ELECTRONIC SURVEILLANCE AS A COUNTERTERRORISM TOOL: IS TECHNOLOGY A VIABLE STRATEGY?

A dissertation presented

By

Andrew Macpherson

to
The Department of Political Science

In partial fulfillment of the requirements for the degree of
Doctor of Philosophy

In the field of

Political Science

Northeastern University
Boston, Massachusetts
April 2018
ELECTRONIC SURVEILLANCE AS A COUNTERTERRORISM TOOL: IS TECHNOLOGY A VIABLE STRATEGY?

A dissertation presented

By

Andrew Macpherson

ABSTRACT OF DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Political Science in the College of Social Sciences and Humanities of Northeastern University
April 2018
Abstract

Electronic surveillance is one of the policy options governments may employ when combating terrorist groups. Public discourse often involves concerns that such programs may substantially reduce citizens’ privacy while providing marginal, if any, gains against terrorists. This study provides much-needed empirical data on the impact of electronic surveillance on terrorism.

The evidence I generate—examining data from 1970 through 2016, using a multivariate negative binomial panel regression model for longitudinal data—supports a hypothesis that the presence of electronic surveillance laws and the related government surveillance capacity decreases both the incidence of terrorist attacks and the number of individuals killed in terrorist attacks. These findings complement, and may be integrated into, broader scholarly work that finds that when constraints on government institutions are relaxed, they are more effective at counterterrorism. These data provide grounds for additional study in this domain. Qualitative, comparative case studies, for example, that examine the relationship among electronic surveillance and other counterterrorism strategies in which the nation-state is the unit of analysis, could reveal an optimal mix of strategies to limit terrorist activity. This study may help inform the debate over the scope of electronic surveillance and personal privacy in nation states.
Acknowledgements

There are many people to whom I owe a debt of gratitude for the guidance, support and love they have provided over the past four years. To my committee, I truly appreciate your patience and support. To the Chair, Professor Stephen Flynn, I thank you for your deep insights on resilience and helping me become a more rounded scholar. Professor Max Abrahms, thank you for your time and support as I broadened my understanding of terrorism. To Professor W.D. Kay, who introduced me to many theories in the philosophy of science—thank you.

I am fortunate to have interacted with the many excellent faculty at Northeastern, including, but not limited to, Professor John Portz, Program Director, MA and PhD Programs, and Professors Aldrich, Beauchamp, Cross, Hedland, and Mayer. Thank you all for your support of my coursework, research, and other academic pursuits.

Most importantly, I would like to thank my family. To my wife Beth and kids Emily, Macgregor, and Sterling: thank you for your ongoing support and encouragement. My mom Jean and dad Michael: thank you for encouraging me to reach my potential. As Dick Proenneke said: “Hard work but I enjoyed it.”
Table of Contents

Abstract ................................................................................................................................. 2
Acknowledgements .................................................................................................................. 4
Table of Contents .................................................................................................................. 5
Chapter 1: Introduction ......................................................................................................... 6
  Statement of the Problem .................................................................................................... 7
  Study Goals ....................................................................................................................... 10
  Theoretical Framework ..................................................................................................... 11
Chapter 2: Literature Review ............................................................................................... 16
  Terrorism as a Phenomenon ............................................................................................... 16
  Terrorism and Regime Type .............................................................................................. 18
  Counterterrorism Policy .................................................................................................. 22
  Electronic Surveillance for Counterterrorism ................................................................. 24
Chapter 3: Methodology ....................................................................................................... 29
  Conceptual Relationship between Terrorism and Counterterrorism ......................... 29
  Research Design ............................................................................................................... 32
  Reliability, Validity, and Limitations ............................................................................... 46
Chapter 4: Analysis ............................................................................................................... 51
  Descriptive Statistics ........................................................................................................ 51
  Inferential Statistics .......................................................................................................... 55
Chapter 5: Surveillance Laws for Counterterrorism in Pakistan, the United Kingdom, and the United States ................................................................. 64
  Attacks Per Capita as a Measure ....................................................................................... 64
  Pakistan ............................................................................................................................. 66
  United Kingdom ............................................................................................................... 69
  United States .................................................................................................................... 73
Chapter 6: Policy Implications ............................................................................................. 79
References ............................................................................................................................ 84
Appendix 1: Countries Included in the Study ...................................................................... 94
Chapter 1: Introduction

The September 11, 2001 terrorist attacks on the United States precipitated substantial changes in the American government’s response to terrorism. President Bush (2001) addressed a joint session of Congress to declare that on “September the 11th, enemies of freedom committed an act of war against our country… Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated.” Since 2001, the United States has spent more on counterterrorism than any other nation in history. Mueller and Stewart (2014) estimate United States government spending on dedicated counterterrorism program, excluding defense, at $90 billion dollars a year. Few governments could sustain this level of spending over time. An analysis of the CIA’s World Factbook (Central Intelligence Agency n.d.) reveals that approximately 86% of the nation-states in the world have annual budgets of less than $90 billion dollars. The Congressional Budget Office (2015) estimated that at least $1.5 trillion dollars (approximately $5 billion per month) were spent on the wars in Afghanistan and Iraq alone from 2001 to 2015. Has the money been well spent?

What are the most effective counterterrorism strategies for nation-states to employ? It appears there is a lacuna in counterterrorism research when it comes to evaluating the effectiveness of one counterterrorism strategy over another. Both the deadly nature of the threat of terrorism and the vast resources spent on counterterrorism strategy warrant empirical study.

What approaches do nation-states employ to combat terrorism? Sandler (2015) writes that counterterrorism strategies may be generally categorized as either defensive or proactive. Defensive strategies are aimed at reducing the likelihood that terrorist attacks will succeed. After
terrorists used aircraft to attack the United States on September 11, 2011, for example, the government developed improved airport-security measures to try to prevent similar attacks. As Straw (2013) notes, the weapons used by the terrorists, small-box cutting knives, were prohibited under the new airport-security measures.

Proactive counterterrorism activities often aim to preempt or destroy terrorist capability Sandler (2015). Proactive strategies include denying terrorist groups safe havens, eliminating their funding sources, and apprehending or eliminating their operatives. The United States pioneered the use of weaponized Unmanned Arial Vehicles (UAVs)—drones—to monitor and kill terrorists. One example is the targeted killing of Anwar al-Awlaki in 2011. Miller (2014) notes that Mr. al-Awlaki was killed by a United States UAV strike after extensive surveillance in Yemen. Recent media articles report that Central Intelligence Agency teams continue to hunt high-value terrorists (Roston 2018). Governments’ developing policy to counter terrorist groups often use a mix of defensive and offensive strategies.

Statement of the Problem

If nation-states use a mix of defensive and proactive strategies to combat the threat posed by terrorist groups, it is important for policy makers to ask what is the optimal mix of defensive and proactive counterterrorism strategies? Are some approaches more effective than others?

Terrorist attacks may be conceived as a notion timeline (MITRE Corporation 2009). As seen in Figure 1, a hypothetical biological weapon attack by a terrorist group may follow a linear process in which terrorists (1) decide to use a biological weapon, (2) acquire the material and expertise, (3) prepare and test the agent, (4) plan the attack, and (5) conduct the attack. The potential target of the attack may develop defensive and proactive measures to counter it.
Considering a spectrum of counterterrorism strategies, nation-states may attempt to limit terrorist activity by addressing the root conditions that lead an individual to terrorism. If these strategies are successful, individuals will not choose to form or join terrorist groups or use violence to achieve their ends. A Congressional Research Service comparison of the United States’ 2003 and 2006 National Strategies to Combat Terrorism noted that the “2006 Strategy differs from the 2003 version primarily in that it sets different priorities for the strategic elements designed to achieve its goals…the most significant of these differences was a major increase in emphasis on democratization as a method of combating terrorism” (Pearl 2007, 2). Following the Bush era, President Obama’s administration continued to promote democracy as a counterterrorism strategy. Obama’s 2011 National Strategy for Counterterrorism states that “a positive U.S. agenda that supports the rights of free speech, assembly, and democracy with the death and destruction offered by our terrorist adversaries helps undermine and undercut their appeal, isolating them from the very population they rely on for support” (United States Government 2011, 5).

Another strategy nation-states use to combat terrorism is the use of intelligence. The academic field of intelligence studies has proposed many definitions of national security intelligence. A 2013 survey of academics and practitioners published in the journal Intelligence...
and National Security notes that defining intelligence is itself one of the principal scholarly debates that is advancing knowledge in the domain (Johnson and Shelton 2013). The 2006 RAND practitioner/academic workshop titled “Toward a Theory of Intelligence” found no consensus on a definition (Treverton et al. 2006). Practitioner discourse in the Central Intelligence Agency’s classified scholarly journal, *Studies in Intelligence*, reveals debate on the definition of intelligence as early as 1958 (Random, 1958). Wark (1993) categorized the debate as the definitional project in the history of the study of intelligence.

For the purpose of this study, I use a modified version of the definition of intelligence offered by Michael Warner. Warner is a practitioner in the Office of the Director of National Intelligence (ODNI). In a paper entitled “Wanted: A Definition of ‘Intelligence,’” he reviews government, private, and academic definitions of intelligence and identifies its essential elements as activity conducted on behalf of nation-states that is secret and focused on foreign entities (Warner 2008). His work, built on the work of Random (1958), is helpful in that a definition of intelligence should address the authority that sanctions the activity and identify its target. I argue that Warner’s definition does not fit the phenomena of intelligence as practiced in many nation-states. Chinese and Russian intelligence activities, for example, are focused on domestic or internal as well as foreign or external threats. In the United States, legal restrictions limit many intelligence activities to foreign threats. We may thus define adapt and modify Warner’s definition. I define national security intelligence as secret activity undertaken by nation-states to understand or influence adversarial entities.

Schmitt and Shulsky (2002) define intelligence collection as a critical activity that countries use to attempt to detect and disrupt threat activity. Intelligence collection, they write, consists of gathering “raw data” in three ways: “espionage; technical means (photography,
interception of communications, and other methods involving technology),” along with the “exploitation of ‘open sources’ (for instance publications, and radio and television broadcasts),” or, they add, “in any other manner” (Schmitt and Shulsky 2002, 37).

My goal for this study is to conduct a scholarly inquiry into the phenomena of electronic surveillance as a counterterrorism tool. National security electronic surveillance is defined by the United State government as “the acquisition by an electronic, mechanical, or other surveillance device of the contents of any electronic communication without the consent of any party thereto” (Department of Justice Criminal Resource Manual n.d.). As technology has advanced, the scope of electronic communications has broadened significantly from wire taps to much broader data collection. The 2013 illegal disclosures of Edward Snowden revealed that the Unites States and allied nation-states were collecting unprecedented amounts of data on their own citizens (BBC 2015). That event precipitated national debates on mass surveillance in many countries. Government officials and citizens alike debated the appropriate amount of electronic surveillance their countries should maintain.

**Study Goals**

Critical linkages between terrorist attacks and surveillance are not understood. Do the adoption of electronic surveillance laws—and the resulting capability to capture and analyze individuals’ communications—result in fewer terrorist attacks? Since it is a secret activity, few public studies exist to help guide policy makers and inform citizens. This study aims to narrowly answer these questions and thus fill the research gap in this domain.
Theoretical Framework

The study is grounded by two theoretical frameworks concerning government policy. Policy studies are defined as the study of the actors, structures, events, and institutions involved in government policy making. Policy may be defined as the decisions that governments make. What are the roles and functions of individuals, groups, and institutions in creating policy? No one grand theory has emerged to definitively settle the question. Instead, a number of lenses, in the form of frameworks and theories, may be used to describe and explain agency and institutions in the policy process. Agency may be defined as capacity of individuals to act independently and to make their own free choices. Institutions may be defined as rules, norms, values and organizations. Agency and institutions play critical or lesser roles, depending on the lens used to analyze a policy process.

What is the policy process? A rationalist may conceive of the process as a series of steps, in which (1) a problem is identified, (2) policy alternatives are identified, (3) the consequences of the policy are identified and analyzed, (4) a decision is made on a policy to implement, and (5) the policy is implemented. These steps fit into the broader model of politics proposed by Easton. In Easton’s (1965) model politics is a system in which inputs and support try to get onto the political agenda.

The political agenda is described as what is important for politicians and citizens to pay attention to politically. Another definition for the political agenda is politics’ priority list (Walgrave and Aelst 2016). Other scholars argue that there are many different political agendas.
(Pritchard and Berkowitz 1993). People and groups attempt to bring issues to the forefront so that they can be addressed via policy.

If policies succeed, they may emerge as outputs in the form of law, programs, and institutions. These outputs generate feedback that may, in turn, stimulate inputs. The orderly nature of the process, presented here, may feel artificial, and policy scholars such as Baumgartner and Jones (2005) have proposed alternative models, in which a political system is viewed as an information processing instrument.

Posing the question, “How do governments respond with policy to incoming information?,” Baumgartner and Jones (2005) argue that individual and institutional decision making that starts with recognizing that there is a problem, assesses the dimensions of the problem, sorts through potential solutions, and then makes the final policy choice. The concept of policy making as an information processing instrument builds on their theory of punctuated equilibrium. Punctuated Equilibrium Theory (PET) focuses the lens of policy development and change on institutions and on the policy monopolies they seek to build and maintain. The authors argue that, once a policy is created, institutions are built to support that policy. In the subdomains of policies, the development of institutions is focused on monopolization. Individuals and groups involved with a policy attempt to build institutions that are difficult to dismantle. The authors provide examples of institutions that have lasted for decades such as the nuclear power policy monopoly in the United States. The development of resilient intuitions as policy monopolies means that changes in the system are usually incremental. Larger changes happen infrequently with an event or other trigger causing “punctuation” in the status quo. PET thus situates institutions as a key focus of the policy process because they are resistant to change.
If institutions are resistant to change, what can trigger a shift in system equilibrium? In the rational model, individuals play a key role in developing policy. An important theory that centers on the role of the individual in policy making is Kingdon’s Multiple Policy Streams (2010). This theory identifies three activities (streams) as essential to policy making: problems, policy, and politics. Each stream is distinct, and each is a continuum. The problem stream contains the issues that can be placed on the political agenda. Problems rise to the top of the problem stream due to such reasons as individual and group advocacy, political leaders’ policy objectives, events in the real world, and media attention. The policy stream contains a primordial soup of ideas on how to solve problems. The individuals and groups working on possible problem solutions include interest groups, academics, and politicians. The political stream is the decision agenda. The essential actor here, identified by Kingdon, is called the policy entrepreneur. This individual is motivated by self-interest to try to bring the streams together in what Kingdon calls policy windows. Policy windows open and close at irregular intervals, which means that policy entrepreneurs must be ready to push their policy when the conditions arise. In Kingdon’s theory, the individual policy entrepreneur is a critical player in the policy process.

What opens the windows for Kingdon’s policy entrepreneurs? In many societies, the media plays an important role in reporting on events and on the reactions of individuals and groups. Many scholars are interested in the media and the role it plays in agenda setting. Eshbaugh-Soha and Peake (2005); Roggeband and Vliegenthart (2007); Tresch, Sciarini, and Varone (2013) all find a moderate link between the media and agenda setting in the United States, Netherlands, and Switzerland, respectively.

Scholars investigating the relationships between terrorism and the press find that media coverage can increase public fear. Jenkins (1974, 5) calls terrorism “choreographed violence” as
groups plan to maximize media attention of their attacks in order to put political pressure on governments. In his book *Inside Terrorism*, Hoffman (2017) describes the calculated use of the media by terrorist groups in two phases. In the first phase, traditional media (newspapers and television) was exploited by terrorist groups. Initially, the media reported events after the fact. As technological advances subsequently allowed for “real time” broadcasts, terrorists learned to exploit the media’s desire to report dramatic events. The 2008 Mumbai terrorist attacks illustrate this. Lashkar-e-Taiba launched attacks on the Taj Palace and Tower Hotel, the Nariman House Jewish community center, the Chhatrapati Shivaji Terminus railway station, and other locations across the city (PBS 2009). The attackers kept in contact with their handlers in Pakistan by cellphone. The handlers monitored the international media coverage, encouraging the attackers to take actions that would create maximum impact (Elkus 2015). Hoffman (2017, 198) argues that, in the second phase, terrorists have gone beyond “violence as communication.” Terrorist groups employ internet-enabled technologies such as YouTube, Twitter, and Facebook to publish their own versions of reality that may contradict the coverage they receive in the mainstream media.

If the Punctuated Equilibrium and Multiple Policy Stream theories have explanatory power, then terrorist events may trigger a convergence of the policy streams *problems, policy,* and *politics* and lead to policy and, potentially, counterterrorism changes at the institutional level. Terrorist attacks force terrorism onto the political agenda, where policy is often debated and adopted. The goal of policy is often to strengthen the tools the government has to stop terrorist attacks. Government counterterrorism policies often include increased government powers to conduct surveillance electronically. By implementing electronic surveillance law governments relax constrains on their security forces to collect information on terrorist suspects.
The security agencies must develop the capability to intercept and analyze communications and data to be effective counterterrorism tool.

This study has six chapters. In this chapter, I provided the rationale for my research and the theoretical underpinning of my analysis. In Chapter Two, I describe the academic literature concerning terrorism that is relevant to the study. I discuss the reasons why democracies as well as authoritarian regimes employ electronic surveillance as a counterterrorism tool. In Chapter Three, I present the research design and review the methodology I employ. I introduce the research hypothesis and briefly review the study’s theoretical underpinnings. I then provide an overview of the sample, define the variables that are used in the study, describe the data sources and discuss the analysis techniques. Following the discussion of dataset creation, I discuss the steps taken in the quantitative and qualitative analysis. I conclude the chapter with a discussion of the reliability, validity, and limitations of the research design.

I present the descriptive and inferential analysis of the study dataset in Chapter Four. I examine the relationship between terrorist attacks and surveillance laws. I then examine terrorist attacks and the resulting electronic surveillance laws and evaluate the capacity of countries to use electronic surveillance as a counterterrorism tool. In Chapter Five, I outline and discuss the electronic surveillance laws in Pakistan, the United Kingdom, and the United States. In the final chapter I review my findings and develop the policy implications of my analysis. The knowledge and theory that is developed may advance an empirical understanding of the nature and effectiveness of electronic surveillance as a counterterrorism strategy.
Chapter 2: Literature Review

Academic research and discourse exists on the relationship between regime type and terrorism. A common question scholars address is whether terrorism is more common in democracies than in authoritarian regimes. As Chenoweth (2013, 357) notes, many academic studies posit that “the more democratic a country is, the more terrorism it should experience.” In this chapter, I provide an overview of the literature that informed my work on this study. My review of academic research findings focuses on terrorism, regime type, and electronic surveillance.

Terrorism as a Phenomenon

How should terrorism be defined as a phenomenon for study? Neither within nor outside the academy is there any generally agreed-upon definition for the term. Poland (2010) provides ten commonly referenced definitions of terrorism used in government, academic, and legal contexts in his *Understanding Terrorism*. Many scholars include deliberate use of force, the target of the force, and the nature of the actor in the definition. Definitions often imply or explicitly state the political nature of terrorism as an activity. Weinberg, Pedahzur, and Hirsch-Hoefler (2004) review the concepts used to define terrorism by academics, practitioners, and the media in their article “The Challenges of Conceptualizing Terrorism.” Their content analysis of 109 definitions finds that academics define terrorism as a method for using the threat of force as a political strategy. Some academics study specifically state-sponsored terrorism (Collins 2014). State-sponsored terrorism occurs when a nation-state supports terrorist activities (Department of State 2004).
Terrorism as phenomenon involves the deliberate use of force. Individuals who choose terrorism as a course of action make a decision that they will employ violence and acts of destruction to achieve their goals. Terrorism differs from other activities in that it must include the deliberate use of force or the threat of it. Why would actors choose to use force to achieve their ends? Lake (2002) describes a form of bargaining theory in which terrorists use violence and the threat of violence to achieve superior positions. Pape (2003, 345) argues that “most suicide terrorism is undertaken as a strategy directed towards achieving particular political goals.” Pape argues that suicide terrorism is a form of political coercion in which the actor is weaker than the adversary. The terrorist seeks to punish the stronger actor by inflicting costs and risks. If the actor or group can overwhelm the stronger actor then the terrorist may achieve their objectives. Another form of terrorism is proposed by Gambill (1998). In *The Balance of Terror*, Gambill introduces “redemptive terrorism.” Redemptive terrorism is defined as actions designed to “force another actor into ceding specific human or material resources” (Gambill 1998, 55).

Definitions of terrorism also include the target of the force used by the terrorist. For example, does the terrorist only target military, security forces, and other government assets or are civilian and private sector also targeted? Lake (2002, 17) defines terrorism as “the irregular use of violence by nonstate groups against nonmilitary targets and personnel for political ends.” He notes that guerrilla warfare is different in that it is directed at military targets. Alex Schmid (1992, 8), in *Political Terrorism*, writes that:

Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby—in contrast to assassination—the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat—and violence—based communication processes
between terrorist (organization), (imperiled) victims, and main target (audiences(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.

The targets of the violence do matter. In his pioneering study, *Why Terrorism Does Not Work*, Abrahms (2006) finds that terrorism strategically fails to result in terrorists achieving their objectives. The scholar finds that “terrorist groups achieved their main policy objectives only three out of forty-two times – a 7 percent success rate” (Abrahms 2006, 51). Abrahms found that target selection is a critical factor. He writes that the “key variable for terrorist success was a tactical one: target selection. Groups whose attacks on civilian targets outnumbered attacks on military targets systematically failed to achieve their policy objectives” (Abrahms 2006, 41).

A definition of terrorism is required for this study to ensure that the construct or abstraction that describes reality does so accurately and uniformly. Based on the brief review of the academic definitions in the preceding passages, the definition of terrorism should include the deliberate use of force, the target of the force, and the nature of the actor in the definition. In this study, terrorism is defined broadly as the use or threat of violence and destruction perpetrated by nonstate actors for political ends.

**Terrorism and Regime Type**

Is terrorism more common in democracies than authoritarian regimes? In the study titled “Does Democracy Encourage Terrorism,” Eubank and Weinberg (1994) examined regime type and incidence of terrorist violence across 172 countries from 1945 to 1987. The authors wished to determine whether the likelihood of finding terrorist groups in democracies is the same as the chances of finding them in non-democracies. Eubank and Weinberg developed a dataset and split
the sample into two groups: nation-states with terrorist groups and nation-states without terrorist
groups. They added regime type to each country, democracy or non-democracy, based on a
classification from *Democracy: A World Wide Survey* by Wesson (1987). The authors used
nonparametric statistical analysis of their quantitative response variables to calculate the
likelihood of terrorist groups occurring in democracies. They found that terrorists are three and
one half times more likely to occur in democracies than in non-democracies. The authors
conclude by writing that their results imply “that it is democracy that attracts terrorist groups and
that this tendency persists across time” (Eubank and Weinberg 1994, 429).

Eubank and Weinberg’s finding, that democracies are more likely to experience
terrorism, may be contrasted with Eyerman (1998). In *Terrorism and Democratic States: Soft
Targets or Accessible Systems*, the author examines terrorist groups and the constraints on them
by regime type. The sample for the study is a count of terrorist events for 154 countries from
1968 to 1986. The author argues that regimes have unique features that make them more or less
attractive for terrorist groups to operate in. Two schools of thought are presented. The strategic
school posits that “democracies encourage terrorist activity by diminishing the risk associated
with violent activity” (Eyerman 1998, 151). The political access school asserts that “democracies
discourage terrorist activity by providing non-violent alternatives for pursuing policy changes”
(Eyerman 1998, 152). Methodologically, Eyerman operationalizes variables that measure the
“incentives and constraints that are encountered by terrorist organizations within each state”
(Eyerman 1998, 156). Using a negative binomial regression, he calculates the interactions
between regime type and probability of terrorism and finds that the “relationship between
established democracy and terrorism is both negative and significant” supporting the argument
that democracies give more avenues of redress and thus individual’s are less likely to employ
terrorism (Eyerman 1998, 164). Eyerman also finds that new democracies are the most prone to terrorism.

In an effort to improve on Eubank and Weinberg and Eyerman’s work, Li (2005) investigates the links between regiment type and transnational terrorist incidents. In his study, “Does Democracy Promote or Reduce Transnational Terrorist Incidents?” Li argues that the work of these authors has methodological problems. Li notes, for example, that Eubank and Weinberg “do not control for additional factors such as economic development and income inequality that may confound their finding” (Li 2005, 279). In regard to Eyerman’s work, Li writes that it “fails to address important statistical problems such as heteroskedasticity and serial correlation in the error term that may affect statistical inferences” (Li 2005, 280). Li’s work breaks democracy down, arguing that it can have both a positive and negative impact on terrorist incidents. Democratic participation is likely to lower transnational terrorist attacks, while institutional constraints may increase them. Li defines institutional constraints as the component of a democratic society that prevents decision makers taking any action to counter terrorist activity. Institutions of law, norms, the free press, and civil society prevent democratic leaders from implementing any policy they choose. In contrast, Li argues that authoritarian governments are only dependent on support from the elite and may thus exercise executive power with fewer hindrances. Thus, for Li, the “effect of civil liberties on terrorism is epiphenomenal of the institutional constraints on government because the extent of civil liberties, particularly press freedom, is fundamentally determined by the strength of those constraints” (Li 2005, 282).

Li draws a sample of 119 countries from 1975 to 1997. The author uses a negative binomial regression model. He finds that democratic participation is statistically significant in decreasing terrorist incidents. Government constraints, on the other hand, are statistically
significant in increasing terrorist attacks. The author writes that for a “one-point increase in the government constraint variable, the expected number of transnational terrorist incidents increases by 6.3 percent in the country” (Li 2005, 287). Li’s control variables prove some insights. He finds that economic development in GDP and external military conflict reduces the number of transnational terrorist incidents in a country. He argues that while “external military conflict creates grievances and opportunities for terrorists, it often leads to tightened domestic security measures” (Li 2005, 287). As in Eyerman’s work, Li finds that regime change increases the likelihood of terrorist attacks.

Li’s evidence supports his argument that variables describing democracies should be unpacked when exploring their relationship with terrorist attacks. Chenoweth (2013) also calls for more detailed investigation of the democracy-terrorism relationship. She cites Vreeland’s (2008) “The Effect of Political Regime on Civil War” as an example of unpacking regime type to examine relationships. As Crenshaw (1981) has written, “modern liberal democratic states whose desire to protect civil liberties constrains security measures.” Li’s evidence supports the hypothesis that more government constraints result in more terrorist attacks.

Are democracies weak counterterrorists? Crenshaw (1981) argues that civil liberties limit the ability of democratic government to counter terrorist groups. Li (2005, 294) writes that “institutional checks and balances create political deadlock, increase the frustration of marginal groups, impose on the democratic government the tough task of protecting the general citizenry against terrorist attacks, and weaken the government's ability to fight terrorism.” Chenoweth (2013) finds that political competition, a feature of many democracies, and the number of terrorist groups are positively related. In her paper “Democratic Competition and Terrorist Activity,” she contends that “the main motivation for terrorist attacks in democracies is
intergroup dynamics, with terrorist groups of various ideologies competing with one another for limited political influence” (Chenoweth 2010, 2). Pape (2003) uses a strategic model, suggesting a low tolerance for civilian casualties may lead governments to make concessions to terrorist groups. As Piazza (2008) notes, “most empirical studies of terrorism tend to demonstrate a positive relationship between democracy and terrorism.” Hoffman (2017) and Poland (2010) suggest that press freedom in democracies maximizes the impact of terrorist attacks. If these findings are accepted, then democratic leaders face the dilemma of living with terrorist attacks or taking steps to change core aspects of their regime, potentially repressing democratic activities, as they attempt to minimize terrorism.

Counterterrorism Policy

In the wake of three terrorist attacks, just prior to the 2017 election in the United Kingdom, Prime Minster May stated that she was willing to weaken human rights to make it easier for the government to apprehend suspected terrorists where there was not enough evidence to prosecute them for a crime. “If our human rights laws stop us from doing it, we will change the laws so we can do it,” she stated at a campaign rally (James 2017). A number of studies provide evidence that democratic societies are willing to sacrifice some civil liberties following terrorist attacks. Berrebi and Klor (2008), for example, find that a terrorist attack within three months of an election causes an increase in the local population’s support for “the right block of political parties” in Israel. Kibris (2011) finds that Turkish voters’ exposure to terrorism “leads to an increase in the vote share of the right-wing parties.” In a survey of United States citizens, Davis and Silver (2004) found that “the greater people’s sense of threat, the lower their support for civil liberties.”
Are academics fundamentally in agreement that democracies, and their institutional constraints, make them poor counterterrorists? Abrahms (2007) argues that, in fact, democracies are not as vulnerable to coercion as the conventional wisdom holds. Evaluating the outcome of terrorist campaigns in the WITS dataset, Abrahms presents evidence that democracies are “more resistant to coercion than illiberal countries” contradicting Pape’s strategic model. In a case study for calendar year 2005, he tests the association between civil liberties and terrorist incidents and fatalities and finds a positive association between terrorist activity and countries with poor civil liberties. He argues that the sample used by Pape to provide evidence is not representative of the universe terrorist campaigns and is thus not currently generalizable. He writes that “not only is his sample of terrorist campaigns modest, but these campaigns were directed against only a handful of countries: ten of the eleven campaigns analyzed were directed against three countries (Israel, Sri Lanka, and Turkey), and six of those ten were directed against a single country (Israel)” (Abrahms 2007, 236). Using data on terrorist campaigns Abrahms empirical demonstrates that there is a positive relationship between terrorists and illiberal countries. Terrorist groups were “more than five times as likely to achieve their policy objectives against illiberal countries” (Abrahms 2007, 238).

Other scholars have found evidence that democracies are effective counterterrorists. Piazza and Walsh (2010, 556) argue that governments “require support from the population, domestic political movements, and from the international community to mount an effective counterterrorism policy.” Findley and Young (2011) note that governments with functional judicial oversight have greater credibility in making counterterrorism commitments, thus providing fewer incentives for terrorist activity. Using the Global Terrorism Database, the authors test whether an independent judiciary (a component of most democracies) affects the
incidence of terrorist attacks. They find that, indeed, an independent judiciary lowers the incidence rate.

What might account for these contradictory findings? A possible explanation is that democracies provide a proportional response to terrorism. Lake (2002, 19) argues that terrorists aim to provoke a disproportionate and indiscriminate response that “punishes the broad population of which the terrorists are part.” Kalyvas (2004, 97) defines indiscriminate violence as an activity in which “victims are selected on the basis of their membership in some group irrespective of their individual actions.” Lake notes that “Timothy McVeigh sought to provoke a backlash by what he perceived as a repressive state that would reveal for all Americans just how oppressive the government had become” (2002, 20). Authoritarian regimes may be unrestrained in their use of indiscriminate violence, but democracies seldom use violence indiscriminately, and thus retain domestic support for campaigns against terrorist entities. Domestic political support is critical in protracted struggles. Abrahms (2007) demonstrates that counterterrorism responses may take decades to complete. Li (2005, 294) finds that political participation “reduced transnational terrorist incidents in a country.” Choi (2010, 940) finds that a nation-state where the rule of law is enforced reduce the “likelihood of any type of terrorist events.”

Electronic Surveillance for Counterterrorism

Do other proportional counterterrorism responses lead to less terrorism? Electronic surveillance, for example, plays a central role in many democratic nations’ counterterrorism strategies. When Matthew Olson, former director of the National Counterterrorism Center, was asked how important the ability to gather electronic surveillance was for the government, he replied that it was “an 11 out of 10” (Olsen and Wittes 2017). Almost every nation-state has some capacity to monitor communications domestically under the auspices of national security.
In addition to their uses for national security and counterterrorism, of course, electronic surveillance programs may be used to monitor and control political dissent.

At the national and international levels, laws generally protect the privacy of individuals. The U.N. Universal Declaration of Human Rights states that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks” (United Nations n.d., Article 12). Most national constitutions contain the right to privacy for individuals. The University of Texas’s Constitute Project is an organization that collects, catalogs, and publishes nation-states’ constitutions (“Constitute” n.d.). The Constitute dataset contains current and historical versions of most independent nations in the world. Of the 192 active constitutions, 171 (89%) are categorized by the Constitute researchers as containing a right to privacy. A right to privacy is operationalized by Constitute as “individuals’ protection against government intrusion into their property, papers, person, or communications without proper authorization” and also protects against such intrusions by private individuals” (“Constitute” n.d.). But while U.N. and national laws grant a right to privacy, the reality is different across countries.

How do governments legally conduct electronic surveillance if most countries’ constitutions protect individual privacy? Generally, surveillance laws are used to expand state power to allow security officials to conduct actions that are otherwise prohibited by law. In the early twentieth century, many countries collected electronic intelligence without laws explicitly allowing it. In the United States, for example, the Supreme Court heard the case of Olmstead v. United States (“Olmstead v. United States, 277 U.S. 438 (1928)” n.d.). Government agents investigating prohibition were “secretly tapping the lines of a telephone company connected with
the chief office and some of the residences of the conspirators, and thus clandestinely overhearing and recording their telephonic conversations concerning the conspiracy and in aid of its execution” (“Olmstead v. United States, 277 U.S. 438 (1928)” n.d., 457). As no Federal law specifically prohibited wiretapping, the court ruled that the admissibility of evidence was “not affected by the fact of its having been obtained illegally” (“Olmstead v. United States, 277 U.S. 438 (1928)” n.d., 277). In the second half of the Twentieth Century the proliferation of technology resulted in many countries adopting laws that specifically authorized the government to collect electronic surveillance, on national security grounds. In 1973, Canada developed and adopted the Protection of Privacy Act, which “governs the personal information handling practices of federal government institutions” bans wiretapping while allowing its use with a warrant by the government (“Privacy ~ Canada’s Human Rights History” n.d.). As internet-enabled mobile devices and facilitated technologies, such as Facebook, Twitter, and YouTube, have proliferated in the twenty-first century, government has adopted data protection laws to expand government surveillance. Currently, many governments are working to legislate Internet Protocol-enabled Closed Circuit Television (CCTV) and encryption approaches that secure mobile devices and other communications (BBC News 2016).

There appears to be a dearth of empirical social science research on electronic surveillance. Esau (2016), for example, compares American and European societal views on government surveillance Esau (2016). Haggerty and Gazso (2005, 169) explore the “politics and social dynamics of contemporary surveillance,” performing a content analysis on New York Times and Toronto Globe and Mail articles following 9/11. They find that “September 11th provided a convenient opportunity for the security establishment to lobby for increased surveillance capacity, despite lingering questions about whether such devices can achieve their
professed goals” (Haggerty and Gazso 2005, 169) This evidence supports Baumgartner and Jones’s (2009) Punctuated Equilibrium and Kingdon’s (2010) policy entrepreneur theories. Sorell (2011, 9) reviews counterterrorism strategy, arguing that “secret, narrowly targeted surveillance where there is reasonable suspicion of involvement in terrorism” may be considered a proportional response to terrorist activity. This evidence supports the thesis that democratic states may be superior counterterrorists, as they provide a proportional response to it. Richards (2012) explores the ethics of intelligence services and the protection of civil liberties. She notes that “terrorism and counter-terrorism have always provoked debate about whether there are cases in which the norms of human rights protection in a liberal democracy can sometimes be adjusted to suit the gravity of the situation. Her work includes an analysis of the opinion of the heads of intelligence agencies who “acknowledged that the post-9/11 era poses particular issues of complexity, if not dilemma, in their intelligence operations, which intensify the questions around the proper limits of intelligence in a modern liberal democracy” (Richards 2012, 779). Brown and Korff (2009, 119) argue that European countries’ surveillance laws are “problematic for democracy and the rule of law, and will lead to practical difficulties for cross-border cooperation between law enforcement agencies.” A common theme in these studies is their qualitative approach. There is no doubt that qualitative research, such as case studies, offers critical academic tools to answer “how” and “why” questions (Yin 2013). What is needed in the study of electronic surveillance and counterterrorism, however, is quantitative studies.

In this chapter, I summarized relevant academic literature regrading terrorism, regime type, and electronic surveillance. Terrorism, broadly defined as the use or threat of violence and destruction perpetrated by nonstate actors for political ends, is a threat to governments in many countries. There is an active academic debate on the relationships between regime type and
terrorist activity. Does democracy encourage terrorism? Most scholars find that terrorism is more prevalent in countries with transitional or democratic regimes (Chenoweth 2013). Which components of democracy have positive and negative relationships with terrorism? Many scholars find a negative association between rule of law, government capability, and terrorism (Li 2005; Findley and Young 2011). The better a country can govern and execute counterterrorism actions, the less likely terrorism is to occur. Are democracies effective counterterrorists? There is no definitive answer at this time. I posit that terrorist attacks provide a shock to the political system, forcing counterterrorism strategies onto the political agenda. As most countries have constitutions that protect individual privacy, it is likely, that following terrorist attacks, solutions that increase government counterterrorism capability will make their way into law. Populations and decision makers seem more willing to accept privacy invasions following terrorist attacks Davis and Silver (2004). National security intelligence is broadly defined as a secret activity undertaken by nation-states to understand or influence adversarial entities. Electronic surveillance provides a strategy for governments to attempt to gather data on terrorist groups and turn the intelligence into actions that can stop attacks before they occur (MITRE Corporation 2009). In the next chapter, I outline the research design I use to explore the relationship between electronic surveillance law and terrorism.
Chapter 3: Methodology

In this chapter I provide a summary of the research design and methodology I employed to conduct this study. I detail the objects of the study, the variables, their theoretical linkages, my assumptions, and the reliability, validity, and limitations of my work. The goal of my study is to determine whether electronic surveillance affects terrorism in nation-states. I employ a quantitative approach to analyze longitudinal (panel) data. I employ empirically tested variables from previous academic studies in my model. To address methodical issues in these studies, I employ negative binomial panel regression techniques applicable to count data.

Conceptual Relationship between Terrorism and Counterterrorism

Terrorism, broadly defined as the use or threat of violence and destruction perpetrated by nonstate actors for political ends, is a threat to governments in many countries. Terrorist activity can be counted. The number of attacks in a country, for example, may be recorded each year. The number of individuals killed in a calendar year may be counted. Nation-states are named and may be counted by their frequency. A nation-state is defined as a “geographical unit who’s government has the supreme power to make laws within its boundaries and as the supreme legal right to use force to guarantee the observance of those laws” (Shively 2009, 2).

For the purposes of this study, counterterrorism is defined as “activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals” (Department of Defense 2018, 57). As seen in Figure 2. I express the relationship between counterterrorism and terrorist activities as negative. That is, as counterterrorism increases, I expect terrorism to decrease.
As Li (2005) contends, government counterterrorism is linked to government capability and constraints. National security intelligence is a component of government counterterrorism. National security intelligence, as previously discussed, is broadly defined as a secret activity undertaken by nation-states to understand or influence adversarial entities. Intelligence and law enforcement organizations employ electronic surveillance to gather data on terrorists. I define national security electronic surveillance narrowly as the acquisition (by an electronic, mechanical, or other surveillance device) of the contents of any electronic communication without the consent of any party thereto. Most national constitutions provide a right to privacy, which has led most countries to enact laws permitting surveillance. Electronic surveillance lowers the constraints on government, allowing it more freedom to gather data on terrorists.

Electronic surveillance law is defined narrowly in this study, as national rules that permit the capture of communications and data for national security purposes. Implied in the definition
is the enforcement of the law by threat of punishment. In many countries, surveillance law is regulated at the national and subnational levels. In Australia, for example, both the national (federal) government and subnational governments (states and territories) regulate surveillance (Office of the Australian Information Commissioner n.d.). In this study, I focus on national surveillance laws because national governments are most often responsible for conducting counterterror activities for a nation-state.

I hypothesize that the governments with electronic surveillance laws are likely to experience less terrorism. I operationalize terrorism as accounts of the number of attacks per year and the number of individuals killed per year as a result of terrorism.

**H1: The presence of electronic surveillance laws decreases terrorist attacks.**

**H2: The presence of electronic surveillance laws decreases fatalities from terrorist attacks.**

A likely consequence of surveillance laws is the government improving its capability to gather, store, and analyze the data it collects. I thus expect that as electronic surveillance increases, terrorist attacks will decrease. The electronic surveillance techniques employed by intelligence services are secret; it is thus not possible to gather complete data on the system and capabilities of each country. As a proxy for capability, I employ the number of surveillance laws identified in a country. If an issue makes it to the political agenda and is passed into law, it is likely an institution will form around the issue, with organizations and resources (Baumgartner and Jones 1993). In light of this tendency, I argue that if electronic surveillance makes it to the political agenda and is passed into law, new or existing government organizations will receive resources to develop technical collection, storage, and analysis capability.
H3: The greater the electronic surveillance capability a country has, the fewer terrorist attacks it will experience.

H4: The greater the electronic surveillance capability a country has, the fewer fatalities from terrorist attacks it will experience.

Regime type may impact a government’s ability to develop and maintain counterterrorism capability. Democratic regimes may face more resistance from their citizens when attempting to implement measures that infringe on civil liberties. Conversely, authoritarian regimes likely face few challenges from their population when implementing counterterrorism policy. Consistent with scholarly counterterrorism literature, I expect to see variation in the effectiveness of electronic surveillance in relation to regime type.

Research Design

Table 1: Research Design displays a summary of my hypothesis, the primary measure, the data sources, and the methods I employ in this study. To test these hypotheses, I select variables that are related to government capacity to implement counterterrorism policy and I build a statistical model to test the relationships. In the following passages, I discuss my data sources, provide definitions for variables, and discuss the procedures I undertook to prepare the dataset for analysis.

In order to investigate any relationship between electronic surveillance law and terrorist events, I developed a new dataset from multiple sources. The dataset is longitudinal (also called panel data). I conceptualized a dataset with $n$ different countries observed at $T$ different time periods. The next passages describe how I created the dataset.

The Global Terrorism Database (GTD) was used as a source for annual data on nation-states, the number of terrorist attacks, and number of individuals killed. The GTD is maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at

Table 1: Research Design

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Measure</th>
<th>Data Sources</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1 The presence of electronic surveillance laws decreases terrorist attacks</td>
<td>IV. Electronic surveillance law DV. Terrorist attacks</td>
<td>Academic journals, Global Media Freedom Dataset, Global Terrorism Database</td>
<td>1. Negative binomial panel regression</td>
</tr>
<tr>
<td>H2 The presence of electronic surveillance decreases fatalities from terrorist attacks</td>
<td>IV. Electronic surveillance law DV. Individuals killed in terrorist attacks</td>
<td>Government reports, Legal research/studies, Media reports, Nation-state laws, Non-governmental origination reports, Polity IV Project, UCDP/PRIO Armed Conflict Dataset, World Bank Data</td>
<td></td>
</tr>
<tr>
<td>H3 The greater the electronic surveillance capability a country has, the fewer terrorist attacks it will experience</td>
<td>IV. Electronic surveillance law DV. Individuals killed in terrorist attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H4 The greater the electronic surveillance capability a country has, the fewer fatalities from terrorist attacks it will experience</td>
<td>IV. Electronic surveillance law DV. Individuals killed in terrorist attacks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The dataset is built from publicly available, open-source materials including “electronic news archives, existing datasets, secondary source materials such as books and journals, and legal documents” (START n.d.). The GTD defines terrorism as “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” (START n.d.).

I developed a purposeful sampling approach for this study (Berg and Lune 2011). Of the 205 countries in the GTD database, I am interested in the countries where the majority of the world’s terrorist events occur. My focus is on the relationships in the sample as they represent the majority of the world’s population and economic production. I downloaded the GTD dataset in Microsoft Excel format and then transformed it to a comma-separated value file that could be
easily manipulated using the statistical packages R and Stata. The software language R is a computational language and environment for statistical computing and graphics (The R Foundation n.d.). R has many built-in statistical techniques, including “linear and nonlinear modelling, classical statistical tests, time-series analysis, classification, and clustering” (The R Foundation n.d.). Stata is a statistical software package with built in statistical techniques for panel data and negative binomial regressions (“Stata | Why Stata?” n.d.).

The GTD dataset is comprised of columns and rows. Each column represents a variable and each row contains the numerical and text representations of each variable. Rows are referred to as observations. I reviewed the 135 variables in the GTD dataset to determine which would be included in this study. I kept four variables: year (iyear), name of the country (country_txt), number of attacks (attacks), and number of people killed in each attack (nkill).

My initial criterion for including a country in the sample is a population of over one million in 2016. I gathered population data from the World Bank (WB). The World Bank is an international organization funded by 184 countries. It maintains international datasets built from the “statistical systems of member countries” (World Bank 2018a). The country name fields in the GTD and WB data did not match, so I used the GTD names as the master names for the dataset, using the variable (country_txt). I converted the WB country names to the GTD names and then merged the data, enabling the population variable (population) for each year from 1970 to 2016 to be added to the dataset.

As Eubank and Weinberg (1994), Li (2005), Piazza (2008), and Chenoweth (2013) have demonstrated, regimen type has a relationship with terrorist attacks. To operationalize regime type, I gathered data from the Polity IV Project. The Polity IV dataset contains coded data on the governments of nation-states (Center for Systemic Peace n.d.) from 1800 to 2016. The Polity IV
Project is maintained by academic scholar at the Center for Systemic Peace. The Polity Score variable regime authority spectrum has a 21-point scale ranging from -10 (hereditary monarchy) to +10 (consolidated democracy). The Polity scores may be “converted into regime categories in a suggested three part categorization of “autocracies” (-10 to -6), “anocracies” (-5 to +5 and three special values: -66, -77 and -88), and “democracies” (+6 to +10)” (Center for Systemic Peace n.d.). I downloaded the Polity dataset in Microsoft Excel format and then transformed it to a comma-separated value file that could be manipulated.

I reviewed the 23 variables in the Polity dataset to determine which would be included in this study. I kept three variables: year (byear), name of the country (country), and ordinal revised polity score (polity2). The (polity2) variable “modifies the combined annual POLITY score by applying a simple treatment, or ‘fix,’ to convert instances of ‘standardized authority codes’ (i.e., -66, -77, and -88) to conventional polity scores (i.e., within the range, -10 to +10)” for use in time series analysis (Center for Systemic Peace n.d.).

In R, the command subset returns subsets of vectors, matrices, or data frames that meet conditions. I used the R function subset to limit the data to observations from the years 1970–2016. I created a new categorical variable (cpolity2) and performed the conversion of the ordinal variable (polity) to (cpolity2). The variable (cpolity2) may take the form autocracy, anocracy, or democracy. I converted the Polity country names to the GTD names and then merged the data so the (polity) and (cpolity2) variables for each observation from 1970 to 2016 were added to the dataset.

Terrorist groups often use a country’s foreign policy as a reason to attack it. Osama bin Laden, for example, made reference to American foreign policy as a reason for launching the September 11 attacks (Scheuer 2006). I gathered data from the UCDP/PRIO Armed Conflict
Dataset as a proxy for a nation’s foreign policy. The Armed Conflict Dataset is maintained by researchers at the Uppsala Conflict Data Program (UCDP) at Uppsala University and the Centre for the Study of Civil War at the International Peace Research Institute in Oslo (PRIO) (“UCDP/PRIO Armed Conflict Dataset - PRIO” n.d.). The dataset provides an indicator as to whether country was involved in an armed conflict in any given year. An armed conflict is defined as “a contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in a calendar year” (“UCDP/PRIO Armed Conflict Dataset - PRIO” n.d.). The Armed Conflict Dataset identifies each country’s role as a primary party in the conflict or as an actor supporting one of the primary parties.

I reviewed the 27 variables in the Armed Conflict Dataset to determine which would be included in this study. I kept four variables: year (year), name of the country (territory_name), text string for the primary party (Side_a), and countries supporting the primary party (Side_a_2nd). In internal conflicts, side A is always the government side. In R, the command subset returns subsets of vectors, matrices or data frames which meet conditions. I used the R function subset to limit the data to observations from the years 1970–2016. I created two new variables, (conflict) and (conflict2). I transformed the text names of the countries in the string variables (Side_a) and (Side_a_2nd) to dichotomous and added them to the (conflict) and (conflict2). I converted the Armed Conflict Dataset country names to the GTD names and then merged the data, so the (conflict) and (conflict2) were included in the dataset. Variables for each observation from 1970 to 2016 were added to the dataset.

As reported by many scholars the media plays a role in terrorist events. To capture the role of media in my model I gathered data from the Global Media Freedom Dataset (GMFD).
The GMFD is maintained by Jennifer Whitten-Woodring at the University of Massachusetts Lowell (Whitten-Woodring and Belle 2017). An ordinal scale is used to measure the media environment in countries, from 1948 to 2014. The GMFD uses the score 1, 2, or 3 for countries where “criticism of government and government officials” by the media is normal, limited, or not possible. I reviewed the four variables in the Armed Conflict Dataset and kept (year), (country), and (mediascore). The GMFD does not have data for the years 2015 and 2016. Using the guide found in the GMFD codebook, I gathered data from the Freedom House’s Freedom of the Press dataset and combined them. I converted the GMFD country names to the GTD names and then merged the data, so that the (mediascore) variable available for each observation from 1970 to 2016 was added to the dataset.

I added one additional control variable to the dataset. I gathered Gross Domestic Product data from the World Bank development indicators index. GDP is likely negatively related to terrorism as it may be seen as a proxy for the capability of a government to implement counterterrorism policy. A larger GDP would be negatively related to terrorism. I gathered GDP data for 1970–2017 from the World Bank Development Indicators dataset (“World Development Indicators | DataBank” n.d.). I converted the country names to the GTD names and then merged the data, so that the GDP (gdp) variable was added to observations from 1970 to 2016 in the dataset. As GDP is a large number, it is often useful to convert it to a Log base 10 value to use in computations. I used the (gdp) variable to calculate a Log base 10 value and then added them to a new variable called (gdplog).

At this point, I inspected the dataset and made a decision about which countries should be considered for exclusion. First, I ran a preliminary search for missing data. Some countries (North Korea, for example) were excluded based on the paucity of data available. Other
countries that may have been in the dataset, but no longer exist (e.g., Yugoslavia), were dropped. If a country was missing significant data for certain years, I made a decision on a case-by-case basis as to whether it should be included in the dataset.

The independent variable surveillance law (slaw) was developed via open source data collection and content analysis. Open sources are defined as those that may be publically observed or requested. For each country, I conducted a search to identify electronic surveillance laws. I followed the same procedure for each country. First, I searched online media sources using a keyword list and the country’s name. The keywords included terms designed to return documents related to electronic surveillance. Keywords examples include “electronic surveillance,” “wiretap,” “wire tap,” “domestic surveillance,” “mass surveillance,” “spying,” and “terrorism law.” Following media searches, I attempted to identify government sources of data. The Library of Congress, for example, has a section on foreign intelligence gathering laws that provides background on electronic surveillance laws in Belgium, France, Germany, Portugal, Romania, Netherlands, Sweden, and the United Kingdom (Roudik 2016). After searching government sources, I ran searches of non-governmental organizations that report on personal privacy. Privacy International, for example, has compiled country profiles of many nations’ electronic surveillance capabilities (Privacy International n.d.). Telecommunications trade publications were identified and annual publications on ongoing regulatory issues were identified and gathered. Law journals and legal research were gathered via open sources using specific keywords such as “transparency report” and “law enforcement disclosure” (“Law Enforcement Disclosure Report - Vodafone” n.d.). Academic journals were searched and data collected using the NEU library portal.
Collected data was stored in a folder for each country. I read each collected data file and identified laws that could possibly be electronic surveillance laws. I attempted to collect the actual text of the law if it was available online. I define national security electronic surveillance narrowly as the acquisition by an electronic, mechanical, or other surveillance device of the contents of any electronic communication without the consent of any party thereto. Specifically, for this study, I narrowed the definition of electronic surveillance law to national rules that permit the capture of communications and data for national security purposes. Thus, in order for a law to be coded as an electronic surveillance law in the data, the law needed to be focused on communications or data. Some countries passed more than one surveillance law per year. During the data collection phase of this research, I kept a separate file of the electronic surveillance law that allowed for multiple observations per year. If the content analysis revealed that the electronic surveillance law was a direct response to terrorism, it was also coded as a separate variable (tslaw). A direct response to terrorism is operationalized as government officials stating publicly that the law is a measure to address terror or that the text of the law indicates that a purpose of the law is to address terrorism.

I created four variables in the dataset for electronic surveillance law. The first is a dichotomous variable for electronic surveillance law (slaw). If any electronic surveillance law was adopted in the year of the observation, this variable is coded 1. The second variable (slaw1) is similar to (slaw) in that if the country has a surveillance law in any given year then (slaw) is coded 1. A (slaw1) attribute from the previous year is inherited. If a country has a surveillance law in 1970, for example, then all subsequent years are also coded 1. The third variable is a total of the surveillance laws for a country (aslaw). For the (aslaw) variable, the number of surveillance laws identified in any year is added to the laws in past years to generate a count. The
count is a proxy for increased electronic surveillance in a country. The third variable measures whether the electronic surveillance law is a response to terrorism. The dichotomous variable (tslaw) records whether the law is a direct response to terrorism.

The compiled dataset is a Comma Separated Values file with the following variables: country name (country_txt), year (iyear), population (population), terrorist attacks (attacks), number of individuals killed in terrorist attacks (nkill), terrorism surveillance law adopted (slaw), terrorism surveillance law adopted in any previous year (slaw1), total surveillance laws (aslaw), polity score (polity2), primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), Gross Domestic Product (gdp), and Gross Domestic Product Log (gdpglog). This dataset includes the variables required to explore the relationship between electronic surveillance law, terrorist attacks, and the number of individuals killed in terrorist attacks. The number of entities in a panel dataset is denoted $n$, and the number of time periods is denoted $T$. In this dataset, we have observations on $n = 98$ countries (entities) for $T = 47$ years (time periods) from 1970 to 2016. Thus, there are a total of $n \times T = 98 \times 47 = 4,606$ observations.

I began my analysis by generating descriptive statistics for the sample. The analysis includes frequency tables, density plots, time series plots, and heat maps. I provide detailed plots that display the incidence of terrorist attacks per capita and years when electronic surveillance laws were adopted by nation-states.

Using the hypothesis that there is a relationship between electronic surveillance laws and terrorist attacks and between electronic surveillance law and the number of individuals killed in terrorist attacks, I developed a multivariate panel regression model. The unit of analysis is year.
Two dependent variables will be tested: (1) number of terrorist attacks (attacks) and (2) number of individuals killed in terrorist attacks (nkill). Both of these variables are count data.

Count data is often modeled using Poisson regression. A Poisson regression is a “generalized linear model where a response is assumed to have a Poisson distribution conditional on a weighted sum of predictors” (Ford, 2016). An issue with Poisson regression is that it may not accurately describe the variability of the counts. In a Poisson distribution, the parameter \( \lambda \), lambda, is both the mean and variance. As seen in Table 2 Variable (attacks) and (nkill) Characteristics the mean and variance of the variables (attacks) and (nkill) are not equal. If the variance is smaller than the mean, the statistical term underdispersion is used. If the variance is larger than the mean the term overdispersion is used. As the variance is of both (attacks) and (nkill) is larger than the mean these data may be described as overdispersed. If a Poisson regression is used on overdispersed (or underdispersed) data, the model does not fit well. Fit of statistical model refers to how close the predicted values are to the observed data values.

**Table 2 Variable (attacks) and (nkill) Characteristics**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Mean</th>
<th>Variance</th>
<th>SD</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>(attacks) Terrorist Attacks</td>
<td>32.65</td>
<td>23698.22</td>
<td>153.94</td>
<td>3926.00</td>
</tr>
<tr>
<td>(nkill) People Killed in Terrorist Attacks</td>
<td>71.64</td>
<td>214843</td>
<td>463.51</td>
<td>13079.00</td>
</tr>
</tbody>
</table>

One approach to address under or overdispersed data is to employ a Negative Binomial Regression. Both the Poisson and negative binomial distributions describe the probabilities of the occurrence of whole numbers greater than or equal to 0. The Poisson’s constraint that the distribution’s mean equals its variance is relaxed in the negative binomial model. Li (2005),
Piazza (2008), and Findley and Young (2011) use negative binomial regression models to test their terrorism-related hypothesis. Findley and Young (2011, 367) writing that “a negative binomial model is more appropriate than a Poisson count model” because “there is considerable variance in the number of terrorist events across countries and over time.”

A methodical issue with the approach that Li (2005), Piazza (2008), and Findley and Young (2011) use is that they may not have adequately accounted for Omitted Variable Bias (OVB). OVB occurs when a variable that is correlated with both the dependent and one or more included independent variables is omitted from a regression equation (Stock and Watson 2014). One approach that researchers may use to mitigate OVB is fixed or random effects regression. Fixed and random effects regression is an approach for controlling for omitted variables in panel data when the variables vary across entities, but do not change over time (Stock and Watson 2014).

I employed Stata to run the fixed and random effect regressions. In the various models I test, the following independent variables—surveillance law (slaw1), total surveillance laws (aslaw), polity score (polity2), primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), and Gross Domestic Product Log (gdpplog)—are tested for a relationship with the dependent variable terrorist attacks (attacks) and number of individuals killed (nkill).

The negative binomial regression model is expressed as the equation:

$$
Pr(Y = y_i | u_i, \alpha) = \frac{\Gamma(y_i + \alpha^{-1})}{\Gamma(\alpha^{-1})\Gamma(y_i + 1)} \left( \frac{1}{1 + \alpha \mu_i} \right)^{\alpha^{-1}} \left( \frac{\alpha \mu_i}{1 + \alpha \mu_i} \right)^{y_i}
$$

Stata contains functions to calculate the fixed and random-effect negative binomial panel regression. The Stata command xtset declares that the dataset is a panel (time series) and set the period (year). The command xtnbreg executes fixed-effects, random-effects, & population-
averaged negative binomial models. The variable *country1* is used by Stata to group by country. The *country1* variable is seen in the Stata table outputs.

To test “H1: The presence of electronic surveillance laws decreases terrorist attacks,” the dependent variable *terrorist attacks* (attacks) is regressed upon the independent variables *terrorism surveillance law* (slaw1), *polity score* (polity2), *primary party in an armed conflict* (conflict), *country supporting an armed conflict* (conflict2), *media freedom* (mediascore), and *Gross Domestic Product Log* (gdplog) using the xtnbreg command in Stata. I ran both fixed effects and random effects models and saved the results.

As Greene (2011) notes, a random effect model treats the individual effects as uncorrelated with the other regressors and thus may display inconsistency as the included variables and the random effect are correlated. Hausman (1978) developed a specification test to identify whether it is the fixed or the random modes that are a better fit. I ran a Hausman for each model to determine whether the fixed or random effect model is a better fit.

The null hypothesis for a Hausman test is that the random effect model is appropriate (Greene 2011). If the probability statistic generated from the test is significant (P<.05), then the fixed effect model is appropriate. Otherwise the random effects model is appropriate. As seen in Table 3, the Hausman test for H1 resulted in the rejection of the null hypothesis because the probability is less than .05—and thus the fixed effects model is appropriate.
To test “H2: The presence of electronic surveillance decreases fatalities from terrorist attacks” the dependent variable number of individuals killed in terrorist attacks (nkill) is regressed upon the independent variables terrorism surveillance law (slaw1), polity score (polity2), primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), and Gross Domestic Product Log (gdplog) using the xtnbreg command in Stata. I ran both fixed effects and random effects models and saved the results. I ran a Hausman test to determine whether the fixed or random effects model is a better fit. As seen in Table 4, the Hausman chi-square test statistic is negative. The negative statistic impacts Stata and it cannot complete the Hausman test. Schreiber (2008) finds that “under the alternative hypothesis the Hausman chi-square test statistic can be negative not only in small samples but even asymptotically.” With a negative statistic, the “result is only compatible with the alternative” and thus the fixed effects model is appropriate (Schreiber 2008).

### Table 3 H1 Hausman Test Fixed Effects / Random Effects

<table>
<thead>
<tr>
<th></th>
<th>Coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(b) fe</td>
</tr>
<tr>
<td>slaw1</td>
<td>-.1605759</td>
</tr>
<tr>
<td>polity2</td>
<td>.0419026</td>
</tr>
<tr>
<td>conflict</td>
<td>.8455846</td>
</tr>
<tr>
<td>conflict2</td>
<td>-.0105522</td>
</tr>
<tr>
<td>mediascore</td>
<td>.0271995</td>
</tr>
<tr>
<td>gdplog</td>
<td>.3744862</td>
</tr>
</tbody>
</table>

\( b = \) consistent under Ho and Ha; obtained from xtnbreg  
\( B = \) inconsistent under Ha, efficient under Ho; obtained from xtnbreg

Test: Ho: difference in coefficients not systematic

\[
\text{chi}^2(6) = (b-B)'[(V_{b-V_B})^{-1}](b-B) = 268.35
\]

\( \text{Prob}>\text{chi}^2 = 0.0000 \)
To test “H3: The greater the electronic surveillance capability a country has the fewer terrorist attacks it will experience” the dependent variable *terrorist attacks* (attacks) is regressed upon the independent variables total of the surveillance laws for a country (aslaw), polity score (polity2), primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), and Gross Domestic Product Log (gdplog) using the xtnbreg command in Stata. I ran both fixed effects and random effects models and saved the results. I ran a Hausman test to determine whether it is the fixed or the random effects model that is a better fit. As seen in Table 5, the Hausman test resulted in the rejection of the null hypothesis because the probability is less than .00001 and thus the fixed effects model is appropriate.

<table>
<thead>
<tr>
<th>Table 4 H2 Hausman Test Fixed Effects / Random Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>aslaw1</td>
</tr>
<tr>
<td>polity2</td>
</tr>
<tr>
<td>conflict</td>
</tr>
<tr>
<td>conflict2</td>
</tr>
<tr>
<td>mediascore</td>
</tr>
<tr>
<td>gdplog</td>
</tr>
</tbody>
</table>

*b* = consistent under *Ho* and *Ha*; obtained from xtnbreg  
*B* = inconsistent under *Ha*, efficient under *Ho*; obtained from xtnbreg  
Test: *Ho*: difference in coefficients not systematic  

\[
\text{chi2}(6) = (b-B)^T [(V_b-V_B)^{-1}] (b-B) = -51.08
\]

*chi2<0 =>* model fitted on these data fails to meet the asymptotic assumptions of the Hausman test; *see ztest* for a generalized test.

To test “H4: The greater the electronic surveillance capability a country fewer fatalities from terrorist attack it will experience” the dependent variable *number of individuals killed in
terrorist attacks (nkill) is regressed upon the independent variables total of the surveillance laws for a country (aslaw), polity score (polity2), primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), and Gross Domestic Product Log (gdplog) using the xtnbreg command in Stata. I ran both fixed effects and random effects models and saved the results. I ran a Hausman test to determine whether it is the fixed or the random effects model that is a better fit. As seen in Table 6, the Hausman chi-square test statistic is negative. With a negative statistic, the “result is only compatible with the alternative” and thus the fixed effects model is appropriate (Schreiber 2008. 1).

Table 5 H3 Hausman Test Fixed Effects / Random Effects

<table>
<thead>
<tr>
<th></th>
<th>Coefficients</th>
<th></th>
<th></th>
<th>sqrt(diag(V_b-V_B))</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(b)</td>
<td>(B)</td>
<td>(b-B)</td>
<td>S.E.</td>
</tr>
<tr>
<td>aslaw</td>
<td>-.0772174</td>
<td>-.0771889</td>
<td>-.0000284</td>
<td>.0016089</td>
</tr>
<tr>
<td>polity2</td>
<td>.0412614</td>
<td>.0418157</td>
<td>-.0005542</td>
<td>.0005472</td>
</tr>
<tr>
<td>conflict</td>
<td>.8302626</td>
<td>.8582965</td>
<td>-.0280339</td>
<td>.0023937</td>
</tr>
<tr>
<td>conflict2</td>
<td>.0884084</td>
<td>.0823016</td>
<td>.0061068</td>
<td>.005313</td>
</tr>
<tr>
<td>mediascore</td>
<td>.0308338</td>
<td>.0435025</td>
<td>-.0126687</td>
<td>.0048199</td>
</tr>
<tr>
<td>gdplog</td>
<td>.4072957</td>
<td>.4188026</td>
<td>-.0115069</td>
<td>.0057709</td>
</tr>
</tbody>
</table>

Test: Ho: difference in coefficients not systematic

\[
\text{chi}^2(6) = (b-B)'[(V_b-V_B)^{-1}](b-B) = 380.93 \\
\text{Prob}>chi^2 = 0.0000
\]

Reliability, Validity, and Limitations

In the following paragraphs, I address the reliability, validity, and the limitations of this study. Reliability is defined as the consistency or repeatability of the measures selected for a study (Trochim 2006). The data from the Global Terrorism Database (GTD) dataset is publicly
available. The GTD is operated by an academic research institution that maintains data collection protocols that are available for review. The data is collected from open sources. These data have some risk to their comprehensiveness. Academic scholars report that terrorist incidents are more frequently reported in countries with a free press (Schmid 1992; Eubank and Weinberg 1994; Li and Schaub 2004). A media reporting bias may therefore result in underreporting in countries where the media is controlled by the state.

Table 6 H4 Hausman Test Fixed Effects / Random Effects

<table>
<thead>
<tr>
<th></th>
<th>Coefficients</th>
<th>(b)</th>
<th>(B)</th>
<th>(b-B)</th>
<th>sqrt(diag(V_b-V_B))</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
<td>Fe</td>
<td>Re</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aslaw</td>
<td>-.0951062</td>
<td>-.096107</td>
<td>.0010008</td>
<td>.0022147</td>
<td></td>
</tr>
<tr>
<td>polity2</td>
<td>.0464712</td>
<td>.0460114</td>
<td>.0004598</td>
<td>.0006541</td>
<td></td>
</tr>
<tr>
<td>conflict</td>
<td>1.277017</td>
<td>1.30388</td>
<td>-.0268634</td>
<td>.</td>
<td></td>
</tr>
<tr>
<td>conflict2</td>
<td>-.0294288</td>
<td>-.0329092</td>
<td>.0034804</td>
<td>.006197</td>
<td></td>
</tr>
<tr>
<td>mediascore</td>
<td>.1070073</td>
<td>.1292781</td>
<td>-.0222708</td>
<td>.0051743</td>
<td></td>
</tr>
<tr>
<td>gdplog</td>
<td>.4503076</td>
<td>.4632278</td>
<td>-.0129203</td>
<td>.0060498</td>
<td></td>
</tr>
</tbody>
</table>

b = consistent under Ho and Ha; obtained from xtnbreg
B = inconsistent under Ha, efficient under Ho; obtained from xtnbreg

Test: Ho: difference in coefficients not systematic

\[
\chi^2(6) = (b-B)'[(V_{b-V_B})^{-1}](b-B) = -50.71
\]

\(\chi^2<0\) -> model fitted on these data fails to meet the asymptotic assumptions of the Hausman test; see systest for a generalized test

The World Bank Data is publicly available. The World Bank Data is compiled from the statistical services of member countries. In some circumstances, World Bank data are estimates that may not be accurate representations of the true numbers (Melamed 2014). Many scholars use World Bank Data for their studies and World Bank Data is generally considered to be a reliable database.
The Polity IV dataset contains coded data on the governments of nation-states. The Polity IV dataset is widely employed in academic study. The Polity dataset is operated by a not-for-profit research institution that maintains data collection protocols that are available for review. The same is true for the UCDP/PRIO Armed Conflict Dataset. As these datasets are widely employed, it is more likely that any reliability errors they may have contained have been identified and rectified. The Global Media Freedom Dataset (GMFD) was compiled for an academic study. As it does not appear to be as widely used as other datasets (such as the Freedom House’s Freedom of the Press), it may not have been subjected to similar scrutiny by academics.

The dataset on surveillance laws collected for this study may not be comprehensive. Searches were only conducted in English. Searches conducted in the native language of a country could result in additional surveillance laws being identified. Many states do not publish documents online. In some states, laws can be a patchwork, making it more challenging for researchers to identify relevant statutes. Searches were conducted using open sources. The use of legal subject matter experts for each country in the study could improve completeness.

Validity is a measure of the study’s ability to test the phenomenon under examination. Testing the independent variable against both terrorist attacks and the number of individuals killed increases the internal validity of terrorism as a phenomenon. If only attacks or the number of individuals killed were tested, richness in the results may be lost. The control variables selected have been scrutinized and used by academic scholars in past studies (Eyerman 1998; Li and Schaub 2004; Li 2005; Piazza and Walsh 2010). The Polity IV variable has been criticized by Treier and Jackman (2008), who believe that the precision of the polity scale could be improved. As the democracy of the nation is not the primary focus of my work, I do not believe
this criticism impacts the validity of my study. Employing these variables assists the study’s validity and has the benefit of testing to see whether similar results are seen.

One problem with the validity of the study is the reality that some countries have not developed laws that specifically restrict the government’s surveillance activities. It is almost certain these countries are conducting surveillance, yet their activities are not captured in the variables measuring surveillance laws. The countries where no surveillance laws were found are Afghanistan, Cameroon, Iran, Iraq, Kuwait, Myanmar, Nepal, Nigeria, Paraguay, United Arab Emirates, Uzbekistan, and Yemen.

This study also employs a non-random sample that weakens external validity. The countries selected for the sample represent the largest countries in the world with the most capability as measured by GDP. Strong external validity would allow the results of this study to be generalized to other countries in the world. These results should not be generalized to countries that are smaller and have fewer resources. The study is also limited to quantitative research. Qualitative case studies could provide more detail and explore interesting components of the relationship between surveillance law and counterterrorism policy.

In this chapter I presented an overview of the methodology I employed for this study. The conceptual relationship between terrorism and counterterrorism is negative. As counterterrorism increases I expect to see terrorism decrease. As countries adopt electronic surveillance laws, as a component of their countetops activity, I expect to see terrorism decrease. Using a negative binomial regression allows the use of count data for terrorist attacks and the number of individuals killed in terrorist attacks. I build a model using country name (country_txt), year (iyear), population (population), terrorist attacks (attacks), number of individuals killed in terrorist attacks (nkill), terrorism surveillance law adopted (slaw), terrorism surveillance law
adapted in any previous year (slaw1), total surveillance laws (aslaw), polity score (polity2),
primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2),
media freedom (mediascore), Gross Domestic Product (gdp), and Gross Domestic Product Log
(gdplog) variables. To develop the dataset I used a number of readily available datasets, GTD,
World Bank, Polity, etc, and a novel dataset on electronic surveillance law created specifically
for this study. I ran both fixed and random effects models to identify which one is a better fit. A
Hausman test was used to determine if fixed or random effect was the preferred regression
approach. In the final section of the chapter I provide commentary on the reliability, validity and
limitations of the study. These data are generally reliable. The study does not have strong
external validity however generalizing to smaller countries with less terrorist activity is not the
purpose of this study. In the next chapter I present the descriptive and inferential statistics and
the related analysis.
Chapter 4: Analysis

In this section, I provide a descriptive analysis of the study dataset and then present the results of the multivariate negative binomial panel regression models. The descriptive analysis presents the measures of central tendency and variability for the data in the study. The panel-regression models provide insight on the relationship between electronic surveillance law and terrorist attacks and electronic surveillance law and the number of individuals killed in terrorist attacks.

Descriptive Statistics

The dataset for this analysis contains 98 countries with populations over one million in 2016. The world population in 2016 was 7,442 billion (World Bank 2018b). The total sample population in 2016 was 6.816 billion, or 91.6% of the world’s population. The world’s GDP in 2016 was 75.848 trillion US dollars World Bank (2017). The total sample GDP in 2016 was 66.765 trillion, or 87% of the world’s population. During the period 1970 to 2016, the 98 countries in the sample experienced 149,837 terrorist attacks. The total attacks for the 205 countries in the Global Terrorism Database were 170,350.
Table 7 Summary of World and Sample Population, GDP, Terrorist Attacks, and People Killed in Terrorist Attacks

<table>
<thead>
<tr>
<th>Measure</th>
<th>World</th>
<th>Sample</th>
<th>Per cent of World</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>205</td>
<td>98</td>
<td>47.8% *</td>
</tr>
<tr>
<td>Population</td>
<td>7,442 Billion</td>
<td>6.816 Billion</td>
<td>91.6% *</td>
</tr>
<tr>
<td>GDP</td>
<td>75.848 Trillion USD</td>
<td>66.765 Trillion USD</td>
<td>88% *</td>
</tr>
<tr>
<td>Terrorist Attacks</td>
<td>170,350</td>
<td>149,837</td>
<td>87.9% †</td>
</tr>
<tr>
<td>People Killed in Terrorist Attacks</td>
<td>383,554</td>
<td>328,765</td>
<td>85.7% †</td>
</tr>
</tbody>
</table>

* 2016
† 1970 - 2016

The 98 countries in this dataset experienced 88% of the terrorist attacks recorded in the GDT from 1970-2016. During this same time a total of 383,554 people were killed in terrorist attacks. In the 98 countries in the sample, a total of 328,765 (85.7% of the total) people were killed in terrorist attacks. The frequency of terrorist attacks and number of people killed from 1970 to 2015 over time is presented in Figure 2 Terrorist Attacks and People Killed 1970 to 2016.

As seen in Table 8 Sample Characteristics Mean, Standard Deviation, and Range the population mean for the sample countries is 52.3 million. The average number of terrorist attacks is 32.65 per country per year. An average of 71.64 people is killed each year in each country. There are, on average, .11 attacks and .23 people killed per 100,000 each year. In Table 8, the mean, standard deviation, and range for attacks, attacks per capita, people killed, and people killed per capita are displayed.
Figure 2 Terrorist Attacks and People Killed 1970 to 2016
This study identified 264 separate electronic surveillance laws enforced by the 98 countries in the sample. Of the 98 countries in the survey, 86 (87.7%) have at least one law governing electronic surveillance. As mentioned in the previous chapter, the countries where no surveillance laws were found are Afghanistan, Cameroon, Iran, Iraq, Kuwait, Myanmar, Nepal, Nigeria, Paraguay, United Arab Emirates, Uzbekistan, and Yemen. Examining the sample by regime type, democracies enacted 204 (78%), anocracies 37 (14%), and autocracies 21 (8%) of the 264 electronic surveillance laws identified. As seen in Figure 3, the number of surveillance laws increased slowly until the late 1980s and then more quickly from 1990 to 2016.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Mean</th>
<th>SD</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>52390009</td>
<td>152872763</td>
<td>1378555486</td>
</tr>
<tr>
<td>Terrorist Attacks</td>
<td>32.65</td>
<td>153.94</td>
<td>3926.00</td>
</tr>
<tr>
<td>People Killed in Terrorist</td>
<td>71.64</td>
<td>463.51</td>
<td>13079.00</td>
</tr>
<tr>
<td>Attacks Per Capita</td>
<td>0.11</td>
<td>0.47</td>
<td>11.22</td>
</tr>
<tr>
<td>People Killed in Terrorist</td>
<td>0.23</td>
<td>1.53</td>
<td>37.36</td>
</tr>
<tr>
<td>Attacks Per Capita</td>
<td></td>
<td></td>
<td>n=98</td>
</tr>
</tbody>
</table>

This study identified 264 separate electronic surveillance laws enforced by the 98 countries in the sample. Of the 98 countries in the survey, 86 (87.7%) have at least one law governing electronic surveillance. As mentioned in the previous chapter, the countries where no surveillance laws were found are Afghanistan, Cameroon, Iran, Iraq, Kuwait, Myanmar, Nepal, Nigeria, Paraguay, United Arab Emirates, Uzbekistan, and Yemen. Examining the sample by regime type, democracies enacted 204 (78%), anocracies 37 (14%), and autocracies 21 (8%) of the 264 electronic surveillance laws identified. As seen in Figure 3, the number of surveillance laws increased slowly until the late 1980s and then more quickly from 1990 to 2016.
Inferential Statistics

In this section, I detail the results of the multivariate panel fixed-effects negative binomial regression. For each hypothesis, the dependent variables terrorist attacks (attacks) and number of individuals killed in terrorist attacks (nkill) are tested separately.

H1: The presence of electronic surveillance laws decreases terrorist attacks.

To test “H1: The presence of electronic surveillance laws decreases terrorist attacks,” the dependent variable terrorist attacks (attacks) was regressed upon the independent variables of terrorism surveillance law (slaw1), polity score (polity2), primary party in an armed conflict
(conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), and Gross Domestic Product Log (gdblog). As seen in Table 9 H1 Fixed-Effects Negative Binomial Panel Regression Electronic Surveillance Law on Terrorist Attacks the coefficient for (slaw1) is significant at the alpha level of .05. The coefficient for (slaw1) is negative, indicating that countries with a surveillance law are predicted to have fewer attacks than those without a surveillance law.

Table 9 H1 Fixed-Effects Negative Binomial Panel Regression Electronic Surveillance Law on Terrorist Attacks

| attacks      | Coef.  | Std. Err. | z      | P>|z|  | [95% Conf. Interval] |
|--------------|--------|-----------|--------|-------|----------------------|
| slaw1        | -.1605759 | .0517048 | -3.11  | 0.002 | -.2619155 to -.0592363 |
| polity2      | .0419026  | .0047398  | 8.84   | 0.000 | .0326127 to .0511924  |
| conflict     | .8455846  | .0511818  | 16.52  | 0.000 | .74527 to .9458991    |
| conflict2    | -.0105522 | .058547   | -.18   | 0.857 | -.1253023 to .1041979 |
| mediascore   | .0271995  | .0418506  | .065   | 0.516 | -.0548262 to .1092252 |
| gdblog       | .3744862  | .0361091  | 10.37  | 0.000 | .3037137 to .4452587  |
| _cons        | -.5.292663 | .4096203 | -12.92 | 0.000 | -.6.095504 to -4.489822 |

The coefficient for polity score (polity2) is significant and positive; indicating that a higher polity score is associated with a greater number of predicted terrorist attacks. The coefficients for primary party in an armed conflict (conflict), and Gross Domestic Product Log (gdblog) are also significant and positive, indicating higher scores on these measures are

---

1 To interpret identify the P>|z| column and check if the variable score is less than .05
associated with an increase in the predicted number of terrorist attacks. The coefficients for country supporting an armed conflict (conflict2) and media freedom (mediascore) are not significant, indicating they have no predictive power with respect to the number of terrorist attacks.

Table 10 H1 Fixed-Effects Negative Binomial Panel Regression Electronic Surveillance Law on Terrorist Attacks Incident Rate Ratios

| attacks   | IRR      | Std. Err. | z      | P>|z|   | [95% Conf. Interval] |
|-----------|----------|-----------|--------|------|----------------------|
| slaw1     | 0.8516532| 0.0440346 | -3.11  | 0.002| .7695761 - .942484   |
| polity2   | 1.042793 | 0.0049426 | 8.84   | 0.000| 1.03315 - 1.052525   |
| conflict  | 2.329339 | 0.1192198 | 16.52  | 0.000| 2.10701 - 2.575128   |
| conflict2 | 0.989533 | 0.0579325 | -0.18  | 0.857| .8822302 - 1.10982   |
| mediascore| 1.027573 | 0.0430045 | 0.65   | 0.516| .9466497 - 1.115413  |
| gdplag    | 1.454244 | 0.0525114 | 10.37  | 0.000| 1.354081 - 1.560894  |
| _cons     | 0.0050284| 0.0020597 | -12.92 | 0.000| .0002253 - .011226   |

The coefficients presented in Table 9 are interpreted as a difference between the logs of expected count values and are somewhat difficult to interpret. By exponentiating the coefficients an Incident Rate Ratio is generated that is easier to interpret. Reviewing Table 10 we can estimate that if a country adopts at least one electronic surveillance law their rate of terrorist attacks would be expected to decrease by a factor of .851 while holding all other variables in the model constant. If a country had a rate of 100 attacks per year, we can predict that it would lower its rate to 84 attacks per year with the introduction of electronic surveillance law and the related government capability. The evidence is consistent with H1 that the presence of electronic surveillance laws is associated with a decreased number of terrorist attacks.
**H2: The presence of electronic surveillance laws decreases terrorist attacks.**

To test “H2: The presence of electronic surveillance laws decreases terrorist attacks,” the dependent variable *number of individuals killed in terrorist attacks* (nkil) was regressed upon the independent variables of *terrorism surveillance law* (slaw1), *polity score* (polity2), *primary party in an armed conflict* (conflict), *country supporting an armed conflict* (conflict2), *media freedom* (mediascore), and *Gross Domestic Product Log* (gdplog). As seen in Table 11 H2 Fixed-Effects Negative Binomial Panel Regression Electronic Surveillance Law on Number of Individuals Killed in Terrorist Attacks Incident Rate Ratios the coefficient for (slaw1) is not significant at the .05 alpha. This indicates that the presence of at least one surveillance law in a country does not have predictive power with respect to the number of individuals killed in terrorist attacks.

**H3: The greater the electronic surveillance capability a country has the fewer terrorist attacks it will experience.**

To test “H3: The greater the electronic surveillance capability a country has the fewer terrorist attacks it will experience,” the dependent variable *terrorist attacks* (attacks) was regressed upon the independent variables of *total terrorism surveillance law* (aslaw), *polity score* (polity2), *primary party in an armed conflict* (conflict), *country supporting an armed conflict* (conflict2), *media freedom* (mediascore), and *Gross Domestic Product Log* (gdplog). As seen in Table 12, the coefficient for (aslaw) is significant at the .05 alpha level.
Using Table 12, we can estimate that if a country adopts additional electronic surveillance laws their rate of terrorist attacks would be expected to decrease by a factor of .926 while holding all other variables in the model constant. The evidence is consistent with H3, that the presence of additional electronic surveillance laws decreases the number of terrorist attacks.

**H4: The greater the electronic surveillance capability a country has, the fewer fatalities from terrorist attacks it will experience.**

To test “H4: The greater the electronic surveillance capability a country has the fewer individuals will be killed in terrorist attacks” the dependent variable number of individuals killed in terrorist attacks (nkill) is regressed upon the independent variables total terrorism surveillance law (aslaw), polity score (polity2), primary party in an armed conflict (conflict), country supporting an armed conflict (conflict2), media freedom (mediascore), and Gross Domestic Product Log (gdpplog). As seen in Table 13, the coefficient for (aslaw) is significant at
the .05 alpha level. Using Table 11, we can estimate that if a country adopts additional electronic surveillance laws their rate of individuals killed in terrorist attacks would be expected to decrease by a factor of .909 while holding all other variables in the model constant. The evidence is consistent with H4, that the presence of additional electronic surveillance laws decreases the number of individuals killed in terrorist attacks.

Table 12 H3 Fixed-Effects Negative Binomial Panel Regression Total Electronic Surveillance Law on Terrorist Attacks Incident Rate Ratios

<table>
<thead>
<tr>
<th></th>
<th>Number of obs = 3,956</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group variable:</td>
<td>country1</td>
</tr>
<tr>
<td>Obe per group:</td>
<td></td>
</tr>
<tr>
<td>min =</td>
<td>12</td>
</tr>
<tr>
<td>avg =</td>
<td>41.2</td>
</tr>
<tr>
<td>max =</td>
<td>47</td>
</tr>
</tbody>
</table>

Wald chi2(6) = 557.82
Log likelihood = -10609.909
Prob > chi2 = 0.0000

| attacks        | IRR      | Std. Err. | z      | P>|z| | [95% Conf. Interval] |
|----------------|----------|-----------|--------|------|----------------------|
| aslaw          | .9256886 | .016022   | -4.46  | 0.000 | .8948127 .95763      |
| polity2        | 1.042125 | .004909   | 6.76   | 0.000 | 1.032547 1.05179     |
| conflict       | 2.293921 | .1175047  | 16.21  | 0.000 | 2.0748 2.536184      |
| conflict2      | 1.092434 | .0698847  | 1.40   | 0.161 | .9654322 1.236143    |
| mediascore     | 1.031314 | .0431095  | 0.74   | 0.461 | .9501895 1.119365    |
| gdplog         | 1.502748 | .0563123  | 10.87  | 0.000 | 1.396334 1.617273    |
| _cons          | 0.0034714| .0014784  | -13.30 | 0.000 | 0.0015065 0.0079988  |
The statistical results support three of the four hypotheses. The presence of electronic surveillance laws decreases the frequency of attacks—holding the other variables constant. The presence of any electronic surveillance law does not allow for the prediction of the number of individuals killed in terrorist attacks. We can predict that a country that relaxes its institutional constraints and increases electronic surveillance laws and capability it will see fewer attacks and numbers of people killed.

The statistical results indicate that there is a relationship between regime type, number of terrorist attacks, and number of individuals killed. In each Incident Rate Ratio table, the variable for regime type (polity2) is significant. As seen Table 10 if a country were to increase their polity score by one unit their rate of attacks would be expected to increase by a factor of 1.04.
The models developed for this study do not support the substantial increase in rates of attacks predicted by other scholars.

The role of a primary party in an armed conflict (conflict) is significant in all four models. As seen in Table 10, if a county is a primary party in a conflict their rate of attacks is expected to increase by a factor of 3.59 while holding all other variables in the model constant. The models in this study indicate that governments involved in conflict are likely to experience challenges from terrorist events at a much higher rate than countries are not the primary party in a conflict.

The Gross Domestic Product control variable (gdplog) results do not align with evidence from previous studies. Li and Schaub find that the “level of economic development of a country, measured by real GDP per capita, reduces the number of transnational terrorist incidents in a country” (Li and Schaub 2004, 232). The models in this study associate Gross Domestic Product (gdplog) positively with terrorism. As seen in Table 10, a country that increases the log value of GDP (GDPLog) by one unit is expected to see a their rate of attacks increase by a factor of 1.43 while holding all other variables in the model constant. One possible reason for this discrepancy is the use of the GTD in this study and the use of the International Terrorism: Attributes of Terrorist Events (ITERATE) dataset by Li and Schaub. The ITERATE dataset is focused on “transnational terrorist events that occur in a country in a year” (Li and Schaub, 239).

From the year 1970 to 2016, the nation-states included in this sample enforced and adopted at least 264 electronic surveillance laws. To date, evidence concerning this impact has been limited. The results of the multivariate negative binomial fixed-effects panel-data models demonstrate a negative relationship between electronic surveillance law and terrorist attacks and the number of individuals killed in terrorist attacks. By investigating the relationship between
electronic government surveillance and terrorism, a deeper understanding of the impact that counterterrorism policy may have is revealed.
Chapter 5: Surveillance Laws for Counterterrorism in Pakistan, the United Kingdom, and the United States

In the previous chapter, I used a negative binomial panel regression model to demonstrate that there are fewer terrorist attacks and fewer individuals killed in such attacks in countries with electronic surveillance laws. I define national security electronic surveillance narrowly, as the acquisition by an electronic, mechanical, or other surveillance device of the contents of any electronic communication without the consent of any party involved in the communication. In this chapter, I analyze this issue in three countries that have adopted electronic surveillance laws: Pakistan, the United Kingdom, and the United States.

Attacks Per Capita as a Measure

An additional measurement is useful when comparing rates of terrorism between countries. The measure is per capita, meaning per person. Per capita is often used by statisticians when comparing two variables that involve people.²

Using the dataset developed for this study, we can see in Table 14 the raw counts of terrorist attacks for Pakistan, the United Kingdom, and the United States. Sorting by the number of terrorist attacks from 1970 to 2016 shows that Pakistan experienced the most, with a total of 13,734. On average, Pakistan experienced 292 attacks per year. Similarly, with the raw count of the number of individuals killed in terrorist attacks, Pakistan experienced the most deaths from

---

² Per capita is calculated by taking a measure and dividing it by a given population. For example, the number of attacks in a country per year may be divided by the population of the country in that year to get a per-capita measure. This statistic is often multiplied by 100,000 to give a rate per 100,000 people. The reason I use per-capita measures is that using the raw values may be misleading. If country A has 500 terrorist attacks per year and country B has 1,000, it appears that country A has less terrorism. It is important to consider population, however. If country A has 500 terrorist attacks per year and a population of 1 million, its per-capita statistic is .0005. Multiplied by 100,000, the number of terrorist attacks per capita for country A is 50 per 100,000 people. If country B experiences 1,000 terrorist attacks per year and a population of 10 million, its per-capita statistic is .0001. Multiplied by 100,000, the terrorist attacks per capita for country B is 10 per 100,000. The rate of terrorist attacks in country A is thus actually five times higher than in country B.
1970 to 2016, with a total of 22,962. The average number of individuals killed in Pakistan per year is 489.

Table 14 Terrorist Attacks and Individuals Killed: Raw Count and Mean Per Year

<table>
<thead>
<tr>
<th>Country</th>
<th>Terrorist Attacks</th>
<th>Mean Attacks per Year</th>
<th>Individuals Killed in Terrorist Attacks</th>
<th>Mean Killed per Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pakistan</td>
<td>13734</td>
<td>292</td>
<td>22962</td>
<td>489</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>5157</td>
<td>110</td>
<td>3370</td>
<td>72</td>
</tr>
<tr>
<td>United States</td>
<td>2786</td>
<td>59</td>
<td>3669</td>
<td>78</td>
</tr>
</tbody>
</table>

As seen in Table 15, the calculation of the per-capita rates reveals that the United Kingdom experienced slightly more attacks per 100,000 than the other countries in this table. When comparing incidents of terrorism it is important that researchers use comparable metrics.
Table 15 Terrorist Attacks and Individuals Killed: Raw Count and Mean Per Capita

<table>
<thead>
<tr>
<th>Country</th>
<th>Terrorist Attacks</th>
<th>Mean Attacks per Capita</th>
<th>Individuals Killed in Terrorist Attacks</th>
<th>Mean Killed per Capita</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>5157</td>
<td>0.19</td>
<td>3370</td>
<td>0.13</td>
</tr>
<tr>
<td>Pakistan</td>
<td>13734</td>
<td>0.18</td>
<td>22962</td>
<td>0.30</td>
</tr>
<tr>
<td>United States</td>
<td>2786</td>
<td>0.03</td>
<td>3669</td>
<td>0.03</td>
</tr>
</tbody>
</table>

Pakistan

From 1970 to 2016, Pakistan experienced 13,734 terrorist attacks (.18 per 100,000). There were 22,962 people killed in terror attacks (.3 per 100,000) from 1970 to 2016 in Pakistan. The Pakistani constitution of 1973 articulates a right to privacy, stating that “the dignity of man and, subject to law, the privacy of the home, shall be inviolable” (National Assembly of Pakistan 2012, 10). Thus we would assume that Pakistani lawmakers created laws to let government officials to conduct electronic surveillance legally for national security purposes. Instead, the military and government used surveillance with little oversight until the early 1990s (Khan 2017). The 1994 Telecommunications Act provided the federal government the ability to “authorize any person or persons to intercept calls and messages or to trace calls through any telecommunication system” (National Assembly Secretariat 2006, 40).
As Figure 4 illustrates, from the mid-1980s to the early 2000s, Pakistan experienced fewer terrorist attacks than during other periods. It appears that two issues prompted the adoption of the subsequent 2013 Investigation for Fair Trial Act and the 2016 Prevision of Electronic Crime bills that both increase government electronic surveillance power. The 1996 Telecommunications Act was not accompanied by a similar restricting of the criminal code in Pakistan. Thus, when electronic surveillance was used by police to identify and apprehend terrorist suspects, their legal teams were able to use non-legal documents, such as email and other electronic communications, as they were considered inadmissible in court (Mir 2017; Hameed 2015). The 2013 Investigation for Fair Trial Act specifically “empowers intelligence and law enforcement agencies to conduct surveillance and interception of electronic and cellular phone communication for the purposes of any investigation into an offense” (Hameed 2015, 3). The 2013 act covers many types of electronic surveillance data, including “data, information or material in any documented form,
whether written, through audio visual device [sic], CCTV, still photography, observation or any
other mode of modern devices or techniques” (Pakistan Senate Secretariat 2013, 3).

The 2016 Prevention of Digital Crimes Act seems to have been a reaction to the 2014
Peshawar school massacre, in which 141 individuals were killed (BBC 2014). International
media coverage and opinion pieces in Pakistan’s national media put pressure on the government
and likely forced electronic surveillance onto the political agenda (Rana 2014). Another force
that may have contributed to the new electronic surveillance is Pakistan’s improved
understanding of what it can accomplish. Following the September 11 attacks, the United States’
National Security Agency (NSA) and Britain’s Government Communications Headquarters
(GCHQ) became deep partners with Pakistan in the conduct of electronic surveillance.

The NSA and GCHQ are two of the most sophisticated communications intelligence
organizations in the world. Documents leaked illegally by Edward Snowden reveal that Pakistan
is an approved signal intelligence partner with the NSA. The partnerships involve sharing of
technology and conducting surveillance (Greenwald 2014). Based on leaked GCHQ documents,
they had “access to almost any user of the internet inside Pakistan” (Government
Communications Headquarters 2008). In 2013, the Pakistani Inter-Services Intelligence (ISI)
sought a mass surveillance system similar to those used by the United States and United
Kingdom. The system would give Pakistan the capability to “collect and analyze a significant
portion of communications” within and through the country at a “centralized command center”
(Privacy International 2015, 1).

Pakistan’s adoption of electronic surveillance laws highlights this theme across
countries. In the period from 1970 to the early 1990s, countries adopted electronic surveillance
laws primarily to address telephone and early digital technologies. As digital and internet-related
communication technologies proliferated in the late 1990s and through the early twenty-first century, countries debated and adopted additional electronic surveillance laws. The importance of internal and external communications is an important takeaway from the Pakistani case. With three undersea international telecommunications cables that land in Pakistan, the government is likely very interested in exploiting them for counterterrorism. The experience in tool and techniques gained from Pakistan’s partnership with the NSA and GCHQ likely prompted the development of a system to access the three undersea international cables in addition to purely domestic electronic surveillance (Privacy International 2015).

**United Kingdom**

From 1970 to 2016, the United Kingdom experienced 5,157 terrorist attacks (.19 per 100,000). There were 3,370 people killed in terror attacks (.12 per 100,000) from 1970 to 2016 in the United Kingdom. The number of attacks per capita in the United Kingdom (.19 per 100,000) is similar to that of Pakistan (.18 per 100,000). The number of killed per capita in the United Kingdom (.13 per 100,000), however, is slightly less than a factor of 2 lower than Pakistan’s rate (.30 per 100,000). As seen in Figure 5, there is variation in the number of attacks in the United Kingdom from 1970 through 2016.

British authorities gained counterterrorism experience from combating the terrorist activities of the Irish Republican Army (IRA). One consequence of the struggle with the IRA is a cooperative interagency approach, in which federal and local resources are used to interdict terrorist plans. Miller (1993, 22) notes that a Director and Coordinator for Intelligence, responsible to the Secretary of State for Northern Ireland, was responsible for “coordinating the efforts of all intelligence agencies, both Army and police, in their work against terrorism.”
The Regulation of Investigatory Powers Act 2000 (RIPA) is the principle law that allows the United Kingdom’s intelligence and security agencies to collect electronic surveillance data. Their ability to collect data is constrained by the Human Rights Act 1998, which incorporates the European Convention on Human Rights into U.K. law. The interception the security agencies conduct falls into two categories: investigatory and discovery. Investigatory interception occurs when an individual is identified as a threat. They may be targeted for communications and data interception following the demonstration of necessity and proportionality to the Secretary of State (United Kingdom 2000).

Discovery, or intelligence gathering, is conducted to search for threats that have not been identified with a person for investigation. Discovery collection is conducted on external communications. At least one end of the communications must be outside of the United Kingdom. Data streams containing communications traffic are monitored or mirrored and selectors are used to pull data of interest. Selectors are keywords, terms, telephone numbers, email addresses, internet protocol addresses, and other identifiers. The data is presented to analysts, who determine the priority and which of the data is processed and read by humans under specific legal conditions.

The communications of people in the United Kingdom are categorized as internal communications; the security agencies must therefore have a targeted interception approval to collect or read any communication. If one of the individuals is overseas, the security agencies may collect and examine the communication as long as their reason for doing so is permitted by law.
The United Kingdom Intelligence and Security Committee of Parliament wrote in 2015 that the electronic surveillance conducted is necessary and proportionate. The committee “examined cases which demonstrate that this capability has been used to find communications indicating involvement in threats to national security” (Intelligence and Security Committee of Parliament 2015, 5). The committee writes that “interception has exposed previously unknown threats or plots which threatened our security that would not otherwise have been detected” (Intelligence and Security Committee of Parliament 2015, 5).

Attacks such as the 2013 death of The Fusilier Lee Rigby by radicalized British citizens continued to stimulate political debate on increasing government surveillance capability. The independent report on Rigby’s death notes that one of the few ways the attack could have been prevented is if the government had had the capability to link the data from a foreign communications service provider with one of the two perpetrators, Michael Adebowale.
(Intelligence and Security Committee of Parliament 2014, 7). In the 2012 exchange, intercepted by GCHQ, Adebowale told an overseas individual that he intended to kill a soldier (Intelligence and Security Committee of Parliament 2014). GCHQ did not know who the unidentified individual (Adebowale) was until later. To address the limitation in the internal/discovery collection, the United Kingdom proposed update surveillance legislation in 2016.

The Investigatory Powers Act of 2016 gives the three United Kingdom intelligence services unprecedented powers to conduct electronic surveillance and analyze the data for national security and criminal purposes. The United Kingdom’s government commissioned an independent review of the Investigator Powers Act 2016. The 2016 act defines bulk surveillance as “the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information” (Anderson 2016, 3). The review used case studies to demonstrate that there were some cases in which there is “no possible alternative” except surveillance for collecting the necessary intelligence to identify threats (Anderson 2016, 88). The report finds that:

Privacy is not simply an interest to which public authorities must have regard, but a right into which intrusions will be countenanced only on tightly specified conditions… the use of bulk powers should only be countenanced if there is a compelling operational case for their use, and if their use is subject to adequate and visible safeguards (Anderson 2016, 121).

The United Kingdom’s laws on electronic surveillance, like in Pakistan, developed to relax privacy restraints on the government. As digital internet enabled technologies are adopted by civil society, governments react with laws that allow their security forces the legal freedom to gather intelligence via electronic surveillance. As noted in government produced investigation of terrorist events there are some attack where the only way they could be identified beforehand was by electronic surveillance. Both Pakistan and the United Kingdom are unique in that they have undersea cables that allow them to gather data on external threats to complement their
domestic collection (Privacy international 2016). It is likely that the electronic surveillance laws have resulted in security agencies increasing their technical capability to scan for terrorist threats. The United States was confronted by the limitations of its electronic surveillance on September 11, 2011.

**United States**

From 1970 to 2016, the United States experienced 2,786 terrorist attacks (.03 per 100,000). There were 2,786 people killed in terror attacks (.03 per 100,000) from 1970 to 2016 in the United States. As Figure 6 illustrates, beginning in the mid-1970s, terrorist attacks generally declined in the United States. On September 11, 2001 President Bush was certain that he had witnessed the deaths of more Americans civilians than any other president in history. The White House, Congress, and many government facilities were evacuated. Michael Hayden, director of the NSA, ordered the evacuation of all non-essential personal from NSA headquarters in Fort Meade, Maryland. The Secret Service moved Vice President Dick Cheney to a cold war bunker hardened to withstand nuclear attacks.

Immediately following the attacks, the President and his executives lacked information. President Bush noted that when they received information, it was often contradictory or wrong (Bush 2011). Kirk Wiebe, a senior analyst at the NSA, noted that “everybody had the TV on because the TV is where the news was. It wasn’t coming out of NSA’s computers, it was on the TV, because we had missed the entire event” (PBS 2015). A surprise attack with 2152 Americans civilians dead occurred without any warning from the intelligence community (9/11 Commission Report).
Until 1973, the NSA collected intelligence, both foreign and domestic, with limited oversight. When Director of Central Intelligence James Schlesinger attempted to brief a United States Senator, the senator replied: “No, no, my boy, don’t tell me. Just go ahead and do it, but I don’t want to know!” (Johnson 2018, Kindle locations 8678–8679). The electronic surveillance data collected by intelligence agencies put them in direct violation of the Fourth Amendment. The Fourth Amendment reads: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (United States Constitution 1789). In 1973, the Supreme Court unanimously ruled that the government must obtain warrants to conduct domestic intelligence collection to comply with the Fourth Amendment (Michigan Law Review 1980).
The same year, a Senate committee, led by Frank Church, revealed that the NSA and other intelligence organizations, including the Federal Bureau of Investigation (FBI), were involved in substantial domestic surveillance activities. The committee reported that the NSA program to collect domestic communications traffic “certainly appears to violate section 605 of the Communications Act of 1934 as well as the Fourth Amendment of the Constitution” (Epsley-Jones and Frenzel 2007). Senator Church said the government could turn the NSA capability “around on the American people, and no American would have any privacy left, such as the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide” (Greenwald 2013).

While President Ford agreed his administration would cooperate, his Deputy Chief of Staff Dick Cheney led an effort to blunt the efforts of the Church Committee. For example, “lists of records to which the Church committee requested access for its investigation were reviewed in detail and Mr. Cheney ultimately decided whether to provide them in each case” (Prados and Jimenez-Bacardi 2015). The Church Committee recommended that the intelligence community be brought under congressional and judicial oversight. These recommendations led to the 1978 Foreign Intelligence Surveillance Act (FISA).

FISA created the Foreign Intelligence Surveillance Court (FISC) to approve or deny applications made by the government for electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes. Media revelations of NSA illegal activity, the Church Committee’s investigations, and the creation of the FISA and the FISC led to cultural change inside the NSA. The NSA became a risk adverse culture (Frontline 2015). The agency was extremely careful to make decisions that would not put it in jeopardy with the congressional and legal entities that oversaw its activities.
Immediately following the 9/11 attacks, the administration was under great pressure to try to stop another attack. Remarking that “we had had terrorists living in this country for a number of months and we didn’t know about it,” White House Counsel Alberto Gonzales asked, “What else didn’t we know?” (PBS 2015). Inside the White House and the intelligence community, a concern arose that they could not connect the dots if they could not collect the dots. Right after his evacuation, due to the 9/11 attacks, Vice President Cheney contacted his attorney, David Addington. He directed Addington to develop a case for expanding executive power to give the president the maximal amount of options when dealing with the crisis.

Addington worked with presidential staff in the Roosevelt Room considering the legislative authorities the President could use in the future (Cheney 2011). Further, the vice president directed Director of Central Intelligence (DCI) George Tenet to develop a wish list of activities it wanted to do, but was prohibited from doing by existing interpretations of the law. Director Tenet called NSA Director Michael Hayden. Hayden recalls the conversation as:

DCI Tenet: “Mike, any more you can do?”
NSA Director Hayden: “George, no, not within my authorities, not within my current authorities.”
DCI Tenet: “That’s not actually the question I asked you. Is there anything more you could do?”
NSA Director Hayden: “I’ll get back to you” (PBS 2015).

The NSA used the United States unique geographic position to tape undersea communications cables for intelligence (Frontline 2015). What it did not have access to was domestic communications. The NSA worked to develop a plan to aggressively collect intelligence from all data sources to try to detect terrorist activity. The plan the NSA director proposed would collect phone call and internet traffic data on hundreds of millions of Americans.

President Bush officially created “the Program” by signing a secret presidential order in the presence of Vice President Cheney on October 4th, 2001 (PBS 2015). The order was
considered so secret that only two copies of it existed. One copy was provided to the NSA, hand-
carried by Vice President Cheney’s attorney, David Addington, and delivered to NSA Director 
Hayden. The White House copy was kept in Addington’s safe in an office outside the White 
House grounds. “The Program” was one of the United States government’s most highly 
classified programs. Attorney General Gonzales stated that the President alone made the decision 
on who could be “read in” to the program (PBS 2015).

A significant issue with the President’s Surveillance Program was its legality. In the years 
following its implementation, and as more people became aware of its existence in the Justice 
Department, certain collection actions were deemed problematic by Justice Department lawyers 
(Frontline, 2015). In response the President’s Surveillance Program was later revised and 
incorporated into overt law in the FISA Amendments Act of 2008.

The United States adopted another law that increased government surveillance in 2001. 
The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept 
and Obstruct Terrorism (USA PATRIOT Act) became public law on October 26, 2001 (United 
States Congress 2001). The PATRIOT act relaxed the legal standard of probable cause for 
electronic surveillance. The U.S. Supreme Court has established that probable cause “exists 
where the facts and circumstances within the officers’ knowledge, and of which they have 
reasonably trustworthy information, are sufficient in themselves to warrant a belief by a man of 
reasonable caution that a crime is being committed” (United States Supreme Court 1949, 175). 
The PATRIOT act changes the standard for what qualifies as reasonable grounds now defined as 
sufficient information for a reasonable person to believe an individual is a danger to the national 
security of the United States (United States Attorney General 2005).
In the case of the United States the secret President’s Surveillance Program and the PATRIOT act both significantly relaxed the legal constraints for the government to conduct electronic surveillance. As Edwards Snowden’s disclosures revealed in 2013 the NSA and GCHQ partnered to build extremely sophisticated electronic surveillance capability. Further, the NSA adopted a “collect it all” approach. The director of the NSA, Keith Alexander, wanted to “more than mere snippets” every text message, phone call, email, that could be collected to allow analysis to identify terrorist threats (Greenwald 2013). This strategy portends electronic surveillance in the future. Governments will likely adopt electronic surveillance laws that allow their intelligence and law enforcement entities for counterterrorism purposes.

In this chapter I find that Pakistan, the United Kingdom, and the United States all adopted electronic surveillance laws that relaxed the legal restrictions on government intelligence agencies to collect and analyze electronic surveillance data for counterterrorism. In these cases, the laws initially adopted seemed to focus on providing the legal authority to conduct electronic surveillance that was already taking place for national security reasons. Subsequent laws seem to have been responses to terrorist attacks and changes in technology. The geographic locations of each of these three countries seem to give them the unique capability to access international communications. Pakistan, the United Kingdom, and the United States initially adopted electronic surveillance to counter national security threats such as espionage and organized crime. As terrorism becomes a primary national security threat, the laws were revised and some have specifically targeted terrorist groups.
Chapter 6: Policy Implications

The terrorist attacks of 2001 in the United States precipitated a wave of counterterrorism legislation around the world. Edward Snowden’s illegal disclosures revealed the extent that American intelligence agencies and their partners in other nation-states have succeeded in implementing mass surveillance systems. The Chinese government is experimenting with extreme measures of surveillance within its borders. Media reports indicate, for example, that Chinese citizens in Kashgar are monitored using integrated systems that include government and commercial data, electronic communications surveillance, biometrics, and closed-circuit television (Rajagopalan 2017). In states where constitutions protect the right to privacy from government intrusion, it may be harder for government to adopt policies for increased government surveillance. What seems to be missing from the debate is empirical evidence on the efficacy of electronic surveillance as a counterterrorism tool.

This study uses a unique dataset to test a hypothesis concerning the effectiveness of electronic surveillance on terrorism. The tests conducted provide evidence to support the hypothesis that the presence of electronic surveillance laws result in lower rates of terrorist attacks and the number of individuals killed in terrorist attacks. Like other scholars the country/year unit of analysis (Findley and Young 2011) in this study should provide useful information to decision makers and privacy advocates alike as they debate electronic surveillance as a counterterrorism policy. For example, metric may be developed to evaluate if the costs for counterterrorism programs derive sufficient benefits for the county.

While the evidence in this study support the hypothesis that electronic surveillance laws are negatively related to terrorist attacks and number of individuals killed in a nation state other
factors should be investigated in future research. Analysis approaches could be developed to see if coordinated group attacks are more likely to be prevented after a country adopts electronic surveillance vs. attacks by individuals. There may be variation in the package of counterterrorism policies that counties adopt. For example the ability to link communications data with CCTV, public records, travel tracking, and other surveillance activities may have far greater impact that when used in a standalone capacity. Electronic surveillance may have benefit for both defensive and offensive counterterrorism activities.

The balance between effective electronic surveillance and the privacy rights of individuals should be studied. It is likely that the tradeoffs are different for each country based on political history and other cultural norms. In democratic states the right to privacy is often guaranteed by the constitution. When this right is weakened the government gains great powers to combat terrorism but could use the same powers for political ends or to suppress dissent. As seen in the wave of public discourse that occurred after Edwards Snowden’s release of classified materials many governments have developed advanced capability. The study of these capability and individuals’ right to privacy warrant additional investigation.

These findings are a stepping stone towards a deeper understanding of electronic surveillance as a counterterrorism tool. Addition studies are required to tease out more granular findings. Several areas for further research may be explored following this study. The focus of this report is the impact of electronic surveillance law on terrorism. The policy theories of Kingdon (2010) as well as of Baumgartner and Jones (2007) postulate that the political system often requires a shock in order for a policy change to happen. The institutions that entrench themselves are resilient and deeply resistant to change. A question worth exploring is: does terrorism precipitate surveillance law? Nation-states adopt surveillance rules as national security
measures. Since the constitutions of most states protect privacy, laws are required to permit legal electronic surveillance by the government. During this study, I coded the laws that were a result of terrorism and discovered a total of 45 terrorism-related electronic surveillance laws across 29 countries. Future studies that explore the power to predict the adoption of an electronic surveillance law could be developed. One could develop, for example, a predictive model based on measures of terrorism, the existence of electronic surveillance law in a country, and other regime-based variables.

The nature of the relationship between terrorism and electronic surveillance law is complex, but it is possible that there is a positive curvilinear relationship between terrorism and government response. From point $Y$ in time, terrorism increases as a terrorist group raises the costs and risks through violence or destruction. At time $T$ the government takes counterterrorism actions, or enough counterterrorism capacity is developed, so that the terrorist activity begins to decrease. Unless the terrorists can adapt their strategy to cope with the government’s actions, the government may succeed in limiting terrorist activity. If the terrorist group is able to adapt, they may be able to increase their activity until the government again improves capacity. Perhaps terrorism may be visualized, and modeled, as a sequence of positive and negative curvilinear relationships.

One approach, to model and predict the hypothetical curvilinear relationship of terrorism, could involve the use of autoregressive integrated moving average (ARIMA) models. ARIMA is a generalization of an autoregressive moving average (ARMA) model. The Box-Jenkins methods for employing ARIMA models provide researchers with useful techniques for parameter estimation and for casting using time series data (Shumway and Stoffer 2017). Both of these
models are fitted to time series data, either to better understand the data or to predict future points in the series (forecasting).

A qualitative approach to investigate the nature of the relationship between terrorism and electronic surveillance could provide new and helpful data to broaden our understanding of counterterrorism policy. This approach was employed by Baumgartner and Jones (2007) and Kingdon (2010) to develop their Multiple Streams and Punctuated Equilibrium theories. A similar approach, applied to a sample of the twenty-nine countries that have terrorism-specific electronic surveillance laws, could generate interesting findings not generally found in quantitative studies. Are there certain categories of terrorist attacks that spur the adoption of terrorism-specific electronic surveillance laws, for example? A comparative approach could be used to analyze the nature and scope of the terrorism-specific electronic surveillance laws. The role and capability of the institutions responsible for implementing the surveillance capacity could be compared across countries. Larger, cross-national trends may provide fertile ground for investigation. It is likely that the increase in electronic surveillance laws from the early 1990s through 2016 was a reaction to the revolutionary information technologies facilitated by internet infrastructure and technical protocols. Rich case studies in these areas would improve our understanding of counterterrorism policy.

Electronic surveillance is one of the policy options governments may employ when combating terrorist groups. Public discourse often involves concerns that such programs may substantially reduce citizens' privacy while providing marginal, if any, gains against terrorists. This study provides much-needed empirical data on the impact of electronic surveillance on terrorism.
The evidence I generate—examining data from 1970 through 2016, using a multivariate negative binomial panel regression model for longitudinal data—supports a hypothesis that the presence of electronic surveillance laws and the related government surveillance capacity decreases both the incidence of terrorist attacks and the number of individuals killed in terrorist attacks. These findings complement, and may be integrated into, broader scholarly work that finds that when constraints on government institutions are relaxed, they are more effective at counterterrorism. These data provide grounds for additional study in this domain. Qualitative, comparative case studies, for example, that examine the relationship among electronic surveillance and other counterterrorism strategies in which the nation-state is the unit of analysis, could reveal an optimal mix of strategies to limit terrorist activity. This study may help inform the debate over the scope of electronic surveillance and personal privacy in nation states.
References


### Appendix 1: Countries Included in the Study

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>Greece</td>
<td>Philippines</td>
</tr>
<tr>
<td>Albania</td>
<td>Guatemala</td>
<td>Poland</td>
</tr>
<tr>
<td>Algeria</td>
<td>Hungary</td>
<td>Portugal</td>
</tr>
<tr>
<td>Argentina</td>
<td>India</td>
<td>Qatar</td>
</tr>
<tr>
<td>Armenia</td>
<td>Indonesia</td>
<td>Romania</td>
</tr>
<tr>
<td>Australia</td>
<td>Iran</td>
<td>Russia</td>
</tr>
<tr>
<td>Austria</td>
<td>Iraq</td>
<td>Rwanda</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>Ireland</td>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>Bahrain</td>
<td>Israel</td>
<td>Singapore</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Italy</td>
<td>South Africa</td>
</tr>
<tr>
<td>Belgium</td>
<td>Japan</td>
<td>South Korea</td>
</tr>
<tr>
<td>Bolivia</td>
<td>Jordan</td>
<td>Spain</td>
</tr>
<tr>
<td>Brazil</td>
<td>Kazakhstan</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Kenya</td>
<td>Sudan</td>
</tr>
<tr>
<td>Cameroon</td>
<td>Kuwait</td>
<td>Sweden</td>
</tr>
<tr>
<td>Canada</td>
<td>Latvia</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Chile</td>
<td>Lesotho</td>
<td>Syria</td>
</tr>
<tr>
<td>China</td>
<td>Lithuania</td>
<td>Tanzania</td>
</tr>
<tr>
<td>Colombia</td>
<td>Macedonia</td>
<td>Thailand</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>Malawi</td>
<td>Turkey</td>
</tr>
<tr>
<td>Cuba</td>
<td>Malaysia</td>
<td>Uganda</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Mexico</td>
<td>Ukraine</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Morocco</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>Denmark</td>
<td>Mozambique</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>Myanmar</td>
<td>United States</td>
</tr>
<tr>
<td>Egypt</td>
<td>Namibia</td>
<td>Uruguay</td>
</tr>
<tr>
<td>Estonia</td>
<td>Nepal</td>
<td>Uzbekistan</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>Netherlands</td>
<td>Venezuela</td>
</tr>
<tr>
<td>Finland</td>
<td>New Zealand</td>
<td>Vietnam</td>
</tr>
<tr>
<td>France</td>
<td>Nigeria</td>
<td>Yemen</td>
</tr>
<tr>
<td>Georgia</td>
<td>Norway</td>
<td>Zambia</td>
</tr>
<tr>
<td>Germany</td>
<td>Pakistan</td>
<td></td>
</tr>
<tr>
<td>Ghana</td>
<td>Paraguay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Peru</td>
<td></td>
</tr>
</tbody>
</table>