TERRORIST ACTIVITY BEYOND TERRORISM: THE PROBLEM AND HOW IT MIGHT BE STOPPED

by
Justin H. Leopold-Cohen

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August, 2017

© 2017 Justin H. Leopold-Cohen
All Rights Reserved
Abstract

The threat of terrorism has become commonplace in society, and though extremists and radicals have plagued the world for more than a century, their evolving nature has made understanding them a continually complex task.

One of the most recent trends in terrorist groups is their ability to latch on to other illicit activities besides actual terrorist attacks, creating various nexuses. Using a series of case studies and comparative analysis, the three chapters of this thesis seek to examine these nexuses to better understand what activities terrorist groups carry out other than terrorism.

The three chapters of this thesis will explore terrorist engagement in Maritime-Crime, ideological differences in terrorist Cyber-Crime, and historical strategies on how to counter the Crime-Terror Nexus. The results of this study found that the Crime-Terror Nexus was still limited for the most part in the Maritime Domain, that cyber activity did not differ based on ideology, and that international cooperation was the most successful strategy for defeating terrorist criminal enterprise.

Readers:
Dr. Cindy Storer
Dr. Mark Stout

Thesis Advisors: Dr. Mark Stout, Professor Alexander Alden, and Dr. Sarah Clark
Acknowledgments

First, I must give thanks to Johns Hopkins University, the professors and my peers: I have learned so much from all of you, and was honored to have studied with you, and I hope to cross paths with everyone again. The lessons I learned from Dr. Kim Thachuk and Professor Charles Blair were particularly impactful on the work that went into the writing of this thesis, from inspiring ideas to suggested source material. Thank you for everything.

I would also like to thank Allison Leopold, the first teacher I ever had. For my entire life, your research and writing has inspired my own. Throughout the writing of this paper, you have been my first reader, my biggest fan, and my most trusted editor. I could not have made it this far without you to guide me.

To my brother Spencer: your constant jokes and asking, “Have you finished yet?” were a source of levity for me throughout the writing of this paper and my degree as a whole. You always helped put a smile on my face when the stress became too much.

To Jamie Schmutter: you came into my life at the outset of this paper and for over a year, have stuck it out with me through every late night writing session and paranoid rant. For your support in this process, I will always be grateful.

I would like to acknowledge the many others whose work is referenced in this thesis, though any shortcomings in my research and representations of the views of others remain my own.
# Table of Contents

Abstract................................................................................................................. ii
Acknowledgements............................................................................................... iii
Table of Contents................................................................................................ vi
List of Figures....................................................................................................... vi
List of Tables........................................................................................................ vi

Introduction........................................................................................................... 1

Chapter 1: Maritime-Terror Nexus: Smugglers, Kidnappers, & Pirates
   Introduction......................................................................................................... 7
   Literature Review............................................................................................... 10
      Maritime Security Threats.............................................................................. 10
      What is Maritime Terrorism?....................................................................... 12
      What is Illicit Maritime Activity?................................................................. 15
      The Crime-Terror Nexus in the Maritime Domain...................................... 19
      Conclusion.................................................................................................... 22
   Theory & Hypothesis......................................................................................... 22
   Data.................................................................................................................. 24
      The Taliban..................................................................................................... 24
      The Islamic State............................................................................................ 26
      Boko Haram................................................................................................... 29
      Communist Party of India (Maoists)............................................................ 32
      Kurdistan Workers’ Party (PKK)................................................................. 33
   Discussion.......................................................................................................... 35
   Conclusion......................................................................................................... 37

Chapter 2: Cyber-Terror Nexus: Is Ideology Relevant?
   Introduction....................................................................................................... 39
   Literature Review............................................................................................. 43
      What is Meant by Cyber?............................................................................... 43
      What is Hostile Cyber Activity?.................................................................... 44
      Terrorism & Ideology..................................................................................... 49
      Conclusion.................................................................................................... 54
   Theory & Hypothesis......................................................................................... 54
   Data.................................................................................................................. 58
      Anarchist....................................................................................................... 58
      Separatist....................................................................................................... 61
      New Left Wing............................................................................................... 65
      Religious........................................................................................................ 68
      Right Wing/Exclusionist............................................................................... 73
   Discussion.......................................................................................................... 76
   Conclusion......................................................................................................... 79
Chapter 3: Criminals & Terrorists: The Response to The Irish Nexus

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>81</td>
</tr>
<tr>
<td>Literature Review</td>
<td>84</td>
</tr>
<tr>
<td>What is The Crime Terror-Nexus?</td>
<td>84</td>
</tr>
<tr>
<td>What are the Challenges for Counter-Terrorism?</td>
<td>85</td>
</tr>
<tr>
<td>What are the Recommendations for Response?</td>
<td>85</td>
</tr>
<tr>
<td>Conclusion</td>
<td>89</td>
</tr>
<tr>
<td>Theory &amp; Hypothesis</td>
<td>90</td>
</tr>
<tr>
<td>Data</td>
<td>93</td>
</tr>
<tr>
<td>Background on the Irish Crime-Terror Nexus</td>
<td>95</td>
</tr>
<tr>
<td>The British: Military Units and MI5</td>
<td>93</td>
</tr>
<tr>
<td>Northern Ireland &amp; The Royal Ulster Constabulary</td>
<td>97</td>
</tr>
<tr>
<td>The Republic of Ireland Police Force and the Garda Siochana</td>
<td>98</td>
</tr>
<tr>
<td>The United States and the Federal Bureau of Investigation</td>
<td>99</td>
</tr>
<tr>
<td>The Columbian Administrative Department of Security</td>
<td>102</td>
</tr>
<tr>
<td>Discussion</td>
<td>103</td>
</tr>
<tr>
<td>Conclusion</td>
<td>105</td>
</tr>
<tr>
<td>Conclusion</td>
<td>107</td>
</tr>
<tr>
<td>Appendices</td>
<td>111</td>
</tr>
<tr>
<td>Bibliography</td>
<td>113</td>
</tr>
<tr>
<td>Curriculum Vitae</td>
<td>132</td>
</tr>
</tbody>
</table>
List of Figures

Figures:
Figure 1: Makarenko Crime-Terror Continuum........................................19
Figure 2: PIRA Organizational Structure..............................................110

List of Tables

Tables:
Table 1: Maritime Terror Incidents 2005-2015...................................... 8
Table 2: Maritime Terror Attack Types 2005-2015................................... 8
Table 3: CNS Known Global Trafficking Incidents 2010-2015.................. 15
Table 4: Maritime Piracy Incidents 2010-2015..................................... 18
Table 5: Terrorist Group Attacks in 2015............................................. 22
Table 6: Chapter 1 Results Illustrated............................................... 34
Table 7: American Opinion of Threat................................................. 109
Table 8: U.S. Cyber-Crime Reports 2010-2015.................................... 46
Table 9: U.S. Cyber-Crime Reports 2000-2010.................................... 109
Table 10: Terrorist Ideologies & Attacks............................................ 55
Table 11: Chapter 2 Results Illustrated.............................................. 74
Table 12: Terrorism In Europe.......................................................... 109
Table 13: Chapter 3 Results Illustrate............................................... 102
Table 14: Irish Republican Linked Attacks.......................................... 110
Introduction

“Study the past if you would define the future.”

— Confucius

The phenomena of terrorism as a means of achieving one’s ends has long been present in civilization, with distinct qualities that continually evolve throughout history.

Since the turn of the century, approximately 64,310 lives have been lost to the ideologically driven violence of terrorist attacks, and inflicted damage to infrastructure resulting in countless billions of dollars. As will be elaborated in the following pages, terrorist organizations have gone through distinct periods of evolution, in tactics, ideology, rhetoric, and funding methods.¹

Part of the evolving nature of terrorism is the growing engagement of terrorist organizations in transnational organized crime. This confluence of crime and terror has resulted in what has become known as the Crime-Terror Nexus, which consists of criminal groups executing terrorist style attacks, and terrorist groups involved in organized crime. This phenomenon has been problematic for those who seek to better understand terrorism, as these crimes and other actions are not viewed as terrorist activity. This thesis, therefore, will be seeking to understand those terrorist activities that are criminal, such as maritime smuggling, cybercrime, how to counter the criminal activities of terrorist groups, and how far along the convergence of crime and terror has gone.

One of the largest issues in understanding the Crime-Terror Nexus is in quantifying it. When a terrorist group is caught committing a crime, terrorist tracking databases usually fail to acknowledge it, as the crime does not fall into any categories of terrorism. This thesis seeks to take a first step at correcting that knowledge gap, by adding data on how terrorist groups engage in nexus activities.

There are three chapters in this thesis, each of which asks a unique question connected by a common theme, that of the Crime-Terror Nexus, and examining what terrorist groups do other than their actual attacks, such as smuggling, cyber hacking, or money laundering.

The majority of the data used in the research is open source, comprised of scholarly research, news articles, along with a heavy reliance on existing databases such as the Global Terrorism Database housed at the Study of Terrorism and Responses To Terrorism (START) Center, University of Maryland.

In this exploration, the research uses a qualitative approach, specifically analyzing a series of case studies, selecting certain terrorist groups based on the level of their activity, the ideological orientations, and historical significance. These cases will be used to test the three hypotheses with a comparative analysis.

It is well known that the political nature of terrorism has caused debate about how to define the phenomenon, such as with insurgent or terrorist group. Within the United States’ government alone, the definition can vary from one office to another, let alone between countries. The data used in this thesis relied heavily on the Global Terrorism Database (GTD), its definition reads as follows:

"the threatened or actual use of illegal force and violence by a non-state actor to attain a
political, economic, religious, or social goal through fear, coercion, or intimidation."

The GTD also holds its data to a set of three questions:

1. The violent act was aimed at attaining a political, economic, religious, or social goal;

2. The violent act included evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) other than the immediate victims; and

3. The violent act was outside the precepts of International Humanitarian Law.

It is under the GTD framework that all groups were selected for this study. By using this as a foundation, the sometimes gray areas of classifying violent non-state actors as insurgent, terrorist, or otherwise became clear; if the group’s activities matched the START definition of terrorism, it was eligible to be included in this study.

In Chapter 1, the focus is on how terrorist groups threaten maritime security. In light of recent acts by violent non-state actors threatening shipping in Yemen and boat travel in the Philippines, the timeliness of examining maritime-terrorism adds a new relevance to this research. The chapter focuses on terrorist engagement in activities such as weapon and drug smuggling, human trafficking, hijacking of ships, and maritime piracy.

Chapter 1’s data sought direct links to these activities, using the five groups that committed the most attacks in 2015 as case studies. Though not the only measure to determine importance, the highest amount of attacks was chosen over other measures.
such as amount of fatalities, since smaller attacks can still cause large amounts of fear and disruption. These groups were selected after reviewing the most recent terrorism statistics of the United States Department of State and Global Terrorism Database available at the time of this writing.

The five groups with the most attacks were the Taliban, the Islamic State, Boko Haram, the Maoist faction of the Communist Party of India, and the Kurdistan Worker’s Party. After examination of available sources, however, the research found only that there was limited engagement with some of the groups, and that the connections were mostly 2nd or 3rd hand sales for example, if a terrorist group bought weapons from someone who bought weapons, and so on.

The second chapter likewise looked at terrorist engagement in activities other than terrorist attacks, though this time in the realm of cyber. Cyber war and hackers are a popular topic for research in the security field, and is constantly making headlines as the result of large-scale cyber-attacks such the recent WannaCry virus. Despite the great amount of attention given to cyber conflict, cyber-terror remains an abstract concept, as no terrorist group has managed to kill anyone with a computer.

Chapter 2 sought to look at what terrorists can do with computers, specifically whether there are any ideological differences in cyber activity among groups that are separatist, religious, right/left wing or otherwise. Using existing research on terrorist ideological leanings, the categories of anarchist, separatist, left wing, religion, and right wing/exclusionists were chosen for examination.

Within the ideological categories, based on data from the Global Terrorism Database and the Terrorism Research & Analysis Consortium, two terrorist groups for
each ideology were selected: the International Anarchist Federation; the Conspiracy of
Cells of Fire; Hamas; East Turkestan Islamic Movement, The Maoist faction of the
Communist Party of India, FARC, the Taliban, the Islamic State, the Donetsk Peoples
Republic, and the Sovereign Citizen Movement. The results of this research showed that
all ideologies engage in online propaganda, that none of the selected cases have been able
to meet the criteria for cyber-terrorism, and ultimately that there was no major ideological
differences in cyber activity, such as use of malware or communication technologies.

The final chapter of this thesis researched strategies against terrorist groups that
fall into the Crime-Terror Nexus. Upon researching through scholarly debate of various
strategies and policies, it was found that there was little quantitative data to suggest that
any one strategy worked more than another.

Thus, Chapter 3 sought to use a historical analysis of a terrorist group no longer
active, the Provisional Irish Republican Army, along with its break-off groups, which
were widely known for their criminal enterprise, to determine if law enforcement
agencies used these strategies effectively.

Through historical research of the various Irish extremist groups that were active
in the United Kingdom, the United States, and Columbia, several law enforcement and
counter terror agencies were selected, including the British Army, the Northern Ireland
Police Force; the Republic of Ireland Police Force; the United States Federal Bureau of
Investigation (FBI), and the Columbian Administrative Department of Security (DAS).
After a historical review of “the Troubles” as it is known, it was found that though the
strategies contained overlap, the use of international cooperation and undercover
informants were the most successful in countering the criminal enterprises of Irish Republican extremism.

Through these three chapters, researchers and counter-terrorism practitioners can gain a better understanding, not only of what types of activities terrorist groups engage in other than terrorism (such as smuggling or hacking) but also what types of counter-terror strategies have proved successful in the past. While focusing on the shootings, rockets, suicide bombers, and other violent aspects of terrorist organizations, the type of research offered through this thesis provides examination into other aspects of terrorist groups. It is only by viewing the whole picture of a terrorist group can said group be fully understood.
Chapter One: Maritime-Terror Nexus: Smugglers, Kidnappers, & Pirates?

“The fishermen know that the sea is dangerous and the storm terrible, but they have never found these dangers sufficient reason for remaining ashore.” — Vincent Van Gogh

I. Introduction:

The year 2016 was busy for the Southern Philippine Islamic terrorist group Abu Sayyaf, which is known to commit “kidnappings for ransom, bombings, assassinations, and extortion…both for financial profit and to promote its jihadist agenda,” as it had begun stepping up its sea presence.³

On November 7th, Abu Sayyaf militants boarded a German flag flying yacht in the “Pegasus Reef, around 40 nautical miles away from Taganak Island in Tawi-Tawi,” killed one female passenger, and kidnapped a 70-year-old German man. Sea-based kidnappings have become a routine tactic for Abu Sayyaf, and when spokesmen for the group relayed their ransom, the German national Juegan Kantner was allowed by Abu Sayyaf to speak, and stated, “pirates took our boat and they took us.” ⁴

Following up on the kidnapping of Mr. Kantner, Abu Sayyaf terrorists struck the maritime domain again on November 11, 2016. The Vietnamese cargo ship, the MV Royal 16 was attacked near the island Basilan, when 10 Abu Sayyaf militants boarded the

---

³ “ABU SAYYAF GROUP (ASG).” National Counter Terrorism Center, United States of America. <https://www.nctc.gov/site/groups/abu_sayyaf.html>
ship and kidnapped the captain and 5 crew members, and promptly exited the area on several speed boats.  

Abu Sayyaf has been launching these types of attacks since the United States Department of State (DoS) designated it a foreign terrorist group in 1997, and has not indicated any change in behavior that might cause the designation to be lifted. 

This is just one example of how the maritime domain is under threat from violent non-state actors. Through the National Consortium for the Study of Terrorism and Responses to Terrorism’s (START) Global Terrorism Data Base, which has recorded terrorist attacks up until 2015, it can be seen that between 2005 and 2015, there were 89 terrorist attacks recorded, when given the parameters to search only for maritime incidents portrayed below in Table 1.

While the findings of the database are accurate under current understandings of maritime-terrorism, the data can be potentially misleading, as it focuses on the more physically violent terrorist attacks such as armed assaults and bombings, as shown in Table 2, leaving out other types of activity that terrorist groups have been known to engage in.

**Table 1: Maritime Terror Incidents 2005-2015**

---


8 Ibid.
While the Global Terrorism Database is commendable as to its recording of attacks, it does not identify other illicit maritime activity in which terrorist groups may be engaging, operating either by themselves or through cooperation with transnational organized criminal organizations that generate funds or material which directly support the attacks. Such cooperation and financial support has become known as the Crime-Terror Nexus. Though there is a seemingly endless amount of research available on terrorism, and maritime crime, there is notably less on the converging of the two on a global scale. It is
that phenomena that this paper aims to investigate and potentially fill the data gap on illicit maritime activities of terrorists groups.

Beginning with the literature review, this paper will explore what current scholarship has established on maritime security threats, the relationships between terrorist groups and criminal organizations, their motivations for maritime activity, and why this research is important for academic scholarship as well as for use by counter-terror agencies.

Following the literature review, the paper will elaborate on the methods used in examining the phenomena, and the hypothesis, and explaining how this research may aid in resource allocation and policy recommendations by researching select terrorist organizations and their potential illicit maritime crimes.

This will be accomplished by examining publicly available data collected from the START database on behalf of DoS, which has identified the top five most active terrorist organizations in 2015 since those groups would warrant a high degree of study, combined with open source research to explore the activities of the terrorists’ organizations, and why they do or do not engage in illicit maritime activity to directly support their operations. This will potentially produce data to show that terrorist groups are more active in the maritime domain than currently perceived when just looking at maritime attacks. 9

II. Literature Review:

Maritime Security Threats:

The United States Geological Survey states that roughly 71% of the globe is covered by water, and “as a largely unregulated space,” Dr. Martin N. Murphy points out

---

that “the sea is potentially an environment that is especially vulnerable” to crime.\textsuperscript{10,11} Reputable scholarship on the maritime domain would agree on the importance of security, as the threats that exist on the seas seem legion and affect most nations the world over, however as people live on land, the threat is usually limited to shipping. This can still be critical, as according to the United Nations International Maritime Organization over 90% of global trade is still conducted through maritime shipping.\textsuperscript{12}

United States Coast Guard Officer Eric Taquechel, in conjunction with security analyst Ian J. Hollan and Professor Ted G. Lewis, elaborate on maritime trade and supply routes, indicating that keeping maritime supply routes secure “is vital to the economic well-being of the United States,” and that American ports are particularly vulnerable to smuggling through the many thousands of shipping containers that travel the waters each day, and how in a “worst case scenario” a weapon of mass destruction (WMD) could be smuggled into the country for an attack.\textsuperscript{13}

The trio is not alone in this fear. Professor Steve S. Sin, along with Brecht Volders and Sylvain Fanielle, have written on the same security aspects. They claim that current counter terror initiatives are encountering numerous problems (mainly legal and jurisdictional obstacles over the authority and responsibility of security). Though the authors focus on Belgian ports, they claim the threat is a high enough risk that all nations

should take note, “given that over 58 million” containers travel over “490 maritime trade routes annually.”

While Murphy is a leading advocate of maritime security initiatives, his research says that a WMD being smuggled into the United States by shipping container, while high risk, is very low probability. It still must be noted however; working in security often means to focus on the unlikely. Murphy does state that due to the value a WMD would have to a terrorist organization, it would be implausible for them to risk putting it in a shipping container, which can be “frequently misplaced, stolen, delayed, dropped, broken open, left out in the sun, drenched with seawater, lost overboard and set on fire.” Murphy does state, however, that terrorist operations can feature maritime smuggling of “equipment, components, money and even personnel in containers.” In general, Murphy’s main argument is that the international security threat from the maritime domain should focus on the more likely threats, such as illicit maritime organized crime including smuggling, trafficking, and piracy, as well as certain terrorist activities, not WMD smuggling.

What is Maritime Terrorism?

As to the above-mentioned purpose of this paper—to explore terrorist activities at sea beyond just attacks—this exploration is needed because the majority of scholarship on maritime terrorism focuses exclusively on various types of assaults as seen in Figure 2, broken down by START. Its parameters for maritime terrorism consist of armed assaults, assassinations, bombings, infrastructure attacks, hijacking, hostage taking,

14 Ibid (P.G.1)
16 Murphy (P.G. 62)
kidnapping, and “unclassified” which could be something such as a collision. While the numbers may be a fraction of that of land-based terrorism, the potential dangers from maritime terrorism are very high given the amount of trade that is conducted by maritime shipping, and due to the congestion of trade routes it is believed that even a small disruption could create an economic disaster. In 2009, Dr. Peter Roell posited that the possible damages that can be seen from maritime terrorism make it a threat not to be underestimated, including disrupted trade, the environmental fallout that could come from an attack on oil freight, and negative impact to energy infrastructure that could come from lost oil. Roell’s main points are that the threat is real, that it is focused on harbors, and that it cannot be countered without significant international cooperation. Roell concludes that the main problem with scholarship on maritime terrorism is creating an agreeable definition that accurately separates it from other types of illicit maritime activity such as piracy.

Akiva Lorenz devoted a portion of his work to exploring the definition of maritime terrorism. Lorenz begins with one commonly accepted definition from the Council of Security Cooperation in the Asia-Pacific (CSPAC):

“The undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities.”

---

Lorenz points out the question of what a terrorist act is, is still undefined, as is whether it is restricted to civilian or also includes military targets. Shaping his own definition, Lorenz expands the CSPAC definition into:

“the use or threat of violence against a ship (civilian as well as military), its passengers, sailors, cargo or a port facility with a solely political purpose...[including] the use of maritime transportation system to smuggle terrorists or terrorist materials into the targeted country.”\textsuperscript{19}

The parameters set by Lorenz for maritime terrorism greatly expand the outlook of terrorist activities beyond just attacks, given the second clause on smuggling, though this must be clarified to be not all smuggling, just what goes to directly supporting the terrorist organization and its mission.

As it is less expansive than Lorenz, Murphy’s work is the better starting point on examining maritime terrorism, concluding that there are six factors of causation: legal and jurisdictional weakness, geographic necessity, inadequate security, secure base area, maritime tradition, charismatic and effective leadership, and government support.\textsuperscript{20}

Murphy points out necessity as the primary motivator for a group to turn to maritime operations as most maritime terrorist attacks originate in island nations and archipelago regions.\textsuperscript{21} Murphy does mention the convergence of crime and terror, pointing out that “despite their different goals, terrorist and criminals...have on occasion found reason to work together,” and that terrorist organizations have at an increasing rate over recent

\begin{flushright}
\textsuperscript{20} Murphy (P.G. 46) \\
\textsuperscript{21} Ibid (P.G. 46-47)
\end{flushright}
years made “use of the human smuggling routes…to bring operatives into Europe, and bought arms and documents from smugglers and forgers.”

What is Illicit Maritime Activity?

As Murphy previously illustrated, the vastness and unregulated nature of the seas leave them vulnerable to those actors who would do harm and commit acts of violence or theft to ensure they meet their goals, whether they are terrorists or otherwise. This “disorder at sea” takes many forms; the larger type of crimes that could be considered transnational threats are usually committed by the organized crime groups and maritime pirates (as opposed to online/cyber piracy), and various smugglers and traffickers whose products can range from weapons, narcotics, and people.

Dr. Kimberley L. Thachuk writes that globalization affected the criminal underworld as much as it did the upper-world, and that the advancement in capability has caused a rise in the “smuggling and trafficking of any number of goods, services, and people.” The United Nations Office of Drugs and Crime (UNODC) has an entire maritime program devoted to these transnational criminal activities, which is involved in crimes that “include not only criminal activity directed at vessels or maritime structures, but also the use of the high seas to perpetrate transnational organized crimes such as smuggling of persons or illicit substances.”

At the Nuclear Threat Initiative, researchers in the Center of Nonproliferation Studies (CNS) have used a mixture of unclassified government documents and open

---

22 Ibid (P.G. 82-83) & Murphy (P.G. 7)
23 Murphy (P.G. 7)
24 Ibid (P.G. 10)
25 Ibid (P.G. 3)
source data to track all known global incidents of trafficking from 2013-2015, and part of 2016. In total, they were able to quantify 591 incidents represented below in Table 3 by year. Though only 84 incidents have been recorded in 2016, the report was last updated on March 23, 2016, leaving the majority of the year unrecorded. As well, the major limitation of this data is that obviously it can only document recorded incidents from arrest reports and news sources, so a great deal more likely go unreported.  

<table>
<thead>
<tr>
<th>Table 3: CNS Known Global Trafficking Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Graph showing number of incidents per year" /></td>
</tr>
<tr>
<td><strong>Year</strong></td>
</tr>
<tr>
<td>2013</td>
</tr>
<tr>
<td>2014</td>
</tr>
<tr>
<td>2015</td>
</tr>
<tr>
<td>2016</td>
</tr>
</tbody>
</table>

Rachel Stohl has written extensively on the global scale of the arms trafficking industry, and how, by way of plane, car, and boat, countless weapons of multiple caliber are transported across borders into the hands of violent actors of all natures.  

An example of a gunrunning case came out of the American Northeast in 2013. This international arms trafficking group was located in New Jersey, U.S. and charged with conspiracy to smuggle a large shipment of firearms in a shipping container to be

---


sold on the black market in Greece. The conspirators had assembled an assortment of pistols, semi-automatic, automatic, and assault rifles, and a supply of over 10,000 rounds of ammunition totaling about $250,000, all hidden inside a car, inside a shipping container. Though the group was discovered and brought to justice, its shipment was relatively small compared to other arms traffickers. What makes it stand out is its domestic nature: it was out of New Jersey, and that the cargo would be shipped past more popular destinations in favor of Greece.  

The other major crime that affects the security of the maritime domain is piracy. Murphy explains “piracy is, very simply, unlawful depredation at sea,” then expands that definition with the UN Convention on the Law of the Sea, which states that piracy is the following:

A. Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew of the passengers of a private ship or private aircraft, and directed:
   I. on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
   II. against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
B. Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft.

Similar to the maritime terrorism analysis, Murphy suggests a series of factors that can allow maritime piracy to occur, though claims that as with most criminal acts, financial gain and opportunity are the main motivators, separating it from modern understandings.

---


30 Murphy (P.G.11-12)
of terrorism, which require an ideological element such as religious or political violence.\textsuperscript{31}

Murphy argues that though maritime piracy is a terrible problem for certain regions, to him it “does not currently represent a problem on a global scale.” \textsuperscript{32} This might be underestimating how costly piracy can be, as Murphy’s own research chronicling estimates on how much piracy costs the global shipping industry, ranges from $500 million to as high as $50 billion over the past few years, still just a fraction of the annual profits accrued by maritime trade.\textsuperscript{33} As well, though piracy may seem to come and go from the news which focuses on Somali Piracy, the phenomena seems to persist in other areas. The private intelligence firm Dryad Security Consulting created an open source database tracking reported piracy incidents globally, suggesting particular hot zones including the Gulf of Guinea, the Indian Ocean, and South East Asia.\textsuperscript{34} With these hot zones popping up, global piracy incidents persists, though at a decline demonstrated below in Table 4, which utilizes data on attempted and actual piracy attacks from 2012-June 2017.\textsuperscript{35}

These results should be taken with a caveat, however, since according to Murphy “under-reporting” is a major obstacle when it comes to quantifying piracy, due to insurance fraud, witness intimidation, or because of instances in which all the witnesses were killed. Murphy states that due to these reasons, the true number of piracy incidents

\textsuperscript{31} Ibid (P.G. 12)
\textsuperscript{32} Ibid (P.G. 11)
\textsuperscript{33} Ibid (P.G. 20)
could range from three times to as high as ten times what is reported, so the 191 reported
incidents in 2015, could, in actuality, range from 570 to as high as 1,900 (figures for 2017
remains unfinished at the time of this paper).\textsuperscript{36}

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
\hline
Incidents & 79 & 191 & 245 & 246 & 264 & 297 \\
\hline
\end{tabular}
\caption{Maritime Piracy Incidents 2010-2015}
\end{table}

The Crime-Terror Nexus in The Maritime Domain:

Though most academic concepts in conflict are hotly debated, government policies
and academics are largely in agreement as to how to describe the Crime-Terror Nexus.
As previously mentioned by Murphy, “terrorist and criminals...have on occasion found
reason to work together.”\textsuperscript{37} Danielle Camner Lindholm and Celina B. Realuyo have
described how, when deprived of state funding or wealthy backers, terrorists will engage
in criminal activity as a source of financing.\textsuperscript{38} On the other side of the nexus, Andre D.
Hollis has explained that in Colombia, it has been common practice for years for drug
smugglers to engage in acts of terrorism against the government.\textsuperscript{39}

\begin{itemize}
\item \textsuperscript{36} Murphy (P.G. 23)
\item \textsuperscript{37} Ibid (P.G. 82)
\item \textsuperscript{38} Miklaucic, Michael. “Convergence: Illicit Networks and National Security in the Age of Globalization.”
\textit{Center of Complex Operations}, National Defense University, April 2013. (P.G. 111-113)
\item \textsuperscript{39} Thachuck (P.G. 23-24)
\end{itemize}
While these examples along with Murphy’s statement offer a straightforward description of the phenomena in practice, most researchers refer to a spectrum designed by Dr. Tamara Makarenko, seen below in Figure 1 for a visual explanation. The spectrum features a continuum of organized crime at one end, terrorism at the other, and provides the various steps that a group must go through to reach the other side, such as alliances, adopting tactics, and adopting targets, and sometimes settling in the middle as a hybrid organization, which she refers to as “the black hole.”

Figure 1: Makarenko Crime-Terror Continuum

In regards to maritime smuggling and trafficking, terrorist organizations have been seen to be engaged in these activities in the 21st century as a means of procuring equipment, selling narcotics, and even moving people. Raheela Asfa Cheema has noted that Pakistani and Afghani terrorist groups which “include Tehrik-i-Taliban Pakistan (TTP), Haqqani network (Hn) and Al-Qaeda,” as well as Lashkar-E-Jhangvi and

---

Lashkar-e-Islam, have smuggled in shipments of illegal American and Russian guns through various ports, mainly Karachi, that then are dispersed throughout the region.\textsuperscript{41}

Besides the previously mentioned FARC, many other terrorist organizations have turned to narcotics trafficking as a source of funding. Dr. Matthew Levitt has written substantially on the Lebanese-based Hezbollah and its drug trafficking activities. Hezbollah has become notorious for its engagement in narcotrafficking, often buying drugs in Latin America, then smuggling in shipments to be sold in Europe.\textsuperscript{42}

Scholarship is divided about a maritime terror-nexus, however, when it comes to acts of piracy. Karine Hamilton writes that many researchers looked to the piracy off the coast of Somalia in the Gulf of Aden and Indian Ocean for links. Still, while what may have begun as political piracy nearing terrorism, in that these pirate groups were attacking commercial ships in order to convince large scale fishing industries to leave Somali waters, along with some speculation regarding tax/protection money to the terror group Al Shabab, as yet there has been “no substantial evidence to support claims that Somali pirates maintain links, or lent support to Somali terrorists.”\textsuperscript{43}

Much of the scholarship on piracy-terrorism cooperation remains focused on limited acts and potential threats. Murphy has echoed this conclusion, reporting that there has not been any significant amount of cooperation between pirate groups and terrorists; however, he does state that there are terrorists groups that “have always used piratical


methods to raise money,” such as “the Liberation Tigers of Tamil Eelam (LTTE), GAM and the Philippine Islamist Abu Sayyaf Group (ASG.)” Thus, groups like these would fall into a piracy-terror nexus style group along the same lines as the Makarenko Continuum.

Conclusion

As can be seen, the literature on terrorism in the maritime domain is heavily debated, with much of that debate relating to how to define Maritime-Terrorism and how big a threat it really is. That debate is enhanced when examining any criminal cooperation, with a great deal of paranoia existing around the potential smuggling of a nuclear weapon. However there is a gap in the theory, as much of the debate goes under supported by any data. This chapter will seek to fill that gap.

III. Theory & Hypothesis:

Theory:

As the literature review suggests, there is a fair amount of back and forth on the presence of a piracy-terrorism nexus, while in regards to other illicit maritime activity, most scholarship and reporting agree that terrorists have taken part in trafficking and smuggling of weapons, narcotics, or people through a multitude of methods, including maritime. As well, a debate exists as to whether or not to include these traditionally criminal activities as terrorist activities.

Hypothesis:

It is the hypothesis of this paper that terrorist groups can be linked to illicit maritime activity that directly supports their terrorism campaigns, which if proven would add

44 Murphy (P.G. 40)
empirical data to an expanded view similar to that of Lorenz, and fill the gap of maritime terror scholarship that while accurate, does not examine a potentially larger terrorist presence in the maritime domain. While it may seem obvious with certain terrorist groups that are already heavily involved in the maritime domain, the full extent is still debated with some scholars saying that groups are not largely involved. This paper expects the opposite, as the aforementioned Lindholm and Realuyo stated that terrorist groups more and more have had to turn to illicit activities to support themselves and their operations, combined with the assertions by Murphy that organized crime profits have reached billions of dollars in the maritime domain. The reasonable conclusion would be that terrorist groups would take advantage of this lucrative industry and vulnerable domain.

**Methods:**

In order to prove this hypothesis, this paper will make use of the small-n qualitative analysis method and build a comparative study. This method, explained by Janet Buttolph Johnson and H.T. Reynolds, calls for the examination of several cases that involve a particular phenomenon and uses specific data sets to draw conclusions.\(^{45}\)

**Case Study Selection:**

Through this method, the paper will investigate the top five, most active terrorist groups of 2015, as determined by the United States Department of State Bureau of Counter Terrorism and Countering Violent Extremism, based on the number of recorded attacks. Represented in Table 5 are each group and the amount of attacks attributed to them in 2015.\(^{46}\) Though other methods such as regional threat, or amount of fatalities


exist, this method was chosen since a smaller or less lethal attack can still produce the fear and disruption of a larger attack.

Table 5: Terrorist Group Attacks in 2015

<table>
<thead>
<tr>
<th>Terrorist Group Name</th>
<th>Attacks in 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Taliban</td>
<td>1093</td>
</tr>
<tr>
<td>Islamic State</td>
<td>931</td>
</tr>
<tr>
<td>Boko Haram</td>
<td>491</td>
</tr>
<tr>
<td>Communist Party of India (Maoists)</td>
<td>343</td>
</tr>
<tr>
<td>Kurdistan Workers’ Party</td>
<td>238</td>
</tr>
</tbody>
</table>

Though not the only measure to determine importance, as the terrorist groups responsible for the most attacks, these five groups should warrant particular attention for counter-terror agencies and policy-makers. This paper will examine each of the five groups, and by way of open source research into news reports, recent scholarship, and unclassified government documents, attempt to establish connections to illicit maritime activity, which under parameters for maritime terrorism established by Lorenz, would mean that there is a larger amount of maritime terrorist activity than currently believed when such activity is used as direct support.

IV. Data:

1. The Taliban:

The Taliban, originally formed in the aftermath of the Soviet invasion of Afghanistan, follow an Islamic fundamentalist ideology and for the duration of the 20th century, fought to impose that ideology upon areas under its control in the Central-Asian and South Asian nations with Pashtun populations, largely Afghanistan and Pakistan. The Taliban became more well-known following the 9/11 Attacks and United States invasion
of Afghanistan in 2001, when it became evident that they had provided refuge to the
attack’s mastermind, Osama bin Laden and his al-Qaeda terrorist organization.\textsuperscript{47}

The violence from the Taliban has continued largely uninterrupted even with the
combined forces of the American-led War on Terror. Among the reasons for the
Taliban’s resiliency is its ability to finance through illicit means.\textsuperscript{48} Presently, there have
been only two known Taliban operations that could be counted as piracy: one in 2005 and
the other in 2009, both hijacking oil tankers.\textsuperscript{49}

Likewise, there are no recent cases of the Taliban operating a human smuggling
ring though they have committed these acts in the past. The Taliban’s narcotics
smuggling operation is believed to earn it hundreds of millions of dollars per year, mainly
from opium, heroin, and hashish.\textsuperscript{50} As Cheema already noted, the Taliban has been
known to smuggle arms through the port of Karachi, and according to the United States
Drug Enforcement Agency, drug busts are frequently made on ships with Karachi as port
of origin, some being traced to Taliban origins and others being speculated as such.\textsuperscript{51}

Karachi is not the only maritime route that the Taliban has made use of in its
terror financing operation. In early October 2016, the Australian naval vessel the HMAS
Darwin stopped a fishing ship in the Indian Ocean and discovered 500 kilograms of


\textsuperscript{48} Ibid

\textsuperscript{49} START. “Global Terrorism Database.” University of Maryland.
<https://www.start.umd.edu/gtd/search/Results.aspx?chart=overtime&casualties_type=b&casualties_max=
&start_yearonly=2005&end_yearonly=2015&dtp2=all&perpetrator=652,20529&target=11>

\textsuperscript{50} Laub & Micallef, Joseph V. “How the Taliban Gets its Cash.” \textit{The World Post}, The Huffington Post, 14
its_b_8551536.html>

heroin. This is believed to be one of the many Taliban shipments, as they are noted to use smugglers that sail through Iran and out of the Makran Coast, and from there, just as through Pakistan, ship “thousands of kilometres across the Indian Ocean carrying an estimated 70 tons of the drug” every year to Africa, Europe and beyond.\textsuperscript{52}

The profits from the Taliban smuggling operations are a vital source of profit to its terrorism campaign. While Taliban operatives have taken part in the smuggling, many of the operations feature them as sending or receiving goods rather than being the actual smuggler, and involved in the maritime part of the crime, which is usually contracted outside of the organization. Though there is evidence of maritime-criminal activity, what can be proven of the Taliban shows it as being several links removed from direct involvement.

2. Islamic State:

Second to the Taliban in most terrorist attacks per year is the Islamic State, called IS, ISIS, ISIL, or Daesh. The Islamic State, which splintered from Al Qaeda, gained renown due to its swift momentum in conquering large sections of Iraq, Syria, and Libya to establish a new Caliphate, and managed to have a plethora of smaller terrorist groups across the Middle East and parts of Africa and Asia to pledge allegiance and become affiliate groups.\textsuperscript{53}

The group made significant headway in the beginning stages of the Syrian Civil War and withdrawal stages of American military forces from Iraq. Fighting its way


throughout the region in its desire to create a Caliphate, ISIS has incurred the wrath of much the world, even causing countries that are usually in opposition to each other, to be on the same side such as Iran and Saudi Arabia.\textsuperscript{54}

The financing machine of ISIS is more complex than most terrorist organizations. Its members have engaged in “oil extraction [which] reportedly constituted the Islamic State’s largest source of income…netting an estimated $1 million to $3 million a day,” on top of wresting taxes from conquered territory, black market antiques trading, ransoming foreign hostages, and some speculated illicit maritime crime.\textsuperscript{55}

There is little evidence to support that ISIS has engaged in much maritime terrorism, beyond a single failed attack on an Egyptian ship off the coast of the Sinai Peninsula. There is a large amount of speculation and fear that it could begin to attack ships traversing the North African coast and Mediterranean regions where affiliate groups hold sway. Many state and commercial ships have begun to strengthen their security measures when traveling near ISIS-controlled regions in preparation for a potential ISIS pirate attack. United States Navy Officer Robert N. Hein, a Surface Warfare expert has stated that “the likelihood of near-shore attacks remains a possibility, including against cruise ships, [but] the chance that ISIS will attack blue water objectives out of sight of land is still remote,” possibly due to ongoing struggles to hold territory on land.\textsuperscript{56}

\textsuperscript{54} Ibid
ISIS has developed some maritime smuggling enterprises providing a portion of funds to its operations.\(^5^7\) As stated, the illegal selling of oil and fuel is ISIS’s most profitable operation to fund its organization. While much of the oil and fuel produced by the wells and refineries under its control is consumed locally, a large portion is smuggled across borders through a number of methods, which include both land and sea. It has even been reported that ISIS “smugglers loaded larger jerry cans (50-60 liters) of oil into metal tubs or small row boats and, using ropes attached to each river bank, pulled its cargo across the river and into Turkey.”\(^5^8\) While this method may feature an aquatic component, it fails to reach the intricacies of most maritime smuggling operations.

While the majority of the ISIS arsenal was seized from the American supplied Iraqi military in 2011, investigators who have tracked ISIS weaponry have traced the origins of weapons to “Sudanese, Russian, Chinese and Iranian” origins.\(^5^9\) Most this foreign gun supply remains a mystery for investigators to conclusively prove one route or another, however there have been documented cases of counter terror agency and law enforcement raids on weapon smuggling operations believed to have been bound for ISIS, such as the September 2015 seizure of a ship by the Hellenic Coast Guard out of Greece, which had hidden in it a container with some “5,000 shotguns and a half million rounds of ammunition.” The ship, the Haddad 1, was crewed by a group of Syrians, Egyptians, and Indians, was bound for an ISIS-controlled port in Libya, and while it


cannot be irrefutably proven that the guns were to be handed over to ISIS, it is the leading theory of the investigators, despite claims from officials the ship’s port of origin in Turkey, that the hidden guns were to be legally delivered to the Sudan police force.\(^{60}\)

Despite this, the ISIS smuggling routes remain largely unknown, and likely feature an equal amount of land smuggling as by sea. Even when examining the case of the Haddad 1, the crew itself was not affiliated with ISIS, and just another group of gun traffickers.

ISIS coffers also have been filled through a large amount of narcotics and human smuggling. Italian authorities have had trouble dealing with the influx of drug shipments since ISIS began operating in North Africa and sending hashish in large freights across the Mediterranean to Southern European nations. Before ISIS operations, there would be an occasional speedboat or Jet Ski carrying small amounts. However, from 2013-2016, twenty cargo ships have been intercepted, carrying “more than 280 tons of hashish valued at 2.8 billion euro.” It has been stated by authorities that this is just one of ISIS’s routes for drug shipments out of North Africa, on top of the believed “48 tons of cocaine, worth approximately $1.8 billion…smuggled along the [similar] routes every year,” though those routes remain unknown as of the writing of this paper.\(^{61}\)

3. Boko Haram:

Operating primarily out of Nigeria in West Africa, the terrorist organization Boko Haram has been responsible for approximately 10,000 deaths and the displacement of 1.5 million people. Originally formed in 2002, the group was a non-violent movement that aimed to install an Islamic fundamentalist legal system across Nigeria. It was only after years of clashes with government forces that the group embraced terrorist tactics as a means to enforce its ideology. Since 2009, when Boko Haram’s campaign of violence began, American intelligence officials have tracked cooperation and communication links with other terrorist groups such as “northwest Africa-based al-Qaeda in the Islamic Maghreb, Somalia's al-Shabab, and al-Qaeda in the Arabian Peninsula,” as well as ISIS. Among Boko Haram’s preferred strategies over the last few years have been suicide attacks, assaults “that have killed dozens of students, the burning of villages, ties to regional terror groups, and the abduction of more than two hundred schoolgirls in April 2014.” In order to finance these operations, Boko Haram has engaged in illicit maritime activity, including cooperation with Nigerian pirates, the smuggling of weapons, drugs, and people.

In West Africa, and especially in Nigeria, piracy has risen dramatically in the years following Boko Haram battling the government. Estimates out of the Gulf of Guinea state piracy went up over a third in 2013 alone. Boko Haram has not been known to engage in much piracy itself as the bulk of its operations are north of the Nigerian coastline, though the United States Federal Bureau of Investigation and private

---


maritime security firms have stated that many of the Nigerian piracy kidnapping ransoms end up paid to Boko Haram, possibly as a tax or tribute demanded from the terrorist group. Larger signs of cooperation have taken place as well, where in exchange for a cut of the ransom money, Boko Haram has provided personnel, ways to clean the money, and supplied weaponry demonstrating the growth of its operations outside of the North.\(^4\) Despite these points of connection, the finances gained from these activities do not measure up to Boko Haram’s larger land operations.

The weapons that Boko Haram supplies occasionally traverse through maritime smuggling as well, though the linkage between Boko Haram and arms trafficking is not that strong. Much of the arms smuggling comes from within Africa, and Boko Haram’s relationship seems to be more business than actual engagement perhaps trying to appear more legitimate, often just purchasing weapons, or providing protection to the non-terrorist arm smugglers, and as well with drug traffickers.\(^5\)

In regards to the smuggling and trafficking of people, Boko Haram has become a large player in the human trafficking world, which has been an outlet for its famed kidnappings. Boko Haram’s strategy is that “women and girls are trafficked for domestic servitude and sex trafficking, while boys are forced into street vending, domestic service,


mining, agriculture and begging.” The majority of victims remain in Africa, though some are placed in shipping containers and sold to buyers across 20 European nations, with a rare case even reaching the United States.66

4. Communist Party of India (Maoists):

Historically, India has had many ongoing violent attacks from “separatist and secessionist movements,” most famously in the long disputed Kashmir region. One often internationally overlooked group is the Communist or Maoist Party of India, also called the Naxalites or Red-Corridor, which has grown in numbers and initiated a recent rise in terrorist attacks. 67

The Naxalites are a reformation of a far left wing group that was brought to near destruction by India in the 1970’s. The remaining factions of the original Naxalites were reformed in 2004, and are heavily influenced by the Maoist approach to communism. They hope to replace the government of India, which they feel has abandoned the country’s poorer rural regions, mostly in the Western Indian states, and where they have been able to gather at least 20,000 armed fighters.68

The Naxalites’ operations and financing methods are fairly diverse, but do not have a notable maritime component. Largely, it imposes taxes on the regions it controls, as well as receiving support from portions of the local populace.69 There has been an

occasional assault on a boat, such as the Balimela Reservoir Incident, when the group ambushed a police boat in the summer of 2008, and killed 38 Indian officers. However, this was not a hijacking, ransoming, or any other element of piracy.

The Naxalites have engaged in gun smuggling as a way to supply its fighters. Though the majority of its guns come from land smuggling across India’s northern border, Indian intelligence has recently increased its investigations into Naxalite maritime smuggling methods involving either illegal shipments or smuggled guns hidden away on ships. These gun smuggling operations often go between the port of Karachi, Pakistan around India to the port of Kutubdia, Bangladesh, and can direct guns to any number of unofficial ports along India’s coast.

5. Kurdistan Workers’ Party (PKK):

The Kurdistan Workers’ Party abbreviated to PKK after its Turkish moniker “Partiya Karkeren Kurdistan” is a separatist insurgency estimated to have between 3,000 and 5,000 armed fighters inside Turkey. Originally formed as a Marxist group in 1974, the group began a wave of terrorism a decade later, fighting at first for Kurdish independence from Turkey, but then gradually shifting to demands for equal rights and autonomous government.

---


The PKK primarily target the Turkish government domestically but also have struck Turkish targets across Europe, maintaining a brutally high casualty rate from “bombings and kidnappings” against civilians who “do not cooperate with or assist them and to kidnap tourists.”

As to a maritime component, there have not been any confirmed piracy-style attacks attributed to the PKK. In November of 2011, Kurdish hijackers believed to be members of the PKK hijacked a Turkish civilian ship full of passengers in the Sea of Marmara. The armed hijackers had explosives similar to the PKK, and reportedly claimed to the captain of the vessel to represent the terror group’s armed wing. While on board they made only a demand for fuel, before ultimately being killed in a Turkish special forces raid and it was never made clear if the PKK were indeed responsible, though it is recorded as such by Turkish authorities.

The PKK does finance its operations through a massive smuggling operation that loads and receives all types of goods onto ships traveling the waters that border Turkey. PKK operatives are deeply integrated into the trafficking operations and have managed to take over approximately 80% of Europe’s drug supply. These maritime trafficking routes are not just for drugs but are also used to sell and secure arms, people, and smuggle

---


human blood; all are used as methods of financing the group’s terrorist attacks against Turkey.  

Discussion:

Results:

After conducting open source research into five terrorist organizations identified as responsible for the largest amount of attacks in 2015, the findings of the data prove that this paper’s hypothesis was at best unable to be proven given available data, and at worst, false. It can be seen that on the Crime-Terror Continuum, these groups are moving into organized crime, being involved in alliances and conducting crime for operational purposes. In Figure 7, the results are illustrated in a table outlining the data as to which terrorist group engaged in or cooperated with illicit maritime crime.

Table 6: Chapter 1 Results Illustrated:

<table>
<thead>
<tr>
<th>Engaged/Cooperated</th>
<th>The Taliban</th>
<th>Islamic State</th>
<th>Boko Haram</th>
<th>Naxalites</th>
<th>PKK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maritime Piracy</td>
<td>No</td>
<td>Suspected</td>
<td>Limited</td>
<td>No</td>
<td>Suspected</td>
</tr>
<tr>
<td>Gun Trafficking by Sea</td>
<td>Limited</td>
<td>Suspected</td>
<td>Limited</td>
<td>Suspected</td>
<td>Limited</td>
</tr>
<tr>
<td>Drug Smuggling by Sea</td>
<td>Yes</td>
<td>Limited</td>
<td>Limited</td>
<td>Suspected</td>
<td>Yes</td>
</tr>
<tr>
<td>Human Trafficking by Sea</td>
<td>Limited</td>
<td>Limited</td>
<td>Limited</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In trying to examine whether there is a much larger maritime terror presence than currently believed by researchers that focuses only on attacks, and the theory offered by Lorenz to include such illicit activities for direct support, this paper has proven that all

---

77 PVC.
five terror groups have limited involvement at most with illicit maritime operations. The groups all have been reported to engage in gun trafficking, either to supply its attacks or as a means of procuring funds though only in isolated and tenuous incidents, where they were primarily buying or selling, rather than engaging in actual smuggling. Excluding the Naxalites who only are accused of the act, all have engaged in smuggling drugs through maritime routes, though all are also known to have smuggled substantial amounts of narcotics over land. There was limited reporting of maritime human trafficking with only the PKK being confirmed to be actively and currently involved, though the PKK are known to smuggle anything with a demand thus having a substantial link to criminal enterprises. Boko Haram has been reported to occasionally cooperate with piracy groups, while ISIS and the PKK are under suspicion of engagement or potential future engagement.

This research is still important as more and more terrorist groups are falling into the crime terror nexus continuum, and one or more of Dr. Thachuk’s classifications of convergence. However, even when including all major forms of illicit maritime activity, the top five most active terrorist groups were not found to be largely threatening the maritime domain. This paper sought to correct a possible gap in the literature, and found that the gap cannot presently be filled with publicly available source material in these selected cases. While strategists and theorists should continue to be watchful as to evolving methods of terrorist organizations, it would seem that the most active groups have found little need to involve their organizations with the maritime domain.

Limitations:
One of the larger limitations of this was the geographic locations of the terrorist groups selected. Though these groups were the most active, terrorist groups based in island and archipelago regions such as the Filipino Abu Sayeff would likely have a more visible nexus with maritime crime. Future research should examine smaller terrorist groups that are local to these geographic regions, to see if results are different.

Further, with any open source research project that is on modern phenomena within security studies, this research was limited by national security classifications by the American and other foreign governments that have yet to release certain reports. Further, even among open source research, a portion of this chapter was based upon results from START’s Global Terrorism Database, which as commendable as it may be, is not up to date past 2015. As well, as indicated earlier by Murphy, due to a number of reasons such as intimidation or insurance premiums, many piracy acts go unreported. This could potentially limit the results of research into terrorist groups that have committed pirate attacks. This similarly applies to other illicit maritime crime, in that “analyzing… trafficking flows or routes is a difficult task given the still hidden nature of the crime and because traffickers regularly shift routes.” Therefore, though the linkages to the maritime domain cannot be conclusively proven at this time, they may very well exist beyond the reach of scholarly research.

V. Conclusion:

The research question that this paper set out to answer was how the maritime domain is threatened by global terrorism. Though initial data would suggest that maritime

---

terrorism is not a major issue for counter terror agencies or for policy-makers due to the lack of terrorist assaults recorded, the scope of this data proved significantly too narrow.

Through the research into the vulnerabilities of the maritime domain, it was found that the convergence of transnational maritime crime and terrorist groups is still a limited threat from these particular terrorist groups. Other groups like the Liberation Tigers of Tamil Eelam (LTTE), GAM and the Philippine Islamist Abu Sayyaf Group (ASG) have been heavily involved in the maritime domain, though not causing the damage to make it into the top five groups with the most attacks.

While the results had a negative to mixed endpoint, it was found that the five terrorist organizations that committed the greatest number of attacks in 2015 have a limited presence in illicit maritime activity, and others were suspected of involvement. The data also suggested that terrorist groups largely do not engage in or cooperate with organized maritime piracy, but all are active in at least one type of maritime smuggling and trafficking to a degree.

The implications of this research can be applied to both government policy and to scholarly research. In government, both policy-makers and counter-terror strategists could use research to counter those who would inflate the current threat of the crime-terror hybrids. As for academia and scholars of terrorism, this data could be used as a starting point when researching maritime crimes and potential connections to terrorism.

As the situation in Philippines situation continues to unfold, there may be questions from policy-makers and scholars on the significance of terrorist groups launching attacks in the maritime domain and freedom of navigation.
Chapter Two: Cyber Terror Nexus: Is Ideology Relevant?

"An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists." –James Comey, Former Director, Federal Bureau of Investigation.

I. Introduction:

Public opinion first began to fear what criminals could do in cyberspace following William Gibson’s coinage of the term in his 1984 book Neuromancer. This fear has persisted to the present day, as demonstrated by the 2014 Pew Research Center Poll, which listed the threat of cyber-attacks as the greatest of those threats to the United States, second only to those from Islamic extremist groups, as displayed in Appendices Figure 1.

The convergence of cyber-attacks and terrorism has also become more prevalent in people’s minds, with upwards of 31,300 magazine or journal articles examining the

---


Leopold-Cohen, Justin H.
phenomena as of 2012. Though many skeptics continually point out that no one has ever been killed by a cyber-terror attack, and assure people that a real cyber-terror event is as unlikely as being killed in a shark attack.\textsuperscript{81}

However, preparing and understanding high risk/low probability scenarios is extremely important, as “security is predominantly in the business of the unlikely.”\textsuperscript{82} Further, given recent 2017 events, one can hardly be blamed for expressing a fear of cyber threats. Early May 2017 marked the 10-year anniversary of the 2007 cyber-attack on Estonia, often thought of as “the first nation on the receiving end of an overwhelming cyber attack” which targeted government and financial websites.\textsuperscript{83} Despite this assumption as the first major cyber-attack, historians of the cyber domain note that “cyber conflict…started in earnest in 1986, when German hackers searched through thousands of US computer files and sold their stolen materials to the KGB.”\textsuperscript{84} The Estonia cyber attack is still significant, as it was conducted by an “ideologically motivated minority of predominantly ethnic Russians,” which makes it resemble an act of terrorism in that it was an ideologically inspired crime by non-state actors.\textsuperscript{85}

The 10 years since have hardly been quiet in the cyber world, from widely publicized leaks and data thefts of government classified documents, to compromising images of celebrities and controversial speculation about Russian interference in the

\textsuperscript{84} Healy, Jason. “A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.” CCSA In Partnership with The Atlantic Council. 2013. (Pg. 10)
\textsuperscript{85} Ibid (Pg. 174)
2016 American Presidential election. Most recent to the writing of this paper, in mid-May of 2017, a large scale cyber-hack known as WannaCry, attacked 200,000 computers across 150 countries, taking control of them in a “ransom-ware” attack, demanding $300 in Bitcoin (the infamous online currency) for the release of the computers; if paid, it could garner well over $1 billion for the perpetrator. This massive cyber-assault targeted both government and private enterprise, disrupting global operations of FedEx, shutting down over 45 British hospitals, and taking hold of 1,000 computers belonging to the Russian interior ministry. While attribution remains unclear, the infamous hacker group known as the Shadow Brokers is believed to be responsible, as well as suspected links to North Korean groups. The act seems to be motivated by financial gain, unlike the more politically oriented “hackivist” group, Anonymous, which claims to fight against perceived government oppression both in the U.S. and abroad:

Conflict is rampant in cyberspace, and non-state actors are very much involved, for financial gain as much as pushing political agendas, all very much emulating the Crime-Terror Nexus examined in the previous chapter.

Terrorist organizations have had a presence online for some time; how long is difficult to determine, but it is fair to say they would have taken note of the attacks that hacker syndicates such as the Shadow Brokers and Anonymous have been able to carry

---


out. However, online terrorist activity remains difficult to measure; as with any illicit activity, the underground nature makes it particularly difficult to estimate its full scope.\textsuperscript{88} It does not help that criminal activity by terrorist groups is seldom monitored as terrorist activity.

As seen with terrorist maritime activity, current systems that track terrorism only consider the presence of violent acts as its measure for terrorism, as seen with organizations like the Global Terrorism Database (GTD). As of the writing of this paper in GTD standards, there has only been a single suspected cyber incident (taking place on a Turkish pipeline in 2008 that was electronically manipulated to explode) that has qualified as a cyber-terror attack. Though Turkey has blamed the Kurdistan Workers Party, a subsequent investigation expressed doubt that a terrorist group could pull off such an attack, stating, “only state actors would have had the ability to carry out a sophisticated cyber-attack.”\textsuperscript{89}

When it comes to measuring terrorist activity in cyberspace, there is clearly a knowledge gap. This paper is attempting to fill that gap in terrorist research by examining terrorist activity in the cyber-domain such as the use of malware and viruses, data theft, communication and planning, or online fraud.

When looking at any terrorist activity, understanding why a group operates and the choices it makes is important for researchers and counter-terror practitioners alike. This can be done by looking at differing terrorist ideologies, which have been shown to

\textsuperscript{88} Miklaucic, Michael. “Convergence: Illicit Networks and National Security in the Age of Globalization.” \textit{Center of Complex Operations}, National Defense University, April 2013. (Pg. 38)

\textsuperscript{89} START. “Global Terrorism Database.” University of Maryland. <http://www.start.umd.edu/gtd/search/Results.aspx?search=cyber&sa.x=0&sa.y=0>
impact groups’ choice of weapons, targets, and tactics, as seen with leftist groups like Earth Liberation Front that focus on property damage rather than harming people, or the religious Taliban placing a ban on opium as the drug violated its principles. This paper will not only examine cyber-terror activity, but also answer the question of how engagement in cyber activity differs among terrorist ideologies.

Though there is significant scholarship on cyber-terrorism, the majority is focused on possibilities and future scenarios, such as former Defense Secretary Leon E. Panetta’s warning in 2012 “that the United States was facing the possibility of a cyber-Pearl Harbor.” Thus this paper will aid in bridging the knowledge gap on exploring terrorist activity in cyberspace, as well contribute to an ongoing debate on the importance of ideology in terrorist organizations.

The first major section of this paper is the literature review, which will provide an overview of the history and theories behind conflicts in the cyber domain and how different actors have been involved. The literature review also will explore established theory on terrorist ideology and why it is important in terrorist research.

In the section following the literature review, the paper will elaborate on the hypothesis and methods used in examining the phenomena, and how the selected case studies were chosen for the data section. The section will elaborate on the assertion that

---


religiously based terrorist groups are the most involved in cyber activity, before the data, discussion, and conclusion sections.

II. Literature Review:

1. What is meant by cyber?

To be online, to use the World Wide Web, and the Internet. These are terms we use to describe conduct in cyberspace and the non-physical realm that contains a flow of approximately 40 trillion emails a day, and 30 trillion individual WebPages, connected to humanity by upwards of 8.7 billion devices.92

The multinational technology firm Cisco Systems conducted a study of various definitions of cyberspace and found that all definitions contain the terms below:

- Activities • Interconnectedness
- Applications • Internet
- Communication • Network
- Human • Services
- Hardware • Social
- ICT/IT • Virtual
- Information

Looking through these key terms, it can be understood then that cyberspace is a technologically enabled virtual communication space, in which humans interact through a series of social and service activities.93 Today the Internet “handles everything from linking electrical plants to tracking purchases of Barbie dolls.”94

What is Hostile Cyber Activity?

---

94 Singer & Friedman (Pg. 2)
The fear that private businesses and the general public have of hostile cyber-activity has led cyber security to be a massive industry with a highly sought-after skill set.\textsuperscript{95} In cyberspace, conflict is abundant, with adversaries that may seek “private information, undermine the system, or prevent its legitimate use.”\textsuperscript{96} The groups that operate in cyber conflict are not very different from those in the physical world; there are thieves, whistleblowers, participants in private and state-based espionage, and saboteurs. The difference is that “there are only three things you can do to a computer: steal its data, misuse credentials, and hijack its resources.” Despite these limitations, interconnectivity in modern civilization means that malicious cyber activity can extend to all areas of society.\textsuperscript{97}

The struggle to understand cyber vulnerabilities have led scholars to debate the nature of cyber conflict, including cyber-crime, and cyber-terror.

It is known that criminals have set up enterprises significantly in the cyber realm; unfortunately it is impossible to know the full extent of the damage, as many cybercrimes go unreported, and with others it is hard to understand the full scope. The total cost to the global economy is generally estimated to be between $100-$500 billion dollars annually, and is projected to reach the trillions by 2020.\textsuperscript{98}

Cyber-crime, like physical crime, is highly varied, including “large scale cyber heists and malware attacks against banking systems and mobile devices.” Cyber-crime’s forms can feature the aforementioned WannaCry ransomware attack, data or financial theft, the

\textsuperscript{95} Ibid (Pg. 3)
\textsuperscript{96} Ibid (Pg. 34)
\textsuperscript{97} Ibid (Pg. 38-39)
shutting down of websites in distributed denial of service (DDoS) attacks, “as well as illicit online trade in drugs, weapons, stolen goods, counterfeit documents and child sexual abuse material.” Much of this takes place in anonymous communication networks such as TOR, which can keep one’s identity, location, and activity, hidden. While some of these cyber-criminals have banded together to create their own organized networks like the Shadow Brokers (a hacker group notorious for data theft and leaking information,) as well as others that have been known to hire out their services in a mercenary fashion.99

There are those who think the threat of cyber-crime is overstated, reasoning that “if getting rich were as simple as downloading and running software, wouldn’t more people do it?” Those on this side of the debate point out that though there are a few who manage to become prosperous, most cybercriminals barely break even, and “cybercrime billionaires” are few and far between. Skeptics still acknowledge there is a threat, but often point to the flawed method of published damage estimates, which they claim are often based on faulty surveys that use sample sizes to portray a larger group, and that more accurate accounts show costs of cyber-crime as not coming close to rivaling that of physical crime.100

In the United States Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) delegates the monitoring of cyber-crime to its Internet Crime Complaint Center (IC3). The mission of the IC3 is to track reported Internet crime and produce information

to distribute to investigative authorities across the U.S. Through IC3 Annual Reports (ARs), it can be seen that cyber-crime over the last 3 years is on the rise, and the inclusion of terrorist perpetrators has become necessary.\textsuperscript{101}

Seen below in Table 8, the amount of reports collected in 2016 is the highest, as well it does show an increase from 2013 to 2016. Additionally, in looking at Appendices, Table 9, a continual rise over the years is very apparent.

What is of particular note within these reports, is that 2010-2013 reports fail to mention terrorism, other than defining its parameters for Internet facilitated crime being related to funding, information, and recruiting in the 2010 AR, but leaving it out of reported statistics as it did not make the Top 10 Reported Crimes list in any of those years.\textsuperscript{102}

\textbf{Table 8: U.S. Cybercrime Reports 2010-2016}

\begin{table}[h]
\centering
\begin{tabular}{|c|c|}
\hline
Year & Reports \\
\hline
2010 & 12345 \\
2011 & 67890 \\
2012 & 10112 \\
2013 & 12345 \\
2014 & 67890 \\
2015 & 10112 \\
2016 & 12345 \\
\hline
\end{tabular}
\end{table}


The parameters of the terrorist category is later changed in the 2015 and 2016 ARs, to a description more closely resembling popular definitions of terrorism: “violent acts that are intended to create fear (terror); are perpetrated for a religious, political, or ideological goal; and deliberately target or disregard the safety of non-combatants.” This descriptor leaves out the subcategories mentioned in the 2010 AR, which could further obscure people’s understanding of terrorist involvement in the Internet.¹⁰³

It is only in the 2014, 2015, and 2016 AR, that terrorism is mentioned in the statistics, where there were 96, 361, and 295 victims of cybercrimes relating to terrorism. Despite this, issues with reporting and attribution make it difficult to say definitively that there were only these cyber-terror acts. Thus it is entirely possible that within the IC3’s reports, terrorist groups may have been involved in any of the other crimes such as ransomware, data breaches, or credit card fraud.¹⁰⁴

While the FBI’s IC3 gave two different versions of what they counted for cyber-terrorism the second version, focusing on the violent act, is a commonly used definition. Other divisions of the FBI have defined cyber-terrorism as:

“premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents.”

This echoes the standards of the GTD, requiring a violent aspect. Under this limitation, cyber-terror skeptics like Peter W. Singer in *The Cyber Terror Bogey Man* often point to the near non-existent physical damage from cyber-terror attacks, and how no people have been killed or harmed through a cyber-attack. This outlook is furthered through the commonly held belief that current terrorist capabilities in the cyber domain will never equal the damage of a bomb, and that Panetta’s cyber Pearl Harbor will only ever be in the future arsenals of state actors.\(^{105}\)

Some scholars find all this misleading, as it can drive people to the assumption that terrorists are not very involved in cyber. Others point out that terrorists are incorporating cyber-crime more frequently into their activities, and that cyber-criminals and terrorists will work together, as they do in the crime-terror nexus of the physical realm.\(^{106}\) Dr. Steven Bucci claims that terrorists actually will soon reach the capability levels that Singer has stated are farfetched, and that it is foolish to think terrorists will not get there one day. Bucci goes on to explain that terrorists excel in the cyber areas in

---

\(^{105}\) Singer, Peter W. (Pg. 1-3)

which they have been involved, listing out communications, propaganda, fundraising, fund transfers, recruitment, intelligence, reconnaissance, planning, DDoS.\textsuperscript{107}

**Terrorism & Ideology:**

When a terrorist attack occurs, as with any unexpected tragedy, two questions often emerge, “who did this and why.” The answer as to “who,” is often revealed by the terrorist organization itself, when it later claims responsibility; the “why” however can be complicated, as it requires understanding the ideology of the attackers. A group of researchers led by Gary Ackerman compiled a report \textit{Assessing Terrorist Motivations for Attacking Critical Infrastructure}, which established a template for understanding terrorist groups, what motivates them, how they operate, what impacts the target, the weapon and a multitude of other aspects, and the answers all fall back on ideology.\textsuperscript{108}

Ackerman et al describe ideology as “the basic set of political, social, cultural, and/or religious beliefs that members of the group hold…what the members are for and what they are against.” The description continues with several subcategories that make up ideology, such as worldview, group norms, and grand strategy, all of which combined describe what a group believes, how its members behave, and what they plan to do to accomplish its goals. While there are other considerations to understanding a terrorist group such as demographics, leadership structure, or relationships, all these relate back in some way to ideology.\textsuperscript{109}

There has been considerable theory developed about various types of terrorist ideologies and what they mean, whether religious, separatist, left or right wing. In David

\begin{footnotes}
\textsuperscript{107} Ibid (Pg. 4-5)
\textsuperscript{108} Ackerman, Gary Et Al “Assessing Terrorist Motivations for Attacking Critical Infrastructure.” Lawrence Livermore National Laboratory, UCRL- TR -227068, January 2007. (Pg. 20)
\textsuperscript{109} Ibid (Pg. 20)
\end{footnotes}
C. Rapoport’s seminal work, *The Four Waves of Modern Terrorism*, Rapoport identifies four distinct terrorist ideologies that have manifested themselves throughout the 20th century and into the 21st. Those are the Anarchist, Anti-Colonial, New Left, and Religious Waves. Rapoport has revamped his theory several times, and openly acknowledges the potential for overlap among waves, as well as that the theory leaves out several types of terrorist groups, such as right-wing groups. Though the study of terrorist ideology was not new when Rapoport published, the Four Waves theory has become a foundation upon which terrorist ideology is studied.

The wave theory dictates that from the turn of the 20th century to the present, history was impacted by each of these waves, which come and go within a generation or so. It began with the politically charged anarchists who were “stimulated by massive political and economic reform,” and defined by their frequent martyr-style bombings and assassination attacks on political targets.

In the 1920s following the anarchist wave, came the anti-colonial wave, made up of self-determination oriented groups. Formed in the wake of World War I, these spread across emerging states such as “Ireland, Israel, Cyprus, Yemen, and Algeria,” and were more militarized than their predecessors, favoring “guerrilla-like hit-and-run” tactics to accomplish their goals. Though colonialism largely faded out in the 1960’s, many of the grievances it spawned remained and became more separatist causes.

As the 1960’s continued, the New Left Wave emerged, featuring groups such as “the American Weather Underground, German Red Army Faction [and] Italian Red

111 Rapoport the fourth wave (Pg. 420)
112 Ibid (Pg. 420-421)
 Brigades…[which] saw themselves as vanguards for the masses of the third world.”
Internationally active and often favoring airline hijackings, this wave largely fell out of
activity at the same time as the collapse of the Soviet Union.113

Enter Rapoport’s fourth wave, the Religious Wave, which peaked in 1979 Islamic
Revolution and Russian invasion of Afghanistan. Though dominated by Islamic-based
terrorist groups, Rapoport notes that throughout modern and even ancient history there
have been non-state actors among Sikhs, Jews and Christians committing ideological
violence, and even apocalyptic millenarian cults like the Japanese Aum Shinrikyo. These
groups were distinct in that their constituency was not a nationality, political cause, or
ethnic group but a higher power, which renders all those who did not share that version of
faith an acceptable target.114

While Rapoport’s wave theory is highly regarded among many terrorism
researchers, there has been recent debate. Tom Parker and Nick Sitter in 2016 sought to
correct what they saw as an insufficient representation of terrorist ideology, with their
paper The Four Horsemen of Terrorism: It’s Not Waves, It’s Strains. Parker and Sitter
argue that there are four “strains” not waves of terrorism, the makeup these being
“socialist, nationalist, religious and exclusionist.” This theory suggests that like a strain
of a disease, ideology is infectious and can be traced from the infected to a carrier, and
eventually to a patient zero. The strains bear a striking resemblance in description to
Rapoport’s Waves. Only the exclusionist strain is particularly new, and is described as
resembling the racist ideology that tends to spring from various nations’ extreme right

113 Ibid (Pg. 421)
114 Ibid (Pg. 422)
Parker and Sitter fill in some of the gaps that Rapoport left out, and have generated responses from within the terrorism research community including a rebuttal from Rapoport, critiquing the Strain theory, though acknowledging the need to examine right-wing exclusionist racist groups like Neo-Nazi-Fascists. The two theories do, however, agree that ideology is important in understanding terrorist behavior and tactics.

The critique of ideological bases for categories of terrorist groups does not end with Parker and Sitter, Sarah V. Mardsen has advocated the use of Social Movement Theory (SMT) to determine typologies and understand terrorist decision making. Mardsen defines SMT as “an orienting device for the sorting of observations.” Mardsen argues that by way of SMT, researchers can gain an understanding of a terrorist group that goes beyond what category it falls into, but how this impacts the relationships it engages in.

Mardsen uses SMT to develop a three part framework which included resource mobilization, political opportunity, message framing. Through these elements Mardsen’s SMT method produced 11 classifications for understanding terrorist group’s actions; state support, popular support, groups support, territory, official wing, developing network, pre-existing fighters, training, membership, political stability, and rights/liberties composite.

---


118 Ibid (Pg.758)
Much of the inspiration for this paper comes from researchers attempting to apply ideological measures to terrorist behavior. James J. Forest attempted to research hostage taking in *Kidnapping by Terrorist Groups, 1970-2010: Is Ideological Orientation Relevant?* As the title implies, Forest sought to apply ideology to a group’s decision to employ the use of kidnapping, to see if there was an ideology more or less likely to employ the method. Forest states that since ideology provides “a motive and framework for action,” it should hold relevance to all a group’s activities, particularly in target selection and allies.\(^{119}\)

Forest continues to support the claim that ideology would be relevant, pointing to examples such as the religious Army of God, which has attacked abortion clinics.\(^{120}\) Despite the many known trends and ideology’s perceived importance, after examining a multitude of different terrorist groups, Forest found that “ideology does not play an important role in determining the likelihood of a group’s involvement in kidnapping.”\(^{121}\)

**Conclusion**

Through this Literature review, it can be seen that there is ongoing debate and several shortcomings in the realm of cyber terrorist activity, such as if cyber terrorism is or isn’t a threat and whether it even should be counted as terrorist activity or criminal. Further there is not much quantitative data tracking the cyber activity of terrorists that rival the tracking of the physical terrorism, which this paper could aid in remedying. Further, this paper could also contribute to the discussion on the importance of terrorist ideology in tactic choice, which has yet to be applied to cyber activity as this paper intends.

\(^{120}\) Ibid (Pg 774)
\(^{121}\) Ibid (Pg. 769-770)
III. Theory & Hypothesis:

Theory:

This paper will seek to apply terrorist ideological measures to various types of cyber activity to better understand if a group’s beliefs have relevancy to this emerging threat. In the literature review, it was established that there is ongoing debate about the place of terrorism in cyber conflict (for example, whether it is limited to propaganda, or could be as deadly as hacking into electric grids).

While the categories of SMT can aid in research, Mardsen herself noted that it is preferred for understanding group-to-group relationships, while the other ideological theories can be applied to a weapon/tactic choice like cyber acts. Further the 11 typologies do not address critical ideological questions, such as religiously motivated groups, or left versus right wing political groups. Thus this paper will use a combination of the ideologies described by Rapoport’s Wave Theory and the Parker and Sitter Strain Theory.

Hypothesis:

As the Literature Review shows, the cyber domain is seldom short of threats and conflict, whether it is spies, thieves, or terrorists. It can further be seen how these activities have been difficult for researchers to categorize.

What types of cyber activity do terrorist groups involve themselves in, and why would one group choose a particular tactic that another group might avoid? Knowing how ideology affects terrorist organizations’ differing choices of cyber activity will help answer that question, and add a basis for answering others. To better understand how ideology affects terrorist organizations, this paper will examine various terrorist groups
that fall into the five terrorist ideologies prevalent in today’s society, and study how terrorist groups are using computers and networked technology to see what, if any, cyber activities these groups are engaged in. The hypothesis of this paper is that at the conclusion of this examination, it will be clear that cyber activity does not differ among various terrorist ideological orientations, similar to kidnapping methods researched by Forest.

**Methods:**

This paper will use a series of case studies, selecting the two terrorist groups with the most attacks from five different ideological orientations to test the hypothesis and expectations of the Literature Review. The usage of case studies can be explained as “the detailed examination of a historical episode to develop or test historical explanations that may be generalizable to other events.”

Within the many modes of case study, this paper will use comparative analysis, specifically the method of a structured, focused comparison. This type of comparison is useful for this research in that the “structured” nature means that the same research question about ideology and cyber activity will be asked of each terrorist group case study. The “focused” aspect limits the research to “certain aspects of the historical cases in mind,” with those aspects being cyber activity, and not other features of the terrorist organizations.

While a solely quantitative approach to terrorist cyber activity could one day yield impressive and useful data, resembling a GTD type platform, for this research question, case studies are preferable as they have greater “potential for achieving high conceptual validity…[and] fostering new

---


123 Ibid (Pg. 68)
hypotheses.” This study will blend quantitative with qualitative, as the results will show data from 10 terrorist groups representing five ideologies.\textsuperscript{124}

**Case Study Selection:**

As previously discussed in the Literature Review, Rapoport identified four distinct terrorist ideologies that surfaced throughout the 20th century and into the 21\textsuperscript{st}: the Anarchist, Anti-Colonial, New Left, and Religious Waves. Later, in Parker and Sitter’s Strain Theory, socialist, nationalist, religious, and exclusionist ideologies were used to trace terrorist ideology. This paper has combined both ideological sets into five categories; Anarchist, Separatist, New Left, Religious, and Right Wing/Exclusionist. Though this still presents the challenge of overlap and multi-cause terrorist groups, the categorization presents a wide net in order to collect a large amount of case studies.

Using open source research, including the State Department’s list of Foreign Terrorist Organizations, the GTD, the Terrorism Research and Analysis Consortium (TRAC), and news reports, identified the two most active terrorist groups of those ideologies, based on attacks occurring between 2010-2015, and resulting in the groups shown in Table 10.\textsuperscript{125} In the Right Wing/Exclusionist category, much of the violence is categorized as non-political hate crimes, which would not be counted in the GTD, thus this the data was drawn instead from the Southern Poverty Law Center’s anthology on Right Wing Terror.\textsuperscript{126} While this method produced terrorist groups that contain overlap, for instance in the separatist category, Hamas and East Turkestan Islamic Movement both

\textsuperscript{124} Ibid (Pg. 19)
\textsuperscript{125} National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database. Retrieved from <https://www.start.umd.edu/gtd>
having strong links to Muslim religious terrorism there are still enough differences to warrant including both of them, such as geography, adversaries, and public perception. Additionally, groups like the Donetsk People’s Republic and the Taliban fall into the grey area of Violent Non State Actors, resembling insurgent groups and terrorist groups. Despite this debate, the activities of both groups fit the START definition of terrorist and will be included in this study, though the results should not be applied to insurgent groups.

Table 10: Terrorist Ideologies and Attacks

<table>
<thead>
<tr>
<th>Terrorist Ideology</th>
<th>Terrorist Organization</th>
<th>Number of Attacks 2010-15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anarchist</td>
<td>Informal Anarchist Federation</td>
<td>32</td>
</tr>
<tr>
<td>Separatist</td>
<td>Hamas</td>
<td>114</td>
</tr>
<tr>
<td>New Left Wing</td>
<td>East Turkestan Islamic Movement</td>
<td>30</td>
</tr>
<tr>
<td>Religious</td>
<td>Communist Party of India</td>
<td>1127</td>
</tr>
<tr>
<td>Right Wing/Exclusionist</td>
<td>USA Sovereign Citizens</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Taliban</td>
<td>4379</td>
</tr>
<tr>
<td></td>
<td>Islamic State</td>
<td>2919</td>
</tr>
<tr>
<td></td>
<td>Donetsk People’s Republic</td>
<td>600</td>
</tr>
</tbody>
</table>

IV. Data:

1. Anarchist:

Informal Anarchist Federation (FAI):

The anarchist ideology has a long history and is often cited as the first inspiration for the modern terrorists of the 1880s.\textsuperscript{127} The \textit{Federazione Anarchica Informale}, or Informal Anarchist Federation, is a contemporary anarchist insurrectionist group in Italy that became publicly known in 2003 and has gained notoriety for various terrorist-

\textsuperscript{127} Rapoport (Pg. 47)
bombing attacks in Italy as well as abroad.128

FAI’s notoriety has come from “a series of bombs and letter bombs, often directed against high profile targets,” though fortunately, most of these attacks have caused more alarm as opposed to casualties.129 Italian authorities have had little success against the group, making only an occasional arrest, and still have been unable to gather substantial intelligence on its organization. Currently, it is believed the FAI has somewhere between 50 to 250 members.130

Most of what is known has come from FAI’s own publications. In 2003, the group sent an “Open Letter to the Anarchist and Anti-Authoritarian Movement,” via paper mail to a local newspaper, which was later read aloud in the Italian Chamber of Deputies by Former Interior Minister, Giuseppe Pisanu.131 In the letter, FAI explained its motivation in three parts: that it used a horizontal structure, that it desired the destruction of capitol and the state, and that it opposes authoritarianism.132

As to involvement in cyber activities, current information suggests only fairly limited connection, as it is not engaged in DDoS, viruses, data theft, or other types of cyber crimes. This could be explained through its ideological leanings, gleaned from two FAI members arrested by Italian police, who noted that they “oppose the techno-industrial system.”133 The group has had its propaganda published online, and is

---

129 Ibid (Pg. 21)
130 Ibid (Pg. 22)
132 Marone (Pg. 22)
133 Ibid (Pg. 24)
suspected of using anonymous internet communication, although it does go through significant efforts to distance its members from direct Internet usage. One journalist who had a source within FAI, stated that the source only communicated “via methods that are virtually untraceable, secretly handing me reams of FAI literature to sift through for research.” The same journalist likewise pointed to FAI’s occasional usage of third party bloggers to publish stories about its attacks, spreading propaganda to inspire others and possibly recruit.134 135 In general, however, FAI has been cautious in its use of the Internet; even when claiming and taking responsibility for attacks, FAI has more often preferred physical means of communication, such as letters to newspapers, or even leaving notes at the scene of an attack.136

Conspiracy of Cells of Fire (CCF)

The Conspiracy of Cells of Fire, also known as the Conspiracy of Fire Nuclei or *Synomosia Pyrinon Tis Fotias*, is a Greek anarchist extremist group that announced its existence in 2008 after a series of arson attacks across the Greek cities of Athens and Thessaloniki.137 Unlike FAI, in its publicity, the CCF has let Greek authorities know that it believes in “revolt and resistance against modern power structures, lack of representation, and the hierarchies of capitalist society.”138 CCF is thought to be a reaction to Greece’s economic problems, often citing “social welfare austerity” in

134 Ibid (Pg. 22)
connection to its displeasure with a multitude of arson bombs, as well as letter bombs to embassies. CCF may have a slightly different type of anarchic rhetoric than FAI, however the two often show solidarity for one and other in their propaganda. CCF has even occasionally identified itself as “Conspiracy of Fire Cells-International FAI,” which has led some Greek and Italian authorities to believe the two have joined into one group.

Unlike FAI, CCF has been connected to more cyber activities, especially favoring online publicity. In one of CCF’s letter bomb campaigns in November 2010, the following online claims called out to other likeminded thinkers to target politicians, police, and tourists with arson, bombs, sabotage, theft, and vandalism. In recent years the CCF has become known for using the website <Athens.indymedia.org> to upload claims of responsibility and various propaganda posts, including a miniature manifesto “Democracy Shall Not Prevail,” mocking a commonly used political phrase by the Greek premier.

CCF’s engagement in cyber activity further goes beyond claims of responsibility and propaganda. There have, likewise, been connections to using the Internet to “plan demonstrations, disorder, and destruction through Google Earth,” as well the sharing of strategy documents to create training guides on multiple insurrectionist activities including “explosives to lock picking,” as well as studying various video footage through Youtube.com in a “lessons learned” style. Though CCF shares the anarchist ideology,

---

140 Ibid (Pg. 32)
141 Ibid (Pg. 29)
142 Kassimeris (Pg. 637)
143 Miller (Pg. 32)
it is uncertain why it differed from FAI in regards to cyber activity, as the only significant
distinguishing features between them were age, and geographic location.

2. Separatist:

Hamas

The Palestinian terrorist group Hamas, or Harakat al-Muqawama al-Islamiya, which translates to Islamic Resistance Movement was founded in 1987 as another Palestinian faction fighting against Israel, and is based primarily in Gaza territory between Israel and Egypt. In late April of 2017, Hamas released a new guiding charter which added that in addition to its long term goal of liberating Palestine and destroying all of Israel, it is dedicated in the short term to establishing a sovereign Palestinian State with borders along the ceasefire lines set prior to the 1967 Israeli-Arab War, in which Israel captured Gaza and the West Bank from Egypt and Jordan respectively.

Since its founding, Hamas has evolved from being solely a terrorist group to taking on more political responsibilities, and in 2006 was democratically elected to lead the Palestinian Legislative Council, though the group still had to fight off an attempted overthrow by rival Palestinian factions. It has since taken total control of the Gaza territory. Despite the fact that the group has taken on political and social responsibilities, it has not yielded in its desire for armed conflict with Israel and has engaged in a plethora of terrorist attacks, including suicide bombers, kidnappings, and armed assaults, and has

---

become known for rocket and mortar attacks on Israel’s southern towns and cities.¹⁴⁶

In Hamas’s campaign against Israel, it has engaged all sorts of cyber actions to further its separatist goals. While Hamas has used the Internet to spread propaganda, the group also has been connected to the use of online methods for collecting donations and money transfers. As early as 2009, it had even cautioned potential patrons on communication encryption, and stated on its website “to use fake” names when sending e-mails about contributions.”¹⁴⁷ As well, in 2015, the DOS Bureau of International Narcotics and Law Enforcement Affairs reported that Hamas had been engaging in online money laundering.¹⁴⁸

Since the beginning of Hamas’s exploration of cyber activities, it has been speculated that it has received training and support from Iran, with which it has a shared enemy in Israel.¹⁴⁹ In 2013, a hacker group using the moniker “Izz ad-Din al-Wassam Cyber Fighters,” and identifying as part of Hamas, began to use DDoS methods against Israeli websites, both private and those belonging to the Israeli government.¹⁵⁰ This shift to more cyber-attack style methods continued as a trend with Hamas, as seen in the Summer of 2014 Israeli-Hamas Conflict when the group began to use large amounts of malware attacks in conjunction with its physical terrorist attacks.¹⁵¹ Hamas hackers also

---

have been linked to the sending of phishing emails to Israeli soldiers and government
officials trying to obtain information, and has hacked phones of Israeli soldiers in
attempts to stealing their identities to use on social media and dating sites for “honey pot”
operations.\textsuperscript{152}

\textbf{East Turkestan Islamic Movement (ETIM)}

The ETIM are one of the insurrectionist groups representing the Uighurs, an
ethnically Turkic population living in Western China’s Xianjing province, as well as
several other central Asian states. While there are several militant groups within the
Uighur population, each with slightly different goals, separating the Xianjing region from
China and establishing a sovereign East Turkestan is a common goal for all of them, with
ETIM being the lead group.\textsuperscript{153}

Due to the Chinese government’s strict legal system and control over information,
there is not a lot of information about ETIM and the Uighur separatists. As well, there are
rumors that the Chinese government inflates the threat to justify increased security
measures, often citing ETIM and Uighurs with terrorist attacks that have not actually
happened. What is known is that ETIM has been linked to “bombing buses, markets, and
government institutions—as well as assassinating local officials, Muslim leaders, and
civilians—in attacks that have killed 162 people” since its founding. Most recently, there
has been a series of knife attacks, as well one attack that featured needles infected with

\textsuperscript{152} Surkes, Sue. "Hamas Upgrades Cyber Espionage Capability --- Report." \textit{The Times of Israel}, February
Yossi. "Analysis: Hamas Honeypot’ Operation Shows a sophisticated Cyber-Epionage Unit." \textit{JPOST},
a-sophisticated-cyber-espionage-unit-478219.

\textsuperscript{153} Beina, Xu, and Holly Fletcher, and Jayshree Bajoria. "The East Turkestan Islamic Movement (ETIM)." 
movement-etim.
the AIDS virus.\textsuperscript{154} Though ETIM denies it, the group has been linked by the Chinese government to other terrorist groups such as Al Qaeda and the Taliban, a claim supported by the United States, which has stated that ETIM and other Uighur separatist groups have received training and funding from these more notorious terrorists for years.\textsuperscript{155}

In 2013, spokesperson Hua Chunying of the Chinese Foreign Ministry stated that as part of China’s commitment to United Nations Security Council Resolution 2129 on countering terrorism, China will be cracking down on cyber-terrorism, and that China has been victim to cyber attacks from ETIM and other East Turkistan terrorist forces. Chunying further stated that ETIM uses the Internet and has “poured audios and videos about terrorism…to instigate the so-called jihad against the Chinese government,” and that ETIM uses the Internet to claim responsibility for attacks.\textsuperscript{156}

Beyond these propaganda and instigation actions, there is little evidence connecting ETIM to cyber activity. There is Uighur separatist activity online, but much of that comes from the Uighur’s diaspora community, which uses the Internet to organize activism and spread information about its cause. However, many of these websites are blocked by the Chinese government, which censors information it deems a security threat. These censoring actions have left the Xianjing region with only severely limited Internet access.\textsuperscript{157} Oddly enough, the Chinese government has been linked to cyber


\textsuperscript{155} Beina, Xu and Holly Fletcher, and Jayshree Bajoria


attacks against various Uighur groups, and not the other way around.  

3. New Left Wing:  

Communist Party of India-Maoist (CPIM)  

As discussed in the previous chapter, the Communist or Maoist Party of India, also called the Naxalites, is a Maoist insurgency group local to India. CPIM has found inspiration in the original 1970’s Naxalite terrorist group that sought to replace India’s government, which in its perspective has instituted a system that is cruel to the poorer rural regions.

Since its inception, CPIM has managed to build a substantial force of approximately 20,000-armed fighters, and even has some territorial control. The majority of CPIM’s methods revolves around guerrilla tactics, with its fighters using “use small arms and homemade explosives, including landmines,” and have also been known to commit kidnappings often targeting military and government officials.

Though only for limited purposes, CPIM has been using some cyber methods in its operations for several years. As early as 2006, it was reported that CPIM fighters had been using online mapping programs such as Google Earth in the plotting of attacks against India’s security establishment. CPIM has been reported to use the Internet to

---


161 Zissis, Carin

recruit in areas where neither it nor the Indian security forces have a substantial presence, and then sending “emails to potential recruits to ask for their qualifications and how they would like to lend support.” Additionally, CPIM has been using handwritten and other physical propaganda less, and instead engaging in online social media platforms to spread its message to India’s unemployed and claim attacks. Most recently, it was reported by Indian police that CPIM members were working with rural criminal elements to conduct various cyber crimes such as stealing credit cards and illegally transferring funds. What may be unique about this coordination is that the CPIM protected cyber criminals seldom use protective measures to hide their locations in an effort to lure Indian authorities to these areas so CPIM can stage ambush attacks.

**Revolutionary Armed Forces of Colombia (FARC)**

In 2016, the infamous Revolutionary Armed Forces of Colombia (FARC) signed a peace accord with the Columbian Government, but as of the writing of this paper, it has yet to be fully implemented and there are those in the U.S. government who do not believe it will last. These individuals include former American Ambassador to Colombia Kevin Whittaker, who noted that despite the accord, “FARC continues to be one of the world’s largest drug-trafficking organizations and an organ of international terrorism.”

---


67 

Leopold-Cohen, Justin H.
Before this most recent attempt at an armistice, FARC was known as a 10,000-20,000 strong Marxist revolutionary group that waged a “half-century war [that] killed at least 220,000 people, uprooted more than 6 million, and left some 8 million registered victims.” 167 While FARC’s current activities revolve around an extremely lucrative narcotics trafficking operation, the terrorist acts they have committed span from bombings, assassinations, guerrilla style assaults, and kidnappings, as well as hijackings plaguing the Columbian government so much that complete amnesty was offered in the current peace deal.168

In the realm of cyber space, FARC has been active since the Internet first became popular, noted for its use of Email in the late 1990’s to communicate to the press. This has continued to the present as the group communicates with the Columbian government during negotiations.169 In efforts to spread its narrative, for years FARC has maintained websites, as well as several on-again/off-again social media profiles, which show “the history of this organization and another page devoted to press releases, most of which praise the FARC and critique the Colombian government,” and also features the ability to make inquiries to the group, or be directed to its YouTube channel which has videos explaining its goals and activities.170 There has been some slight censorship on the part of

the Columbian government, which has taken down FARC’s WebPages in the past, when the content is recruitment or incitement-based rather than propaganda, though large-scale regulation has not been enforced.\(^\text{171}\) Despite the long history of FARC’s online presence, there is no evidence of any use of hacking, malware, DDoS attacks, or any financial cybercrimes.

4. Religious:

The Taliban

In 1989, after the withdrawal of Soviet Union forces from Afghanistan, and the 10-year Russian war, some of the Afghanistan irregular forces known as Mujahideen banded together to create the Taliban, which translates from Pashto to the Students. The group is configured of Islamic fundamentalists who used violence to systematically take control of the country in the 1990’s, and installed a strict conservative religious governing system that blended Sharia and Wahhabi doctrines, and would gain the U.S.’s attention for sheltering Osama bin Laden and Al Qaeda when it orchestrated the 9/11 attacks on and Washington D.C. and New York. The Taliban would hold majority control of Afghanistan from 1996-2001, when the U.S. invasion pushed its leadership out of Kabul.\(^\text{172}\)

As of the writing of this paper, for 16 years the U.S. military has maintained varying degrees of presence in Afghanistan maintaining order, primarily fighting the Taliban as it uses armed assaults and suicide bombers against U.S. and allied forces.\(^\text{173}\) Despite the


allied invasion, the Taliban’s strength has intensified, as it drives its narrative of fighting against foreign conquerors, with approximately 7,000 fighters in 2003, increasing to closer to 30,000 in 2012. At the same time, the Taliban has built an opium-smuggling operation, and even extorts taxes from regions it controls.\textsuperscript{174}

Since the early 2000’s, the Taliban has been active in many different online activities. One of its first engagements with the Internet was maintaining an English language website to explain the Taliban narrative. This was done by a “computer engineer” who supported the Taliban, and explained how “all over the world the Jewish controlled media is brainwashing Muslims and non-Muslims who want to know the truth. That’s why I, as a Computer Engineer, decided to use Internet, most powerful tool, to convey the message to all Muslims.”\textsuperscript{175} This has continued over the years, and though “the Taliban are paranoid that modern technology will betray hiding places…[they] regularly promote their attacks, opinions or exploits online in a publicity war with the West.\textsuperscript{176} This online publicity includes the use of cellular applications and photo sharing, which frequently feature pictures of wounded or killed allied forces.\textsuperscript{177} This same cyber communications technique is used in social media platforms, where Taliban operatives not only spread their message, but also attempt to recruit new members.\textsuperscript{178}

\textsuperscript{174} Staff. "Taliban Narrative." \textit{National Consortium for the Study of Terrorism and Responses to Terrorism}, July 2015. \texttt{<http://www.start.umd.edu/baad/narratives/taliban/>}
\textsuperscript{177} Ogun, MN. \textit{Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses}. Washington DC: IOS Press, 2015. (Pg. 97)
Taliban use of the Internet does not end at communication; the group has a well-established history in financial crimes as well. In the early 2000’s, the charity organization, Global Relief Foundation, claiming to work with emergency medical aid and education was designated as a financer for terrorism with links to the Taliban and other groups, where it was funneling money through its website donations. These types of financial crime and cyber money laundering are one of the ways terrorists raise funds, though the Taliban has not yet been linked to any malware or aggressive hacking.

**Islamic State (IS)**

The Islamic State, also known as ISIS or *Daesh*, among other names, is one of the most notorious terrorist groups operating today, with its global reach linked to terrorist attacks across 29 countries, leaving thousands dead in the few years since its inception. IS was created out of the chaotic state of Iraq in the later years of the American invasion of Iraq, formally declaring a Caliphate or Muslim state under the banner of militant Sunni Islam. IS forces have since waged a terrorist campaign seizing territory mostly across Iraq, Syria, and Libya, and has had “insurgent groups in Afghanistan, Bangladesh, Egypt, Indonesia, Nigeria, Pakistan, the Philippines, Saudi Arabia, and Yemen have sworn allegiance” to IS, which hopes to spread its rule to all Sunni Muslims so it can initiate an apocalypse.

Since 2014, the U.S. has led a coalition of 60 nations in the fight against IS, with

---

179 Jacobson, Michael


all types of combat from air strikes and Special Forces to humanitarian aid and economic sanctions. Even so, IS fighters and others who have pledged their allegiance continue to launch devastating terrorist attacks of all forms including planting explosives, using suicide bombers, shooting attacks, car ramming, as well as knife attacks and connections to airline hijackings.

In its quest for global domination, IS has shown great prowess in using the Internet. In its communication efforts, online methods have gotten to the point where “large social media and web platforms have become the command-and-control networks of choice,” not only for propaganda and recruitment but for sharing content relating to training and methods as well, and often uploading candid video footage of battles from fighters using go-pro devices.

Though known for inspiring physical attacks, other supporters have taken up fighting for IS through cyber methods, launching DDoS attacks on websites or even taking control and defacing them with IS propaganda, as well using malware to attack organizations critical of IS’s actions. Some of these IS hackers have managed to break into government websites to steal data. In March of 2016, IS hackers broke into the New Jersey Transit Police website and publicly posted the information of some 3,000

---

residents, calling for their deaths.186 The hacking of public information also extended to
government officials. In 2015, the Kosovo hacker Ardit Ferizi worked with IS hacker
Junaid Hussain and provided the personal information of almost 100,000 people noting
who were employees of the U.S. government.187

Social media websites such as Twitter and Facebook have begun to face lawsuits
from terror victims and their families, who claim these sites’ capabilities are aiding
terrorists, and though judges have ruled the websites are not liable, Twitter, Facebook,
and others continue to remove radicalizing propaganda, over 250,000 per year in some
cases.188 This has been a contributing factor of the group moving to “Dark Web” methods
where online activities remain anonymous and unregulated. Through the Dark Web, IS
can easily encrypt communications and share content without it being quickly monitored
or removed.189 As well, IS has managed not only to communicate but to freely move
funds using anonymous online currencies like Bitcoin, as well as virtually managing
lone-wolf attackers and helping them plan out attacks in their home countries.190

5. Right Wing/Exclusionist:

---

Donetsk People’s Republic (DPR)

While the 600-recorded attacks from DPR in 2010-2015 already make it a deadly terrorist group within the GTD, Jane’s Terrorism and Insurgency Centre has attributed 3,417 attacks to DPR in 2016 alone which would make it one of the most deadly in the world.\textsuperscript{191} The DPR, formed in 2014, is a far right group in Ukraine that exercises an exclusionist philosophy within its mission.\textsuperscript{192} While the DPR maintains nationalist goals, many of leaders are politically aligned to Ukraine’s far right, with a history of fighting against pro-democracy groups, though it claims to be opposed to fascism.\textsuperscript{193} In areas that the DPR control, a strict legal system is imposed, curbing the rights of the press, and targeting non-Russian populations with oppression, particularly Jewish communities who are forced to register with DPR authorities.\textsuperscript{194}

The fighting of the DPR is localized to Ukraine, and though it may not be making the same headlines it did early on in the Ukraine conflict, there has been a noted rise in violence with “more than six-fold increase in the number of attacks recorded in 2015.”\textsuperscript{195} The DPR is organized in a militia structure and wages a terrorist guerrilla war, primarily


\textsuperscript{195} Staff. "2016 Global Attack Index."
using explosives and armed assaults, though it also occasionally uses kidnapping and hijacking methods to advance its goals.\textsuperscript{196}

The DPR has had mixed use of cyber activity. The groups do utilize social media to explain its narrative to garner support, though does not seek to recruit or inspire others through online communications. In January of 2017, the DPR was named as one of the groups that may have been using a type of spyware known as \textit{Finspy} to conduct cyber espionage against its targets, though there is currently no evidence to suggest the group has used virus style malware in cyber-attacks.\textsuperscript{197} DPR has also made statements that it has considered getting more involved in the online anonymous currency Bitcoin due to the ease it provides for moving funds across borders, though it has yet to be publically linked to using it.\textsuperscript{198}

Though DPR may not directly be using cyber methods, there is significant cyber activity being conducted in the Ukraine conflict. The Russian hacker group, APT 28, believed by U.S. intelligence officials to be part of the Russian government, were accused of having “used a malware implant on Android devices to track and target Ukrainian artillery units from late 2014 through 2016” as well as stealing classified data from Ukrainian law enforcement agencies and using the information to aid DPR and other pro-Russia groups.\textsuperscript{199}

\begin{flushleft}
\textsuperscript{196} National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database Retrieved from https://www.start.umd.edu/gtd
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\end{flushleft}

\begin{flushleft}
\end{flushleft}
Sovereign Citizens Movement (SCM)

Though the GDT only implicates the Sovereign Citizen Movement (SCM) in 4 terrorist attacks, the threat these extremists pose is much more significant, with other sources such as the Southern Poverty Law Center’s naming them as responsible for at least 40 attacks. The SCM is not a single unified organization, but a collection of lone antigovernment extremists. Similar in belief to the growing radical “patriot” militias, the SCM in the U.S. are far right extremists who oppose what they believe to be an authoritarian federal government.200 The activities of the SCM can range from not paying taxes and refusing court orders, to more criminal and extreme actions such as financial fraud and murder as they do not recognize the authority of the government.201

Though this cannot be said of all those affiliated with the SCM, many of them are “white men with some military background, and extreme-right, often racist values,” and of the approximate 300,000 people affiliated, roughly one third are violent. The attacks of the SCM are seldom part of an organized group, but rather spontaneous outbursts brought on by something as simple as being pulled over for a traffic violation. The insurrectionist activity originating from the SCM has featured everything from falsifying government liens and harassment, as well as bombings, shootings, and one particularly notorious event in 2010, when Joseph Stacks crashed a small plane into an Internal Revenue

---


Service building in Texas.\textsuperscript{202} Due to the violence that comes from the SCM and the difficulty in identifying or tracking its members, law enforcement often rank them as one of the larger, if not largest, domestic terror threats in the U.S.\textsuperscript{203}

As there is no organized structure, the online presence of the SCM is different from other groups; it has no group Facebook or Twitter, and does not recruit to any formal body. There is still, however, a lot of cyber activity coming from the SCM. Believers in the SCM cause frequently use the Internet to spread propaganda and exchange ideas. There also is known “cyber-stalking” of government employees and those who disagree with their views, often harassing and threatening them.\textsuperscript{204} In what resembles online training of sorts, many SCM affiliates use the Internet to spread information about how to tie up government officials in unsubstantiated lawsuits, and how to engage in financial schemes of different kinds.\textsuperscript{205} Though the SCM is still growing, there is no evidence that SCM individuals have engaged in more aggressive cyber activities such as DDoS, malware, online money laundering, or data theft.

V. Discussion:

Results

Seen below in Figure 5, the results of the data are displayed in a chart. As shown, the results vary, with no clear ideological slant towards any one cyber activity. Similarly to the first chapter, the terrorist groups examined here can be seen on the Makarenko

\footnotesize
\begin{itemize}
  \item \textsuperscript{202} MacNab, JJ. "What is a Sovereign Citizen?" \textit{Forbes}, February 13, 2012. https://www.forbes.com/sites/jjmacnab/2012/02/13/what-is-a-sovereign-citizen/#eb44f666012e.
  \item \textsuperscript{204} MacNab, JJ
\end{itemize}
Continuum being engaged in criminal activities for operational purposes within the Cyber Domain, and in the case of the Communist Party of India explicitly having formed alliances with criminal cyber gangs.

**Table 11: Chapter 2 Results Illustrated**

<table>
<thead>
<tr>
<th>Terrorist Ideology</th>
<th>Terrorist Organization</th>
<th>Hacking</th>
<th>Crime</th>
<th>Communication</th>
<th>FBI Definition Cyber Terrorism</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DDoS</td>
<td>Malware</td>
<td>Financial</td>
<td>Data Theft</td>
</tr>
<tr>
<td>Anarchist</td>
<td>Informal Anarchist Federation</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Separatist</td>
<td>Hamas</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Left Wing</td>
<td>Communist Party of India</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Religious</td>
<td>FARC</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Right Wing/Exclusionist</td>
<td>Islamic State</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Donetsk People's Republic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Sovereign Citizens Movement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

The cyber activities are broken up into three main categories: hacking, crime, and communication, and a fourth category to represent the earlier mentioned FBI definition of cyber terrorism, which calls for cyber-enabled violence against non-combatants. There also are sub-categories that were developed from the most common cyber activities mentioned in the literature review, such as DDoS and malware for hacking, financial crimes and data theft under crime, and plans, propaganda, claims and recruitment under communications.

It can be seen that in regards to the threat of cyber-terrorism, none of the groups have managed to operationalize a cyber-enabled attack that has resulted in real harm to anyone. Thus the days of terrorists using computers to kill people remain in the future.
The hypothesis of this paper was cyber activity would not change among various terrorist ideologies, the way that ideological differences have been shown to affect a groups engagement in illegal narcotics, or targeting civilians versus military/government. The results show no ideology dominated a particular cyber method, thus the hypothesis was proven correct.

Particularly noteworthy is that the results show that each terrorist group, regardless of ideology, uses the Internet for propaganda purposes. Further, almost all have linkages to the entire communications category. Only the Religious Islamic State had connections to all cyber activities, followed by the separatist Hamas which has engaged in all but two communication subcategories. The least amount of cyber engagement came from the Left Wing FARC, and the Right Wing Sovereign Citizens Movement, with all other groups in the middle. It should also be noted that due to the anonymity of these cyber acts, and difficulty in tracking, it cannot be definitively stated if the data collected was based on the terrorist groups themselves, or with affiliate and/or support groups.

Limitations

While there are clear implications to be drawn from this data, the results are not without their limitations. As was seen in the literature review, the theory behind terrorist ideology is still debated, due to the issues of new ideologies and the overlap that many modern terrorist groups exhibit today. Though the cases studies were separated based on the primary features of the group’s ideology, the issue overlap was still present in many of them. Hamas and ETIM, while separatist groups, are both also religious. The DPR, a leading right wing group in Ukraine has nationalist/separatist undertones. As well, the SCM are known for their affiliation to right wing extremism, but the anti-government
rhetoric could also be described as anarchist. Terrorist groups being multi-purpose adds to the issue of ideological overlap, and makes certain distinctions difficult, forcing categorization based solely on primary objective.

In regards to the evidence collected for the data, it is only from publically available sources, which leaves open the possibility that certain terrorist groups or cyber activities may be much more present than currently known. That said, this data does not have the ability to say where there was not a connection, only where a connection is definitively provable. As time passes and more information becomes publicly known, future researchers should reexamine the questions of this study. Further data on criminal acts of any kind is always suspect, many crimes go unreported while others may not be known at all, which is a problem compounded in cyber space where there are issues of attribution. This means that while known data may have shown a lack of cyber engagement in a particular category, it is possible that the terrorist group may be engaging and just was not caught.

VI. Conclusion:

The question that this paper sought to answer was how choice of cyber activity changes among different terrorist ideological orientations. The goal in this study was primarily meant to see if ideology is meaningful in cyberspace the same way it has been shown to be in the past, such as a group’s choice of target, or acceptance/dismissal of a particular tactic. As researchers have not conducted an ideological survey of terrorist groups’ engagement in cyber activity, answering this question would fulfill a knowledge gap in the field of terrorism research.

Secondary to ideological importance, this paper likewise sought to add to the debate
about the threat of cyber-terrorism. In the literature review, Peter W. Singer pointed out that the fear of cyber-terrorism is inflated, and that no deaths or physical damage have come through any cyber-terror event. As well, law enforcement agencies like the FBI point out the necessity for violence and harm for an act to be counted as cyber-terrorism. There are still many who are concerned that terrorists will be able to kill with computers. The answer to this paper’s question also would show what terrorist groups are capable of doing with computers.

Taken as a whole, the hypothesis that ideology does not play a role, was proven correct. Cyber activity of terrorist groups showed no ideological trends, and almost all groups using cyber communication methods. As well, no group, even the Islamic State has been able to launch an attack that would meet the criteria of the FBI.

The conclusions of this paper have created other questions for research. If ideology does not play a role in cyber activity, what other factors may there be? Perhaps geography, age, or group size could be factors involved in cyber activity. In this case study selection, there were rural and urban groups, young and old, as well as small and large. Additionally, future researchers could take the answers to those questions, combined with implications of this study, to create an alternative database similar to the GTD that tracks cyber-activity which would be beneficial for terrorism research. If terrorists do one day manage to launch violent cyber-attacks, knowing more about cyber capability and activity over the years would be useful for future counter-terror practitioners and researchers alike.

**Chapter Three: Criminals and Terrorists: The Response to the Irish Nexus**
“To achieve victory we must mass our forces at the hub of all power and movement. The enemy’s center of gravity.” –Carl Von Clausewitz

I. Introduction:

In May of 2017, the United States issued a Travel Alert cautioning Americans over terrorist fears in Europe, particularly in connection with Islamic State and Al Qaeda.\textsuperscript{206} Terror attacks across Europe have been dominating media headlines for quite some time, and have initiated a rise in public concern that similar attacks will soon come to the United States. This is not a new occurrence, a 2015 Gallup poll showed how concerns about terrorism have steadily increased over the past few years and are spiking due to these attacks across Europe.\textsuperscript{207}

While the Gallup poll may be correct in that recent attacks in Europe are contributing to American anxiety over terrorism, Europe was hardly free of terrorism prior to the new millennia. Referring to Appendices Table 12, based on data from the Global Terrorism Database, it is clear that during the 2000’s, terrorism was at record lows across Europe; only in the last few years has it reached the heights it had during the 1970’s.\textsuperscript{208} Since the late 1960’s, some of the most active perpetrators of European terrorist attacks were Irish Republican extremist groups operating across the United

\textsuperscript{208} National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database (Western Europe; Eastern Europe) <https://www.start.umd.edu/gtd>
Kingdom, as well as other parts of Europe and beyond, which only wound down in the early 2000’s.\(^{209}\)

The largest of the Irish dissident groups was the separatist group, the Provisional Irish Republican Army (PIRA). Without going into detail about the centuries long conflict, for the purpose of this paper, it will have to suffice that Irish nationalists wanted independence from the United Kingdom, and felt that the British Protestants were oppressing the Irish Catholics. This grievance brought about the rise of Irish Republicanism, and with it the various dissident groups willing to commit acts of terrorism to further its cause. The PIRA modeled itself after the Irish Republican Army (IRA) that continued its fight for Irish independence long after the original Irish Republican Army signed the 1921 Anglo-Irish treaty with the British. It was this treaty that created the independent Irish Free State, later becoming the Republic of Ireland.\(^{210}\)

Though starting dates vary depending on what side of the conflict one falls, it is largely agreed that after a string of clashes in the late 1960’s between Irish Republican protesters and British police forces, the historical period known as “the Troubles” began. This episode is marked by a campaign of terror launched by Irish Republican dissident groups as they attempted to remove the British presence and unite Northern Ireland with the Republic of Ireland. To do this, the PIRA or Provos and other nationalist groups engaged in a wide range of attacks including bombings, assassinations, and kidnapping.

\(^{210}\) Ibid.
When the Troubles largely ended in 1998 and the Good Friday Agreement was signed, the conflict had claimed the lives of 3,600 people, and caused thousands of injuries.\textsuperscript{211}

In addition to their more well-known terror tactics, these Irish groups also had a notable “involvement in organized criminal activities, such as extortion, bank robbery, smuggling, and counterfeiting.”\textsuperscript{212} This involvement would sometimes consist of their own members acting as an organized crime group in order to procure arms or funds for continuing operations; other times, it would involve collaboration with established organized crime groups for similar objectives.\textsuperscript{213}

The collaboration between terrorist organizations and organized crime groups, known as the “crime-terror nexus” as seen during the Troubles, is now a growing concern for governments under attack from terrorists, as it has shown itself to be difficult for present counter terrorism strategies to defeat. Given this evolving nature of terrorism, it stands to reason that counter-terrorism strategy must evolve as well.\textsuperscript{214}

The question that this paper hopes to answer is how governments responded to the crime-terror nexus that evolved out of Irish Republican terrorism. Though there is a great deal of existing scholarship on Irish terrorism, only a fraction of that is focused on the Irish group’s interactions with transnational organized crime groups, and even less is devoted specifically to examining the government responses. Beginning with an explanation of what the crime-terror nexus is, the literature review will then examine the

\textsuperscript{211} Kelters, Seamus. “Violence In The Troubles,” British Broadcast Company (2013) <http://www.bbc.co.uk/history/topics/troubles_violence>
\textsuperscript{212} Gregory, Kathryn. (2010).
challenges presented to counter-terror organizations, and conclude with what present
scholarship has suggested in the way of a strategy for response.

In the following hypothesis and method sections, this paper will elaborate on how
it will attempt to prove that government agencies utilized a strategy of target
readjustment, and focused on the organized crime elements of the Irish terror groups as a
way to disrupt terrorist activity. This will be accomplished by examining case studies
on five different agencies all of which had interactions with the Irish nexus.

In current United States strategy circles, those in command sometimes look to the
British use of counterinsurgency tactics against the Irish Republican dissidents. Believing
that “future U.S. adversaries will almost certainly apply insurgent-like tactics…a study of
historical cases can sometimes provide new perspectives on current problems.”

By looking more closely at the crime-terror nexus that existed in Irish Republican
linked terrorism, not only will this paper serve as a scholarly contribution to an under
researched topic, but it could potentially aid counter-terrorism organizations seeking to
discover how to counter the crime-terror nexus that exists today.

II. Literature Review:

What is The Crime Terror Nexus?

Recalling the first chapter of this thesis, it was discussed that there is little debate on
the description of the crime terror nexus. Chapter 1’s Figure 2 on page 19 presents the
spectrum designed by Dr. Tamara Makarenko. The spectrum features organized crime at

---

215 Freeman, Michael, “Terrorism and Organized Crime.” Organizational and Psychological Aspects of
216 Jackson, Brian A. “Counterinsurgency Intelligence in a Long War: The British Experience in Northern
one end, terrorism at the other, and the various steps that a group must go through spread across the middle, such as alliances, adopting tactics, and adopting targets. The crime-terror nexus continuum theory describes how a group can go left to right across the spectrum, and sometimes settle in the middle as a hybrid organization.  

Thomas M. Sanderson has noted that the convergence first came to a noteworthy level in the aftermath of the United States-Soviet Union Cold War in 1990, when certain terrorist groups lost state-sponsorship for their activities, and began to branch out in their search for operational funds.  

**What are The Challenges for Counter-Terrorism?**

Major Nathan Minami of the United States Army elaborates on the many challenges that counter terror organizations face when confronted with the crime-terror nexus, and how this convergence of tactics is advantageous for the terrorist group. Minami argues that jurisdiction is the largest problem, as government agencies are by and large limited to their own borders, unlike the entities that they pursue. Further, conducting counter-terror operations is an expensive task, whereas the terrorist attacks average only a fraction of the cost. Minami points out “terrorists don’t need a lot of money to conduct operations, 9/11 only cost an estimated $300,000 for Al Qaeda to conduct.” Thus the terrorist group that engages in criminal activities will be able to fund more attacks.  

**What are the Recommendations for Response?**

---


218 Ibid (P. 50)


220 Ibid (P. 5)
The majority of scholarship on how to defeat the crime-terror nexus seems to fall into two main camps: first are those who favor international cooperation, and second, those who argue that governments should begin to adjust their operations, so that they focus the counter-terror resources towards targeting the organized crime groups. As well, there are several fringe strategies that do not fall into either category such as promoting working with organized crime groups, and using disruption tactics to prosecute all offenses, not just terrorist related charges. Though the theories do not suggest that these strategies are mutually exclusive, (in fact some go so far as to promote overlap), there is the implication by each theorist, that his or her suggested strategy is the best approach, and an alarming lack of identifying each other’s strengths and weaknesses which could aid practitioners in developing the best holistic approach.

Dr. Michael Freeman of the Department of Defense Analysis at the Naval Postgraduate School offers several counter measures that fall into the adjusted targeting category, which would better focus government agencies on organized crime groups that work with terrorists. Most notably, Freeman recommends government agencies should focus more on the logistical and operational units of terrorist organizations, not just the violent ones. It is these terror cells that link with organized crime for financing their operations.221

In the same camp, Sanderson stresses “both organized crime and terrorist groups are learning from past mistakes while probing recent defenses erected by targeted nations.” Focusing government efforts on the organized crime elements thus disables the ability of terrorists to use them as a tool. His strategy calls for “much greater local

221 Freeman, Michael. (P. 107)
intelligence…and a deeper understanding of personalities, modus operandi, culture, and financing.” 222

However, Sanderson is aware of the common complaint that the crime-terror nexus cannot be countered single handedly, and favors the utilization of international bodies to target the organized crime activities globally, such as the Southeastern European Cooperative Initiative (SECI) whose anti-terrorism task force supports coordination among member states in combating the crime-terror nexus.223

This targeting of the organized crime element is not without its problems, however. As Sanderson notes, in certain cases, organized crime groups can be used as an intelligence source against terrorist organizations.224

This introduces one of these fringe strategies, elaborated on by Vanda Felbab-Brown, senior fellow of Brookings’ Center for 21st Century Security and Intelligence. Felbab-Brown recommends a strategy for combating the crime-terror nexus by way of police-criminal collaboration. What the Felbab-Brown strategy suggests is the shaping of these transnational organized crime groups into “good criminals.” The concept of the good criminal comes from the idea that law enforcement should have an almost unofficial pact with these criminals, that if the criminals can reduce violence, distance themselves from society, and most importantly, not work with terrorists, then law enforcement will back off from prosecution, ideally allowing the two to work together against terrorism. 225

222 Sanderson (P. 56)
223 Ibid (P. 57)
224 Ibid(P. 58)
While this strategy is on the fringe of recommended responses, the idea is not without a small amount of traction. Giovanni Gambino, “son of infamous mob figure John Gambino,” stated in an interview that La Cosa Nostra is in a better position to combat the Islamic State in New York, than the NYPD and willing to show society that the Italian Mafia is on its side in the fight against terrorism.\(^\text{226}\)

However, there is no real endorsement of cooperation between counter-terror agencies and criminals, this scenario has a bit of historical backing to it, in regards to agencies and criminals working together for the greater good. Recalling American operations in Cuba during the Cold War, in 2007 former CIA Director Michael Hayden released documents proving rumors that the “CIA worked with three American mobsters in a botched gangster-type attempt to assassinate Cuban leader Fidel Castro in the early 1960s.”\(^\text{227}\) More recently it was revealed that the U.S. Government and the Latin American drug smuggling Sinaloa Cartel had a lengthy history of cooperation against other cartels.\(^\text{228}\) Despite these revelations, there has never been any official endorsing of this tactic against terrorist organizations.

On the subject of criminal groups, one of the other interesting recommendations for countering the crime-terror nexus is the “Al Capone Model,” or disruption strategy.\(^\text{229}\) As explained by Daveed Gartenstein-Ross and Kyle Dabruzzi, both terrorism scholars with

\(^{229}\) Gartenstein-Ross, Daveed and Dabruzzi, Kyle. “Crime and Terror: Law Enforcement Opportunities and Perils.” (June 2007,) Center for Policing Terrorism at the Manhattan Institute. (Pg. 8)
the Foundation for Defense of Democracies, this Al Capone model is a tactic that almost falls into the larger strategy of targeting the organized crime groups with counter terror resources. 230

The moniker has its roots in the takedown of mobster Al Capone in 1931. At the time, Capone’s offenses were widely known and included “murder, bribery, and running illegal breweries.” The government, however, was having difficulties proving these offenses legally, so instead brought down the notorious criminal with a charge of tax evasion.231

The idea was that even though the prosecutors could not go after Capone for his more heinous crimes, justice could still be served by disrupting his operation. The disruption tactic blossomed into charging known criminals with whatever could be proved against them; as a result, “prosecutors were aggressive, using obscure statutes to arrest and detain suspected mobsters” such as lying on a home loan application, or as in one case, of violating the Migratory Bird Act. Former Attorney General John Ashcroft has advocated for the disruption tactic to be applied to counter terrorist operations; that way even if there is no terrorism charge, terror plots are disrupted and possibly prevented.232 This has been used to a degree by the United Kingdom in its post 9/11 domestic counter terrorism strategies. For example, punitive measures can be brought against those suspected of terrorism, for “curfews, [or they may] have their internet and phone use curtailed and even be forcibly moved to another city.” 233

Conclusion:

230 Ibid (Pg. 4)
231 Ibid (Pg. 8)
232 Ibid (Pg. 8)
Through the collected scholarship on the crime-terror nexus, it is apparent that academia is largely in agreement as how to define and frame the phenomena, as well as on the problems that it presents to government agencies that are trying to combat its effects. Where researchers on the subject break into factions is on the best method for going about said combating. A solid middle ground also has developed, where many of the experts appear to favor an all-encompassing strategy drawing on the best parts of the main camps.

There are several shortcomings that were encountered when conducting the research into the established scholarship. The primary issue is the lack of substantial case studies in favor of one approach versus another regarding the success or failure of the argued strategy. Further, when a particular strategy was argued with data, the case studies were almost exclusively related to narco-terrorism, a subset of the crime-terror nexus in which a terrorist group engages in narcotics trafficking either alone or in conjunction with drug dealing organizations.234

The most suitable explanation for this lack of conclusive case study data is that the crime-terror nexus has presented an ongoing challenge for government response, which means that there has likely been little opportunity for either strategy to be tested to the point of an arguable definitive success or failure. It is for this reason that just as RAND Corporation’s Dr. Brian A. Jackson looked to the response to Irish Republican groups for historical data in regards to counter-insurgency strategy, this paper looks to the Irish for answers on the crime-terror nexus. 235

---

235 Jackson, Brian A (Pg. 75)
III. Theory and Hypothesis:

As the Literature Review suggests, there are several strategies currently in debate as to how government agencies can best counter the crime-terror nexus, and that despite the range of scholarship, little data has been developed to support any one claim over the other, and there is a need of more conclusive data. The majority of the reputable scholarship on the crime-terror nexus has been developed in the years following the 1998 Good Friday Agreement and the decline of Irish Republican attacks, making the Irish crime-terror nexus an excellent area to find historical data that may add support to the strategies offered by academia. Further, examining Irish Republican terrorism has the added benefit of the fitting into multiple ideological classifications. In David C. Rapoport’s seminal work, “The Four waves of Modern Terrorism,” Rapoport identifies four distinct terrorist ideologies that have surfaced throughout the 20th century and into the 21st, the anarchist, anti-colonial, New Left, and Religious Waves. Irish Republican extremism not only falls into the anti-colonial wave with their separatist agenda, but also New Left agenda as they held Marxist ends, and arguably a religious element as well, as much of the violence came down to Catholics versus Protestants. The fact that Irish extremism falls into multiple ideologies could make the results more widely applicable to other terrorist organizations.

Hypothesis:

This paper will seek to prove that counter-terror and other government agencies used a combination of two of the strategies outlined earlier in the Literature Review to successfully respond to the Irish crime terror nexus. The first strategy is the one recommended by Dr. Michael Freeman: that government agencies adjusted operational targeting to focus on the organized crime element within Irish terror groups.\textsuperscript{238} The second strategy is that agencies used the disruption, or the “Al Capone” model against the Irish Republican dissidents, recommended by Daveed Gartenstein-Ross and Kyle Dabruzzi.\textsuperscript{239}

**Methods:**

In order to prove this hypothesis, this paper will use a small-\textit{n} qualitative analysis, and comparative study. This method, as explained by Janet Buttolph Johnson and H.T. Reynolds in *Political Science Research Methods*, is the examination of several cases that involve a particular phenomenon and uses specific data sets to draw conclusions.\textsuperscript{240}

Through this method, the paper will investigate a set of historical case studies focusing on the different government agencies that were involved in combating Irish Republican terrorism, specifically researching their strategies, thus testing the hypothesis multiple times.\textsuperscript{241} As the Irish Republican groups did not have a particularly large global presence, the law enforcement agencies in this study are limited to:

- The British Army and MI5
- The Northern Ireland Police Force; The Royal Ulster Constabulary (RUC)

\textsuperscript{238} Freeman, Michael (P. 107).
\textsuperscript{239} Gartenstein-Ross, Daveed and Dabruzzi, Kyle. (Pg. 8)
\textsuperscript{241} Ibid (P. 196-198).
• The Republic of Ireland Police Force; The Garda Siochana (GS)
• The United States Federal Bureau of Investigation (FBI)
• The Columbian Administrative Department of Security (DAS)

It is expected that by examining the operations these organizations launched in regards to the Irish crime-terror nexus, and comparing the elements of success, enough historical data will be gathered to properly support the theories of Dr. Freeman, Gartenstein-Ross and Dabruzzi, as effective in countering the crime-terror nexus. The United States FBI and Columbian DAS were included as they were some of the few known areas of Irish dissident activity outside of the United Kingdom.

To complete the comparative study, this paper will use various types of historical sources both primary and secondary. This will include scholarly articles, news reports, and firsthand accounts that detail the structures and histories of the law enforcement agencies, as well as the relationships between Irish terror groups and organized crime.

Evidence that supports the hypothesis would be a mention of specific strategies or elements in those strategies that led to an arrest of Irish Republican terrorists or disruption of an operation. Evidence that goes against the argued thesis would be the detailing of a strategy that did not incorporate any of the elements in the theories presented by Dr. Freeman, or Gartenstein-Ross and Dabruzzi, or a strategy mentioned but failing to produce positive results.

V. Data:

Background on the Irish Crime-Terror Nexus:

In advance of the case studies, it is necessary to elaborate on the crime-terror nexus that existed for the agencies to combat.
Among the PIRA, there was a very organized command structure in place, with the Army Council or General Headquarters (GHQ) on top, and various departments commanding groups of Active Service Units, similar to cells (refer to Appendices Figure 2, for a full command breakdown). Though there was overlap in various departments such as the Quartermaster being responsible for procuring arms, or the Foreign Operations dealing with other groups, terrorist or otherwise, the largest element of the PIRA crime-terror nexus came from the Finance Department, which raised funds “through illicit means such as bank robberies, smuggling, as well as protection and extortion.”

Unlike many other terrorist organizations that participate in the crime-terror nexus, the PIRA largely avoided narcotics trafficking, and in general the Irish Republican movement was against drugs. This opposition to drugs was so strong that one of the Irish Republican extremist groups made it a main focus, taking on the name Republican Action Against Drugs (RAAD), along the lines of a vigilante group that has attacked and sometimes killed drug dealers in Ireland, particularly in the city of Derry. As of 2012, RAAD has joined forces with one of the remnant Irish terror groups, the Real Irish Republican Army (RIRA), which has sought to keep the mission of Irish Republicanism alive since the end of The Troubles. Together, the two groups took on the title of the New Irish Republican Army (NIRA), though even combined their activity level is minimal.

Some smaller IRA offshoots and other post-peace groups have had no qualms regarding drug trafficking and have dived completely into the crime-terror nexus; these

---

242 Clarke, Ryan & Lee, Stuart. (Pg. 382, 385)
include RIRA, the Continuity Irish Republican Army (CIRA), and especially the Irish National Liberation Army (INLA). The INLA, which started in the mid 1970’s, is a Marxist Irish Republican group whose members proclaimed themselves “the military wing of the Irish Republican Socialist Party,” and was known during The Troubles for the brutality of its attacks. Since the end of The Troubles in 2006, this changed and now “the INLA is known as much or more for its participation in the drug trade and other criminal activities as it is for outright terrorism.” As can be seen in Appendices Table 14, though these groups still commit the occasional attack, which has pushed the British government to raise alert levels, they are a shadow of what they once were.

**The British: Military Units and MI5**

At the outset of The Troubles, the bulk of the Irish conflict was largely situated in Northern Ireland after the civil rights clashes. Thus dealing with dissident Irish Republicanism was meant to be the primary responsibility of the Northern Ireland police force and the Royal Ulster Constabulary (RUC) whose strategies will be detailed in Case Study. However, given its resources at the end of the 1960’s, the RUC “felt it could not control the riots, and formally requested Army assistance,” leading to the deployment in 1969.

While MI5, the British domestic intelligence agency was more familiar with the growing problem in Northern Ireland, even having “warned the British government about the sources of and prospects for violence at least eight months before,” the army was less

prepared. Initially, army units were meant to reinforce order and “supplement the police,” conduct patrols and prevent open violence. This was successful for a while which meant, “the Army was seen as neutral,” when compared to the largely Protestant RUC. When the PIRA began its more violent campaign in 1970, the army was instructed to conduct counter-insurgency (COIN) methods against them. While the strategies incorporated with COIN are widely debated, “the process of criminalization of IRA terrorist violence” provided opportunities for some success.

The army’s early operations consisted of traditional COIN tactics, including disruptive measures like curfews, large-scale house searches, random vehicle checkpoints, and finally “internment without trial” in 1971, for suspected Republican dissidents.

It was around 1976 that the army began to base its tactics on the “criminalization of the PIRA rather than a counterinsurgency approach.” This was primarily by working as an arm of the British intelligence service MI5, rather than as a traditional military operation. Focusing more on “covert action and intelligence gathering,” the British made long distance surveillance a primary method for uncovering arms smuggling routes between suppliers and weapon caches. The increase in arrests allowed for more PIRA members to be captured and turned into informants, though for a while the Special Air Service (SAS) did gain a reputation for not leaving any PIRA members alive to turn.

---

248 Wood, John.
249 Ibid.
250 Ibid
It was through the use of informants and agent infiltrators that the army and MI5 made the most substantive dent in Irish Republican activities. The informers were actual members of a particular organization who had either become disenfranchised with violence or had been arrested and sought to avoid a larger prison sentence. The agent infiltrator role is more voluntary, and almost acts as a spy, usually either an intelligence officer or local civilian trying to get into the organization in question. Through these means, the army and MI5 were able to gain information on areas such as existing PIRA networks of contacts with criminal arms smuggling.\textsuperscript{251}

**Northern Ireland and The Royal Ulster Constabulary**

As previously stated, at the start of the Troubles, the RUC was not prepared to take on a large scale operation such as combating the PIRA, and quickly requested military aid. The RUC had been founded in 1922, out of fear of violence from the Catholic population in Northern Ireland. Thus it was seen “by many Catholics as the armed wing” of the Protestant majority, a viewpoint furthered by its only 8% Catholic membership.\textsuperscript{252}

The RUC’s first actions consisted mainly of coordinated anti-IRA activates with government sponsored Protestant militias such as the Ulster Special Constabulary and the Ulster Defense Regiment (not to be confused with Irish Protestant paramilitaries such as the Ulster Volunteer Force or Ulster Defense Association). These activities produced minimal results, and once the military and MI5 assumed more active roles, were abandoned.\textsuperscript{253}

\textsuperscript{251} Charters, David A. (Pg. 217, 224)
\textsuperscript{252} Kearney, Vincent. “Security Forces in The Troubles,” British Broadcasting Corporation. (February 2013) <http://www.bbc.co.uk/history/topics/troubles_security_forces>
\textsuperscript{253} Ibid.
The main unit in charge of countering Irish Republican groups was RUC’s Special Branch intelligence unit, which after learning from MI5 quickly became “the lead agency with regard to intelligence-gathering in the counter terrorist apparatus in Northern Ireland.” Due to its large network of informants, at first it produced mass convictions. However, once the British justice system stopped accepting informant testimony as admissible evidence, “the RUC turned more towards using informants for disruption not prosecution,” and is credited with “partial neutralization and undermining” of terrorist activity in Northern Ireland.

The Republic of Ireland Police Force and the Garda Siochana

In the Republic of Ireland, the equivalent to the RUC were the Garda Siochana (GS/ Gardai), Gaelic for the Guardians of Peace. While the bulk of the damage from the Troubles was seen in Northern Ireland, “in the Republic, 113 deaths and 2,500 injuries were directly attributed to the conflict,” leaving plenty for the Gardai to do regarding counter terrorism, mostly through its own version of the Special Branch Intelligence Unit, the Special Detective Unit (SDU.)

At the start of The Troubles, the Gardaí were even less equipped than the RUC, due to the fact that before The Troubles, the Republic was largely crime free, and saw little reason to have much international work with the RUC, which was generally considered the more elite of the two police forces. Further, once The Troubles were in full swing, the Gardai “did not have the might of the British Army to fall back upon.”

254 Moran, Jon. “Evaluating Special Branch and the Use of Informant Intelligence in Northern Ireland.” Routledge (February 2010) Intelligence and National Security, Vol.25, N0. 1, (Pg. 3)
255 Ibid. (Pg. 7)
257 Ibid. (Pg. 6,8, 26)
258 Ibid. (Pg. 28)
The impact of The Troubles in the Republic came first in the form of robberies in small towns, where there was a minimal amount of unarmed police, making such towns easy marks for PIRA members to target. In response, the new Gardai were recruited “in increasing numbers to the Border divisions,” along with resources to provide all stations with “radio and teleprinter communications,” though there was still no standard operating procedure for the largely baton-equipped Gardai who continued to be subdued by armed PIRA men.

What finally made the difference was restoring full diplomatic relations with the British, which had been suspended after the events of Bloody Sunday, the name given to a 1972 mass shooting of unarmed civilians by British soldiers at a civil rights protest in Derry, Northern Ireland. British intelligence agents were already gaining information on dissident Republican activity in the South through agents and informants, and once relations were restored, “British spymasters” were able to get more involved in the Republic. Soon enough, the Gardai had its own system of informants in place. Despite occasional attempts at bureaucratic interference, the Gardai system was a heavily valued tool against dissident Republican activity within the Republic of Ireland.

The United States and Federal Bureau of Investigation

Though the Irish terrorist attacks were almost entirely local in Ireland and England, a large amount of crime-terror nexus activity came from PIRA members

---

259 Ibid. (Pg. 29-30)
260 Ibid. (Pg. 41, 44)
262 Ibid. (Pg. 52)
263 Ibid. (Pg. 106)
working in the United States for funds but more so for guns. Procuring arms locally was
difficult to the point that “the only reliable source for guns was the…United States.”

When The Troubles first began, American law enforcement largely dismissed
Irish Republicanism as something outside of its concerns. “It was not until the late 1970’s
and early 1980’s that pressure from Margaret Thatcher on the Reagan White House
persuaded the FBI to turn its attentions to the IRA.”

“The IRA had come to Boston in the 1960’s to explore the possibility of robbing
banks and armored cars to support their [sic] cause.” However, there was a large Irish
diaspora community that was angered over stories of Catholics being persecuted.
Thanks to this diaspora community, donations to Northern Aid Organization (NORAID)
were always plentiful. The Boston Irish mob, with prominent gangsters such as Patrick
Nee and the notorious James “Whitey” Bulger began its IRA donations by shaking down
bookies and running protection, all the while sending a share of the profits to NORAID,
or sometimes directly to IRA men in the United States, at the same time that Bulger was
informing to the FBI about other organized crime groups.

Nee and Bulger eventually became gun runners for the PIRA, sending weapons
from Boston to the PIRA in coffins, transported in a van inside a shipping container, and
in 1984, tried to send “the largest shipment of guns ever smuggled to Ireland” (7.5 tons)
aboard the fishing vessel The Valhalla. That shipment contained “163 assault rifles,
71,000 rounds of ammunition, one ton of military explosives, a dozen bulletproof vests,

---

265 Ibid. (Pg. 16)
266 Nee, Patrick (Pg. 4)
267 Ibid. (Pg 135)
268 Ibid. (Pg. 142)
269 Ibid. (Pg. 142-146)
rocket ammunition pouches, 13 military-surplus weapons, weapons manuals, and military operation manuals.\textsuperscript{270}

To attempt such a large arms shipment, Bulger reached out to the organized crime world, approaching major drug dealer Joe Murray who had built a reputation for smuggling drugs up and down the east coast in the late 1970s and early 1980’s.\textsuperscript{271}

Government authorities eventually caught up with Nee and Bulger’s operation. “A former IRA commander” Sean O’Callaghan who had turned informant for the Garda Siochana provided his Gardai handlers with all he knew about the \textit{Valhalla} shipment.\textsuperscript{272} Through O’Callaghan’s handlers, the information was passed through intelligence and made its way to the United States.\textsuperscript{273} Though Irish naval authorities stopped the shipment, the FBI was still searching for the crew that sailed it across the Atlantic. Fortunately one crewmember, John McIntyre, was arrested in “Quincy for driving under the influence,” and while being questioned turned over the entire smuggling operation. This minor DUI charge led to the multiple arrests, including the arrest of Patrick Nee, thus disrupting the Boston Mob-IRA connection.\textsuperscript{274}

Within a year of their release from prison, however, Nee and his organized crime associates instigated an armored car robbery in Abington, MA. All involved were Irish sympathizers who agreed to send 20% (approximately $400,000) of their expected “earnings” to help the PIRA.\textsuperscript{275} But once again, the FBI got wind of the planned robbery through the individual who had supplied Nee’s crew; a Dorchester man, Davie Ryan,

\begin{flushleft}
\textsuperscript{270} Ibid. (Pg. 3)  
\textsuperscript{271} Ibid. (Pg. 169, 170)  
\textsuperscript{272} Ibid (Pg. 199)  
\textsuperscript{274} Nee, Patrick (Pg. 204)  
\textsuperscript{275} Ibid. (Pg. 5) 
\end{flushleft}
who was an FBI informant. As a result, the day the heist was to take place, Nee and his crew were arrested and found to be in possession of multiple automatic weapons.\textsuperscript{276}

\textit{The Columbian Administrative Department of Security (DAS)}

The final case study on the strategies used to combat the Irish crime-terror nexus activity is based in Columbia, where PIRA members collaborated with the FARC (Revolutionary Armed Forces of Columbia), a Marxist rebel group that also engages in the crime-terror nexus particularly in narco-terrorist activities.\textsuperscript{277} Despite the PIRA’s noted abhorrence for the drug trade, there is an abundance of accounts regarding an ongoing relationship between the PIRA and the FARC, in which the PIRA trained FARC members in “explosives and firearms” in exchange for cash or drugs that would then be used as currency, as they were reported to have done when collaborating with Croatian arms traffickers where “payment for new weapons was made with FARC-supplied narcotics.”\textsuperscript{278}

Despite statements from those involved, much of the PIRA-FARC collaboration remains alleged. It is known that “the IRA had never been shy of fostering relations with fellow revolutionary groups around the world” and in 2001, this relationship suffered a hiccup by way of Columbian authorities, when three known Irish Republicans were apprehended at the Bogotá airport by a force of “150 Colombian policemen and soldiers” waiting for them.\textsuperscript{279}

The trio, later known as the “Columbia Three,” had been targeted by the Colombian Intelligence agency DAS, and was arrested for “traveling on false passports.”

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{276} Ibid. (Pg. 14)
\item \textsuperscript{277} Clarke, Ryan, & Lee, Stuart. (Pg. 378)
\item \textsuperscript{278} Ibid (Pg. 391)
\item \textsuperscript{279} Moloney, Ed.(Pg. 486-487)
\end{itemize}
\end{footnotesize}
after “the Colombian army had been tipped off by an international security organization.”\textsuperscript{280} After the initial arrest for the false passports, further charges were levied against the three, consisting of aiding FARC with weapons and training, and corroborating information by a “FARC deseter…[who] stated that Irish insurgents brought missiles and launchers” for use by the FARC. Unfortunately for the Columbian prosecution, it was unable to convict the men of the terror-related charges, and after crediting time served for the false passport conviction, the trio was allowed to leave Columbia.\textsuperscript{281}

**VI: Discussion:**

**Results:**

The findings of the data section prove that this paper’s hypothesis was largely wrong, as outlined in Table 13 below, which shows the strategy was used by each agency. In trying to prove that targeting of the organized crime elements was the most successful strategy in response to a crime terror nexus organization, the data revealed that only the FBI had engaged in this strategy. The hypothesis is still partially correct, as three of the agencies--MI5, the RUC, and DAS--utilized disruptive tactics, and all but the RUC engaged in international cooperation. Though as previously stated and demonstrated in the results, there is a fair amount of overlap from one strategy to the next.

**Table 13: Chapter 3 Results Illustrated**


<table>
<thead>
<tr>
<th></th>
<th>Targeting Organized Crime Element</th>
<th>Disruptive Tactics</th>
<th>International Cooperation</th>
<th>Infiltration: Undercover &amp; Informers</th>
</tr>
</thead>
<tbody>
<tr>
<td>MI5/Army</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>RUC</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Gardai</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>FBI</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>DAS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>?</td>
</tr>
</tbody>
</table>

The results also show how widespread the use of informants was during The Troubles. Four of the five case studies have confirmed evidence that an informant was a key element in combating Irish Republican terrorism. The fifth case study in Columbia is left open-ended, as the only available data says that the DAS was tipped off by an international security organization. How said organization learned about the PIRA trio traveling to Columbia is open to speculation. It is known that the use of informants was widespread during the entire period of The Troubles, to the point where one in four Irish Republican extremists was at some point involved in cooperating with one of the security agencies. All also incorporated the recruitment of informants into their counter-IRA strategies, a practice still widely used by police in Northern Ireland to gain information on Belfast’s criminal underworld. In fact, in 2014 police were paying informants as much as £1,000 per day, despite objections from former PIRA member and current Sinn Fein politician Gerry Kelly.  

---

Though terrorist groups have been seen to work with criminal groups in the past, this research is important, as terrorist groups are believed to be engaging in crime more so than previous years. While the established scholarship in the Literature review section points to a few strategies, it does not have much data for support. This paper sought to fill that gap; however the findings end up supporting a strategy that was not discussed by any of the theorists. The implications could strongly suggest that theorists should consider adding the use of informants to the recommended strategies on countering the crime terror nexus. That said, the use of informants does not contradict any of the established strategies, and could very well be implemented to complement any one of them.

**Flaws & Limitations:**

Some potential flaws of this paper are the chosen evidence that went into each case study. Given that the Troubles spanned a period of 30 years, and another 15 years of minor Republican dissident behavior, the strategies of the five case study agencies were limited to the most highly documented events. To have a more complete examination of the Irish crime-terror nexus, the hundreds of other government operations and potentially thousands of arrests made by these five agencies have to be examined for elements of crime-terror nexus strategy.

As well, the five case study agencies were chosen due to the existence of highly documented and highly available research; further investigation into smaller scale Irish Republican activities in Eastern Europe, North Africa, the Middle East, and other areas of South America and the respective government agencies would likewise add more to the body of research that could possibly add evidence to any of the noted strategies.

**VII: Conclusion:**
The question this paper sought to ask was how did counter terror strategies respond to the crime terror nexus that existed during The Troubles. The aim was that by examining the agencies that dealt with a past conflict, historical data could be used to support one of the scholarly theories on how to counter the crime terror nexus today. However, the data pointed to a strategy not considered by the scholarship, the use of informants, which was present in each case study, save for Columbia, where it can only be speculated.

While this paper’s hypothesis was only partially correct, the larger surprise from the data is how consistent the use of informants was across all the case studies. This is surprising due to the fact that none of the existing scholarship had recommended the use of informants as a path to countering the crime terror nexus. The possible inference of this is that perhaps strategists should explore a more extensive use of informants in combating the crime terror nexus.

Among scholarship on counter terrorism, the theory on the use of informants dictates, “the only weapon that can destroy a subversive organization in the end is information given to the government from within the terrorist ranks.” 283 Perhaps the use of infiltration would be the best strategy to counter the crime-terror nexus. In the case of The Troubles, “informers literally crippled the IRA. Their information has led to the arrest of hundreds of members of the organization…operations were prevented, activists arrested or killed, and arms seized.”284

283 Sarma, Kiran. “Informers and the Battle Against Republican Terrorism: A Review of 30 Years of Conflict. (May 2005,) Routledge, Police Practice and Research, Vol. 6, No. 2. (Pg. 166)
284 Ibid. (Pg. 177)
A potential flaw in this approach is that while The Troubles may have been declared over as a result of the political solutions enacted by the Good Friday Agreement, and the PIRA having long since disbanded, other groups have continued the fighting, such as the previously mentioned CIRA, INLA, and the NIRA (the combined RIRA and RAAD), all of which are active participants in the crime terror nexus. Further looking to Appendices Table 14, while there certainly has been a massive decline in Irish Republican linked attacks, such attacks still continue to plague Northern Ireland on a semi-frequent level to the point of having raised the terror threat level from moderate to severe in May of 2016 as the groups attempt to stay relevant, though still are nowhere near approaching their former levels of activity.  

Given the continued nature of the conflict, it could be inferred that while the strategies used played a part in attacking the crime terror nexus, they were unsuccessful in defeating the nexus to the level achieved by political solutions.

---

Conclusion

This thesis was attempting to look into the activity of terrorist groups outside of actual terrorist attacks. This type of study is important, as too often researchers, policy makers, and security practitioners get hung up on the violent aspects of a terrorist group’s lifespan.

As new policies are made and terrorist groups learn and adapt, having a full understanding of a terrorist group’s activity will become increasingly necessary.

Hoping to fill that knowledge gap, the three chapters of this thesis all examined various aspects of terrorist acts that are not considered attacks. While terrorism is illegal, these actions more closely resemble the world of transnational organized crime, with terrorist groups engaging in drug smuggling, arms dealing, money laundering, the use of malware, and shutting down websites.

In the first chapter, terrorist maritime activity was explored. This ranged from engagement in the maritime piracy actions of kidnapping and hijacking, or the smuggling and trafficking of narcotics, arms, and people, all of which make up the bulk of maritime crime, and could generate funds to further terrorist groups’ goals. Operating under the hypothesis that terrorist groups would be directly engaged in these activities, the five terrorist groups with the most attacks were all examined, and for the most part found only limited engagement and removed connections.
This conclusion could mean that a lot of the theory around the Crime-Terror Nexus and Maritime Terrorism is more hype than reality. Though given the limitations of researching through open source material, and the fact that maritime crime is estimated to be much larger than can be proven, it is entirely possible that a Maritime-Crime Terror Nexus does exist, but leaves no trace for investigators, and a geographic based study could yield more results for the maritime domain. Further, if the domain was changed from maritime to land or air, the results would change, in addition to the fact that these results are limited to the five groups examined.

The second chapter continued the examination of the theories around the Crime-Terror Nexus, but under the ark of Cyber-Terror and Cyber-Crime, both loosely defined concepts that have stirred great debate among scholars, politicians, and security operators. Instead of looking only at direct engagement in types of Cyber-Crime, this chapter chose to look at the possible differences in cyber engagement, based on ideological orientation, whether it is anarchist, separatist, religious, and politically left or right wing, all of which have affected groups decisions in other activities.

As the hypothesis predicted though, the results showed fairly limited deviation between the different ideologies, all of which use the internet for communication purposes, and only Hamas and the Islamic State having known engagements in types of hacking or online financial crimes. While the research showed some ideological reasons for increased or decreased engagement, such as one of the anarchist groups being anti-technology, as long as attribution of cyber acts remain difficult to know, substantial conclusions will mostly allude researchers. Further questions remain on the Cyber-Terror
Nexus, such as financial capability, access to technology, and even rural versus urban bases.

As the first two chapters showed, the Crime-Terror nexus remains elusive for researchers to pin down whether in the Maritime or Cyber Domain; this comes down to the problem of being unable to know for sure how much crime is really committed, as well as attribution. However expansive or limited criminal acts by terrorist groups may appear, it is known that this phenomenon does exist and has been present for some time. Many scholars and policy makers have put forth ideas and strategies on how to combat these types of groups, but they have little to no quantitative data to support their theories. The third chapter tries to add to the work of these scholars, and takes the historical example of Irish Republican Extremists, who were well known for their criminal enterprises, and examines if law enforcement and counter-terror organizations had more successes with a particular strategy.

Looking into the responses to Irish Republican extremism by the British Army, the Northern Ireland Police Force; the Republic of Ireland Police Force; the United States Federal Bureau of Investigation, and the Columbian Administrative Department of Security, this chapter concluded that while all the strategies contained a degree of overlap, the use of international cooperation and undercover informants were the most successful. This conclusion adds valuable research to the literature, and also can inspire new research into questions about current use of undercovers and informants in modern terrorist groups, and issues in international cooperation.

At the outset of this thesis, the goal was to study the activity of terrorist groups other than the actual terrorist attack. This type of research is important not only for filling in
gaps in scholarly research, but can also aid policy makers and practitioners hoping to combat terrorist groups. Though the limitations of open source research into terrorism and crime may make it difficult to prove, the continued engagement of terrorist groups into organized crime is likely the next stage of terrorism adaptation, and could become the biggest threat to transnational security.

Appendices

Table 7. American Opinion of Threat:

<table>
<thead>
<tr>
<th>Percent saying each is a major threat to the U.S.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Islamic extremist groups like al Qaeda</td>
</tr>
<tr>
<td>Cyber-attacks from other countries</td>
</tr>
<tr>
<td>Iran’s nuclear program</td>
</tr>
<tr>
<td>N. Korea’s nuclear program</td>
</tr>
<tr>
<td>China’s emergence as a world power</td>
</tr>
<tr>
<td>Global climate change</td>
</tr>
<tr>
<td>Economic problems in the EU</td>
</tr>
<tr>
<td>Growing authoritarianism in Russia</td>
</tr>
</tbody>
</table>

Table 9: U.S. Cyber Crime Reports 2000-2010
Table 12: Terrorism in Europe

Figure 2. PIRA Organizational Structure
Table 14: Irish Republican Linked Attacks:

<table>
<thead>
<tr>
<th>GHQ</th>
<th>Quarter Master</th>
<th>Security</th>
<th>Domestic Operations</th>
<th>Foreign Operations</th>
<th>Finance</th>
<th>Training</th>
<th>Intelligence</th>
<th>Publicity</th>
<th>Education</th>
<th>Engineering</th>
</tr>
</thead>
</table>
"ABU SAYYAF GROUP (ASG)." National Counter Terrorism Center, United States of America. <https://www.nctc.gov/site/groups/abu_sayyaf.html>


<http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf>

<https://www.files.ethz.ch/isn/110282/MaritimeTerrorism.pdf>


Gartenstein-Ross, Daveed and Dabruzzi, Kyle. “Crime and Terror: Law Enforcement Opportunities and Perils.” Center for Policing Terrorism at the Manhattan Institute. (June 2007)


National Consortium for the Study of Terrorism and Responses to Terrorism. *Global Terrorism Database*, University of Maryland. <https://www.start.umd.edu/gtd/search/Results.aspx?search=irish+republican&sa.x=63&sa.y=17>


START. “Global Terrorism Database.” University of Maryland. <http://www.start.umd.edu/gtd/search/Results.aspx?search=cyber&sa.x=0&sa.y=0>


**Curriculum Vitae**

Justin H. Leopold-Cohen was raised in Manhattan, New York. He attended Clark University completing a Bachelor of Arts in American History. After graduation, he enlisted as a foreign volunteer in the Israeli Defense Forces Infantry Division, where he
served as a sergeant in the 932nd Battalion of the Nahal Brigade. Upon being honorably discharged, he moved to Washington D.C. and enrolled in the Global Security Studies program at Johns Hopkins University. He has written on international security for *Foreign Policy News, The Diplomatic Courier, and International Affairs Forum*. He lives in Washington D.C., and works at the Department of Homeland Security, in the Office of Infrastructure Protection.