminals in Russia. Russia began the process of integrating cyber criminals into the Russian state apparatus under a roof system.\footnote{Michael Goldstein, “Russian Espionage Piggybacks On A Cybercriminal’s Hacking,” The New York Times, 2017, https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html.; Vadim Volkov, Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism (Ithaca: Cornell University Press, 2002), 68.} The roof system is an important aspect of understanding how private enterprise, organized crime, and government interact with each other and society. Each operates in a separate sphere but overlap in many ways. This intermixing between the three actors means that any policy recommendations must address the multifaceted nature of Russia’s use of several types of actors. Organized crime bosses have become successful businessmen, while intelligence agencies now have personal connections to various private security firms. Despite being separated by specific laws and rules, Russia’s many power players have created a web of both personal and professional connections that transcend the traditional bounds of each of the three worlds.

While Russian hackers may fall under the definition of non-state actors, the system of control the state exerts over them to help achieve state goals is unique. State complicity in cyber-crimes launched from its own territory combined with the use of cyber criminals in espionage point towards an attempt by the state to accommodate non-state actors. Given the fact that these cyber criminals target the United States, there runs the possibility that actions previ-
ously seen as criminal could in fact be used to disguise actions by one state against another. While it is possible for criminal groups to commit acts to benefit states, the criminal enterprise around gathering and selling information has added a whole new dimension to the aspect of relationships between criminals and the state. Cyber-crime can be utilized for espionage and interference, as well as financial gain. This shift in crime could potentially alter how states view criminals. Instead of viewing them as violators of state and international laws, some states may begin to view hackers as potential partners in furthering state policy goals. New synergies between non-state actors and states may have a dramatic impact in global politics.

The origins of this interplay between criminals, private enterprise, and the government began with the collapse of the Soviet Union security apparatus and the rise of both private security firms and large-scale organized crime groups in Russia. The collapse of public security organs began immediately after the collapse of the Soviet Union. The problem was so severe in the MVD (Ministerstvo Vnutrennikh Del, the Russian Interior Ministry responsible for domestic state security) that substantial amounts of replacements had to be found each year. “In 1989, 83,500 employees were dismissed from the MVD, including 37,000 commissioned officers… According to a rough estimate, in 1991–96 up to 200,000 officers were leaving the MVD each year, a quarter of them dismissed for violations of the law.”


By the time private security firms had become ubiquitous throughout Russia, it was clear that there was one dominant security agency that held huge sway over the sector. “Their influence is hard to overestimate, since most of them, especially former members of the KGB, occupy key managerial positions in the sector. The reemployment of state security officers has been partly managed by the professional association Business and Personal Security created by former FSB employees in 1992.” These professional associations would ensure that professional connections developed during service in the FSB could continue to be utilized even after leaving government service. Utilizing personal connections and institutions, the FSB had developed the ability to tap into the private sector in ways even the GRU or MVD were incapable of.

The second crucial player in the post-USSR collapse was organized crime. The rapid privatization of industries from the late 1980s to the early 1990s led to a legitimization of many organized crime heads. With the opening of the Soviet economy to private enterprise, organized crime groups used their ill-gotten gains to flood the market and buy up various enterprises. This meant that many “legitimate” businessmen could either be linked to the intelligence agencies, organized crime, or both. According to the MVD, as much as 40 percent of turnover and services were mafia-run by 1993. Back when the USSR was still functioning, many of these organized crime groups built vast “grey” and “black” markets. These markets revolved around the “acquisition of state goods” or selling illegal contraband. By liquidating these markets into the legitimate businesses being sold during privatization, the mafia had effectively “legitimized” the cash they had earned through “black” and “grey” markets.
To counteract the loss of both manpower and funding in the public security sector, the government began allowing officers to work in private industry while also being employed by the government. This created a system where the three actors began mixing in the realm of providing security to private businesses. This system called “roofs” exploited the weakness in state security organs and the collapse of business enforcement mechanisms within Russia. Utilizing state technical and logistical resources, these security officers moonlit as security advisors in the private sector. Their professional networks and state surveillance networks became legitimate with a new law passed in March 1992. This allowed local MVD directorates to create special units that were solely devoted to protecting paying customers rather than the public at large.\(^7\)

The government was not the only actor involved in the private security industry. Criminal elements also began to appear as players in the private security sector. In one case, the MVD moved to shut down one PPC called Barrs Protection. The director general of Barrs Protection was a former KGB major who was accused of beating and threatening the CEO of a client.\(^8\) His demands included 35 percent of the company’s shares and $20,000 for an alleged debt. These types of actors were well known even among the MVD. One MVD official was quoted as saying, “The business of private protection is impossible without relations with criminal structures. I do not mind strelki, they have been and will be. But I am strongly against what is called razborki.” (Strelki are members of criminal organizations, normally considered somewhat high ranking. Razborki are shoot outs agreed to beforehand between two groups that are vying for territory or resolving a dispute.) However, this did not stop the MVD from going after some security companies. RUBOP, a Russian anti-mafia unit within the MVD, actively pursued a PPC called Scorpion and many of its employees were arrested.\(^9\) Even without using strictly government connections, many former government employees found ways to draw upon organized crime as another partner in the security field.

Cyber criminals have also been a prevalent fixture in Russia. Russians have often dominated cyber-crime markets, with a RAND report citing Russian and Ukrainian as the primary language found on most forums hawking malware and various kinds of support systems for malware.\(^10\) However, news stories have emerged that indicate the Russian government has moved towards utilizing the vast world of cyber-crime for its own state purposes.

Evgeniy M. Bogachev is an infamous Russian-affiliated criminal hacker who currently has a $3 million FBI bounty. By developing a tool called “GameOver ZeuS” Bogachev caused over $100 million in losses while controlling between 500,000 and 1 million computers. Targeted queries on the networks of infected computers suggested ulterior motives besides pure financial gain. Queries on the network included topics such as “weapons transfers” in the time frame of when the Obama administration was sending arms to Syrian rebels. Ukrainian security services have even noted that he is “working under the supervision of a special unit of the F.S.B.”\(^11\)

Bogachev was not the only hacker working for the FSB. Another hacker named Alexsey Belan

\(^{8}\) Ibid, 356.
\(^{9}\) Ibid.
penetrated Yahoo’s email system and utilized the system for his own financial gain. However, he also targeted people of interest to the FSB. Belan used these credentials to not only sell personal information, but also sell email addresses to scammers who sent spam emails.

Belan also passed these email addresses along to another hacker, Karim Baratov, who used these email addresses to target other accounts on different platforms. Baratov was then paid bounties for each target by Dimitry Dokuchaev, who was an FSB officer assigned to the FSB Center for Information Security.12

The inherent relationship between the Russian government, organized crime, and private sector has now been extended to Russian cyber criminals. This means that not only should Russian cyber-crime activities against US firms be reexamined, but raises real concerns about how companies, and the US government view threats from now on. Previously innocuous or seemingly financially-related crimes may now take a new, more sinister state-related dimension. Given the prevalence of security incidents that are attributed to Russian cyber criminals, there is a very real possibility that Russia has subsequently gained information through cyber-crime on a large amount of the American populace or those Russia has taken a keen interest in.

12 United States vs. DMITRY DOKUCHAEV, a/k/a “Patrick Nagel,” IGOR SUSHCHIN, ALEXSEY BELAN, a/k/a “Magg,” and KARIM SARATOV, a/k/a “Kay,” a/k/a “Karim Taloverov,” a/k/a “Karim Akehmet Tokbergeno-e (United States District Court for the Northern District of California November 2, 2017).
In the age of increased terrorism and extremism, how institutions reorganize themselves to combat these threats from international actors is an extremely important part of the equation when it comes to developing and employing a comprehensive counterterrorism strategy. A comprehensive review and analysis does not yet exist on the effectiveness of institutional changes that were initiated after a major attack. This research will thus seek to expand the base of knowledge on counterterrorism strategy by conducting an in-depth exploration of institutional changes to law-enforcement agencies, intelligence gathering apparatuses, and national security focused organizations, offices, and bureaus and look at their track records of success across nations to evaluate just how effective these organizations and institutional changes are.

Since 2001, terrorist attacks perpetrated by radical Islamist elements have targeted Western and developed Middle Eastern countries.1 These attacks have undermined security and overshadowed the optimism that marked the early turn of the century. Because of these attacks, many countries have pursued institutional changes to combat what they see as weaknesses in their systems.2 These changes include operational changes for local law enforcement, changes to the security and surveillance apparatus, shifts in immigration law and policy, as well as broad packages of laws regarding the authority of the government to conduct and institute various counterterrorism measures domestically.3

Yet how effective are these measures? Have these institutional changes really gone further in preventing terrorist attacks on the homeland? Are there shortfalls in the current systems that are currently being employed and if so where do they possibly exist? These are some of the main questions that this article will examine as I try to assess just how successful and effective institutional change has been in the wake of major terrorist attacks.

To assess the effectiveness of institutional change in combatting terrorism I use a case-study based approach. The four cases evaluated for this research are Spain after the Madrid

---

1 David C. Rapoport, “Before the bombs there were mobs,” in Terrorism, Identity and Legitimacy, ed. Jean E. Rosenfeld (Routledge, 2010), 137-167.

---

Rahmon Ross graduated with a BS in International Relations and Politics and his BA in French and Francophone Studies from Carnegie Mellon University in 2017 and earned his MS in International Relations and Politics from CMU in 2018. He previously worked for the Office of Senator Tim Kaine and New Leader’s Council. He currently serves as a staff member in the Office of United States Senator Robert P. Casey Jr.
bombings in 2004, the United States after 9/11, the United Kingdom after the 2005 London bus and train bombings, and India after the 2008 Mumbai attacks. These cases all saw massive attacks take place and as expected, a series of institutional changes followed. The changes that will be examined in this paper fall along three broad lines:

- Changes in Law Enforcement (National, State/Regional, and Local)
- Changes to the Legal Regime
- Changes to the Intelligence Community

By focusing on these three categories I hope to set a baseline for analyzing counterterrorism institutional change, seeing both how profound or not changes are within cases and how that varies between cases. Types of changes include enlargement of law enforcement, creation of new departments, consolidation of old ones, expansion of powers and authorities, creation of official posts within agencies for interagency cooperation and other discernible changes to counterterrorism institutions.

Spain

In the wake of the 11-M attacks, Spain completely overhauled its counterterrorism institutions and implemented a host of reforms that gave rise to a vast counterterrorism apparatus that focused on domestic intelligence gathering, law enforcement, and an enhanced legal regime, the three broad categories that I focus on in this article. 4 As Spanish newspaper El País notes, the small group of 140 domestically-focused, counterterrorism agents that focused on possible jihadi attacks grew to a shadow army of 3,000 agents and officers that worked exclusively on the threat posed by radical jihadi terrorism in 2017. This dramatic shift represents a more than 2100 percent increase in size for the counterterrorism intel community in Spain. The legal and judicial regime also changed dramatically to account for the threat of jihadi terrorism in Spain. 5 Preventative arrests spiked, and new positions were created within the legal system such as the Prosecutor's Coordinator of Terrorism Cases that deal directly with the prosecution of terrorist subjects and help coordinate the arrest, detainment, and convictions of terrorist suspects. 6

The result of this move is that in over thirteen years since the 11-M attacks, more than 700 arrests have been made along with dozens of convictions solely on terrorism charges according to numbers from the Spanish Ministry of Justice. 7 This is in stark contrast to the almost non-existent law and judicial regime that existed to handle the Islamist terrorist threat facing Spain.

India

In the years following the Mumbai attacks, the Indian government launched a series of changes to bolster security and better institutionalize its counterterrorism regime. Unlike Spain where changes included sweeping reforms of legal regimes and the creation of new legal offices to prosecute terrorists and suspected terrorists alongside changes to law enforcement and intelligence agencies, India focused much more heavily on changes to its security forces

---

5 “Jihadist Terrorism: Could There Be a New Attack on Spanish Soil?”
6 “Jihadist Terrorism: Could There Be a New Attack on Spanish Soil?”
7 “Jihadist Terrorism: Could There Be a New Attack on Spanish Soil?”
with more minor changes made to the intel community. These changes included a substantial increase in the number of police officers and security forces patrolling Mumbai and other large cities as well as an increase in the Indian coast guard to facilitate better coastal monitoring and defense. Hundreds of additional coast guard members were recruited. Institutional change seems much more fragile in India however, as many of these changes appear more for show and lack a clear commitment as opposed to more concrete and well-implemented changes that we see in Spain and as I will discuss later, in the cases of the United Kingdom and the United States.

The United States

The American government demonstrated an incredible capability to push through reforms in the wake of 9/11. Almost immediately after the attacks, Congress crafted a bill of provisions to bolster security and make institutional changes in the pre-existing security and counterterrorism apparatus. The resulting USA PATRIOT Act went into effect on October 26, 2001, resulting from the compromise legislation of two bills H.R. 3004 and S. 1510 that had passed the House and Senate respectively less than two weeks prior. The PATRIOT Act initiated sweeping changes to the counterterrorism regime of the United States. Among its many provisions the PATRIOT Act institutionalized the use of roving wiretaps, removed institutional barriers in the form of laws that had previously prevented intel sharing and instead allowed and, in some cases, mandated greater cooperation and intelligence sharing between the intelligence community and law enforcement agencies at the federal and local levels. Furthermore, the PATRIOT Act made changes to the legal regime of the United States, codifying new definitions for what counted as terrorism, expanding who could be charged, allowing for the use of secret or sealed warrants for terrorism through the FISA Courts, and increasing the penalties and charges associated with crimes of terrorism and attempted terrorism.

In addition to the changes pushed by the PATRIOT Act, subsequent appropriations bills and budgets allocated more financial resources to federal law enforcement, the Department of Justice, and intelligence agencies so that these institutions could formally increase their numbers to meet their increased scope of authority. The United States also created an entirely new cabinet level department, the Department of Homeland Security, to better coordinate its counterterrorism response and shore up the protection of land and maritime borders with the passage of the Homeland Security Act in 2002. The law consolidated what had been twenty-two separate agencies including the Coast Guard, FEMA, ICE, and the Secret Service into one department and gave cities and states one centralized point of contact within the federal

---

14 “The USA PATRIOT Act: Preserving Life and Liberty,” The United States Department of Justice.
government for all homeland security needs.\textsuperscript{17} The law also established a fund for disaster and domestic attack recovery and relief that could more easily be deployed on an as-needed basis, giving more flexibility to relief efforts.

**The United Kingdom**

After the terrorist attacks on July 7, 2005, the British government implemented a series of reforms to bolster their authority to catch and prosecute terrorists and potential terrorists and devoted less effort to changing the intelligence apparatus through passage of the Terrorism Act of 2006.\textsuperscript{18} This piece of legislation made several changes to the legal regime of the United Kingdom. It established what constitutes terrorism through establishing an official legal definition in the UK legal code, it established which acts, and in some cases speech, constituted terrorism under this new definition, who can be charged for terrorism, and broadened the scope of what crimes could be prosecuted under the law as terrorism.\textsuperscript{19} This broadened class of crimes included associating with certain organizations and the outright criminalization of other organizations.\textsuperscript{20} Additionally, the law increased the punishment for many of the pre-existing crimes that had been codified under the category of terrorism under previous laws and granted law enforcement increased authority to conduct surveillance and pursue suspected terrorists and their sympathizers both for crimes already codified as terrorism and those that were newly codified as terrorism.\textsuperscript{21}

\begin{center}
\begin{tikzpicture}
\begin{axis}[
    width=\textwidth,
    height=0.3\textwidth,
    legend style={at={(0.5,-0.15)},anchor=north},
    ymajorgrids=true,
    grid style=dashed,
    ylabel={Number of Terrorist Incidents},
    xlabel={Year},
    ytick={0, 200, 400, 600, 800, 1000},
    yticklabels={0, 200, 400, 600, 800, 1000},
    legend entries={India, Spain, United States, United Kingdom},
]
\addplot[red,mark=*] table [x expr=\thisrow{year}-2000, y index=0] {data.csv};
\addplot[green,mark=*] table [x expr=\thisrow{year}-2000, y index=1] {data.csv};
\addplot[blue,mark=*] table [x expr=\thisrow{year}-2000, y index=2] {data.csv};
\addplot[purple,mark=*] table [x expr=\thisrow{year}-2000, y index=3] {data.csv};
\end{axis}
\end{tikzpicture}
\end{center}

**Analysis and Conclusion**

These cases demonstrate that institutional change matters a great deal when evaluating the success of counterterrorism regimes, at least in the United States, the United Kingdom, and Spain. These three cases all manage to prevent major transnational attacks after an initial event and they were the three cases that implemented and committed to institutional changes to their counterterrorism regimes.

\begin{itemize}
\item \textsuperscript{19} “The Terrorism Act 2006,” GOV.UK.
\item \textsuperscript{20} “The Terrorism Act 2006,” GOV.UK.
\item \textsuperscript{21} “The Terrorism Act 2006,” GOV.UK.
\end{itemize}
In all of these countries the ten-year trend according to the GTD for transnational terrorism incidents appeared to be flat. Indeed, we do not see evidence that terror incidents are dramatically increasing in instances, even when one considers the premise laid out by David Rapoport that overall ideological terrorism is increasing, and we should expect the stated targets of these ideologically driven terrorist groups, largely the West, to come under fire. In combination with the numbers from the GTD, this indicates that something has radically altered the ability of groups to perpetrate attacks on these countries.\(^{22}\) Given that attacks in these countries hold steady while increasing in other parts of the world according to the GTD and the Global Terrorism Index, the trend indicates that the driving force is domestic as opposed to international. This directly refutes those who may try to credit the War on Terror and deployment of troops abroad.\(^ {23}\)

The most significant of these domestic changes in each of these cases was the institutional reforms and structural changes to counterterrorism taken by domestic intelligence, legal, and law enforcement regimes. That is not to say definitively that institutional change drives all advances in security and can fully take credit for holding the success rate of transnational terrorism down. Other variables could be at work here, such as shifts in where terrorism comes from, the increased use of the internet in growing domestic terrorism, changes in targets, and the success of technology at catching potential attackers. Keeping that in mind, more research needs to be conducted by those with more resources to conduct broader and more in-depth multivariate and case-study based analyses that can better narrow down the effectiveness of institutions and structural reform at targeting and preventing transnational terrorist events.

Additionally, commitment to these changes accounts for a great deal of the success in combating transnational terrorism. In the cases of the United States, and Spain, massive investments and changes to institutional structures followed the respective 9/11 and 11-M attacks. These changes represented a major shift in the way the two countries organized themselves to combat the occurrence of transnational terrorism and included changes to all three measures. In the United Kingdom, at least two of these measures saw meaningful change. In India however, while the government did pursue institutional change in writing for law enforcement, the intelligence community, and the legal regime, the institutional changes undertaken were not nearly as sweeping as they were in the United States or Spain, containing neither a broad restructuring of institutions nor a broader bolstering of national law enforcement agencies. These changes were so poorly committed to that it was almost as if the legislation granting them was not passed. The result was a continued series of transnational attacks and attacks that had no clear origin due to overlapping credit claiming.

Taken together with what is observed in the cases of the United States, the United Kingdom, and Spain, a case can be built that indeed institutional changes are important to combating transnational terrorism and so too are the quality and commitment to those changes. In the future it would be interesting if more research could be done to establish just how much importance can be assigned to institutions and to what extent institutional change plays a role.

\(^{23}\) Global Terrorism Index 2016, Institute for Economics & Peace.
Interview with Debbie Lee James, Former Secretary of the Air Force

On September 27, 2018, Debbie Lee James, Former Secretary of the Air Force, visited Carnegie Mellon University to speak about US national security, to tour the campus’s Cylab, and to speak with students about leadership. During her time on campus, she sat for an interview with CIRP Journal Guest Editor and CIRP Research Coordinator, Hillary Tanoff. They were able to cover a range of topics, including Ms. James’s journey to becoming Secretary of the Air Force, US national security issues like Russia, China, and terrorism, and a RAND report on sexual assault in the military. Ms. James is the 23rd Secretary of the Air Force. She has thirty years of senior homeland and national security experience in the federal government and the private sector.

Tanoff: With such a distinguished career in public service, can you tell me what public service and purpose mean to you?

James: I was a very determined young person and I was determined to be a diplomat. So from my earliest years, the beginning of high school, I wanted to be in public service. Although I did everything that I thought were the right things to lead me to a path of becoming a foreign service officer, it didn't work out for me. Instead, I pivoted to what became the next best thing. In reality, it was the best thing of all, I just didn't ever consider it before. And that was service on behalf of the US military, another important part of national security just as the State Department is. That is where I found my purpose.

By the way, public service is one way to find that purpose, but the private sector is another way, also working on national security matters, where I have been able to find purpose. Overall, to me, purpose means doing whatever floats your boat individually. So, you can find purpose in all different careers. But if you look for something where you are somehow contributing to something bigger than yourself and particularly to the betterment of people, that is where I have found my greatest purpose in both the public and in the private sector.

Tanoff: You actually touched upon my next question, on national security- how did you get involved in that realm of public service?

James: I had an older sister who worked for an airline, and because of that, in the 1970s when air travel was really quite expensive and most middle-class Americans couldn’t afford it, she would receive free airline passes, which made it affordable for us to go once a year. So, I was smitten with the travel bug fairly early on, which led to my desire to be a diplomat. I thought it would be a way to see the world and to work on important issues of trade and international flow of people and other important issues that the State Department is responsible for. So that is how I became interested in the
arena. But when I ultimately applied to the State Department at the age of about twenty-two or twenty-three, they rejected me. Although I thought I did all the right things, I didn't achieve that dream. And I remember crashing for about five days but on the sixth day I got out of bed. I said to myself 'I must get a job' and I started applying elsewhere.

The year was 1981 and that was the first year of President Reagan’s defense build-up. Defense had most of the jobs. Although I wasn't particularly interested in defense- probably because I had no exposure to it- that is where I got a job offer. So I threw myself into it. After a few months, I discovered- [three things]. [First], the work was extremely interesting and I was feeling that purpose. I remember reading in the morning my *Washington Post* every day and looking at the headlines of the day and seeing just a little bit of myself and work that I was doing in those headlines of the day. So it gave me that feeling of- I'm part of something much bigger than myself. Second, I had a great team of people around me, all of whom were much older but they took me under their wing and it was a very collegial and collaborative experience. And third, I had a fantastic first boss who turned into a great mentor, who gave me valued advice and who helped me make connections and open doors for other possibilities that otherwise would not have been open for me.

So I like to say that everybody needs a plan A, which for me was the State Department. But sometimes your plan A doesn't work out. Sometimes you achieve plan A and it’s not always what you hoped it would be. So be prepared always to pivot to Plan B, whatever that Plan B may be. Because it could just be the best thing ever. And that is indeed what happened for me. Because you don't know what you will find interesting, until you get into it and explore it a bit, and then you can find your greatest passion of all.

**Tanoff:** You have mentioned before that talent acquisition really needs to change. How do we get younger generations interested in public service in general and then military service in particular?

**James:** The military and other departments of government should step up their own public affairs strategies to get the word out across America about what it is to be in public service. They need to step up their recruiting efforts at some of the top universities. They need to streamline some of the morass of what is today the hiring authorities for the federal government. It takes too long. It's too complicated. Salaries need to be reviewed, because on average, the government can’t begin to match some of the private sector salaries, particularly for the in-demand skills like cyber, engineering, and technical skills. We'll never in the government be able to match them. But we can do better to advertise the purpose that the government has; the fact that people who come to the government will be working on the most important, vexing challenges of their generation. And the leadership opportunities and the educational follow-on opportunities are unmatched in the government. So we need to kick it up a notch.

From a military perspective, we need to look at changing some of the very rigid structures of today that put in place requirements for accepting new people into the military which are still valid in some cases but I
would argue not valid in all cases. We should look at waving some of those requirements; particularly when it comes to key talent like cyber, like space, like [artificial intelligence]- that we so desperately want and yet we're having a hard time keeping up and attracting.

Tanoff: Moving over to national security topics- with Russia and terrorism being some of the biggest threats to our national security- how has Russia changed as a threat over the course of your career?

James: Back when I was going through school, the Soviet Union, which of course was broader than Russia, was the singular threat that my generation was concerned with. It was an extremely dangerous threat because the nuclear capabilities of Russia could decimate the United States. Of course the United States could decimate them and hence the strategy in those days was called mutual assured destruction. It held both sides at bay from taking a first strike. The Soviet Union, as dangerous as it was, we understood. It was containable through the strategies, and approaches, and the diplomacy of that era. It was largely a bipolar world- we had the United States and we had the Soviet Union.

Flash forward to today, the world is anything other than bipolar and containable and predictable. It is multipolar, it is messy, and you never can quite predict what happens next. For years, after the dissolution of the Soviet Union, there were active attempts, some even being successful, to partner with Russia and to have a new day with Russia. I would say all of that ended in 2014 when Russia… invaded Crimea. That is the watershed moment where the West said ‘no more’. It has been different with Russia ever since.

Considering actions since 2014, it has seemingly deteriorated more and more. They entered the war in Syria on the side of Syrian dictator Bashar al-Assad and they tipped the balance of power toward Assad. Obviously, the United States is not happy about that. But it’s a fact and it has happened. Going into Syria also allowed Russia to have real-world combat experience that they had not had elsewhere. They were able to test out weaponry, concepts of operations, and become a better military as a result of that practice- which is another worrisome aspect for the United States. And finally, they are investing and testing in a new generation of nuclear weapons, in hypersonic [weapons], which is very worrying. And, the whole world now knows of their cyber warfare and the meddling in elections in the United States and elsewhere. So that’s some of what’s happened with Russia.

Meanwhile terrorism went on before September 11, 2001, but with that horrific event the United States swung heavily toward the War on Terror in terms of security spending and focus, which has been going on for seventeen years now. Although progress has been made on certain fronts, I suspect that there’s no end in sight. So we’re going to have to continue to keep that focus but now also concern ourselves once again with Russia.

Even more important is China, a pacing threat nowadays for the United States military. China was around in the Cold War but it wasn’t a major power then. Now it is an economic and military behemoth. The United States has really sat up and taken notice. China has also been investing and testing in ways that are worrisome, not the least of which is in counter-space capabilities. They have developed an anti-satellite approach which would have the capacity to knock out our satellites in orbit. That’s extremely worrisome because space is so important to everything that we do. Finally, China has laid claim to virtually the entirety of the South China Sea. They are creating islands out of what heretofore had been coral reefs. They’re putting military equipment [on those islands]. They’re militarizing those islands. The concern there is that they would control trade and limit access and freedom of navigation, which
would be certainly against our interest and the interest of our allies. We don't accept that.

These are some of the new threats, the so-called return of great-power competition that we're now facing. And we're adjusting our security spending, our investments, our concepts of operations, to be able to deal, once again, with great-power competition. But we can't let the ball drop on terrorism either.

**Tanoff:** Can you talk more about Russia as a conventional threat to the United States? It's clear that Russia's a cyber-threat, an unconventional threat. What Russia did in Crimea is against international norms and law but it's hard to make that connection of Russia as a conventional threat for a lot of Americans.

**James:** The concern about Crimea is that although Ukraine is not a member of NATO, if Russia were to move against a member of NATO, the United States is bound by treaty to go to the defense of NATO. Every individual nation has made that same promise. If there were to be a troop movement using the same pretext [as Crimea], that the Russian-speaking people of Lithuania or the Russian-speaking people of Estonia feel like they're not fully accepted within those societies, Russia [can] move in- that's essentially what happened in Crimea. Those two are NATO states, so we would be bound by treaty to respond. That would mean... massive numbers of Americans would be drawn into the fight. I daresay US citizens would sit up and take notice if that were the case.

Of course, we don't ever want to fight. Those people who are in the military don't want to fight. They, of all people, realize what war is like because they've seen it. So they want to deter and they want to beef up the member states of NATO, so that... those states can similarly deter. That's really the approach. But there are insidious ways, coming back to the theme of cyber, where Russia has increasingly been spoofing. It's difficult to say with absolute certainty that it is Russia. The whole point is to confuse and to upset civil society and cause unrest. So that's another form of what is now called hybrid-warfare. The other element is when they have, usually Russian citizens, who are military or paid for by the military who go in under the guise of being local citizens, confusing the situation.

**Tanoff:** Switching to China, which you've mentioned a couple of times, one of the ways in which the United States needs to improve in relation to China is the acquisition process. Can you tell me about how the United States is improving the acquisition process- it's very long, it's very complicated- and what more needs to be done?

**James:** The concern on the acquisition process, particularly when it comes to some of the new technologies, where we believe that these new technologies, will be the next big generation of warfare capability- and I'm speaking here of things like robotics, artificial intelligence, cyber, space assets, autonomy- [is that] these technologies are changing at the speed of software. They're not changing in a slow way but rather they change constantly. If our acquisition systems are designed to purchase equipment and systems over the course of five, ten, fifteen years, that is way too slow. Somehow we need to speed it up. China, North Korea, some of these states who are potential adversaries, they are able to move much more quickly. Although those countries, of course, have some level of bureaucracy as well. They seem to also not have the regulations, the laws, that we have that are designed for good reason- to make sure that we have competition, to make sure that selections are done fairly. There are reasons why we have thousands of pages of acquisition regulations. Yet somehow, we're going to have to find a different way of ensuring competition and fairness but move more quickly or we will get left behind. So that is the challenge.
A variety of teams have tried to do better, and in my opinion each team makes incremental improvements. So, for example, when I was in the government I think our team made incremental improvements. I think the team that is in government right now in the Pentagon is making more improvements. We just have to keep the pressure up, this is a continuum. We have to strip out as much of the regulation as we can—still having competition, but strip out as much of the red tape as possible. We have to get our own workforce in the Pentagon who is making these judgements to be less risk-averse, and be willing to take more chances and prototypes. If it doesn’t work, throw it out, try something new. Right now, the workforce is very risk-averse because whenever anything does go wrong, you usually get hauled before Congress, your career ends. That’s not a good culture to promote innovation, so somehow we’ve got to reverse that and make the workforce less risk-averse. We need to take advantage of some new authorities that we’ve been given in recent years, that are specifically designed to go faster and to encourage companies, including startups, who have some of these fantastic innovations, to be more willing to work with DoD. Right now we’re very hard to understand, we’re hard to navigate. It takes too long; startups can’t wait a year for DoD to make a decision. There are new authorities designed to allow us to work more efficiently with some of the very innovative, new companies.

**Tanoff:** Moving on to a different topic of drones—how do you see that they’ve changed aviation? Do you think that manned aircraft will become obsolete or that drones will really stay in a support role?

**James:** Remotely piloted aircraft, as most of America refers to them—drones—I think they have changed the face of the modern Air Force. I think they’re very much here to stay. But I suspect, so are manned-aircraft, at least throughout my lifetime. One hundred years in the future, perhaps not, but I think for the foreseeable future we are going to have both. The unmanned will take on increasing importance. They have been a game-changer in the modern wars that we’ve had on terrorism because they have allowed, with great precision and without putting pilots directly at risk, for watching and waiting until the pilots who perhaps are on the other side of the world manning these aircraft, are certain that they have the right target. And then as I said with great precision, within inches, they’re able to hit that target. What that has done is it has allowed the United States and our allies to greatly minimize the loss of innocent human life—not eliminated completely, mistakes sometimes are made. This is an enemy that mixes deliberately with civilian populations because they know that we take great care and we are less likely to hit, so it is part of their strategy. But I am certain that there are fewer lost lives and fewer wrongly hit buildings and destruction as a result of this technology. So I think it’s been positive but I don’t envision a world, certainly in my lifetime, where manned-aircraft will be totally out of the loop. I think there’s room for both.

**Tanoff:** Another topic that is really important is the civil-military divide. We have a small group of people fighting our wars. A lot of people don’t understand what’s involved in the military. But that being said, with a
government civilians, have been under siege in recent years because they don't get the same respect for their work products as the military gets. I do think most of America, even those who don't know a whole lot, respect our military. They have a sense of gratitude for the military that they are bearing this burden.

And yet as you point out they don't quite understand what exactly that burden is, other than if they see a wounded military member, then they get it. But the other burdens, of course, are frequent deployments. Even if you come back whole with all of your limbs, there are frequent deployments, family separations, things of that nature, which are other forms of burden. By the way, people in the military don't necessarily understand the rest of America either. They may have grown up on a military base so they're not used to dealing with the healthcare on the outside or ever having to apply for a job directly. They don't understand as well as they could either.

I think more awareness on both sides is the answer. This comes back to the media highlighting some of these issues. More and more of our military live off base these days, which gives them more of a mix[ing] in with people who are not like them, which I think is a healthy thing. I think more Americans who don't know about the military, I would wish that they would try a little harder to educate themselves, reach out a little bit more, to be able to understand. But I think there's no silver bullet. It's a matter of being much more aware and getting involved with one another.

Tanoff: Last, this is a very timely topic- sexual assault, sexual harassment, and gender discrimination. RAND recently came out with a report with statistics from 2014, commissioned by DoD on those three topics in every branch of the military. The Air Force fared the best in each of those categories. What do you think the Air Force is getting right and what do you think the military needs to keep working on?

I will say someone like myself, I've never served in uniform, yet I've always been a civilian in the national security space. Civilians in national security or any other smaller group of people fighting those wars you get expertise, you get training, you get people who know what they're doing- so there are different ways to views this divide. How do you view the civil-military divide in this country? Do you think it's an asset or do you think that it's something we need to work on?

James: I do think there is a substantial civil-military divide in this country, just as you said. The military is increasingly becoming a family affair and a regional affair. What I mean by that is if you have a parent or an uncle or aunt or a sibling who has been in the military, you are more likely to be in the military yourself, than someone who has no direct family connection. It's also become very much a regional affair. The greatest numbers of people tend to come from the south, they come from middle America, not so much on the coasts. There are people who join the military who are [from] either the west coast or east coast, but the statistics are [that] we get them from certain regions. That leaves out entire other regions of the country. Because we haven't had a draft for a very long time, there are generations of people in families who have never served and who simply don't know.
James: The number one thing I would say the Air Force is getting right, is that the Air Force has the highest percentage of women in the force. I’m one who believes that there is a tipping point among the genders in any given organization, and I think if I were to speculate on what that tipping point is, it’s something like 30-35 percent. Once there are 30-35 percent women in any organization, the culture of that organization will come to a point of change where behaviors will no longer be accepted, where some of the issues like sexual assault, discrimination, gender bias, will start to go down in much more dramatic ways. When men see enough women in the environment and realize that women can do the job and that they do the job very well and they can be depended on, just like male colleagues can be depended on, that is an ‘Aha’ moment for many people. We in the Air Force had the highest percentage and we were striving to go even higher because after all, 50 percent of the population in America is female, so 20 percent may be the highest, but I don’t consider that to be good enough. We need to strive and do better.

When I was Secretary of the Air Force, I made it a leadership imperative and I made sure everyone knew what I was doing, working personally on sexual assault and greater diversity and inclusion in the Air Force across the board. I put it in my talking points, every speech I would give, every town hall meeting, every testimony before Congress, everybody knew it was tops with me. Everywhere I travelled I would meet locally in private with the front-line defenders against sexual assault, to hear- How is it going on this base? What’s the climate like at this base? Do you get support from the commanding officer at this base? I would take those lessons learned back to Washington and then I would work with policymakers to try to make things better.

While I was in office our statistics improved somewhat, not dramatically, not as much as I would have liked. The key statistics we always looked at were the number of reports— that is to say you want your number of reports to actually go up— because when they go up that means more people have confidence in the system. Our reports did go up. The other thing you want is the number of actual incidents of sexual assault to go down. Because sexual assault is such an underreported crime, we would get our incident data from anonymous surveys where women and men could report. So, you want the incidents to go down and they did somewhat. The one [statistic] where we didn’t make headway, I’m sorry to report, is the one about retaliation. Something like 60 or 70 percent of the survivors feel retaliation. It could be direct retaliation that they feel they’ve gone through from a boss in the environment or it could be the retaliation of the peers in the unit who take sides and who perhaps act in a disrespectful way. It’s the feeling of retaliation, whether it rises to the level of retaliation that an inspector general or that somebody could actually do something about, that’s a different matter. That’s the one [statistic] where we haven’t been able to crack the code yet. To me, this is going to be something that we’re going to have to constantly focus on and not take our eye off the ball or we could well backslide.
Interview with Clint Watts, Author of *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*

On November 14, 2018, Clint Watts visited Carnegie Mellon University to speak about his new book, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. Watts is a Distinguished Research Fellow at the Foreign Policy Research Institute and a Senior Fellow at the Center for Cyber and Homeland Security at The George Washington University. During his talk he discussed misinformation campaigns, fake news, and electronic espionage operations that have become the cutting edge of modern warfare—and how we can protect ourselves and our country against them. Prior to his current roles, Clint served as a US Army infantry officer, a FBI Special Agent on a Joint Terrorism Task Force (JTTF), as the Executive Officer of the Combating Terrorism Center at West Point (CTC) and as a consultant to the FBI’s Counter Terrorism Division (CTD) and National Security Branch (NSB).

**Tanoff**: One of the issues we've discussed on campus is America's biggest national security threat. People see three of the biggest threats to America's national security as Russia, China, and terrorism. Obviously, some are newer than others and some are recurrent. What do you think is America's biggest national security threat among those three?

**Watts**: I would pick a fourth. I think the biggest threat to US security right now is the lack of a collective American identity—meaning that Russia, China, terrorism, none of them alone would destroy the United States. Only other Americans can really weaken [our country]. We've always talked about existential threats but really only endogenous threats, internal threats, will be the ones that ultimately defeat us—so things like the national debt or not reacting to climate change. Those things precipitate internal conflict, internal strife. That's really what the Russians did in the 2016 election[s]. I don't actually see Russia as a serious national security threat in the sense that they don't want to invade us or necessarily dominate us...

I think China is more interesting because we take it as them trying to destroy us. But they're only destroying us because we keep selling them our debt. It's an economic conflict predominantly...

Terrorism has never been an existential threat to our country. It is something that will exist but terrorism is actually a sign that you don't have state versus state actions. You don't have those sorts of wars. I think it's going to take a back seat as we move towards this nationalism not globalism approach in the United States or even abroad— that is par-
titioning and breaking up alliances. Breaking of alliances almost always historically leads to state-to-state conflict.

That's what I'm most concerned about now is that we don't really know what we stand for as a country and there's not a defined majority opinion in this country about what America is and what America means. That is [our] greatest national security weakness. Whoever plays on that threat can have great gains.

**Tanoff:** As a follow-up question on Russia— you were talking about these alliances—what about NATO? If Russia invaded another country, relations with them could escalate.

**Watts:** I think that's a very serious concern. It speaks to whether there will be a democracy-led world or an authoritarian-led world. Russia smartly recognizes that the break-up of NATO and the European Union allows Russia to then have the ability to go one-on-one against almost any adversary in Europe or the Middle East... NATO and the European Union are the buffers—you have to have those in place. If you don't, each individual nation in Europe stands much weaker against Russia and can get bullied around.

I think the critical part is do we want democracy to continue to be the predominant form of governance around the world? Do we believe in civil liberties, freedoms, human rights or not? It's not really that clear at this point. Even in our US government, [in] much of our agencies [that language] it's been removed, it's been stripped.

I think that's the biggest concern to me, is [that] these unions falling will also have an economic impact. There's some foolishness right now around nationalism and tariffs. These things will ultimately lead to economic decline in many ways. We're not going to go back to steel factories like Pittsburgh had. When I was a kid in the 1970s and 80s, Pittsburgh was known for its steel. Even if we do go back to steel in Pittsburgh, it's not going to be people as much as automation.

**Tanoff:** That's a good way to bring Pittsburgh into the conversation. I think that not a lot of people here believe the steel mills are going to come back. I grew up near Youngstown, Ohio which is very much a contrast to Pittsburgh in that it was also prominent for steel but it didn't evolve the way that Pittsburgh has evolved. Here you have UPMC, one of the best research hospitals around.

**Watts:** Pittsburgh's a great success story. Pittsburgh could have been like all these other cities in the rust belt but [there's] healthcare, science, innovation, cybersecurity. This is one of the biggest places for cybersecurity in the entire world. I came from around St. Louis and St. Louis's core is rotted out but St. Louis's suburbs have evolved tremendously. The biggest data centers in the entire world are located there. They are now buying into this economic nationalism and I wonder what they do when those data centers crumble around them because [those data centers are] globalism at its core.

**Tanoff:** Staying with cybersecurity, sometimes this time period of cybersecurity is compared to the lack of preparedness before 9/11. After years of investigations, we now know that the intel community was talking about an attack for a while, but for various reasons it wasn't prevented. Cybersecurity experts have been talking about a lack of preparedness for years now. Do you see that we're prepared or moving in that direction? Do you see a similarity between those two time periods?

**Watts:** It goes in waves—terrorism and cybersecurity... they all sort of evolve. Disinformation and cybersecurity [are] the new counterterrorism. In national security, those are domains that everyone became hyper-focused on. What's interesting to me is that
the public doesn’t demand cybersecurity protection in the same way. The difference is after 9/11 the public demanded they be protected from terrorists. We had massive legislation [and] regulation. We moved in all sorts of ways to try and counter this threat [of terrorism]. That has not happened in cybersecurity.

The public has said ‘someone stole my identity’… ‘someone hacked into my bank account’, ‘my business got all its IP stolen’. They turn to the government and the government [says] ‘we don’t know what to tell you’. The United States has such a heavy and large footprint in cybersecurity. It can’t really, as a government, protect every American… That begs the question- well if you can’t protect me, can I protect myself? There’s lots of weird things that come up. For example, as a private citizen I’ve been hacked before. If I figure out who that hacker is, can I hack them back? The government would probably say ‘no’. But I would say ‘you just told me you’re not protecting me’. Part of deterrence is responding. We’ve not gotten our heads around this at all.

It’s because we’re very scared that we’re vulnerable in terms of our weaknesses. From all accounts, in terms of offensive cyber, we’re the best. We just don’t use it because we’re also the weakest maybe in terms of cyber [vulnerability]. The public has not demanded this sort of resilience yet. Even when they did after the elections, [with] election infrastructure this past week it was entirely predictable that Georgia was going to be a disaster- either from the machines not being capable, knowing the integrity of the vote, or that people wouldn’t be influenced that there is voter fraud or voter suppression, depending on what side you’re on in that debate. It’s a perfect storm, even though there have been outcries, our legislature hasn’t moved towards [regulation] and the executive hasn’t really buttoned it down.

**Tanoff:** You actually brought up another of my questions. What are your thoughts on the elections that just happened in terms of foreign interference?

**Watts:** In terms of national security and foreign interference, there are three things that you look for- hacking, infiltration, and influence. You have to hack the year before the elections that you want to influence. We did see that in very limited circumstances. I believe [a few] senators and congressmen were targeted but it doesn’t seem that any sort of compromising information was gained.

The other part was infiltration and what you did see either from the special counsel Mueller indictments or in the eastern district of Virginia a criminal complaint [was] filed- they did shut down accounts even going into 2017 and 2018, which makes it hard to infiltrate audience space. Facebook picked it up. A lot of the social media companies picked it up. That numbed the ability of the Russians…

In terms of influence, there’s a cost-benefit calculus. What does Putin get from winning one local election? Not only is it harder to influence a local or state election, what does he really gain and what might he provoke if he gets caught in a serious way?

What I think you only really saw from the Russians was the end of dumping out
there- ‘oh we have fake accounts on all these platforms and we were influencing for both Democrats and Republicans in certain districts’. That’s not really the case. Whenever they’re overt and sloppy, they’re trying to convince you of something they didn’t do. When they’re covert and manipulative over a longer duration, they’re trying to hide what they’re actually doing. It’s a yin and yang of disinformation.

They didn’t have a massive effect and that’s largely because American misinformation and propaganda far outweighs [and] is so much larger now in 2018 than the Russians were in 2016. What could the Russians do that Americans aren’t already doing to themselves? Everyone’s sort of adopted the playbook.

Tanoff: Do you think this is just going to be continuous until we can figure out a solution?

Watts: Well, now it’s more overt and it’s more about convergence. In 2016, it was more covert and about influence and getting the person they wanted elected but also undermining faith in democracy, which they did very successfully. Going forward though, they want to build alliances in the United States, so it won’t be that covert necessarily. The best way to get around the terms of service changes of social media and the US government trying to keep them from influencing Americans is to play to freedom of speech and freedom of the press, to enter into the US public debate and say ‘we want to be allies with you on certain things’ or ‘we want to engage with you’. Their long-run strategy always has three levels: it’s state-to-state, which is actually lesser, party-to-party, which they’ve been doing for quite some time, and then people-to-people. People-to-people [is] predominant on social media.

I’ll give you an example where they did one successfully and more openly- ‘Russia and United States, we should be allies in the fight against terrorists’. That’s an example of one convergence. I think you’ll see more of that convergence around national identity. Nationalism over globalism has from the beginning been the mandate of Putin and the Kremlin… They’ve done that very successfully and they have lots of natural allies. … They are on the upswing because people are using similar rhetoric. They’re using similar tactics. And, they’re actually thinking similarly to what Putin has been advancing.

Tanoff: What kind of solutions do you see for a lot of these problems? What role do both private industry and government have?

Watts: On the government side, it’s restoring faith in democracy. The Secure Elections Act that they tried to pass in the Senate, has still not gone anywhere for reasons no one can seem to explain. The Honest Ads Act about integrity in terms of advertising, ‘who sponsors what’. Those regulations are super simple and those are things that government can immediately do. The other thing is that they can correct their behavior. It’s country over party. That’s ultimately what the goal is right now. We don’t have a common understanding of what that priority would be.

National debt is a great example. One party advocated ‘we need to shut down the government’ in 2010, 2011, and 2012, which I suffered from having worked in government. The debt was raised by an enormous amount without any sort of external provocation like the fall of the housing market. Ten years ago, that was a period where you saw an external shock [and] both the Republicans and Democrats [came] together [to] say ‘we can’t let the economy completely collapse, let’s work together and we will increase our debt to do that’. Now we don’t have that. It’s just partisan acceleration in one direction or another. There has to be some sort of resolution to be successful.
On the social media side, there you should be very focused on the integrity of information. That speaks to the trust on their platforms. Social media companies are 100 percent tied to the level of trust people have with the platform— that the information they're getting there is true and that their information is protected. [Companies] have not been doing this until recently.

I have to say, Facebook has advanced very quickly in two years putting in lots of solutions— trying to make sure alternative news outlets that spring up out of nowhere spreading falsehoods don't trend. [These companies] don't move very quickly. This is going to be tough for them to do without destroying user experience. They are going to struggle with it. I think that's why we're starting to see people back away from Facebook and other social media platforms. They don't trust what's on there and you're seeing that in terms of perspective. People saw social media in 2016 as a way to yell back and forth at each other about ideology. Facebook immediately pivot[ed] and said 'let's go back to cats and kids, we're going to downfeed news and political partisanship.' We're making all these changes but I don't know that it will bring people back. It really will take civil society, something in between, where the public will have to advance their own issues.

Tanoff: Speaking of the public and people who are actually using social media, do you think there's a generational divide between being able to discern what's a bot, what's fake news?

Watts: Sure— I think the challenge of older people when I talk to them about the social media influence and the nefarious aspects of it, [they] will often times jump immediately to 'you gotta tell kids about this, this is so bad.' Well actually, your kids should tell you about it because you fall for it more than your kids do. They have trouble sorting out fact versus fiction online because they haven't operated in this technology platform from birth.

For the younger generation though, it's about apathy. They like and are moving towards applications which are temporary, where the content doesn't live forever, where there are more trusted networks. They also aren't participating and engaging in dialogue that's necessarily political or about policy issues. I think that the danger for young people is apathy. If you don't know what to believe, you just back away from the system entirely. For the older people it's going to be partisanship, 'my truth is better than your truth' or 'my facts are better than you are facts.' I'm not sure how those will play out together in the future.

Tanoff: You talked about in a lot of interviews and wrote about interacting with terrorists through social media. Have you ever tried interacting with Russian accounts?

Watts: Not in the same way, but I did interact with accounts that were doing foreign influence. They were trying to convince me or move my position. That was in the early years of it and the idea is [to] take people who are in different policy debates and push them towards your preferred policy outcome or try and nudge them that way by saddling up to them in direct messages and then bringing other people into the conversation so it looks like everybody agrees with the other person's position and not yours. It's much more about persuasion and engagement. Russian accounts, you can engage with them. I did in the very early days. The engagement isn't that sustained like you would have with a terrorist. When you're dealing with a troll farm or somebody who isn't really who they say they are, they don't want to engage too much because they can show their hand. At least the terrorist I was engaging with you could figure out if they were authentic or not. You get into trouble if
you’re a foreign manipulator like that and if you’re not really good in the culture then it gets dangerous.

One of them I was engaging with had a picture that they had posted and I said ‘oh hey I didn’t know you lived in [place]’ and they said ‘yeah it’s a wonderful place’. I said ‘I’m there today, why don’t we meet up and talk through things’. The account went away within seconds. It’s different— you’re not really discussing, you’re jousting and you’re trying to figure out authenticity. With extremists, you got to a point where you knew each of you was as authentic as to who they said they were without even necessarily knowing their names and then you were having a dialogue back and forth. There’s no real dialogue with a propaganda machine. They’re just going to advance their interests.

**Tanoff: As someone who was part of both the military and civilian apparatus of national security and in the private sector still aiding the public sector— what does public service mean to you?**

**Watts:** Public service is the best, right? Because you’re actually doing something you believe in. You’re representing your people, you’re advancing the cause. Corporate America is great too but it’s very straightforward -you’re doing it for your own benefit. It’s for money; maybe for the benefit of the company too and your coworkers but it’s different. When you’re doing public service, you’re actually doing something that no one else can do. Most of the world is oriented around making things or providing services. [Public service] is very different because you’re trying to advance an entire governance system or you’re trying to protect people from things that are bad.

The reward, despite the frustration of the bureaucracy, is much more enriching. You get to see the world in a very different way. I think the people that you work with are fantastic in public service because they’re all in it for the same reasons that you are. That’s not always the case in a business. I think public service is great and unless you’ve done it, it’s very hard for me to listen to people criticize public service. I don’t think they understand how challenging it can be.

**Tanoff: A lot of your career is focused on intel issues but you started out as an infantry officer. How did you decide to make that transition from being an infantry officer and move to intel issues?**

**Watts:** I didn’t decide, it sort of fell on me because of 9/11. I had put in the card for the FBI because somebody [told me] ‘if you want to be an FBI agent, it might take two to three years’. I was an infantry company commander at Fort Lewis Washington [and] I put the [FBI] card in the mail of August 2001 and September 11th happened right after. In the Army, I thought I was going to be going to Afghanistan but they actually ramped that down pretty quick in early 2002. In the meantime, the FBI hired a thousand new agents that year. I went from putting the card in to doing my first test and getting my first call by [about] October 2001 and being in the FBI by April of 2002. I started in August [2002], so it was a rapid transition. I went from witnessing 9/11 on television in an infantry company to a year later on the first
anniversary I was at the FBI. It was that fast. It happened really, really quickly. I wasn’t really looking to get out of the army, and it’s just how the timing worked out.

I don’t regret necessarily leaving. I loved everything I did. I had been a company commander and you kind of move into staff roles after that, which would have been fine. But I’ve had an amazing experience by just complete luck of getting to go to different agencies and working [with] different branches of the government. I’ve been a public service tourist. I totally lucked out. It wasn’t anything I designed, it just sort of fell that way.

Tanoff: That touches on my last question. Your career path is certainly very interesting—would you say it’s equal parts decisions and opportunities that just presented themselves?

Watts: No, it was more by default often. I was a military spouse for a good part of that so I had to figure out—how do I stay relevant in my field and work in an area that I was passionate about, and also move around every eighteen months. Between the FBI and Special Operations Command, jumping around between projects I got to be like an intelligence consultant and work with state and local law enforcement. I was like a tourist of counter-terrorism. I got to work on great projects but you could have never designed it that way. I think the most important thing is to get a variety of experiences and know what you like and what direction you want to go.