# National Security’s Triple Threat: Terrorists’, Spies’, and Hackers’ Converging Motivations

Beth L. Eisenfeld

Henley-Putnam School of Strategic Security

National American University

September 5, 2019

Harry I. Nimon, Doctor of Business Administration, Committee Chair

Frank G. Nolan, Juris Doctor, Subject Matter Expert

Denise D. Greaves, Doctor of Philosophy, Committee Member

Dissertation submitted in partial fulfillment of
the requirements for the degree of
Doctor of Strategic Security

While nothing is easier than to denounce the evildoer, nothing is more difficult than to understand him.

*—Fyodor Mikhailovich Dostoevsky*

## Dedication

To everyone who helped me pursue my dreams.

## Acknowledgements

*They* say it takes a village to raise a child. *They* do not tell you the same holds true for completing a dissertation before you begin the journey. Rather, *they* let you figure that out on your own. Although I am the author, it took a combination of enthusiasm and the effort of other people to help me achieve the result:

To my husband: For your encouragement and help along the way. Thanks for reminding me to eat when I became lost in my thoughts, overly focused on my computer screen, and forgot to look at the time, often skipping lunch and dinner. I appreciate you making all those lunches and dinners—and cleaning up despite our lifelong deal. To my mother and father (although he is no longer here to read this); You both guided me along life's journey and made this opportunity possible. To my in-laws, who encouraged me and helped me in ways I appreciate more than you can imagine.

To my committee: Each of you provided inspiration and insight at just the right moment, both times I embarked on this journey under your guidance. You helped me move forward from an idea to a completed research project. Dr. Nimon, your guidance made this a rewarding journey. Professor Nolan, your insights and suggestions always kept me heading in the right direction. Dr. Greaves, you provided inspiration from the first to the last class on this trek.

To the Henley-Putnam School of Strategic Security Staff: Thanks to each of you who enrolled me in the correct classes, ensured I had the proper classroom access, and took care of the little details that could have easily slipped through the cracks. I also want to thank Dr. Burke for her ear and encouragement along the way, first as a friend, and second as my program Associate Dean. We kept each other going during our respective lulls in the action. To Dr. Maye,

thank you for reviewing the terrorism data and coding processes, even though you were not officially on my committee.

To my fellow classmates: Thank you for being part of this journey. I learned something from everyone and hope in doing so I also gave back. A special shout out to Tom Fox, Kristen Hangstorfer, and Rob Jordan who served as listeners, proofreaders, and sanity checkers. Going through this process with each of you made the task easier and definitely more enjoyable than going it alone. Finally, to Todd Weiser, a classmate from the beginning of this journey who stuck with me as a peer reviewer, even though we wound up at different schools. Life is a team sport.

# Abstract

The actions of terrorists, spies, and hackers represent, with increasing frequency, national security's triple threat. The nefarious actions of these actors are converging and blurring to become a multi-faceted threat. Sometimes it is difficult to differentiate between the motives of a traditional spy and one that commits espionage by hacking or a terrorist using cyber methods to frighten the populace and cripple a country's economy. The discourse on these actors is diverse; researchers narrowly focus on each actor independently, rarely if ever, assessing the significance of the triple threat. This research explores the motives of national security's triple threat. If researchers can identify the similarities and differences between the motives of terrorists, spies, and hackers to develop recognizable patterns, then United States counterterrorism specialists can develop tactics, techniques, and procedures to minimize or thwart some of the threats these actors collectively pose. The research questions consider the themes, similarities, and differences between these actors' motives. This study uses the qualitative method of inquiry and content analysis of the literature on each actor to create a motivational topology that the researcher subsequently tests by conducting a content analysis of the motives in a database specially created containing case studies for each actor group. A second mode of inquiry, interviews, confirms the topology. The findings support the convergence hypothesis. This study advances the corpus of strategic security literature through its examination and rigorous analysis of national security's triple threat where no previous combined study exists.

*Keywords*: terrorists, terrorism, spies, espionage, hackers, hacking, motivation, national security

# Table of Contents

## List of Tables

## List of Figures

## List of Terms, Abbreviations, or Symbols

| | |
|---|---|
| 9/11 | September 11, 2001 Terrorist Attacks |
| ALF | Animal Liberation Front |
| APA | American Psychiatric Association |
| ARPANET | Advanced Research Projects Agency Network |
| BCE | Before the Common Era |
| CI | Counterintelligence |
| CIA | Central Intelligence Agency |
| DDoS | Distributed Denial of Service Attacks |
| DHHS | Department of Health and Human Services |
| DHS | Department of Homeland Security |
| DHS/OIA | Department of Homeland Security’s Office of Intelligence Analysis |
| DNI | Director of National Intelligence |
| DOD | Department of Defense |
| DOJ | Department of Justice |
| FBI | Federal Bureau of Investigation |
| GTD | Global Terrorism Database |
| IC | Intelligence Community |
| IRB | Institutional Review Board |
| KGB | Komitet gosudarstvennoy bezopasnosti |
| MEECES | Money, Entertainment, Ego, Cause, Entrance To Social Groups, and Status |
| MICE | Money, Ideology, Compromise or Coercion, and Ego |
| MINCE | Money, Ideology, Nationality, Compromise or Coercion, and Ego |
| MINCES | Money, Ideology, Nationality, Compromise or Coercion, Ego, and Sex |
| MSP | Motivational Style Profile |
| NAU | National American University |
| OS | Operating System |
| PARC | Palo Alto Research Center |
| PDF | Portable Document Format |
| PERSEREC | Personnel and Security Research Center |
| PII | Personally Identifiable Information |
| PLO | Palestine Liberation Organization |
| RAT | Routine Activity Theory |
| RASCLS | Reciprocation, Authority, Scarcity, Commitment, Liking, and Social Proof |
| SAT | Situational Action Theory |
| SLT | Social Learning Theory |
| START | Study of Terrorism and Responses to Terrorism |
| STT | Space-Transition Theory |
| TTPs | Tactics, Techniques, and Procedures |
| US | United States |

| | |
|---|---|
| USSR | United Soviet Socialist Republic |
| WEF | World Economic Forum |
| WWI | World War I |
| WWII | World War II |

# Chapter 1: Introduction

Many scholars claim modern terrorism took its present form during the latter part of the nineteenth century or in the twentieth century, after World War II (WWII) (Gage, 2011; Schouten, 2010). However, it dates from biblical times (Gage, 2011; Laqueur, 1996; Rapoport, 1999). The *Bible* refers to spies (Cardwell, 1978; Hulnick, 2004; Knightly, 1986). Espionage is called "the world's second oldest profession and just as honorable as the first" (Barrett, 1984, p. 13). Hackers, albeit believed to be a recent phenomenon, came into existence in the late 1800s to the early 1900s (Hong, 2001; Marks, 2011; Rutkowski, 2010) can be traced to the invention of the teletype, telegraph, and telephone.

Each of these actors and their sinister actions is a threat to national security. The United States (US) has counterterrorism policies, strategies, and tactics, techniques, and procedures (TTPs), and laws designed to address national security threats. These actors are alike in that they pose a threat to national security. It is uncertain how similar or different are their motivations, behaviors, methodologies, or means. However, neither categorizing these actors separately nor using a one-size fits all approach to understand their motives provides an effective defense. This research defines the problem, research questions, and purpose of this study to compare and contrast, and understand the convergence of the motivations of terrorists, spies, and hackers—national security's triple threat.

This research project began in 2016 after completing coursework for a dissertation in partial fulfillment of the requirements for Doctor of Strategic Security (DSS) at the former Henley-Putnam University (H-PU), a school recognized by the United States Department of Education and accredited by the Distance Education Accrediting Commission. In 2018, National American University (NAU), also a school recognized by the United States Department of

Education regionally and accredited by the Higher Learning Commission (HLC) acquired H-PU. Subsequently, the HCL formally accredited the DSS program and NAU developed a path for former H-PU DSS recipients to obtain a regionally accredited doctoral degree building on the prior dissertation by extending the research. This path aligns with the Naval Postgraduate School's guidance on the use of prior research (NPS, 2007). In addition, NAU neither considers the reuse of any of the work self-plagiarism nor is it research misconduct (HHS, n.d.; NPS, 2007). As such, under the direction of my dissertation committee, I reviewed, revised, and updated the introduction and literature review. I extended the research methodology to include a second method of inquiry to investigate the problem and gather additional data from experts in the field familiar with the actors' motivations. Finally, I extended the results and discussion section and updated the conclusion accordingly. The research that follows is a culmination of my efforts in partial fulfillment of requirements for the DSS from NAU.

## Problem Background and Significance

Terrorism, espionage, and hacking are top-of-mind national security concerns. Since 2009, the Director of National Intelligence (DNI) consistently assessed at least two of these three threats and the degree to which the threats may affect national security in the yearly *Worldwide Threat Assessment* before Congress (ODNI, 2009, 2010, 2011, 2012, 2013, 2014, 2015a, 2016, 2017, 2018, 2019). In 2019, the DNI once again led the *Worldwide Threat Assessment* to the Senate Select Committee on Intelligence with the Intelligence Community's judgment of cyber and technology. Although the DNI asserted the order of topics "does not *necessarily* [emphasis added] indicate the relative importance or magnitude of the threat," (ODNI, 2019, para. 2), 2019 marked the seventh year in a row in which the discussion began with cyber threats; terrorism ranked as the second or third topic; and counterintelligence (espionage) was lower in the list.

Irrespective of the topic order, clearly, the threats of terrorism, spying, and hacking are causes for national security concerns. In addition, the continued mention of these actors in articles found in the popular press warns of the perils of their actions. Consider the following examples of each actor and his or her associated threat to illustrate the problems.

Terrorists have access to weapons of mass destruction, may possess extreme religious beliefs or political ideologies to fuel their actions and change tactics as rapidly as technology (Laqueur, 2003). The terrorist attacks in the US on September 11, 2001 (9/11) were the worst attacks on US soil since the Japanese bombed Pearl Harbor (9/11 Commission, 2004). Since then, and as of July 2018, the Heritage Foundation counted 104 plots against the US (Inserra, 2018). Terrorists continue to taunt the government by using violence to spread fear amongst the populace in pursuit of the terrorists' objectives such as political or social change, power, control, or to eradicate other threats to themselves in an effort to narrow the beliefs they hold sacred (H. Nimon, personal communication, April 9, 2019). The Center for Counterintelligence and Security Studies (CI Centre) logged eight US-based terrorism cases (as of April 14, 2019), involving 13 terrorists—some acting together, and some acting alone—in its database for 2019 (CI Centre, 2019). For example, the Federal Bureau of Investigation (FBI) investigated and thwarted a terrorist event in Maryland on March 28, 2019. Police arrested and charged Rondell Henry, a naturalized US citizen, of possessing a stolen vehicle with the intent to commit mass murder at Maryland's National Harbor, following the pattern of foreign terrorist groups (*United States v. Henry*).

Although economic espionage cases regularly appear in the news, US-born and naturalized citizen-spies continue to commit traditional espionage against the US. In a plea bargain with the FBI, former Defense Intelligence Agency case officer Ron Hansen, a retired US

Army warrant officer, pled guilty to attempted espionage (DOJ, 2019). The government indicted Hansen in June 2018 on 15 counts, including attempts to deliver defense information to the Chinese government (*United States v. Hansen*). Federal prosecutors charged Edward Snowden, a former National Security Agency contractor, with espionage in 2013. Snowden stands accused of stealing government property, unauthorized disclosure of classified national intelligence, information, sources, and methods, and communicating this information to unauthorized entities or agents (*United States v. Snowden*). The government convicted then-Private First Class Bradley (now Chelsea) Manning of violating the Espionage Act on July 30, 2013 (*United States v. Manning*). Manning divulged classified intelligence documents to WikiLeaks, an unauthorized entity, committed computer fraud, and failed to obey the Uniform Code of Military Justice, receiving a 35-year imprisonment sentence. The government released her from prison after serving seven years following a presidential commutation of her sentence in 2017. More recently, the government indicted former Air Force officer Monica Witt et al. of spying for Iran (*United States v. Witt et al.*).

Hackers seeking to exploit weaknesses in technology continue to aim for public and private computer systems. Just five years ago, the DNI asserted, “for the first-time, destructive cyber-attacks [were] carried out on US soil by nation state entities” (ODNI, 2015b, para. 6). According to the Government Accountability Office, there were 35,277 federal cyber incidents in 2017 (Wilshusen, 2018). The number of threats against non-government US enterprises remains unknown. The National Cybersecurity and Communications Integration Center (NCCIC) reported it received over 106,000 incident reports in 2017 (NCCIC, 2018). Cyber consulting firm 4iQ asserted it confirmed 12,499 authentic breaches in 2018, representing a four-fold increase over 2017 (4iQ, 2019). Finally, in one of the most high profile hacking cases, the

US Government held Manning in contempt of court for failing to testify at a grand jury investigating WikiLeaks founder Julian Assange (Weiner, 2019). On April 11, 2019, authorities in the United Kingdom arrested Assange in accordance with the charges the US Government filed against him in 2010 (*United States v. Assange,* 2018), and on May 23, 2019, in a superseding indictment the a federal grand jury in Virginia charged Assange on 17 counts of espionage and other crimes (*United States v. Assange*, 2019). In addition, some government officials assert WikiLeaks was the recipient of hacked emails during the run-up to the 2016 presidential election (Zapotsky & Barrett, 2018). According to the National Institute of Standards and Technology website on April 14, 2019, 115,158 Common Vulnerabilities and Exposure entries were in the database (NIST, 2019) and the number new of vectors continues to expand.

Researchers in disciplines such as military science, history, political science, intelligence, psychology, and sociology have each weighed in with theories and identified motives. Terrorism scholars include Borum (2004), Cottee and Hayward (2011), Crenshaw (1981, 1986, 1987, 1995, 2000), Post (1998, 2005, 2007), Swann, Jetten, Gómez, Whitehouse, and Bastian (2012), Taylor (1988), Tilly (2004), Tzu (1910), and Victoroff (2005). Notable espionage researchers are Charney (2010), Herbig (2008), Herbig and Wiskoff (2002), Kramer and Heuer (2007), and Thompson (2013). Finally, luminaries such as Campbell and Kennedy (2014), Denning (1999, 2011), Hitz (2008), Holt (2007), Holt and Bossler (2014), Jaishankar (2011), Sarbin, Carney, and Eoyang (1994), Shaw, Ruby, and Post (1998), and Xu, Hu, & Zhang, (2013) investigate hackers.

Finally, while the *Worldwide Threat Assessments* suggest the line between actors is blurring, there is no mention of motivation within or between actors. Each group of actors presents a danger to the country; together they are a multi-faceted national security threat. While the line between these actors and their actions is blurring, it is increasingly difficult to differentiate between the motives of a traditional spy and one that hacks into computers committing espionage or a terrorist using cyber methods to frighten the populous and cripple a country's economy or disrupt business operations.

To say that none of the previous researchers studying terrorism, espionage, or hacking understands the triple threat is improper; however, to say that each researcher fully understands the effect of convergence is also inappropriate. Although the discourse is diverse, researchers tend to maintain a narrow focus on each actor, rarely if ever, assessing the significance of the triple threat. To address the triple threat in the 21st century effectively, national security practitioners must recognize the similarities and differences of these actors and explore their psyches to develop a comprehensive picture of their converging motives and actions. The most effective defense perhaps lies in understanding what causes these actors to behave the way they do by investigating the motives of terrorists, spies, and hackers. The threat is no longer single-faceted; it is a multi-dimensional problem posing a triple threat to national security.

## Research Questions

From a psychological, behavioral, and motivational perspective, the study of the phenomena of terrorism, espionage, and hacking are at present poorly integrated. The literature consists of research and studies about each actor type. Post's (1998), Crenshaw's (1987, 2000), and Sageman's (2004) primary research focus is on terrorists and terrorism. Sarbin et al. (1994), Kramer and Heuer (2007), and Charney (2010) each conduct research on spies and espionage. Finally, Denning (2011), Wikström (2010, 2014), and Campbell and Kennedy (2014) concentrate on cyber security, hackers, and hacking.

If researchers can identify the similarities and differences of the motives of terrorists, spies, and hackers, and develop recognizable patterns, then US counterterrorism and security specialists can develop TTPs to minimize, or thwart, the threat these actors collectively create. Since the research problem is to explore and gain an understanding of the collective and common motivations of national security's triple threat, the central question is, are there commonalities between the motives of non-state sponsored terrorists, spies, and hackers?

The two guiding sub-questions shaping the study are:

1. What are the motives, themes, and patterns attributed to each actor?
2. What are the similarities and differences between the motives of each actor?

### Purpose of the Research

The purpose of this study is to answer the research questions by exploring the motivations of non-state sponsored US born or naturalized citizens acting as terrorists, spies, and hackers. Based on the preliminary literature review, no single open-source study exists that collectively examines, compares, contrasts, or analyzes the motivations of national security's triple threat. Thus, the results of this study contribute to the ongoing discourse by filling that gap.

The value of the research is to raise awareness, add to current knowledge, and understand the relationships between motives of terrorists, spies, and hackers better, first by identifying, and second by examining the motives that cause each actor to behave in the ways they do. The research conclusions provide insights into the motives and causes of each actor group individually, while the analysis and comparison of motives across all groups provide insight into the similarities and differences between these actors, and illustrates convergence. The audience for the findings includes scholars, researchers, academicians, Intelligence Community (IC) stakeholders, security and protection personnel, and policymakers at the federal, state, local, and tribal levels. In particular, policymakers can use the results to update and supplement TTPs to bolster the country's security posture against national security's triple threat.

## Definition of Terms

Although Chapter 2 contains a detailed discussion about the definitions of terrorism, espionage, and hacking, the definitions below establish this researcher's use of the three important words central to this study. In addition, due to the discourse and disagreement of these words in the strategic security field, these definitions provide clarify for the reader.

**Terrorism** is the intentional violence by non-state actors guided by political or private motives. The actors' intentions are to intimidate or coerce the civilian population to influence government policy applying mass destruction, assassination, or kidnapping using methods that are dangerous to humans, are outside the laws of war, violate US criminal laws, and occur within the US' mainland borders and territories.

**Espionage** is the threat, theft, or compromise of national intelligence or other classified or military information acquired through covert or overt methods and divulged to a third-party unauthorized possess of the information.

**Hacking** is the malicious activity individuals commit using technology to gain unauthorized access to computer systems and networks.

## Assumptions/Limitations/Delimitations/Researcher's Role

All research projects contain assumptions based on the philosophical approach taken; no research or researcher is immune. In particular, the assumptions guiding the philosophy of the researcher, and the research include "ontology (the nature of reality), epistemology (what counts as knowledge and how knowledge claims are justified), axiology (the role of values in research), and methodology (the process of the research)" (Creswell, 2013, locs. 675-681). These assumptions are implicit, and the degree to which these assumptions affect the study depends on the experience and perspective of the researcher, and the participants in the research study. See Table 1 for a summary of the assumptions underlying this research.

*Table 1.*

*Summary of Philosophical and Interpretive Assumptions*

| | |
|---|---|
| **Ontology** | Realist |
| **Epistemology** | Interpretivist |
| **Research Type** | Qualitative |
| **Reasoning** | Inductive |
| **Research Methods** | Case study and interviews |
| **Data Collection** | Content analysis and semi-structured interviews |

Source: Author

### Philosophical and Interpretive Assumptions

As a result of the pragmatic and interpretive views of the primary researcher, the ontological assumptions are that multiple views of reality ranging from objective to subjective exist, and these views are "independent of human understanding to subjective truths" (Christ, 2013, p. 112). Epistemological assumptions imply the researcher constructs social reality based on life experiences, thereby necessitating case study reviews and discussions between the researcher and research participants. "Both the etic and emic perceptions can co-exist in a single study" (p. 112) because each view lends credibility to the study, and the researcher can compare and contrast evidence during data analysis.

Realism and interpretivism are the primary underlying philosophical assumptions, supported by behavioral and psychopathological theories to reinforce this study (Crenshaw, 1987; Post, 1998; Watson, 1913). Briefly, realism is the philosophy that reality exists irrespective and independent of perceptions (Smith, 2006) because it "embraces the view that constructed reality is seen [sic] through *perceptual filters* [emphasis original], a theme common to interpretive qualitative research" (Christ, 2013, p. 114). Since the research is about the triple-threat actors' motivations, the interpretivist epistemology is appropriate.

The researcher employed the qualitative research type using inductive reasoning to interpret cases studies in addition to interviews with experts to help interpret the case study findings. Qualitative research depends on primarily non-numeric data, such as contentment analysis, interviews, and observations, yet descriptive quantitative statistics may support observations. Inductive reasoning enables the researcher to use data about the phenomenon under study and derive a theory or generalize about the results (Creswell, 2013). The goal of the interpretivist is to understand meaning rather than to predict cause and effect. Finally, see Chapter 3 for specific ethical considerations, and methodological assumptions, limitations, and biases.

### Limitations

In addition to assumptions, all research contains limitations some of which may constrain the researcher. This study has potential limitations, including the researcher's bias, research design, methodology, and time constraints. Although limitations may represent potential research weaknesses, when the researcher takes precautions, where available, to minimize the limitations, validity increases and ethical questions abate. The following paragraphs outline precautions employed to increase the value of the conclusions.

Researchers cannot eliminate biases. However, researchers can minimize biases by paying attention to the cognitive aspects of decision-making and analysis as the study progresses. For example, using random sampling techniques to choose case studies is an objective method of sample selection and eliminates personal convenience that could introduce bias and degrade research quality. A small number of interview subjects resulted because the population of experts with knowledge of the motivations of terrorists, spies, and hackers is difficult to access and NAU's Institutional Review Board (IRB) declined the researcher's initial request to interview terrorists, spies, and hackers known to the researcher's committee chairman. Therefore, the researcher used experts (proxies) that provided insights into the motivations of terrorists, spies, and hackers from having had prior access to these actors. The implicit methodological biases, due to the qualitative case study and interview formats require methods, questions, and the process itself to evolve continually as the research process unfolds. To minimize analytical biases, the researcher used multiple methods of data gathering such as content analysis and interviews to view evidence from various perspectives.

### Delimitations

In contrast to the limitations, delimitations are the result of the researcher's choices. To ensure time does not become a limitation, the researcher limited the number of research questions. The research excluded state and state-sponsored acts committed by terrorists, spies, and hackers, as well as the legal aspects of terrorism, espionage, and hacking. The definitions of each actor contain the scope of the study to US-born or naturalized citizens, controlling the study boundaries. Thus, the conclusions may not directly apply to other countries; however, generalized results and conclusions may help shed light on the phenomenon under study irrespective of the citizenship of the actors.

### Role of the Researcher

Finally, for this study, the researcher's role is etic, acting as a data collector or facilitator, operating from an outside-view perspective. This role exhibits an objective view whereby the researcher is responsible for creating, administering, and analyzing the qualitative data in case studies, as well as for asking probing questions, and listening in interview situations. The external role helps to identify the themes revealed in the qualitative data and merging the data from case studies and interviews to conduct analysis, in addition to program managing the research effort. This role of a researcher is consistent with a qualitative research design that requires listening, thinking, asking questions, and striving to understand thick and rich data (Creswell, 2013, 2014) to generalize conclusions.

### Study Organization

Chapter 1, the Introduction, provides the foundation for this study. The purpose of this chapter is to introduce the topic, provide general information and background on the topic, and use evidence to demonstrate the problem exists and warrants further study. The chapter includes the introduction, background, problem statement, purpose statement, research questions, and significance of the problem, assumptions, limitations, delimitations, and researcher's role, as well as describes the organization of the remainder of the study.

Chapter 2, the Literature Review, is the story of the body of literature about the three actor groups comprising national security's triple threat. For each group—terrorist, spy, and hacker—the chapter outlines the history, definitions, categories, and theories. The chapter summary provides an understanding of the seminal, older, and current research to confirm the gap in the body of research and leads the reader to understand the contribution triple threat research adds to the existing body of work.

Chapter 3, the Methodology, outlines the study design. It describes the research method and dual approaches to this qualitative research. Sub sections include case study selection, sampling strategy, an explanation of the database built for analysis, evidence, data sources, and data collection. Additional sub sections include interview participant selection and sample size, interviewee protection, data collection and instrument, analysis, ethical considerations and the researcher's role. The content in this section helps the reader understand the data collection procedures, the integration of multiple methods of data collection, and explains the overall design that sets the stage for the analysis.

Chapter 4, the Results and Discussion, briefly restates the problem, purpose, describes the refined motivations and definitions resulting from the analysis, and presents a proposed typology for assessing motivations by and across actors. It explains the processes culminating in the results and findings, and provides details on the research findings and data analyses. Assertions in this chapter directly support the data analysis.

Chapter 5, the Conclusions, explains the findings, recommendations, and presents suggestions for future research. In this final chapter of the study, the researcher fuses the information gleaned while executing the study. Further, the researcher clarifies and elucidates the importance of the findings.

## Chapter 2: Literature Review

Chapter 1 introduced the concept of national security's triple threat, provided an overview of the problem, the research questions, and assumptions underlying this study. Chapter 2, the Literature Review, presents a comprehensive appraisal of academic and other professional practitioners' (think tanks, military) works on each of the three actor-groups comprising national security triple threat. The literature review provides context of the historical and foundational research prior to studying the motivations of non-state terrorists, spies, and hackers. The intent is to identify, evaluate, and elucidate important characteristics—history, definitions, and theoretical perspectives to reveal the prior knowledge about these actors—setting the groundwork for the research and to demonstrate where the new research fits into the "ongoing dialogue in the literature, filling in gaps and extending prior studies" (Creswell, 2014, p. 28). Underlying the literature review is an interpretivist theoretical approach because as the researcher gathered literature, the changing context, patterns, and themes revealed "meaning in actions and events" (Taniguchi, 2014, p. 54). In addition, multiple objective-to-subjective views of reality (Christ, 2013) and multiple assessments support the connection between individuals or groups of individuals in society (O'Donoghue, 2018). Further, as O'Donoghue (2018) asserts, although the actors and groups of actors in society are inseparable, researchers can assess individuals and groups without overlooking the societal perspective.

Building on the seminal foundation of literature on each actor group, the body of literature demonstrates how the waves of change influence these important actors and their threats to national security. Older literature constitutes the largest number of publications and viewpoints demonstrating the preponderance of evidence and analysis for two actors—primarily terrorists and spies—during the period when the country established its footing as a global leader. Current literature, published within the last five years, provides the new thinking or modern perspectives, and demonstrates the degree to which researchers' views adapted over time as the world system continues its transformation into a globally integrated ecosystem—economic, political, and cultural, increasingly enabled by technology.

### Documentation

The literature review for this study consisted of primary and secondary searches of academic and open source databases. Examples include EBSCO Academic Search Premier, EBSCO International Security & Counter Terrorism Reference Center, Gale, JSTOR, ProQuest databases, ProQuest Dissertations & Theses Global, Taylor & Francis Online, PsychINFO, Science Direct, and PsycARTICLES.

Of significance, an extensive examination of these academic and open source databases revealed a lack of research examining terrorists, spies, and hackers in single, combined studies. For example, using the 49 ProQuest databases containing 21,507 publications in National American University's online library with the keyword *terrorist* anywhere in the text of peer-reviewed publications resulted in over 81,683 results. Repeating the search using the keyword *spy* exposed 40,581 results and using the keyword *hacker* uncovered 37,997 results. Conducting a search using the three keywords together revealed 320 articles. Continuing the search within those results using subject search terms *national security*, *terrorism*, *espionage*, *hackers* narrowed the results to 109 documents. An investigation of those documents failed to yield a study either comparing or contrasting the three actors, or a study investigating the motivation across each of the three actor groups.

Searches of ProQuest Dissertations & Theses Global database revealed 15 doctoral dissertations and master's theses associated with the keywords *terrorist, spy, or hacker*.

However, none of the resulting research studies examined the three actors' behaviors or motivations in combination. Two of the 15 dealt with hacker or cybercrime behaviors and contributed to this study (McBrayer, 2014; Rogers, 2001). Nevertheless, relentless searching revealed one older article in a software trade journal whose author briefly described the types of hackers and their exploits. Radcliff (1997) used the clever title "Hackers, Terrorists, and Spies" to instill fear, uncertainty, and doubt in readers unfamiliar with the need to provide security when connecting computers to the internet. Indeed, in the text of the article, the word terrorist appeared only once, while the word spy was absent.

Consequently, the researcher conducted an alternative literature review strategy examining the research of each actor individually. To execute the alternative literature review strategy, searches of the previously mentioned databases consisted of primary search terms *terrorist*, *spy*, and *hacker* individually with various combinations of *national security* and *terrorism*, *national security* and *espionage*, *national security* and *hacking*. These searches were qualified further using limiters to focus results on full text, peer reviewed scholarly journals and books. Additional subject keywords such as *terrorist, terrorism, counterterrorism, spies, hacker, threats*, *history*, *behavior*, *psychology*, and *theory* used in various combinations with the primary search terms, helped to narrow search results to the study's focus.

Secondary web searches of Google and Google Scholar used topic and luminary author keywords in various combinations to identify additional works not found in proprietary academic databases. Employing Google and Google Scholar enabled identification of works written by private enterprises, think tanks, and government entities such as RAND, the Council on Foreign Affairs, Terrorism Research Initiative, and the Congressional Research Service. Using keywords as previously described also helped to narrow search results. Author keywords for noted luminaries in the fields of terrorism, espionage, and cyber supplemented broader searches. In addition, scans of local public university and county library book collections extended online library searches. Finally, targeted searches for writings and speeches of representative actors in each of the three groups provided primary source perspectives. Table 2 presents an overview of literature by category consulted for this study.

*Table 2.*

*Overview of Literature by Category*

| | Seminal (prior to 1960) | Older (1960-2013) | Current (2014 to present) | No Date | Total |
|---|---|---|---|---|---|
| Peer Reviewed Journals | 5 | 94 | 23 | 0 | 122 |
| Non-Peer Reviewed Journals | 2 | 2 | 4 | 0 | 8 |
| Dissertations and Theses | 0 | 1 | 1 | 0 | 2 |
| Books – peer/non-peer reviewed | 5 | 64 | 11 | 0 | 80 |
| Other (research reports from .edu, .gov, .org, internet sites, laws, court decisions, general references, etc.) | 8 | 42 | 54 | 18 | 122 |
| Total | 20 | 203 | 93 | 18 | 334 |

*Note*. The researcher reviewed literature in addition to that represented in this table. This table and the reference list contain only sources cited in the text, per the Publication Manual of the American Psychological Association guidelines.

The inclusion of seminal research (prior to 1960), older research (1960-2013), and current research (2014-present) facilitated multiple perspectives as the waves of change influenced these actors and their threats to national security. Prior to the proliferation of internet technology and increased globalization, the convergence of threats posed by non-state actors was scant. Each actor operated principally independent from the other and there was little reason to consider studying commonalities and differences amongst the three actors. This explained the void of current literature examining the convergence amongst these actors.

Despite the increasing distortion between actors such as terrorists hacking, hackers conducting espionage, and spies using any means available, there is a lack of researcher curiosity in conducting empirical—or case-based research—to help inform US national security policy. These reasons explain the paucity of current research and the weak comprehension of the converging threat. Within the body of research examined, no single publication comparing and contrasting these three non-state actors' motivations and behaviors was located. As such, the research contained in this dissertation contributes to the ongoing discourse by integrating the results of research on individual actor types into a single study thereby filling the identified gap.

The sections below present the review of the literature on each actor. Within the sections on each actor, the researcher examined the history, definition, types, behavioral theories, and characteristics of the associated actors. A précis of each actor wraps up each section. The chapter closes with a summary of research reviewed and a transition into the next chapter.

**Terrorists and Terrorism**

The word *terrorism*, originated in the fifteenth century from the Latin word terror, derived "from *terrēre* to frighten" (Merriam-Webster Online, n.d.) is perhaps an *onomatopoeia*—"the use of words whose sound suggests the sense" (Merriam-Webster Online, n.d.). The feeling and perception of the word evokes a mental picture of the act itself: fear, intimidation, coercion, horror, panic, and a sense of unlawful behavior by actors who practice this form of extreme violence. Terrorism is both a strategy and a tactic (Carr, 1996; Chaliand & Blin, 2007); some scholars refer to it as "a weapon of the weak against the strong" (Gage, 2011, p. 77). Nonetheless, to understand how terrorism evolved from its origin to its now near synonymous meaning with the contemporary Global War on Terror, a review of its history, the definitional discourse, theories, and the behaviors of the individual actors frame this research.

### History of terrorists and terrorism.

According to Gage (2011), “terrorism, like any other word or concept, has changed according to its moment in time and its political context” (p. 74). Scholars in many disciplines have studied terrorism including military science, history, political science, social science, intelligence, psychology, sociology, medicine, and economics. However, Gage (2011) contends historians were silent on the topic. Citing Richard Hofstadter, a noted historian, Gage (2011) asserts, “for a generation…the profession had ignored the issue” (p. 73). Since the 1970s, following Hofstadter’s plea for historians to “engage in the subject of violence” (p. 73), and the September 11, 2001 (9/11) attacks on the World Trade Center and Pentagon, there is still confusion as to the roots of terrorism from an historical perspective.

When summarizing the literature or beginning a discussion on terrorism, many scholars skip the deep historical perspective and jump to terrorism as a modern phenomenon that began with the French Revolution (Crenshaw, 1986; Fromkin, 1975; Rapoport, 1984, 1999, 2001, 2004; Schmid, 2004; Strozier, 2008; Tilly, 2004). However, Walter Laqueur (1987, 1996, 2003), another prominent historian, “is generally credited with linking history and terrorism” (Duyvesteyn, 2004, p. 442). He claimed it was important to understand the phenomenon yet cautioned, “the roots of terrorism…[in] the twenty-first century cannot be based exclusively on the experience of earlier phases.…[because] the assumption that terrorism has no prehistory….would be even more misleading” (p. 29). Hence, to study terrorism, researchers must recognize that terrorism dates from biblical times. The fascination with the etiology of the word dating from the French Revolution neglects this view. Since 9/11, some scholars debate *new* terrorism (Bolanos, 2012; Duyvesteyn, 2004; Duyvesteyn & Malkki, 2012; Matusitz, 2013). Yet the concept of terrorism is not new; rather there are certain essentials such as “easier access to weapons of mass destruction and greater importance of religious-political fanaticism as a motive" (Laqueur, 2003, p. 8), in addition to different tactics as technology changed.

The *Bible*, both Old and New Testaments, refers to terrorism (Kainz, 1999). Masada was perhaps "the earliest terrorist campaign in history" (Rapoport, 1999, p. 498). Other early examples of terrorists include the Zealots and Sicarri, the Thugs, and the Assassins (Rapoport, 1999). The first *recorded use* of the word terrorism appeared during the French Revolution (Gage, 2011; Rapoport, 1999). During the Early Modern Period, (1500-1750), terrorism meant, "'either government by intimidation' or 'a (government) policy intended to strike with terror those against whom it is adopted'" (Rapoport, 1999, p. 499). It was not until the Mid Modern Period, (1750-1914), that terrorism took on a new meaning. The "Narodnaya Volya ('The People's Will,' 1879) emerged, [as] the first rebel movement to characterize *itself* as terrorist" (Rapoport, 1999, p. 499). In addition, "anarchist Alexander Berkman boldly—and plausibly—claimed that he had committed 'the first terrorist act in America'" (Gage, 2011, p. 75) after his attempted assassination of Henry Clay Frick. That proclamation marked the beginning of the trend Gage (2011) called "revolutionary conflict from below" (p. 76).

The Contemporary Period (1914-present) was ushered in with the Russian Revolution, and in the US was marked by Hunter's (1914/2010) book *Violence and the Labor Movement*, in which he introduced Michael Bakounin as "the father of terrorism" (loc. 201). Hunter (1914/2010) credits Bakounin with "[bringing] into Western Europe and [planting] there seeds of terrorism" (loc. 172). The establishment, government, and the church were Bakounin's adversaries, "and no weapon was unworthy of use which promised in any measure to assist in their complete obliteration" (loc. 186). Rapoport (1999) asserted, "*publicity* and *provocation* (emphasis in original), not pure terrorism…were the objectives of Tsarist atrocities, a lesson

Russian revolutionary terrorists absorbed" (p. 499). These events were the catalysts that "transform[ed] society through publicizing a cause and provoking the opposition to violate its own norms in efforts to root the terrorists out…creat[ing] serious international concern" (p. 499). The rise of totalitarianism in the 1930s brought with it the modern notion of state terrorism, and socialism preoccupied the world.

Social movements took place the 1940s (Abel, 1937; Heberle, 1949; McCormack, 1950; Strauss, 1947). On the heels of victory in WW II, the communism versus capitalism ideology eventually drove a wedge between the east and west—the Soviet Union against the US. The two superpowers locked horns in a battle known as the Cold War. Although a war of words and proxies, it resulted in an arms race and an international relations strategy of deterrence. It was a time of change, when social and political viewpoints collided, tempers ran hot and cold, and people were longing to identify and belong to something—a peer group, a social circle, a cause, or an institution.

A shift from conservative to liberal thinking took place in the 1960s, which exhibited less formal behavior than in prior decades. The push for independent ideas, sparked by President Kennedy's *New Frontier*, and President Johnson's commitment to eradicating poverty and social injustice with his vision of a *Great Society,* forever changed both the social and political landscape. These changes and ideas resulted in permanent modification to the fabric and underpinnings of US culture, prompting a generation of young adults to set themselves apart from their parents, and the establishment. Current events sparked race riots and the Civil Rights Movement. A counterculture atmosphere prevailed throughout the country. The result was a decade fraught with various types of social unrest, rebellions, and violence, both nationally and internationally. In 1967, the Six Day War between Israel and the Palestine Liberation

Organization (PLO) “became the heroic model when the Vietnam War ended” (Rapoport, 2001, p. 421). Chalmers Johnson (1982) asserted, “the world…witnessed at least fifteen revolutions of diverse types” (p. ix) during this time. It is against this background, and within a social science context of internal and external change, that social unrest took hold and “the problems of [terrorism] definition took hold” (Rapoport, 2001, p. 499).

By the 1970s and 1980s, the world had changed. Gage (2011) asserted “the lively but troubled field of terrorism studies” (p. 77) emerged from the turmoil of the 1970s when political scientists, sociologists, psychologists, and anthropologists took interest in studying terrorism. Revolts against Western ideology were rampant, and nations in various quarters began dealing with social unrest. Non-state actors engaged in airline terrorism, including hijackings and bombings. Examples of these terrorist groups include the Weather Underground in the US, the Irish Republican Army in the United Kingdom, the Red Army Faction in Germany, the Palestinian Black September group responsible for the Munich Olympic Massacre, and the African National Congress in South Africa. In the 1990s, signaling apartheid was on the wane, the South African government freed Nelson Mandela. Libyan Terrorists bombed a Pan Am flight over Lockerbie, Scotland. China found itself in the spotlight with pro-democracy students revolting in Tiananmen Square. In Eastern Europe, Poland saw turmoil, and in Latin America, many countries experienced a return to more democratic governments. Margaret Thatcher’s influence on the Soviet Union helped to cause fragmentation inside the communist bloc, with the collapse of the Berlin Wall and German reunification not far behind.

The final decade of the 20st century will forever be known for key events—the end of the Cold War, global economic growth, and expansion of the Internet in both the public and the private sectors. In 1990, Iraq invaded Kuwait, and in what was perhaps the last symmetric, yet highly lopsided conventional war of the century, the US and coalition forces intervened in what would become the first of several military actions in the Middle East—Operation Desert Storm—with the mission to return Kuwait’s sovereignty from the hands of Saddam Hussein. By 1993, terrorists struck closer to home with the first bombing of the World Trade Center towers. In 1995, an Israeli radical assassinated Yitzhak Rabin, and again at home that same year, in Oklahoma, a right-wing US citizen, a radical who blamed the government for the mishandling and siege of the Branch Davidians in Waco, Texas bombed the Murrah Federal Building.

The astonishing attacks on the World Trade Center and the Pentagon on 9/11 ushered in the new millennium. These catalysts “transform[ed] society through publicizing a cause and provoking the opposition to violate its own norms in efforts to root the terrorists out…creat[ing] serious international concern” (Rapoport, 1999, p. 499). Indeed, Gage’s (2011) assertion, “a coherent historiography of terrorism, a definable way to think about the role violence [had]…played in the American past” (p. 81) was widely unknown outside academia, the government, and the military. Her assertion was accurate: terrorism “was both visible and invisible, absent and present, before September 2001. What changed…to borrow Hofstadter’s words, [was] ‘our sudden awareness of it’” (p. 81). Although past acts may appear random, with a progression of increasing frequency, Rapoport (1999, 2001, 2004) developed a wave model in which he categorized incidents, in contrast to an event-driven or organizational focus as previously noted. “A crucial feature [of each wave] is its international character…. [and the wave] name reflects its dominant but not only feature” (Rapoport, 2004, p. 47). Table 3 summarizes the model.

*Table 3.*

*Rapoport's Four Waves of Terrorism*

| | First Wave | Second Wave | Third Wave | Fourth Wave |
|---|---|---|---|---|
| Date | 1880 | 1920 | 1960 | 1979 |
| Name | Anarchist | Anticolonial | New Left | Religious |
| Critical Factors | Communication and Transportation; Doctrine/Culture | National Self-Determination | Six Day War and Collapse of Arab Armies | Iranian Revolution, New Islamic Century, and Soviet Afghanistan Invasion |
| Catalyst | Domestic | Versailles Peace Treaty | Vietnam War End and Rise of the PLO | Religion and Ethnic Identity |
| Weapons | Dynamite Assassinations | Money; Concealed Weapons | Assassinations; Raids; Hijackings; Kidnapping; Hostages; Sponsored Groups | Self-Martyrdom/Suicide Bombing |
| Purpose | Tsarist Reform | Divest Colonial Possessions | Topple Capitalism and Destroy Israel | Destroy America and Secular State Creation |
| Primary Targets | Politicians | Military | National and International "Theatrical" Targets; Americans | Civilian and Military Installations; Military Ships |
| Self-Reference | Terrorists | Freedom Fighters | Revolutionary | Jihadists |

*Note*. Adapted from "Terrorism" by D. Rapoport, 1999, "The fourth wave: September 11 in the history of terrorism" by D. Rapoport, 2001, "The four waves of modern terrorism" by D. Rapoport, 2004, and "An end to the fourth wave of terrorism?" by L. Weinberg and W. Eubank, 2010.

Each wave begins with a catalyst, an "unexpected turning point" (Rapoport, 1999, p. 501) that roughly every 35 to 40 years causes one wave to crest exerting force causing the next wave to begin. Rapoport (1999, 2001, 2004) began theorizing about the wave concept in 1999 and continued to refine components of each wave as the international system evolved.

Similar to Rapoport's (1999, 2001, 2004) waves, Lizardo, and Bergesen (2003) also developed a model that "contribute[d to] recent debates on the classification of terrorist activity assuming a wider theoretical and historical perspective" (p. 163). It is a two-dimensional model based on two variables: "structural location in the international system, and ideological justification" (p. 163). Using this model, the authors argue today's religiously dominated terrorism is a nod to “the anarchist-nihilist brand of terror that swept Europe and the United states [*sic*] during the end of the 19th century” (p. 166).

Studying the history of terrorism and terrorists in the form of Rapoport’s (1999, 2001, 2004) waves or Lizardo’s and Bergesen’s (2003) model, leads to two final questions: What exactly is new terrorism and when will the fifth wave begin? Duyvesteyn (2004) questions the concept of new terrorism citing, Rapoport (1999, 2001, 2004) and Laqueur (1987, 1996, 2003) as examples in footnotes (p. 439, 451). She fittingly points out the word “‘new’ can signify that a phenomenon has not been witnessed before….[or] can rightly be applied when it concerns seen-before phenomena but an unknown perspective or interpretation is developed” (p. 439). Her thesis is terrorism since 9/11 is not new; rather what changed is “it became ‘significant’…when it ‘increased in frequency’ and took on ‘novel’ dimensions’” (p. 439) in addition to its worldwide focus. Her arguments are sound as is her conclusion; the label new does not add to the discourse, rather it “should only be applied when on the basis of historical research the phenomenon has not been seen before or when it is the subject of a new historical interpretation” (pp. 450-451). Based on historical accounts of terrorists and terrorism, her point is valid.

Weinberg and Eubank (2010) address the second question in part. They analyzed Rapoport’s (2004) terrorism waves by conducting an empirical analysis using data from the Memorial Institute for the Prevention of Terrorism’s database. The Anticolonial and Religious Waves behaved as predicted with a “beginning, middle, and end” (p. 596) and the New Left Wave lasted ten years less than Rapoport’s (2004) assertion (p. 596). According to Weinberg’s and Eubank’s (2010) analysis, “some evidence indicates the Fourth Wave of modern terrorism may be on” (p. 600) its descent suggesting the crest of a fifth wave has begun. Indeed, Post’s (2015) idea of the fifth wave fits with Weinberg’s and Eubank’s (2010) suggestion. Post (2015) asserts 2010 as the start date of the fifth wave, the Communications Revolution, characterized as social protest of oppressed societies or groups, as a virtual community of hatred. While it is difficult to know if Post's (2015) assertion is correct without the benefit of historical perspective, his characterization is logical. The characteristics that comprise the fifth wave are unfolding, perhaps more rapidly than in prior waves. Nonetheless, one thing is certain: terrorists and terrorism will adapt to changes in the international system both at home and abroad, as history has proved.

Terrorism has ebbed and flowed over time. Some aspects have come and gone; some have reappeared. Although the past provides insight into the future, it cannot be used alone to predict it. One thing is certain however; terrorism is not going away. The history of terrorism recounted here began with the thought that perhaps the word terrorism itself is an onomatopoeia. Paradoxically, "the words thug, assassin, and zealot have become part of our vocabulary (often to describe terrorists)" (Rapoport, 1984, p. 659). These words are now part of the common lexicon used to describe actors who operate outside social and behavioral norms, and they too, are onomatopoeias. It is against this history that definitional challenges developed.

**Defining terrorism.**

The definitional discourse on terrorism is diverse and confusing (Rubin & Rubin, 2008). There are nearly as many definitions of terrorism, including its national and international characteristics, as there are writers about the subject. Thomas Thornton's 1964 definition of terrorism (as cited in Crenshaw, 1986) "is one of the earliest definitions" (p. 380). He suggested, "in an internal war situation, terror is a symbolic act designed to influence political behavior by extranormal means, entailing the use of threat or violence" (p. 380). Since then, the number of definitions expanded. Taylor's (1988) definition has three perspectives—the legal, the moral, and the behavioral. This literature review excludes the legal and moral definitions. It concentrates on the behavioral definitions due to the research focus. As Ruby (2002) suggested “the behavioral perspective seems to be the best one for behavioral scientists….[because it] permit[s] a reliable operational definition” (p. 13).

Perspective is one of the significant reasons the search for a universal definition is challenging. Researchers say, “one man’s terrorist is another man’s freedom fighter” (Ganor, 2002, p. 287; Laqueur, 1987, p. 7; Schmid, 2004, p. 397). Although Laqueur (1987) dismisses this saying as banal, it is appropriate because the definition depends on who is responsible for defining it, their motives, associated biases, and perspectives (Schmid, 2004). For example, when explaining the purpose of the Irgun, Menachem Begin (2013), one of its former leaders, recounted how the British, “called us ‘terrorists’ to the end” (loc. 1624) however, he asserted Irgun’s “purpose, in fact, was precisely the reverse of ‘terrorism’” (loc. 1651). Rather it was “to rebel and fight, not in order to instill fear [*sic*] but to eradicate it” (loc. 1655). By contrast, Hoffman (2015) identified the Irgun as one of two terrorist groups formed in the 1930s to “challenge Britain’s rule over Palestine” (loc. 99).

The word itself is pejorative (Crenshaw, 2000; Ganor, 2002; Schmid, 2004), and due to its changing nature “any definition, fixed in time, [is] problematical” (Schmid, 2004, p. 399). There is literary discourse arguing for broad definitions (Carr, 2007) as well as narrow definitions (Taylor, 2010). Still, Schmid (2004) asserted, “both types of definitions bring problems with themselves” (p. 402), and he believed seeking a common definition would always present difficulty (Schmid, 2011). According to Hoffman (2006) “most people have a vague idea or impression of what terrorism is, but lack a more precise, concrete and truly explanatory definition of the word” (p. 1).

An all-encompassing definition, to which the international community will agree, is likely unrealistic because reflecting upon the history, there are multiple aspects to terrorism (Laqueur, 1996, 2007; Miller, 2007; Post, 2005; Schmid, 2004, 2011). Many English language words are polysemous; such is the case with the word terrorism. The best definition may be the one most closely associated with its use, as suggested by Ruby (2002), and in the case of terrorism, by its type. As used in this study, terrorism is the intentional violence by non-state actors guided by political or private motives. The actors' intentions are to intimidate or coerce the civilian population to influence government policy applying mass destruction, assassination, or kidnapping using methods that are dangerous to humans, are outside the laws of war, violate US criminal laws, and occur within the US' mainland borders and territories.

**Categories of terrorism.**

As Schmidt and Jongman (1988) observed, "one of the problems with typology building is the absence of a commonly agreed-upon definition of terrorism" (p. 56). Once again, the discourse in the literature is extensive. Examples of types of terrorism include state versus non-state, actor-based, cause-based, motivation-based, political orientation based, ideological-based, target-based, and structural-based (Lizardo & Bergesen, 2003; Miller, 2007; Schmid & Jongman, 1988; Tilly, 2004).

Categorizing terrorism as discussed in this section refers to the action—the deed. Reasons for categorization are to help differentiate the kinds of terrorism appear to be multi-faceted. Schmid and Jongman (1988) discussed several types of terrorism and asserted, "a good typology should be able to say something meaningful about the relationship between a group of terrorists and its modus operandi" (p. 53). The typologies of Lizardo and Bergesen (2003), Schmid (2004), Tilly (2004), and Miller (2007) discussed below relate to individual and group behavior to set the stage for the literature review on the non-state actor behavioral aspects of terrorism.

Lizardo and Bergesen (2003) categorized three types of terrorism by its actors' relationship to governments: core governmental organizations (Type-1), peripheral or semi-peripheral government or government-backed organizations (Type-2), and Type-3 where Type-2 organizations turn against Type-1 organizations. Schmid's (2004) typology split state from non-state actors and drilled down via its components such as left- and right-wing social revolutionaries, "racist, religious (and millenarian, national and separatist (including ethnic), and single issue (e.g. eco-terrorism)" (p. 398, Table 16). Tilly (2004) made a distinction between "the degree of specialization in coercion" and "major locus of violent acts" (p. 11), and categorized terrorist groups by these variables on a two-dimensional, four-quadrant model resulting in the identification of four actor types: autonomists, zealots, militias, and conspirators (p. 11, Figure 2). Autonomists attacked "authorities, symbolic objects, rivals or stigmatized populations on their own territories without becoming durably organized specialists in coercion" (p. 11). Zealots were returning exiles that inflicted terror "outside their own base" (p. 11) who returned "home to attack their enemies" (p. 11). Militias conducted terror inside their own backyard, in contrast to conspirators who directed their terror away from home.

Crenshaw (1995), Laqueur (1987), Miller (2007), and Post (1998) type terrorists by their motivation. Miller (2007) identified four types: national-separatists, revolutionary (left wing), reactionary (right wing), and religiously motivated (pp. 335-336). National separatists sought to divorce themselves from current regimes or pursued association with another state while revolutionaries (left wing) changed society with violence. Reactionary (right wing) terrorists, in contrast to the revolutionaries, sought to stop change or reverse it (Miller 2007). Religiously motivated terrorists justified their actions based on a higher authority, attempting to “replace secular governments with more fundamentalist regimes” (p. 336).

Finally, the US Department of Homeland Security’s (DHS) Office of Intelligence Analysis (OIA) essentially categorized domestic terrorist types, although it called these actors *extremists*, when the DHS/OIA released two, at-the-time controversial, reports on right-wing and left-wing terrorism within US borders (Ackerman, 2012; Lake & Hudson, 2009). The DHS/OIA characterized right wing extremists as

> those groups, movements, and adherents that are primarily hate-oriented (based on hatred of particular religious, racial or ethnic groups), and those that are mainly antigovernment, rejecting federal authority in favor of state or local authority, or rejecting government authority entirely. It may include groups and individuals that are dedicated to a single issue, such as opposition to abortion or immigration. (DHS, 2009b, p. 2)

In contrast, DHS/OIA considered left-wing extremists as “groups or individuals who embrace radical elements of the anarchist, animal rights, or environmental movements and are often willing to violate the law to achieve their objectives” (DHS, 2009a, Appendix).

The DOJ and FBI do not maintain domestic terrorist lists; however, both entities recognize domestic terrorism as a threat conducted by actors “who commit crimes in the name of ideologies supporting animal rights, environmental rights, anarchism, white supremacy, anti-government ideals, black separatism, and anti-abortion beliefs” (Bjelopera, 2013, para. 2). Irrespective of classification or categorization, domestic terrorism is a type of terrorism the US government recognizes and defines as “acts dangerous to human life that are a violation of the criminal laws of the United States or of any State” (Patriot Act of 2001). These domestic terrorists conduct nefarious crimes within the territorial borders of the country or its possessions.

With background on both the definitions and types of terrorism, a review of the behavioral literature follows.

### Behavioral theories and motivations of terrorists and terrorism.

Often credited with founding the branch of science known as psychology, John Watson (1913) turned his fascination with animal behavior into a new discipline. Watson (1913) asserted psychology was an objective experimental branch of natural science viewed from the behaviorist perspective. “Its theoretical goal [was] the prediction and control of behavior” (p. 284) he said as he observed how man and animals responded to stimuli “of their environment by means of hereditary and habit requirements” (p. 284). Employing the behaviorist view of psychology is one of the primary methods for studying terrorism.

In attempting to understand terrorist behavior, researchers and practitioners turned to profiling. According to Schouten (2010), “the modern history of profiling began in the 1950s” (p. 374). Although there is value in profiling in certain situations, profiling does not mean the commonly observed characteristics hold true one hundred percent of the time; therefore, its exclusive use is discouraged. Like many types of tests and analyses there will be false positives and false negatives. Schouten (2010) concluded if “‘profiles” [were] of any predictive value, that value is limited to cases that are virtually identical to cases previously studied. Extrapolation to other contexts invariably diminishe[d] both reliability and specificity” (p. 375). However, he asserted profiles “[held] great potential” (p. 375) in the effort to understand certain aspects of terrorism. Nevertheless, other researchers disagree, concluding there is no terrorist profile (Post, 1998).

The literature on terrorists and terrorism based on behavior theories is plentiful. The most important social science approaches include psychological, psychopathological (Post, 1998, 2005, 2007; Sageman, 2004), rational choice (Crenshaw, 1981), sociological (Victoroff, 2005), and individual, group theory and organizational theory (Crenshaw, 1981, 1986, 1995, 2000; Post, 1998, 2005, 2007; Swann et al., 2012; Taylor, 1988), and identity fusion. While each theory contributes to the dialogue, none is sufficient to fully explain or predict terrorist behavior. In combination, a broad view emerges which illuminates terrorist behavior.

Early studies concentrated on understanding the psychology of the individual, erroneously concluding terrorists were mentally ill. Scholars such as Post (1998, 2005, 2007) and Sageman (2004) disproved the psychopathological theories of terrorism. As trained psychologists, these researchers concentrated on both the group and individual to explain terrorists' behaviors. Although behavioral theories contributed significantly toward understanding terrorism, the main criticism was the lack of empirical research (Taylor, 2010).

The roots of psychopathological theory stem from the clinical diagnosis of personality disorders. The American Psychiatric Association (APA) categorized personality disorders using a multi-axial paradigm (APA, 2000). The most familiar are Axis I clinical disorders, which include illnesses such as schizophrenia, major depression, panic attacks, anxiety disorders, cognitive and dissociative disorders, and impulse-type control disorders not classified elsewhere. Axis II disorders are personality and intellectual disabilities, generally attributed to life-long issues appearing in the childhood years. Axis II disorders include antisocial personality disorder, dependent personality disorder, narcissistic personality disorder, paranoid personality disorder, and mental retardation (APA, 2000). At one time, researchers thought terrorists "must be insane or psychopathic" (Victoroff, 2005). However, after a thorough assessment of the research including Crenshaw (1981), and Post, Sprinzak, and Denny (2003), Victoroff (2005) concluded, "on the basis of uncontrolled empirical psychological studies…terrorists do not usually exhibit…Axis I or even Axis II psychiatric disorders" (p. 12).

Post (1998) attributed terrorist behavior to "terrorist psycho-logic" (p. 25) where he asserted "*political terrorists [were] driven to commit acts of violence as a consequence of psychological forces,* and their special psycho-logic [was] constructed to rationalize *acts they [were] psychologically compelled to commit* (emphasis in original)" (p. 25). In other words, terrorists choose the violent path because of their inherent make-up, which justify their actions (p. 25). In addition, he found terrorists did not significantly differ from their counterparts in society that do not practice terrorism.

After years of study, researchers disproved the connection between mental illness and becoming a terrorist. Indeed, Crenshaw (1981) asserted, "the outstanding common characteristic of terrorists is their normality" (p. 390). Weatherston and Moran (2003) concluded, due to the lack of evidence supporting the often-made claim, "apart from certain pathological cases, there is no causal connection between an individual's mental disorder and engagement in terrorist activity" (p. 698). Hence, in the quest to understand terrorist behaviors, other theories may be more appropriate.

Apart from the clinical psychological and psychopathological diagnoses, what then are the characteristics driving terrorists' behaviors? According to Post (2007), terrorists' identities are "established early, so that hatred is bred in the bone" (Post, 2007, p. 12). After studying terrorists, and spending hours interviewing them, Post (2007) concluded, "there is a multiplicity of individual motivations" (p. 12). However, the most powerful explanation was to study terrorist group dynamics, and its "collective identity" (p. 12). Due to Post's (1998, 2005, 2007) comprehensive research, much of the literature now centers on the effect of groups on the behavior and motivations of individuals, in addition to the individual behaviors alone.

Borum (2003), another clinical psychologist, looked at terrorism as an ideological process. He asserted understanding the enemy from the process perspective would provide additional insights into terrorists' motives. The four ideological processes in Borum's (2003) model are "it's not right," "it's not fair," it's your fault," and "you're evil" (p. 8). The model perhaps leads to an understanding of the radicalization process, and ultimately contributes to a deeper understanding of the ideological motive. Yet refreshingly, Borum (2003) asserts, "ideology may be *a* factor, but not necessarily *the* factor in determining motive (emphasis in original)" (p. 9).

Sociologists and psychologists focused on the terrorist organization as a rational actor (Crenshaw, 1981), noting as Watson (1913) did over 100 years ago, the environment is a causal variable based on situations in which individuals and groups find themselves. Crenshaw (1981) called "factors that set the stage…[and] specific events that immediately precede the occurrence of terrorism" (p. 381) preconditions and precipitants, respectively. Rapoport (1999, 2001, 2004) reinforced and supported her observations with his Wave Theory in which certain environmental characteristics, critical factors, and catalysts initiate a new wave every 30 to 40 years.

Group theory is also germane to this research because there is a strong link between individuals and group dynamics, particularly regarding identity fusion (Post, 2005; Swann et al., 2012). Individuals are driven by the camaraderie of the group—whereby "a single common emotion that drives the individual to become a terrorist" (Crenshaw, 1981, p. 394) is the feeling of revenge which "the terrorist aspires to represent" (p. 394). Characteristics of individuals can include their anger, ambivalence, aggressiveness of which they are unaware, the feeling of a lack of importance, and stress seeking (pp. 384-390). Leaders may be extraverted versus followers who feel a need for more structure. In essence, "the terrorist group is a family substitute" (p.

390). Participation in the group offers a form of identification often lacking in a terrorist's background.

Academics also use organizational theories to understand terrorists' preferences and the internal dynamics of terrorist organizations. According to Crenshaw (1988), organizational theories highlight "the internal politics of the organization" (p. 19) and the concept of organizations' survival (Crenshaw, 1988; Özdamar 2008). In contrast to other approaches, "organizational theory permits us to disaggregate the complexity of the opponent's values and to differentiate among different types of organizations according not only to purpose but to incentive structures and competitiveness" (Crenshaw, 1988, p. 28). In addition, organizational theory is "less coherent and more complex" (p. 28).

A newer theory, identity fusion, helps to explain how membership in groups becomes personal (Swann et al., 2012). The roots of identity fusion stem from social identity theory and date to the 1890s when "fusion-like constructs" (p. 441) of Durkheim were in vogue. From these beginnings, scholars identified "people's feelings of allegiance to the collective" (p. 442). The research advanced slowly until the late 1990s and 2000s when scholars took a greater interest in its development. According to Swann et al. (2012), "over the last three decades, the social identity perspective has shaped almost all major theorizing regarding group processes" (p. 442). Identity fusion is concerned with the "visceral feeling of oneness with a group" (p. 442). There are four principles of the theory that are distinct from prior theoretical iterations. The principles are the agentic-personal principle, identity synergy principle, relational ties principle, and the irrevocability principle (Swann et al., 2012). The authors conducted several experiments to test the principles, proving identity fusion is associated with groups such that "the personal self and the social self will combine synergistically to motivate unusually extreme sacrifices for the group" (p. 450). Identity fusion simultaneously "*augments* and *empowers* the group (emphasis in original)" (p. 452). Although an underexplored theory in terms of the behaviors of terrorists and terrorist groups, it advances the discourse and warrants continued investigation through this lens.

Victoroff (2005) reviewed other popular theories and concluded the sociological theories, such as relative deprivation theory, national cultural theory, and cognitive theories including novelty seeking and humiliation-revenge, though understudied, may play a larger role in understanding terrorism because of the influences of cognition on individuals. One of the problems with terrorism theory is, as a social phenomenon, it is difficult to systematically study primarily due to the inaccessibility of terrorists from which to interact directly to conduct empirical studies. Nonetheless, based on number of theories that dominate the research, it is evident there are "a combination of innate factors, biological factors, early developmental factors, cognitive factors, temperament factors, environmental influences, and group dynamics" (p. 34) that contribute to an understanding of terrorists' behaviors.

Rapoport (1999, 2001, 2004) asserted the catalyst for the Fourth Wave of terrorism was religion. Since 9/11, religion has been a primary topic for researchers studying terrorists and terrorism and it continues unabated. However, a promising new perspective (Francis, 2016) widens the perspective from religious ideology to *sacred* as a means to understand terrorists' motives. As Francis (2016) explained, sacred places the emphasis on issues that are of higher or lower value to a person, and thus, are non-negotiable beliefs and values that are "separated or protected from everyday ideas" (p. 913). The point of expanding the discourse by using the word sacred is to recognize motives are more than a religious ideology. That which is sacred to the terrorist or terrorist group may provide insights into ideological motives beyond religion.

Understanding the mind of terrorists is an important building block for devising counterterrorism techniques, strategies, and tactics to thwart the threat. Most germinal and older research does not assess the existential perspective of why terrorists do what they do. Cottee and Hayward (2011) consider human reasons and motives "however morally despicable their actions" (p. 980). The strengths of this research included exploring terrorism from a non-mainstream perspective, which traditionally attracted less attention, and the breadth and depth of the sources cited bolstered its validity and reliability. Since a paucity of research exists with this line of thinking, there is a further opportunity to explore motive theory.

### Terrorists and terrorism summary.

The body of literature on terrorism—its history, definitions, and behavioral theories is vast. It has progressed steadily post WW II and increased tremendously because of 9/11 with research focused primarily on the religious aspects of terrorism. Perhaps a real model of terrorism lies in a multi-disciplinary theory that has yet to be developed. With the number of definitions, types of political terrorism, and individual and group behaviors that contribute to the phenomena, advancing the literature by comparing its likeness to other nefarious actors such as spies and hackers can help elucidate the behaviors and characteristics of the individuals and groups that gravitate to this form of violence.

## Spies and Espionage

Espionage is a top-of-mind issue facing the nation. Consider the following examples. On January 27, 2015, the government convicted former Central Intelligence Agency (CIA) officer Jeffrey Sterling of multiple counts of espionage for illegally disclosing national security information and obstruction of justice (*United States v. Sterling*, 2015). In March 2015, former CIA director General David Petraeus (retired) admitted disclosing classified material in a plea deal (Schmidt & Apuzzo, 2015) with the government sparing him formal espionage charges (*United States v. Petraeus*, 2015). Walter Liew became the first person convicted of economic espionage, in March 2014, when a California US District Court jury convicted the former DuPont employee of divulging and theft of trade secrets (*United States v. Liew*, 2014). In September 2015, Liew's wife entered into a plea deal with the government after pleading guilty to conspiracy and evidence tampering related to her husband's activities (*United States v. Liew*, 2015).

In June 2013, the Federal Bureau of Investigation (FBI) charged Edward Snowden, a former National Security Agency contractor, with espionage for stealing classified government property related to national security information, and willfully communicating classified intelligence to unauthorized persons (*United States v. Snowden*, 2013). Although the case against Snowden is pending, Oleson (2015) claims Snowden "has done things that make him appear to be [a spy]" (p. 21). In July 2013, the Army convicted Private First Class Bradley Manning of violating the Espionage Act (*United States v. Manning, 2013*). He provided classified military reports, videos, and cables to WikiLeaks, an organization unauthorized to possess the information.

These high-profile cases illustrate the threat espionage poses to national security. Via the Constitution, the Founding Fathers, concerned about similar threats to the newly formed country, established and defined treason as a criminal offense (U.S. Const. art. III, § 3). The government also considered espionage a national security threat, albeit legally distinct though closely related to treason. Indeed, under certain conditions, espionage can be a form of treason (DOJ, n.d.). The legal basis for espionage is the Espionage Act (1917), while the Economic Espionage Act (1996) is the legal basis for economic espionage and protection of trade secrets. Although this research and literature review exclude the legal aspects of espionage, it is important to recognize these public laws. Following the same format as the prior section, the next sections recount history, definitions, types, theories, and the behavioral theories and characteristics of spies—the second of national security's triple threats.

**History of spies and espionage.**

Espionage is one of the oldest and most well documented strategies of the military arts beginning with its roots in ancient history to its use in the 21st century. Knightly (1986) referred to espionage as "the world's second oldest profession" (n.p.). Egyptian hieroglyphs recount tales of court spies. The ancient craft of espionage appears in the *Bible*, albeit not by name (Cardwell, 1978; Knightly, 1986) in the 13th century Before the Common Era (BCE) stories of Moses and Joshua (Champion, 2008). Moses sent scouts to "spy out the land of Canaan" (Numbers 13:2, JPS), seeking information about the Promised Land's populous, cities, climate, and other natural resources for informational purposes prior to embarking on the voyage to Canaan (Numbers 13:27, JPS). Forty years after Moses, Joshua, also seeking information, sent "two spies secretly" (Joshua 2:1, JPS) into the Promised Land for similar purposes.

In *Origins of Intelligence Services*, Dvornik (1974) notices priests and academic scholars, provided detailed analyses of intelligence, including espionage in ancient times. He traced history from the Assyrian civilization to Russia under the Mongol's rule in the late 1500s. One of the first accounts of espionage outside the Bible took place in the 10th century BCE when the Assyrians surveilled merchants' activity including cargo and personnel (Dvornik, 1974; Russell, 1999).

In Asia during the sixth century BCE, Chinese military strategist Sun Tzu (1910) described espionage as a tool of statecraft, devoting an entire chapter in *The Art of War* to espionage methods and types of spies. Espionage and spies were also prevalent in India. According to Indian scholars, Kautilya (1915) wrote *Arthashastra* sometime during the fourth century BCE. The 15-book treatise on Indian statecraft provided guidance for the kings' rule, law, and governance, and included a chapter titled "The Institution of Spies," which described spies, espionage, secret agents, and sting operations (Kautilya, 1915, p. 24).

By the fourth century BCE, Cyrus disguised troops as "'brigands' in order to authenticate their covert missions" (Champion, 2008, p. 531). Indeed, in his guidance for the *Cavalry Commander*, Greek historian Xenophon (1925/1946) observed, "it is an old maxim that, in attempting to discover what the enemy is about, it is well to employ spies (Xenophon, 1925/1946, p. 263), encouraging officers to enlist spies "before the outbreak of war" (p. 261). Not only did Xenophon (1925/1946) provide strategic advice for using spies, he also offered tactical advice and a categorical nomenclature for different types of spies.

Although not widely recognized, Champion (2008) claimed the Romans use of spies pre-dated the Greeks when he asserted, "as early as the fifth century BCE Roman corn buyers, when dealing with southern Italian tribes or with Sicilians, were occasionally suspected of being spies" (p. 533). Yet, prominent historians credit the Carthaginians with the early use of spies prevalent during the Punic Wars (Dvornik, 1974; Sheldon, 1997). By the first century BCE, the Romans became masters of espionage using merchants to provide information and relying on *frumentarii* for information as traders travelled the country. Intelligence officers also disguised themselves as traders, leading to Champion's (2008) assertion, "this may be the first evidence of the employment as spies and political agents of the *frumentarii*, or grain-dealers" (p. 534). As travel throughout the region increased, so did the number of spy disguises and the numbers of men and women practicing espionage (Champion, 2008; Dvornik, 1974; Russell, 1999). Following the collapse of the western portion of the Roman Empire, there is a rich historical accounting of ancient civilizations including the Byzantine, Arab Muslim, Mongolian, and Muscovite empires also relying on travelers, merchants, deserters, and other traitors as spies (Champion, 2008; Dvornik, 1974; Russell, 1999; Sheldon, 1977).

Moving into the Common Era, the birth of nation-states during the Middle Ages fueled the need for espionage, as spies carried diplomatic messages between monarchs and other state leaders. This "web of allegiances gave rise to laws prohibiting treason, double allegiances, and political espionage against allied lords" (Lerner & Lerner, 2004, p. 418). The Crusades and Inquisition solidified the Church's place in espionage history when it "employed spies to report on defenses surrounding Constantinople and Jerusalem" (p. 418).

During the Early Modern Period, (1500-1750), Machiavelli (1515/2006) promoted espionage as a means of retaining power, advocating deception and spying to protect one's power base. In Elizabethan England, Sir Francis Walsingham served as the queen's spymaster (Budiansky, 2005), perhaps the first official head of a covert service employing espionage. Actors outside the dubious profession at the time viewed it as crafty, devious, and dishonest. Civil servants, reluctantly, and primarily because they were ordered to do so, followed orders despite "dislik[ing] having anything to do with this sort of gentry" (Rothenberg, 1992, p. 101). Nonetheless, England's contribution to furthering the profession is noteworthy because its "intelligence community employed linguists, scholars, authors, engineers, and scientists, relying on professional experts to seek and analyze intelligence information" (Lerner & Lerner, 2004, p. 418). In spite of these advancements, spying in the early 18th century was not the force multiplier it would later become.

In the Mid Modern Period, (1750-1914) espionage for state purposes evolved. During the French Revolution, Robespierre, the infamous dictator, used spies to track down traitors. He brought them to trial and subsequently executed those found guilty (Lerner & Lerner, 2004). Throughout the modern period, economic espionage emerged in another prominent form. In 1811, during the Industrial Revolution in England, wealthy American Francis Cabot Lowell became “the most skilled economic spy of his generation” (Fialka, 1997, p. 48). After the Cartwright loom revolutionized the British textile industry, Lowell capitalized on the economic opportunity by reportedly using his photographic memory to steal blueprints (Fialka, 1997).

Espionage in the US began with the American Revolution (Halleck & Davis, 1911). From his experiences in the French and Indian wars, General George Washington recognized the need for “tactical information on the enemy’s positions and movements” (Rose, 2006, p. 16). Initially Washington did not have a cadre of spies to infiltrate enemy territory. Instead, he ran spies at night. However, when this method proved insufficient, he stood up The Knowlton Rangers, a permanent regiment dedicated to intelligence. In one of its first missions, the Rangers put spy Nathan Hale behind enemy lines to report on British troop movements. Although that spy mission was a disaster, Washington continued to press on enlisting Nathaniel Sackett to manage espionage. In 1777, Sackett teamed with Benjamin Tallmadge and together the two recruited a network of agents for the job. As America’s first “spy chief” (p. 48), Sackett developed the earliest “documents of American espionage” (p. 49). By the time Washington considered taking Philadelphia and other points south, his intelligence apparatus transformed espionage from the rag-tag days of Nathan Hale to become the force multiplier Washington needed to win the war. Yet following the war and despite recognition by Congress that espionage was a necessary tool of statecraft, the business of espionage waned. The pattern of standing up intelligence and counterespionage capability during wartime and disbanding it at the conclusion of war would repeat itself until the mid-20th Century.

Espionage at the beginning of the Contemporary Period (1914-present) caught many nations off guard. In the years prior to WWI, with the exception of Britain and Germany, most nations, including the US, failed to maintain robust foreign intelligence agencies, overt or covert. The result was a dearth of intelligence provided by “a hodgepodge of federal agencies thrashing about to find enemy spies” (Sulick, 2012, loc. 320). Through the creative genius of the British, and its well-developed intelligence service consisting of sophisticated espionage tactics and a cadre of spies, the Allies received the intelligence necessary to sabotage the Central Powers and win the war (Hiley, 1985, 1986; Lerner & Lerner, 2004; Rankin, 2009; Sulick, 2012; Wheeler, 2013). Advances in technology because of WWI, such as the airplane, the telegraph, photography, wiretapping, cryptology, and the practice of economic espionage forever changed intelligence and the business of spying.

Responding to a growing fear of German sympathizers in the US interfering with US military efforts in WWI, Congress passed the Espionage Act of 1917 making it a crime for anyone to divulge information about US national security, including military and political policies. Espionage is a violation of Title 18, United States Code, Sections 792-798, and Article 106, Uniform Code of Military Justice (UCMJ, 2019). Two prevalent domestic national security threats during the interwar period were anarchy and communism, which caused fits and starts of hysteria such as the first Communist scare from 1918-1920 and the Palmer Raids of 1919. Ultimately, the government-initiated programs to ferret out suspected spies proved less successful and led to the breakup of government entities related espionage and to counterespionage.

In the 1930s and 1940s, the rise of totalitarianism, anarchy, and communism prompted an increase in the use of spies. The US became a ripe target for espionage by countries such as Germany, the United Soviet Socialist Republic (USSR), and Japan due to the fear of another war involving America, despite its isolationist preferences and policies, and its protected location between two oceans (Champion, 2008; Rankin, 2009; Sulick, 2012, 2013). According to Sulick (2015), “the Soviets had thoroughly penetrated the US government by the 1930-40s” (p. 47). In contrast, from a counterespionage perspective, as the US entered WWII, once again the country relied on the British to jumpstart its intelligence capability (Aspin-Brown Commission, 1996). Together the countries expanded espionage, propaganda, and disinformation capabilities that helped the Allies win another world war (Rankin, 2009).

Due in part to the lack of a formal intelligence process that included integration of commands and missions, many signals regarding Japan’s plans for Pearl Harbor got lost in the noise (Wohlstetter, 1962). For the first time in history, and breaking with tradition, Congress stood up permanent institutions responsible for intelligence activities. The National Security Act of 1947 created the CIA. Indeed, to avoid controversy and prevent Constitutional challenges “intelligence was explicitly cordoned off from domestic and law enforcement affairs” (Hitz & Weiss, 2013. p. 2). The CIA assumed responsibility for foreign intelligence while the FBI became responsible for domestic law enforcement.

The 1950s ushered in the Cold War, a period of hysteria and distrust amongst the world’s superpowers. The height of espionage took place during the Cold War, from 1947 through 1991, which was characterized by few individual spies, none of which “singlehandedly [had] a major impact on national security” (Sulick, 2015, p. 47). However, “like pieces of a jigsaw puzzle…[when connected]…the information from individual spies proved vital during crises or could have changed the balance of power" (p. 47). In addition, the accusations of communist sympathizers working in government positions, by Senator Joseph McCarthy, triggered suspicion and fueled the frenzy. Abroad, the US flew secret reconnaissance missions over the USSR. Following the trial of Alger Hiss, which ultimately ended with a perjury rather than espionage conviction, the executions of Julian and Ethel Rosenberg, and the Soviet downing of a US spy plane, America regained its sensibility.

According to Sulick (2012), the pendulum swung the other way in the 1960s and 1970s as government involvement and investigations into espionage waned. Major and Oleson (2017) assert, "beginning in 1966, CIA's offensive HUMINT [human intelligence] operations against the USSR came to a halt" (p. 64). Despite the *Dark Ages* reference with respect to counterespionage of the period from 1965 through 1975, primarily due to the CIA declining to recruit new sources, espionage against the US did not wane. The Centre for Counterintelligence and Security Studies recognized 20 espionage cases during this timeframe (CI Centre, 2019).

The government unearthed the largest number of espionage cases during the 1980s. Due to the high number of espionage cases uncovered in 1985 alone, the media dubbed it *The Year of the Spy* (Shapiro, Willenson, & Monroe, 1986). According to several scholars, the primary recipient of espionage during the 1980s was the USSR (Major & Oleson, 2017; Richelson, 1995; Sulick, 2013). However, that trend changed in the 1990s with the breakup of the USSR, the fall of the Berlin Wall, the beginnings of globalization, and the digital revolution; economic espionage prevalent during the Industrial Revolution reappeared. Sulick (2013) and D. G. Major (personal communication, December 30, 2015) asserted spying by the Chinese, Russians, and other foreign governments concerned with competing in the global economy became prevalent.

Indeed, Louis Freeh, Director of the FBI at the time, testified before Congress and asserted, “the ever increasing value of proprietary economic information in the global and domestic marketplaces, and the corresponding spread of technology, have combined to significantly increase both the opportunities and motives for conducting economic espionage” (Economic Espionage: Hearing, 1996, p. 43). Freeh reported the FBI investigated 800 cases representing 23 foreign countries involved in state-sponsored economic espionage against the US (p. 64). To bolster the laws for divulging commercial information in contrast to classified, national security and military defense information covered by the Espionage Act of 1917, Congress passed the Economic Espionage Act of 1996, making economic espionage and the theft of trade secrets a federal crime.

Increasingly, since the beginning of the 21st century, “the phenomena of terrorism and espionage more often appear together” (Herbig, 2008, xii) leading to an increase of non-state actors opting into the business of spying (Lewis, 2004). The government used the Espionage Act 11 times since the 1970s (Greenberg, 2014). D. G. Major asserted, “217 spies have been apprehended and prosecuted from 1949 through 2015” (personal communication, December 30, 2015). Throughout history, although rare by the numbers, “when undetected [espionage] can have devastating consequences for national security” (PERSEREC, 2009b, p. iv). Figure 1 presents a summary of espionage cases, by decade, since 1949. Similar to terrorism, although the tools of the trade transform, the waves of change influence the nature of the business.

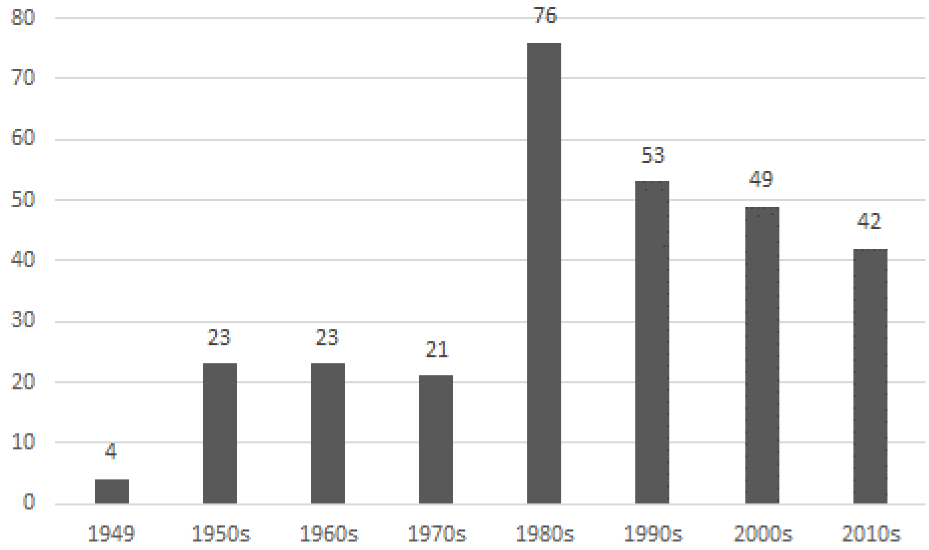


*Figure 1.* Number of Espionage Cases by Decade.
Note: Data from CI Centre. (2019, April 14). SPYPEDIA®: Espionage Cases. Retrieved from https://cicentre.com/page/case_spies. Author was an active SPYPEDA member as of dissertation date.

**Defining espionage.**

After conducting numerous Google and academic library searches, reading many journal and other scholarly publications, and searching government (.gov) websites, locating a consistent definition of espionage proved futile (Halleck & Davis, 1911; DOD, 2019; Dulles, 1963/1965/2006; Hulnick, 2004; Lerner & Lerner, 2004; Reagan, 2014; Tzu, 1910). Although Tzu's (1910) fifth century treatise on war provides guidance on spying and spy types, and Xenophon's (1925/1945) fourth century discourse references spies, the word espionage is absent in both translated manuscripts. Rather, Tzu (1910) used the word secret throughout the treatise and in particular in the chapter on spies. He reasoned secret intelligence, or foreknowledge could "only be obtained [*sic*] from other men" (p. 162) while asserting successful leaders would "use the highest intelligence of the army for purposes of spying" (p. 160). Xenophon (1925/1945) used the word spies without ever defining it. Even the evidence of the mighty Roman Empire "shows a very clear trail of covert operations, subterfuge, deceit, and mendacity" (Sheldon, 1997, p. 300) yet in the historical record, the word espionage is absent. Nonetheless, with respect to statecraft, these early writings contain three important ideas that would influence the discourse on espionage and its definition once it entered the English language: secrecy, advance knowledge, and its method of collection.

By the mid-18th century, “the association of secrecy [and]…opinions on the legitimacy of spying were far from unanimous” (Bertucci, 2013, p. 822). Indeed, Diderot, Voltaire, and Ange Goudar denounced secrecy (Bertucci, 2013). Irrespective of “admiration or contempt…readers were accustomed to the idea that travelers could be spies” (Bertucci, 2013, p. 823) due to their use in the silk industry of the 1750s, in addition to their use in the king’s court. The French word *espion* (spy) appeared in the First Edition of the *Dictionnaire de l’Académie Française* (1694) elucidating the use of “‘good spies’ in the enemy’s camp, in the city” (n.p.); the dictionary contained no definition of the word *espionage*. However, by 1798, the definition of *espionage* appeared, and indicated it “[was] a vile trade” (n.p). The French encyclopedia of the time began maintaining definitions of words pertaining to military arts. Topics such as spying, espionage, and quite unexpectedly, the word *surprise*, meaning “the events in war, or rather unexpected attacks” (Diderot & Alembert, 1751-1772/2013, pp. 693-694) emerged. Most noteworthy, the translated entry on surprise refers to Polybius’ accounts of revelations during war (p. 694).

The etymology of the word *espionage* is noteworthy. According to Lerner and Lerner (2004), it

> is interesting philologically, since French, Italian, and German have very different historic roots: the first two derived from the Latin of the Roman Empire, while the third comes from the language of the Romans’ ‘barbarian’ foes across the Rhine. It is perhaps fitting that the very etymology of *espionage* (emphasis in original) would reflect surreptitious connections. (p. 413)

The words spy and espionage entered the English language via the French, sometime during the American Revolution. Both the Americans and the British employed spies and prosecuted them during the war (Cullum, 1865; Halleck & Davis, 1911; Rose, 2006) absent legal or other definitions. One of the earliest definitions hails from the *Instructions for the Government of the Armies of the United States in the Field* (General Orders, 1863). Known as the Lieber Code, and signed into law on April 24, 1863, by President Lincoln, General Orders No. 100, Article 88 affirmed:

> A spy is a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy. The spy is punishable with death by hanging by the neck, whether or not he succeed in obtaining the information or in conveying it to the enemy. (1863, under Section V)

Ever since this definition appeared, discourse between legislators, military professionals, and legal scholars ensued, primarily due the concept of secrecy (Cullum, 1865; Halleck & Davis, 1911). Perhaps this is one reason why, when Congress vigorously debated the Espionage Act of 1917 before its passage, the secrecy debate was absent favoring other elements of language to preserve free speech and press freedoms. Nonetheless, Congress passed the Act after careful language considerations, and the Act's provisions focus on "very specific military concerns" (Stone, 2003, p. 352) during times of war, absent an articulated definition of espionage. Without a definitive definition of espionage and spies, as the country matured, so too did the definitional discourse.

For example, Congress' Committee on Un-American Activities (1949) defined a spy as "a person employed by or in the service of a foreign government, either with or without pay, to secure information considered vital to the waging of a shooting or economic war against another country" (p. 113). More recently, Hulnick (2004) defined espionage as "the use of spies or secret agents to steal information from enemies, adversaries, or competitors" (p. 165). According to the Department of Defense's (DOD) 2010/2016 *Dictionary of Military Terms*, the definition of espionage was:

> the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. (DOD, 2010/2016, p. 80)

Interestingly, the term espionage is absent in the current *Dictionary of Military and Associated Terms* (DOD, 2019).

The *Counterintelligence (CI) Glossary* (Reagan, 2014) lists several definitions for espionage and spies, recognizing the fact that depending on the circumstances surrounding the crime, different definitions may apply. The *CI Glossary* includes multiple pages of spy and espionage definitions, each from various sources, in addition to referencing components of the definitions related to the crime, the Espionage Act of 1917, and elements of espionage. The most general espionage definition refers to "intelligence activity directed towards the acquisition of information through clandestine means" (p. 130) yet in other definitions, (Reagan, 2014) cites the definition from the CI Community Lexicon, which considers espionage "overt, cover, or clandestine activity" (p. 130).

The definitional difficulty with espionage is similar to that of terrorism. As former CIA inspector general Hitz (2008) asserted, "in the circumstances of espionage and betrayal, one country's heroic spy is another's traitor" (p. 28). A comprehensive definition is unlikely because there are many aspects to the crime (Nolan, 2014). Consequently, the best definition is perhaps the one most closely associated with the offense. However, for a study such as this, espionage is the threat, theft, or compromise of national intelligence or other classified or military information acquired through covert or overt methods and divulged to a third party unauthorized to be in possession of the information.

### Categories of espionage.

Categorizing espionage as discussed in this section refers to the actors—the spies themselves—to correspond with the unit of analysis for the research and in consideration of the military strategist historical perspectives as a basis for intelligence and security. Tzu (1910) was perhaps the first to contemplate espionage as a networked system of spies, each with a unique specialty, while asserting a sovereign's effectiveness against his enemy was dependent on the integration of the information each obtained (p. 152). Kautilya (1915) also advocated espionage and categorized spies by the actions and type of information each was responsible for collecting (p. 25). Likewise, Xenophon (1925/1945) encouraged using different types of spies to collect information in addition to recommending the military commander himself spy by watching from a vantage point to observe first-hand, an enemy's blunders (p. 263).

Tzu's (1910) "five classes" (p. 152) of spies included local, inward, converted, doomed, and surviving (p. 152). Kautilya (1915) identified nine categories, meticulously defining each with a narrow focus ranging from "a fraudulent disciple (*kápatikachhátra*) (emphasis in original), a recluse (*udásthita*), a householder (*grihapaitika*), a merchant (*vaidehaka*), an ascetic practising austerities (*tápasa*), a class-mate or a colleague (*satri*), a fire-brand (*tíkshna*), a poisoner (*rasada*), and a mendicant woman (*bhikshuki*)" (p. 25). Xenophon's (1925/1945) categories included neutral state citizens, merchants, and military deserters (p. 261).

Efforts to locate a modern topology or classification scheme such as those used in the past proved unsuccessful. The closest categorization was when Congress passed the Espionage Act of 1917 shortly after the US entered WWI to address anti-war and other concerns related to the US' prosecution of the war. Subsequently, it was not until the mid-1990s that Congress recognized a difference between national security military-type espionage and economic espionage. Indeed, Congress authenticated the differentiation when it passed the Economic Espionage Act of 1996. Herbig (2017) defined five types of espionage—classic, leaks, agent of foreign government, export control laws violations, and economic (p. viii), and suggests reexamining the definition of classic espionage considering the similarities across the types.

Finally, although "there is no official definition of 'leaking' in US statutes or policy…in security and intelligence contexts" (Borum, Shumate, & Scalora, 2006, p. 97), disclosing sensitive information with significance to national security can be a type of espionage. Major and Oleson (2017) claimed, "leaks of classified information to the press are akin to a spy stealing information" (p. 69). Unsurprisingly, as compared with traditional espionage, leaking as a form of espionage is on the rise. For example, Herbig (2017) identified eight individuals charged with espionage categorized as leakers from 2005 to 2013. Yet researchers do not agree on the classification of leaking. Thompson (2018) differentiates leakers from traditional spies asserting the relationship a spy has with a foreign case officer or intelligence agency is clandestine and this type of relationship does not exist with a leaker. Nonetheless, with leaks, the US government recognizes the immediate compromise of protected information in contrast to traditional espionage, where the compromise is unknown until the government or some other party unearths the spy. Bruce (2016) asserted both leakers and traditional spies were one of the greatest threats to national security while Thompson (2018) asserted leakers supplant or augment conventional espionage and these actors have the same motives. Therefore, in this study, espionage includes leakers and leaking.

Irrespective of the historical classifications, and the modern recognition of economic espionage, today's spies collect much of the same types of information as their predecessors yet are not classified or categorized by the same terms. Perhaps this is due the changes in technology that enabled convergence of roles, responsibilities, and multi-tasking brought about by the industrial revolution and the information age. Nonetheless, behavioral and motivational theories apply to both spies and leakers.

### Behavioral theories and motivations of spies and espionage.

There is a dearth of recent theoretical literature on behavior theories and characteristics of spies and espionage, and most studies that exist are dated. Sarbin, Carney, and Eoyang (1994) explored motives that drive people to spy. This seminal book is a foundation from which to conduct research although subsequent research demonstrated weaknesses in the themes of several chapters—that most spies are in it for the money, while minimizing the effect of ideology and other motives such as revenge and ego.

The common social science models include psychological theories (Charney & Irvin, 2014; DHRA, 2012; Eoyang, 1994; Schwartz, 2007; Stone, 1989, Thompson, 2018), reversal theory (Apter, 1984; Apter, Fontana, Murgatroyd, 2014; Wilson, 2012), and behavioral and motivational theories (Charney, 2010; DCIC, 2002; Dulles, 1963/1965/2006; Herbig, 2008; Herbig, 2017; Herbig & Wiskoff, 2002; Kramer & Heuer, 2007; Levchenko, 1988). Recent research on spies revealed social norms might have an effect on the spy motivated by ideology (Lillbacka, 2017). While each theory advances the dialogue, a grand theory has yet to emerge that adequately explains or predicts the behavior of spies. Nonetheless, continued research suggests broad patterns persist.

Just as their counterparts studying terrorism, researchers first turned to clinical psychology. Eoyang (1994) asserted personality traits and situational factors contributed to espionage. Other studies concluded spies suffered from personality disorder-related diagnoses such as antisocial behavior, deviant behavior, narcissism, impulsiveness, and risk-seeking (DHRA, 2012). Unfortunately, researchers found the same personality disorders affecting spies influenced executives in the business world too, and thus, “any real attempt to use this psychiatric diagnostic concept to spot potential spies would actually result in an overabundance of ‘false-positive’ selection errors” (Stone, 1989, p. 216). In addition, results from these studies suggested, “spies are not very different from many people in the general population” (p. 220). The conclusion was similar to other white-collar crimes; espionage was a crime of opportunity, echoing the sentiment expressed by Dulles (1963/1965/2006) years earlier.

Reversal theory is a model of human behavior based on the concept of psychological turnarounds (Apter, 1984). The précis of this theory is that a person experiences tension between opposing motivations to behave in a certain manner depending on his or her internal or external environment. The most notable aspect of the theory is the identification of five pairs of *metamotivational* modes

> labeled: Telic/Paratelic, Arousal-avoidance/Arousal-seeking, Negativism/Conformity, Mastery/Sympathy and Autic/Alloic. Since they are based [*sic*] on motives, but each give rise to a whole orientation to the world-what one might think of as a whole ‘way of being’—they are also referred to as ‘motivational styles.’ (Apter et al., 1998, p. 8)

The metamotivational modes represent bipolar opposites toward which a person has dominant tendencies while at the same time exhibits salience across them (Apter et al., 1998, p. 8). To measure a person's personality changes over time, these researchers developed the Motivational Style Profile (MSP). Using MSP, numerous researchers in various disciplines explained behavioral and motivational tendencies of subjects across many topics including personality, creative processes, religious diversity, personal relationships, and social relations (Apter et al., 2014).

One of the most interesting applications of reversal theory is its applicability as an underlying theory for espionage mitigation. Wilson (2012) employed the theory to study the meta-modes of spies from three perspectives: the motivational styles, protective frames, and external emotional events (p. 77). Using the case study approach and secondary sources, Wilson (2012) assessed noted spies, including Ames, Walker, Hansen, Pollard, and Montes. Through this research, Wilson (2012) concluded the MSP was an appropriate test the government should administer routinely to security professionals, in addition to regular background checks, security clearances, polygraphs, and financial disclosures to ferret out behaviors and motivations leading to espionage, thus lessening the number of breaches of the public trust.

With respect to the behavior and motivational theories, Dulles (1963/1965/2006), in one of the earliest IC assessments asserted, "the essence of espionage is access" (p. 59). Former Soviet spy Levchenko (1988) described money, ideology, compromise or coercion, and ego (MICE) as the motives for espionage. Due to the numerous spy cases unearthed during the mid-1980s, scientists and researchers sought a behavioral profile to identify spies. The IC initiated Project Slammer to study the behavior of convicted spies, while the Defense Personnel and Security Research Center (PERSEREC) began studying spies and espionage in response to shortcomings in DOD security policies and practices (Fisher, 2000; PERSEREC, n.d.; Stilwell, 1985) during the "decade of the spy" (Rafalko, 2004, p. 217).

In 1993, based on interviews of 25 spies, the now declassified Project Slammer reports described multiple motivations for spying (DCI, 1990; DCIC, 2002) while acknowledging elevated personality disorders contributed to a person's proclivity to spy. Motivations included, but were not limited to anger, revenge, disaffection, stress, and money. Spying, concluded the Project Slammer Report, was the result of anger in contrast to greed (DCIC, 2002). The Defense Personnel and Security Research Center published four reports about espionage by Americans (Herbig, 2017, 2008; Herbig & Wiskoff, 2002; Kramer & Heuer, 2007). Although PERSEREC's (2009a; 2009b) research supported MICE, the research also provided additional explanations and notably identified the motives for conducting espionage changed over time. While contrasting findings across PERSEREC's espionage studies, Herbig (2017) indicated of the 209 individuals in the study, money remained the top motivation at 28 percent in the most recent study; however, its dominance declined from over 40 percent in earlier studies (p. vii).

Hitz (2008) asserted seven motivations—ideology, money, revenge, blackmail, friendship, ethnic or religion, and love of espionage—were the primary drivers underlying the actions behind spying. While none of these motivations is new, Hitz (2008) suggests martyrdom, a powerful concept driving much of today's Islamist-based terrorist activity, is an underlying factor "that makes the war on terrorism a formidable threat psychologically as well as physically" (p. 187). In addition, Hitz (2008) argues the "corruption of jihadism of Islam" (p. 187) and "the corruption of the concept of *takfir* (emphasis in original)" (p. 187) are additional factors driving Islamist terrorists' motivations today, and hence the country's espionage machine must consider these factors. While Hitz's (2008) perspective is rational and perhaps insightful with respect to terrorism, these motivations are a subset of the previously identified motivational factor ideology; hence, these concepts do not constitute a new motivation.

In 2008, journalists joined the discourse and began to hypothesize about what motivated spies. Writing for *The New York Times*, Shane (2008) advocated nationality and sex as additional espionage motives while cleverly creating two new acronyms: MINCE or MINCES. However, analysis of the cases upon which Shane (2008) based his suggestions revealed neither nationality nor sex was a new motivation. Rather, PERSEREC's researchers (Herbig & Wiskoff, 2002; Kramer & Heuer, 2007) had described each as part of its prior analysis.

Charney (2010) advanced the MICE theory using it to examine spying to describe espionage originating from within the US IC. His *Ten Life Stages of the Insider Spy* (pp. 48-52) updated MICE. Although Charney (2010) claimed his research focused on insiders, the 10 stages have broader application to the study of spies and espionage as defined in this research. While the 10 stages supported theories on motivation and behavior, it did not provide a complete explanation. Indeed, Burkett (2013) asserted MICE "was a good step in trying to understand agent behavior" (p. 17), yet noted the framework did not account for human behavior described by scientific studies such as Charney's (2010) or Cialdini's (2009) *Influence: Science and Practice* in which he identified six principles of human behavior. Burkett (2013) refers to Cialdini's (2009) principles as RASCLS—"reciprocation, authority, scarcity, commitment (and consistency), liking, and social proof" (p. 7).

Thompson (2013) asserted, "espionage occurs at the collision of an opportunity, a perceived life crisis, and a moral failing, which is then actuated by a trigger" (pp. 58-59). Such was the case with Aldrich Ames who took up espionage because of economic pressures resulting from his trigger: divorce. Ames initially considered his actions "a scam to get money from the

[Komitet gosudarstvennoy bezopasnosti] KGB" (SCCI, 1994, p. 11). He also claimed his actions resulted from the collapse of the Soviet Union while admitting moral failings such as arrogance believing he knew better than the government "what's best for foreign policy and national security" (Weiner, 1994, para. 14).

Mickolus (2015) assembled a book of espionage cases from 1700 to 2014. Although admittedly the book does not contain every case of espionage against the US, Mickolus' (2015) attempt is one of the most comprehensive open source resources found. There are hundreds of short vignettes about spies and espionage cases set in chronological order. To augment the cases, Mickolus (2015) also described tools, technologies, and methods. Although the research did not illuminate additional motives as previously identified in this literature review, Mickolus (2015) briefly explained shifts in motivations across the decades to bring currency to the discussion. Finally, in one of the most recent publications on counterintelligence, Lillbacka (2017) asserted prior espionage research overlooked social factors as possible predictors of ideological motives. His quantitative research demonstrated that spies motivated by ideology justify and judge their actions as consistent with his or her socially coherent group. Therefore, an analysis of a spy's social background and his or her network of social connections may provide insight into the loyalties of the ideologue who commits espionage.

#### Spies and espionage summary.

The literature review on spies and espionage confirms the lack of comprehensive research and scholarly investigation of motivations between spies and other actors in the public domain. To put this assertion into perspective, the literature searches revealed hundreds of studies on the behavioral and motivational aspects of terrorists, although spies have existed since biblical times. If specific literature on behaviors and motives of spies and espionage comparing and contrasting these actors with others exists, its publication has been outside of the public domain. Therefore, the proposed research contributes to the ongoing discourse about spies by filling the gap in research. That said, there are numerous biographies, memoirs, journalistic interpretations, newspaper articles, legal case reviews, individual case studies on notorious and infamous spies, anthologies, and encyclopedias about spies and espionage (Lerner & Lerner, 2004; O'Toole, 1988; Polmar & Allen, 2004), yet the study of commonalities of motivations and behaviors between actors is absent.

**Hackers and Hacking**

Hackers are the final group of actors comprising national security's triple threat. The DNI continues to mention cyber threats as the lead threat in the annual *Worldwide Threat Assessment* (ODNI, 2019) before Congress. In Ponemon Institute's *2018 Cost of Data Breach Study: Global Overview* study sponsored by IBM Security, Ponemon (2018) asserts the average total cost of a data breach was $3.86 million, an increase of nearly six and a half percent over the prior year. In the US alone, the estimated cost of breaches is close to $8 million, up seven percent over the prior year. Non-state hackers and malicious insiders are the cause of most data breaches in the Ponemon (2018) study. In addition, according to the World Economic Forum's (WEF) (2018) analysis of global risks, cyberattacks—a result of hacking—have an above average impact and above average likelihood of occurrence. Indeed, the WEF ranks cyberattacks and data fraud or theft in the top five for a likely global risk (2018, Figure IV). Furthermore, the WEF estimates that through 2023, cybercrimes will cost businesses $8 trillion (p. 15). Finally, the WEF asserts the growing trend of cyberattacks targeting governments and critical infrastructure worldwide will continue and is likely to cause increased disruption "and in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning" ( p. 6). As technology advances and continues to be easily accessible, hacking for both nefarious and virtuous purposes will endure.

Innovators, industry, and governments generally follow a similar behavioral pattern with respect to technology development. “Excitement, euphoria, and innovation by geeks are followed by industry assimilation and exploitation, which gives rise to pervasive public implementations, and then conflict among nations to maintain perceived advantages” (Rutkowski, 2010, p. 5). Today’s technology lifecycle continues to repeat this pattern; exploitation in the form of hacking is now a critical issue. In the early days of telecommunications, “the problem [stemmed from] any kid’s wireless transmitter in a garage…[that] wreak[ed] havoc on a network somewhere else in the world—including those supporting critical business, national security, or emergency needs” (p. 6). Due to the proliferation of the internet, its low cost, and its virtually unlimited barrier to entry, anyone with an internet-capable device and network access—not just kids in garages or nation-states—has the capability to inflict economic injury and threaten national security.

In 1995 for example, Kevin Mitnick, one of the most famous hackers and a teenager at the time, hacked into the Los Angeles bus system to acquire the punch tool required to validate bus transfer slips he found in the garbage. Mitnick took free rides by punching the transfer slips thereby extending the rides paid for by others (Mitnick & William, 2002). Jeanson Ancheta, the first hacker to take control of and tie several computers together, created a *botnet* in 2004 to send spam—unwanted email—to thousands of computers inserting malicious computer code for fun and profit (FBI, 2006). In 2015, the Obama administration confirmed hackers accessed government agencies’ computers, stealing personally identifiable information on millions of people (Davis, 2015), and nation-states stand accused of hacking into government systems (DOJ, 2016; Riley & Robertson, 2015). The FBI secured a conviction against Paul Laing, who in February 2016 received a 10-year prison sentence for his role in a fake lottery social engineering hack defrauding elderly targets (FBI, 2016).

These high-profile cases demonstrate the threat hacking poses to the nation’s economic and national security. Recognizing this, the National Security Agency began a two-year reorganization combining its offensive and defensive hacking operations into one unit (Volz, 2016). The final section of this literature review follows the same format as prior sections; it includes the history, definitions, types, and the behavioral theories and characteristics of hackers, the final actor comprising national security’s triple threat.

### History of hackers and hacking.

Counterculture technologists and groups of inquisitive individuals have historically exploited new technologies. The roots of today’s cyber era date from the development of Morse code and the invention of the telegraph in 1837. According to Florida State University’s National Magnetic Laboratory (National MagLab), by the mid-1850s, telegraph cables ran through much of the US and England. After meeting with executives at the Newfoundland Telegraph Company in 1854, inventor Cyrus Field became enamored with the possibility of connecting the US with England by laying a transatlantic cable. It was Field “and his team of investors, collectively known as the ‘Cable Cabinet’ [that] decided the cable should stretch from Ireland to Newfoundland” (National MagLab, 2014, para. 4). After several failed attempts, in 1858 the first network connecting the US with Europe became operational. However, problems ensued, and the cable failed. Years passed until, in 1866, engineers installed a permanent link between the US and England (National MagLab, 2014, para. 10).

As early as 1878, “boys played pranks with [AT&Ts] switchboard plugs” (Denning, 1999, p. 44) mostly for fun. “In the late 1890s…[a]s radio waves were unbounded by traditional nation states, wireless internets rapidly emerged worldwide” (Rutkowski, 2010, p. 6). Inventors, the government, and the private sector capitalized on new technologies, causing the technology lifecycle to progress at a rapid pace “ushering in ‘[t]he first great cyberwar era’” (p. 5). By the early 1900s, “electric jerks*”* (Hong, 2001, p. 111) conducted “attacks of a ‘scientific hooliganism’” (pp. 112-113) when Nevil Maskelyne sent “derogatory messages from his own simple transmitter” (pp. 89-90) to Guglielmo Marconi’s transmitter during the first public wireless transmission (Hong, 2001; Marks, 2011) for which Marconi won the 1909 Nobel Prize (Nobel Media, n.d.).

The international community banded together in 1904 to standardize wireless regulations and to thwart threats to the integrity of the new wireless network (Rutkowski, 2010). During the International Wireless Telegraph Convention—the 1906 Berlin Convention—participating nations ratified the first comprehensive wireless agreement governing wireless telegraphy. The US failed to endorse initial agreement. It was not until 1912, when President Taft signed the agreement, that the US became a party to the “first multilateral agreement” (p. 5) on cyberspace.

Caton (2009) asserted “although the cyberspace process has existed for centuries, cyberspace as currently envisioned came into existence with the introduction of the personal computer (circa 1975), the Internet (circa 1982), and the World Wide Web protocol (circa 1989)” (p. 210). It evolved into the internet that we know today (see Figure 2), including its nefarious past where certain actors exploited new technologies and networks for sinister purposes.

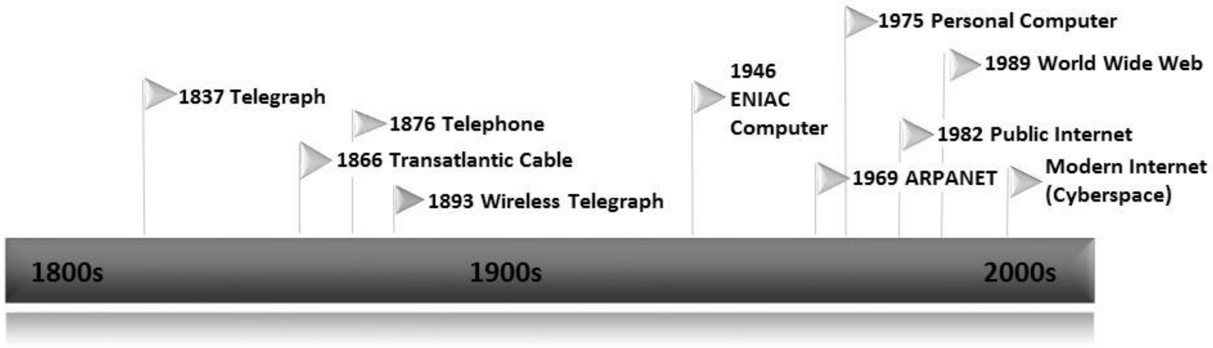


*Figure 2.* Development of the Modern Internet.
Source: Adapted with permission from publisher NDU Press (Caton, 2009).

Hacking, as we know it today, dates from the late 1940s when John von Neumann presented a theory asserting computer programs could reproduce (Scientificamerican.com). In 1957, The Whistler, a pseudonym used by Joe Engressia, discovered the Bell Telephone Company used the 2600Hz frequency to end its calls. This was the same frequency of the whistle in the Cap'n Crunch cereal box (Rosenbaum, 1971). In the 1960s and 1970s, technology enthusiasts began using words such as *crackers* and *phreakers* to describe their exploits (Krebs, 2003). Figure 3 illustrates the results of numerous high profile hacking exploits since von Neumann's assertion.

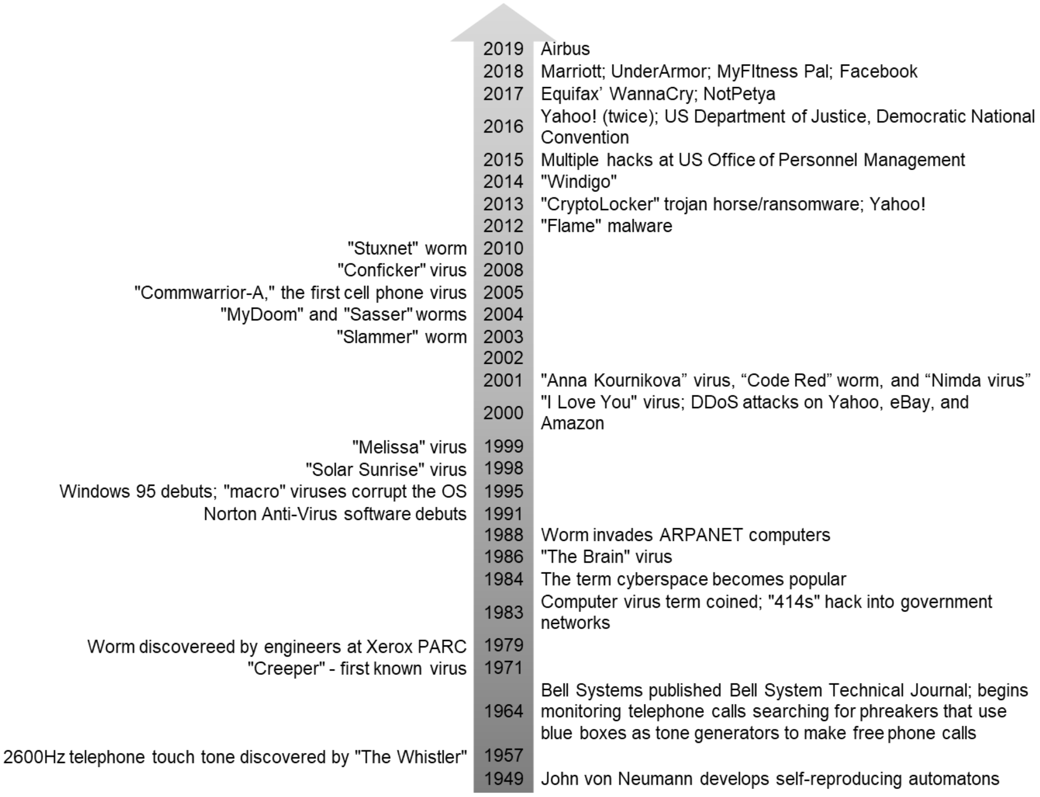

2019 Airbus
2018 Marriott; UnderArmor; MyFItness Pal; Facebook
2017 Equifax' WannaCry; NotPetya
2016 Yahoo! (twice); US Department of Justice, Democratic National Convention
2015 Multiple hacks at US Office of Personnel Management
2014 "Windigo"
2013 "CryptoLocker" trojan horse/ransomware; Yahoo!
2012 "Flame" malware
"Stuxnet" worm 2010
"Conficker" virus 2008
"Commwarrior-A," the first cell phone virus 2005
"MyDoom" and "Sasser" worms 2004
"Slammer" worm 2003
2002
2001 "Anna Kournikova" virus, "Code Red" worm, and "Nimda virus"
2000 "I Love You" virus; DDoS attacks on Yahoo, eBay, and Amazon
"Melissa" virus 1999
"Solar Sunrise" virus 1998
Windows 95 debuts; "macro" viruses corrupt the OS 1995
Norton Anti-Virus software debuts 1991
1988 Worm invades ARPANET computers
1986 "The Brain" virus
1984 The term cyberspace becomes popular
1983 Computer virus term coined; "414s" hack into government networks
Worm discovereed by engineers at Xerox PARC 1979
"Creeper" - first known virus 1971
1964 Bell Systems published Bell System Technical Journal; begins monitoring telephone calls searching for phreakers that use blue boxes as tone generators to make free phone calls
2600Hz telephone touch tone discovered by "The Whistler" 1957
1949 John von Neumann develops self-reproducing automatons

*Figure 3.* Key Hacking Events.
Sources: Data adapted by author from CSIS (2019); Greene 2015; Infoplease 2014; Krebs 2003; Orth 1971; Rosenbaum 1971; Scientificamerican.com 2001; Shapiro 1987; Totty 2011.
Note: Advanced Research Projects Agency Network (ARPANET), Distributed Denial of Service Attacks (DDoS), Operating System (OS), Palo Alto Research Center (PARC).

### Defining hacking.

For better or worse, yesterday's crackers and phone freaks morphed into today's hackers who exploit technology flaws despite the numerous countermeasures the government and private sector have undertaken to thwart the actors constantly developing new methods to circumvent security measures. Hacking was originally a non-pejorative word (Young, Zhang, & Prybutok, 2007). Apple Inc. cofounder Steve Wozniack, a reformed phreaker said, "the word hacker actually had two meanings….hackers were the heroes of the computer revolution but became outlaws in a world they created" (RCW39RJ, 2013). Over time, investigators, prosecutors, victims, journalists, and scholars began to consider hackers' activities as nefarious behavior (Chandler, 1996; Denning, 1999; Taylor, 1999; Young et al., 2007).

One early definition, used by the National Institute of Standards and Technology, refers to hackers as "people who either break into systems for which they have no authorization or intentionally overstep their bounds on systems for which they do have legitimate access" (Bassham & Polk, 1992, p. 11). A more recent definition from the National Initiative for Cybersecurity Careers and Studies, the Cybersecurity Education and Awareness Branch of the Department of Homeland Security's Office of Cybersecurity and Communications is "an unauthorized user who attempts to or gains access to an information system" (DHS, 2018). The common theme in these definitions is unauthorized *access*. Therefore, hacking, in this study, is the malicious activity individuals commit using technology to gain *unauthorized access* to computer systems and networks.

**Categories of hacking.**

There is no singular profile or persona to identify hackers. Hackers come in all shapes and sizes: the co-worker in the adjacent cubicle or a kid down the block. They come from many walks of life, any socio-economic strata, with or without a formal or technical education. Despite the intentions to simplify the cognitive thought process for the sake of study, researchers and practitioners cannot agree on a common lexicon; hence, categorization remains elusive.

For example, to study these actors, researchers have attempted to define taxonomies categorized by the type of action performed such as crackers, coders, script kiddies, crasher, and cyber-punks (Chandler, 1996; Denning, 1999, 2011; McBrayer, 2014; Mitnick & William, 2002; Rogers, 2005; Rutkowski, 2010; Wade et al., 2011). Of note, Rogers (2006) expanded his action-type taxonomy by extracting motivation from the categorization creating a second dimension, adding to the taxonomy challenge. Still, other researchers opted to categorize hackers by methodology and tactics such as distributed denial of service or website hijacking attacks

(Hatamleh, 2012). The hacker community itself attempted a similar exercise (Raymond, 2002) coming up with categories such as darksiders and elites (Adamski, 1998). One of the newest attempts to categorize hackers is by the type of knowledge they exchange (Zhang, Tsang, Yue, & Chau, 2015).

Finally, researchers, journalists, and industry watchers began referring to three categories of hackers by color of their hats, borrowing Hollywood symbolism that bad people wear black hats, while good people wear white hats. Therefore, the terms white, grey, and black hats describe hacker activity depending on the hacker's ethical or behavioral perspective (Best, 2003; Kirwan & Power, 2013; Wade et al., 2011; Yagoda, 2014). Such a categorization is fitting for this research because of its behavioral focus. White hats are generally security professionals that hack to discover and correct security flaws. Grey hats fall somewhere in the middle, perhaps stealing information, and penetrating systems for the sake of the challenge more so than for less-than-ethical purposes. Black hats are those hackers with nefarious intentions and are the subject actors of study for this research.

#### Behavioral theories and motivations of hackers and hacking.

Although a large body of research on computer security exists, in comparison, Holt and Bossler (2014) assert there is little empirical research into theories and characteristics that lead to hacking. Instead researchers relied on qualitative social science investigative methods to explain hacking based on clinical psychological theories (Campbell & Kennedy, 2014; Denning, 1999, 2011; Holt, 2007; Shaw et al., 1998; Taylor, 1999, Young et al., 2007), criminal learning and control theories (Rogers, 2001; Xu et al., 2013), and newer theories such as space-transition theory (Jaishankar, 2011). The literature search revealed a recent quantitative analysis of hacking behavior by Madarie (2017) using Schwartz's (2012) Theory of Basic Values. Similar to the other actors considered in this research, there is yet no comprehensive theory to describe why people hack.

Early research on hacking focused on the clinical psychological theories suggesting hackers exhibited antisocial behavior and lacked self-esteem, while maintaining a deep understanding of technology (Denning, 1999, 2011; Holt, 2007; Taylor, 1999). Campbell and Kennedy (2014) acknowledged some computer criminals (hackers) possessed narcissistic or anti-social behavior personality disorders as demonstrated by Shaw et al. (1998), although the researchers cautioned generalizing psychological disorders to the hacker population was a mistake due to the lack of a number of empirical studies. However, Rogers', Smoak's & Liu's (2006) empirical study demonstrated lower scores for hackers on the Five Factor Personality Model's social and moral choice measures. In addition, some clinical researchers, and reformed hackers alike, speculate a relationship between Autism Spectrum Disorder (Schell & Melnychuk, 2011), in particular Asperger's Syndrome, and hacking (Zuckerman, 2001) although some empirical studies suggest otherwise (Schell & Meluychuk, 2011; Seigfried-Spellar, O'Quinn, & Treadway, 2015). Perhaps because clinical psychological theories failed to explain hackers' behaviors, researchers turned to studying hackers and hacking through the criminology lens.

According to Rogers (2001), hacking is a criminal activity. Hence, understanding the criminal learning and control theories such as social learning (Akers & Jensen, 2006; Bandura, 1971), routine activity theory, situational action theory, space-transition theory (Jaishankar, 2011), and behavioral and motivational theories (Bossler & Burruss, 2011; Holt & Bossler, 2014; Holt & Kilger, 2012; Rogers, 2001; Wikström, 2010, 2014; Xu et al., 2013) can help explain hacker behavior. The number of theoretical lenses by which to study hacking suggests there are multiple aspects to explain hacking behavior.

Social learning theory (SLT) is one criminal theory researchers attribute to the hacking. Initially described by Bandura (1971), SLT posits three aspects of motivation—external reinforcement, vicarious reinforcement, and self-reinforcement—guide behavior. People learn via observation from their relationships with other people in the groups with which they associate and from their surroundings. Bossler and Burruss (2011) asserted "much computer hacking could be explained…by the social learning process and low levels of self-control" (p. 60), although individuals with high levels of self-control were also prone to hacking. Using the theory to describe criminal activity, Akers and Jensen (2006) demonstrated crime is a learned deviant behavior. At a cognitive level, hackers adopt behaviors from each other because, as part of the hacker culture, learning takes place from association with one another (Holt & Kilger, 2012; Rogers, 2001).

Criminal situational and action theorists associate hacking with routine activity theory (RAT) and situational action theory (SAT) (Holt & Bossler, 2014; Wikström, 2010, 2014; Xu et al., 2013). As it relates to hacking, RAT portends that when hackers meet targets in the absence of supervision, cybercrimes such as hacking are likely to occur. According to Xu et al. (2013), each of the above conditions "must be present, but they are only the necessary conditions" (p. 72). Situational action theory seeks to explain why people break rules and commit crimes. It considers the *person*, the *place or setting*, and the *action*, collectively thought of as the situation; SAT posits individuals make choices based on moral judgment and the action is a result of the situation (Wikström, 2014). Rogers (2001) demonstrated the connection of these three theories in his dissertation, which supported the hypothesis regarding association and reinforcement. Similarly, Xu et al. (2013) supported their hypothesis that SLT, RAT, and SAT are, in part, explanations of the progression of hackers from white hats to black hats. At the same time, Xu et al. (2013) assert critical elements of hacker behavior, such as motivation and opportunity, remain unexplained by these theories.

One of the newest theories regarding cybercrimes is space-transition theory (STT) (Jaishankar, 2011). Due to the failure of other theories to explain cybercrimes and to advance the discourse, Jaishankar (2011) proposed STT, which posits people's behavior changes as they move from the physical to the cyber world. The most notable of the seven aspects of the theory, as related to hacking, are the anonymity provided by computers, the lack of deterrents, and the conflict in behavioral norms between the physical and electronic worlds. While aspects of STT helped to explain hacker behavior, the motivational theories where researchers sought reasons are germane to this research in a similar manner as these theories were for the other two actors consisting of national security's triple threat.

The behavioral-based theoretical literature on hacking builds upon the behavioral theories used to describe espionage. Kilger, Arkin, and Stutzman (2004) and Holt & Kilger, (2012) transformed the MICE motivations of espionage to apply to hackers and hacking. Eventually these researchers settled on six motivations: money, entertainment, ego, cause, entrance to social groups, and status, creating the acronym MEECES. Using this model, researchers attempted to explain the motivations of hackers by developing a profile to identify proactively, hacker motivations. While Wade et al., (2011) acknowledge the MEECES motives, they identify additional motives such as addiction, curiosity, and revenge. The thought was by gaining a deep understanding of motives and behaviors strategic security professionals and others, such as co-workers, could perhaps prevent nefarious behavior before it caused harm.

For example, Thycotic™, a cybersecurity company, regularly attends the annual Black Hat hacker conference. At the 2014 conference, the company conducted a survey containing questions on hacker motivation. According to B. Stucky (personal communication, May 5, 2016) the response choices "were based on the MEECES model." In fact, the results of the study demonstrated the top two motives were entertainment and social. Of the 127 respondents to the motivation question, 51 percent cited entertainment (fun/thrill-seeking) while 37 percent indicated their motivation was social consciousness/moral compass (B. Stucky, personal communication, May 5, 2016; Thycotic™, 2014). This is consistent with a study of 54 Israeli hackers conducted by Turgeman-Goldschmidt (2005) where the hackers helped the researcher identify 10 motives related to entertainment.

Researchers (Holt & Bossler, 2014; Holt & Kilger, 2012; McBrayer, 2014) continue to rely on the MEECES model as evidenced by the recent research, although additional behaviors are also considered. Returning to Madarie's (2017) quantitative study, the hacker-reported motivations in the study are similar to those identified in prior qualitative studies. Interestingly however, Madarie's (2017) study suggests hackers' narratives describing their reasons for hacking diverge from the prioritizations found in prior literature. Despite the increasing prevalence of hacking and other cybercrimes, Holt & Bossler (2014) assert, the behavioral and motivational aspects of hackers and hacking remain under-examined. Therefore, the behavioral theories that underpin this study help to fill the gap.

**Hackers and hacking summary.**

The corpus of literature on hackers and hacking is diverse. There is relative consensus about the history of hacking. However, beyond that aspect, the theories and scholarly investigations branch out into multiple directions. While the early researchers identified behaviors and posed theories, later researchers focused on the types of attacks and methods of attack somewhat forsaking the will to press onward to understand the behaviors and motives more fully. Perhaps this is because it is easier to study technical aspects of cybercrime vice the softer and more challenging aspects involving human behavior. The dearth of recent hacker related behavior scholarship supports this assessment. Nonetheless, in the pursuit of understanding behaviors of actors posing threats to national security, the behavioral theories on hackers and hacking provide a foundation for the current study and contribute to the identification of characteristics across the three actors by advancing the literature to assess the convergence or divergence of behaviors.

### Literature Review Summary

The combined body of literature on terrorists and terrorism, spies and espionage, and hackers and hacking is vast. Researchers build upon the history, definitions, and behavioral theories of each actor as new studies are completed. Despite vertical progress to advance the depth of research on each actor individually, there is a paucity of research examining the horizontal breadth. Therefore, investigating similarities and differences amongst these actors and their actions across a common set of variables provides the impetus for the central research question. Additionally, in the context of the problem, a multi-dimensional triple threat to national security, this lacuna paved the way for this study, which advances the body of literature to understand the motives of the actors that gravitate to these forms of violence.

# Chapter 3: Methodology

The process by which a researcher undertakes a project depends largely on the type of research contemplated and the questions the researcher seeks to answer. One of the most important aspects of a research project is selecting the best method or methods of inquiry from which to approach and structure the proposed project. The most common approaches are qualitative, quantitative, and mixed methods. Each approach has traditions and norms; each has its strengths and weaknesses (Creswell, 2013, 2014; Mahoney & Goertz, 2006). Irrespective of the approach selected, the researcher's goal is to produce valid inferences about the topic and to support or refute hypotheses or answer questions posed. Several scholarly publications influenced selection of the methods, approaches, and techniques for the research on terrorists, spies, and hackers (Crowe et al., 2011; Creswell, 2013, 2014; Mahoney & Goertz, 2006; Merriam, 2014; Merriam & Tisdell, 2016; Patton, 2015; Yin & Heald, 1975).

## Research Methods and Approaches

This research employed the qualitative research methodology using an interpretive approach (Taniguchi, 2014). Two methods of inquiry comprised the research: Case studies and interviews. The researcher used the case study method to review historical documents containing the descriptions of the motivations of terrorists, spies, and hackers, created a database of the combined data and proposed a typology of converging motivations. The interview method enabled the researcher to test the validity of the proposed typology and to identify other motivations, perhaps not identified via case studies. Using both methods of inquiry permitted the researcher to develop and understand the converging motivations of each of the three actor groups—terrorists, spies, and hackers—while increasing the validity of the study. See the summary of the study design in Table 4.

*Table 4.*

*Study Design*

| Methodology | Method | Mode | Tools | Analysis |
|---|---|---|---|---|
| Qualitative, Interpretive (Creswell, 2014; Taniguchi, 2014) | Case Study (Creswell, 2014; Merriam, 2014, Stake, 1978; Yin and Heald, 1975) | Historical Documents (Creswell, 2014) | MAXQDA | Content Analysis (Mayring, 2014; Morgan, 1993) |
| Qualitative, Interpretive (Creswell, 2014; Taniguchi, 2014) | Semi-structured Interviews (Creswell, 2014; Lincoln & Guba, 1985; Mayring, 2014; Patton, 2015); Robinson, 2014) | Telephone (Creswell, 2014) | Audio Recorder | Text and Keyword Analysis (Creswell, 2014; Mayring, 2014) |

Source: Author

Because the case study method of inquiry did not involve research on living subjects, the case study research received an Exempt determination by Henley-Putnam's Institutional Review Board per Title 45 – Public Welfare, Part 46–Protection of Human Subjects Exempt Review section. For the interview method of inquiry, NAU's IRB reviewed the proposed research method and procedures in accordance with Title 45 – Public Welfare, Part 46–Protection of Human Subjects, review section and approved the research protocol as Expedited. See Appendix A for the NAU IRB approval letter and Appendix B for the researcher's confidentiality statement. The following sections of this chapter describe the methods of inquiry, protection of participants in this study per Title 45 – Public Welfare, Part 46–Protection of Human Subjects, and the guidance of the US Department of Health and Human Services (DHHS), including the Belmont Report (DHHS, 2016).

**Case Studies**

The researcher built a database of case studies to analyze for this research. Computer-assisted content analysis, using MAXQDA software, served as both a form of data collection and analysis. Based on the motivation literature reviewed for each actor, the researcher used

MAXQDA to reveal the key motivational themes and details (variables if this were a quantitative study) for investigation. Purposive sampling was the primary method for case selections in each actor group normalizing for US citizens, or in the case of terrorism, to US-based events. However, the procedure for selecting cases for each actor group varied slightly based on the sources available.

To analyze cases after selection, the researcher endeavored to collect primary and secondary historical data from at least three sources per case. The researcher reviewed data sources for each case and consolidated sources into a summary record of the details and evidence for each actor's nefarious action or actions. Finally, content analysis of the summary evidence for each case in the database facilitated identification of the motivations for each actor or event within the database. There were several reasons for this method and approach.

First, qualitative methods facilitate understanding the hows and whys of human behavior, and interpretation of social interaction (Compton-Lilly, 2013; Mahoney & Goertz, 2006; Yin, 2012, 2014). Second, a single, simultaneous study of the three actors facilitated concurrent, synchronized data collection and analysis to investigate the topic in greater depth than previously attempted. According to Merriam (2014), case studies are "a means of investigating complex social units consisting of multiple variables of potential importance in understanding the phenomenon" (p. 50) under study. Third, case studies are a common approach to inquiry in the social sciences (Creswell, 2013, 2014; Crowe et al., 2011; Stake, 1978; Thomas, 2011, Yin, 2012, 2014). According to Crowe et al. (2011), the case study is "particularly useful to employ when there is a need to obtain an in-depth appreciation of an issue, event, or phenomenon of interest" (p. 1). Yin and Heald (1975) assert, "a common feature of most policy literatures is that the bulk of the empirical evidence is embodied in case studies" (p. 371). For these reasons, the case study approach to this research was appropriate.

Although the case study has come into its own over the last quarter century, the method is not without its detractors. While a single case study "may provide rich insights into a specific situation, it is difficult to generalize about the…whole" (Yin & Heald, 1975, p. 371). The case survey approach helps to overcome this criticism because it "carries the classic case study one major step forward; it enables aggregate reviews of individual studies to be undertaken [*sic*] with scientific rigor" (p. 372). This assertion justifies selecting the case surveys.

In addition, the case survey approach is a new angle from which to research national security's triple threat to enable a deeper understanding of the motives than in previous studies as determined in the literature review. In consideration of these perspectives, and with a view to the intended audience, the case survey approach using content analysis of historical data was an appropriate combination and pragmatic methodology for conducting this research.

#### *Case selection.*

With the case survey approach, the unit of analysis is the case—multiple cases (Yin & Heald, 1975). Researchers conducting case studies generally do not test a priori hypotheses; rather, the method relies on seeking answers to central and sub-questions to identify patterns and themes within the context of the case and between cases. Therefore, "case selection is the primordial task of the case study researcher, for in choosing cases, one also sets out an agenda for studying those cases" (Seawright & Gerring, 2008, p. 294). Due to a relatively small population of cases from which to choose, "purposeful strategies instead of methodological rules" (Patton, 2015, p. 311) guided sample selection.

***The sampling strategy.***

There were three goals for sampling. First was to create a representative, objective, and unbiased sample from which to conduct the case survey analysis by creating a combined database with names of actors, or in the case of terrorism, the events, in each of the three groups. The second was to select a realistic and equal number of cases to enable an analysis of the actors' motivations without over- or under-counting, and to complete the analysis in the period allotted for the research project while answering the research questions. The third was to use commonly accepted sampling techniques to increase the validity and re-creation of the study, a best practice in academic research. For these reasons, the researcher used a two-step case selection sampling strategy to create the sample of cases for each actor in the combined database.

Using the purposive maximum variation strategy, the researcher determined criteria for selecting an initial set of cases to consider for the case survey sample (Creswell, 2013; Patton, 2015). The maximum variation sampling strategy yields cases with "important shared patterns that cut across cases and derive their significance from having emerged out of heterogeneity" (Patton, 2015, p. 283). Although weakness in maximum variation is a common critique due to a diverse set of cases, Patton (2015) argued the weaknesses are actually strengths because "common patterns that emerge from great variation are of particular interest and value in capturing the core experiences and central, shared dimensions of a setting or phenomenon" (p. 283). In addition, maximum variation sampling typically leads to larger sample sizes than are desired for case survey analysis. To reduce the size and narrow the sample to characteristics found amongst identified crosscut variations, the researcher employed a second strategy based upon random sampling. Merriam & Tisdell (2016) suggest that random sampling is a valid method of selecting cases for multiple case studies to increase validity. Using these two sampling strategies, the researcher constructed a database containing multiple cases for each of the three actor groups.

Patton (2015) asserted, “there are no rules for sample size in qualitative inquiry” (p. 311). Creswell (2013) recommended, “4 or 5 [*sic*] cases in a single study” (loc. 3094). The point is that the sample size is a matter of judgment; it must be an appropriate size for the researcher to obtain a rich set of evidence from which to conduct analysis. Fusch and Ness (2015), Merriam and Tisdell (2016), and Patton (2015) each stress sample sizes in qualitative case study research should depend more on saturation than on a fixed, pre-determined number of cases. As defined by these seminal methodological researchers, saturation is the point at which no new information contributes to the phenomena under study. In addition, Mason (2010) contended samples “are drawn to reflect the purpose and aims of the study….[such that] the sample size becomes irrelevant as the quality of data is the measurement of its value” (p. 14).

Finally, Mason (2010) conducted research on 560 qualitative dissertations and found of the 213 studies using content analysis, the median number of case studies was 25, the mean was 28, and the mode was 30 (Table 1, p. 8). For all qualitative dissertation studies, “the most common samples sizes were 20 and 30” (p. 13). Recognizing the disparate guidance regarding sample sizes, the concept of saturation, and the time to complete the study, the target sample size was 60 cases divided evenly between each actor, which is in line with Mason’s (2010) findings.

***Building the case study database.***

The first task in case selection was to build an actor case study database since no single database containing the three actors groups existed. As required for using the purposive maximum variation strategy, the researcher determined initial criteria. The criteria for including cases in the initial sample varied depending on the actor under consideration as described below:

Terrorists The main criterion for inclusion of a terrorist case was the perpetrator must be an identifiable US citizen or identified terrorist group, actor that intentionally committed an act of violence to incite fear, intimidation, or coercion against the US to threaten national security outside the commonly accepted rules of engagement for war. For this exercise, the researcher used the FBI's definition of domestic terrorism found in 18 U.S. Code § 2331(5) – Definitions (FBI, n.d.). In addition, details of the case must be accessible through unclassified publicly available sources such as books, journal articles, and government documents or be available via Freedom of Information Act requests.

Spies The main criterion for inclusion of an espionage case was the spy must be a US citizen who committed a breach or compromise of information deemed of importance to national security. As a result, the government indicted the suspected spy for espionage under the Espionage Act, Title 18, United States Code, Sections 792-798, or Article 106, of the Uniform Code of Military Justice. The reason the criteria does not specify an espionage conviction is because of the difficulty of prosecuting espionage cases according to the high standards and legal precedents proving espionage (Appel, 2003; Sun, 2003). To achieve the government's goals, it often prosecutes these cases under lesser charges. In addition, details of the case must be accessible through unclassified publicly available sources such as books, journal articles, and government documents or be available via Freedom of Information Act requests.

Hackers The main criterion for inclusion of a hacker case was he or she must be a US citizen who intentionally penetrated other entities' computer systems gaining unauthorized access. Since a commonly accepted legal definition of the term hacker is absent, the key aspect of consideration for this research is the intruder accessed a system "without authorization" (Eltringham, 2015, p. 5). In addition, details of the case must be accessible through unclassified publicly available sources such as books, journal articles, and government documents or be available via Freedom of Information Act requests.

With these criteria in mind, research to select each actor sample began. To build a database of case summaries of terrorists or terrorist events from which to execute the sampling strategy, the researcher relied on the University of Maryland's Global Terrorism Database (GTD), "an open-source database including information on terrorist events around the world from [January] 1970 through [December] 2015" (START, 2016a, para. 1). The GTD is perhaps the most comprehensive, current, and respected collection of terrorism cases such that the US State Department relies on START, and the GTD data to compile the annual Country Reports it provides to Congress (START, 2016b).

From this database containing 156,772 records, the researcher used GTD's filters to narrow case selection. The initial selection included cases where both the place (location) in which the incident occurred and nationality (natlty1) of the target attacked was the US. In addition, cases selected showed no doubt (doubterr) the incident was terrorism, GTD coders considered the attack domestic on all dimensions (INT_ANY), and a perpetrator or group claimed responsibility (claimed) for the event, as described in the *Codebook: Inclusion Criteria and Variables* (Codebook) (START, 2016c). The resulting database included 86 records. However, it excluded the year 1993 due to the loss of data as explained in the Codebook. To rectify this, the researcher explored the separate 1993 publicly available database provided by START using the above-mentioned criteria and located an additional 13 cases. Consequently, the initial terrorist selection database built for this research included 99 terrorist event records from 1970 to 2015.

The researcher was aware of two databases containing information on spies. The Personnel and Security Research Center (PERSEREC) Espionage database includes "case summaries in which US information or assets have been targeted" (PERSEREC, 2009b, p. iv). PERSEREC's data (Herbig, 2008; PERSEREC, 2009a, 2009b) contains case summaries from 1947 to 2008. The SPYPEDIA® database, available by subscription from the Centre for Counterintelligence and Security Studies (CI CENTRE, 2019), contains espionage case summaries from 1945 through the present day. To develop the list of espionage cases from which to execute the sampling strategy, the researcher combined and de-duplicated the names of US spies found in these sources. In addition, the researcher conducted internet searches, and consulted the academic books and journals used in the literature review searching for additional names and espionage incidents to add. The researcher was unable to locate additional case studies using additional sources. The resulting espionage database contained the names of 309 spies from 1949 to 2016.

Unfortunately, the researcher was unable to locate a credible database of hackers. Consequently, the researcher explored books, journals, websites, and used search engines to identify cases about hackers. From conducting numerous searches, the researcher identified 99 hackers by name or pseudonym. To build the initial database for selecting hacker cases, the researcher only included cases where a named individual, versus pseudonym, was available and the individual was a US citizen. The resulting database contained the names of 40 hackers from 1971 to 2016.

With the initial database of actors identified, the researcher executed the second step of the sampling strategy. The researcher generated a random number for each of the cases within each actor group using Microsoft Excel's random function. Within each group, the researcher sorted the cases into ascending order based on the random number generated for each case and selected the first 20 cases in each group for the study sample. Thus, 60 case studies became the combined database—the foundation for the research and subsequent data analysis.

***Data sources (evidence)***

As noted, the goal for sample size was to amass sufficient data to answer the research questions based on the concept of saturation. Similar to the multi-step approach for case selection, the researcher also used a multi-source approach for data collection to amass motivational evidence for each case. Qualitative data collection relied upon document review of primary and secondary sources (Yin, 2012). If possible, the researcher located primary sources to provide the first-hand accounts by the actors of his or her motives for conducting terrorism, espionage, or hacking. Primary source documents included autobiographies, interviews, testimony, speeches, photographs, and websites such as YouTube videos to obtain terrorists', spies', and hackers' first-hand accounts of events and their actions.

Secondary source reports by third parties that did not personally experience the phenomena of interest (Merriam, 2014) augmented the evidence and data collection effort.

Examples of secondary sources included biographies, archival records, and media accounts of allegations, charges, incitements, and conviction records of terrorists, spies, and hackers. Using primary and secondary sources, the researcher attempted to locate at least three pieces of evidence to identify motivations and to increase validity by data triangulation. Triangulating sources and analysis methods confirmed data points and improved study validity and reliability.

### ***Data collection and qualitative content analysis.***

When using the case study method, according to Hartley (2004), "data collection and analysis are developed together in an iterative process" (p. 329). Using this technique enabled the researcher to conduct initial analyses and make adjustments as data collection progressed, a hallmark of the qualitative approach (Creswell, 2013, 2014; Merriam, 2014; Merriam & Tisdell, 2016; Patton, 2015). In addition, content analysis, "quantitative analysis of qualitative data" (Morgan, 1993, p. 113) served as an additional data collection and analysis methodology. Content analysis of the literature reviewed for each actor facilitated data collection helping the researcher identify the motives for the coding system (Erişen, Erişen, & Özkeçeci-Taner, 2013; Hsieh & Shannon, 2005; Kohlbacher, 2006; Mayring, 2014; Moreira & Costa, 2016; Morgan, 1993). The primary question answered during the content analysis coding process of the literature for each actor was, what motivations do researchers identify as the reasons for that actor's actions—terrorizing, spying, or hacking? For an overview of the data collection and qualitative content analysis process, see Figure 4.

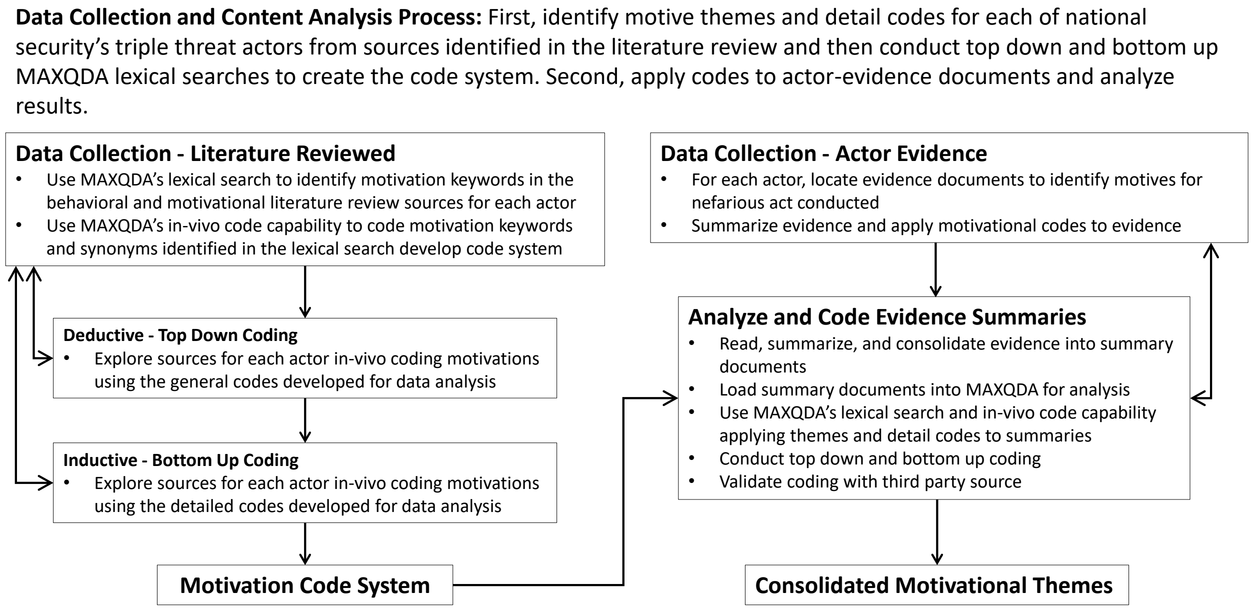

Data Collection and Content Analysis Process: First, identify motive themes and detail codes for each of national security's triple threat actors from sources identified in the literature review and then conduct top down and bottom up MAXQDA lexical searches to create the code system. Second, apply codes to actor-evidence documents and analyze results.
Data Collection - Literature Reviewed
• Use MAXQDA's lexical search to identify motivation keywords in the behavioral and motivational literature review sources for each actor
• Use MAXQDA's in-vivo code capability to code motivation keywords and synonyms identified in the lexical search develop code system
Deductive - Top Down Coding
• Explore sources for each actor in-vivo coding motivations using the general codes developed for data analysis
Inductive - Bottom Up Coding
• Explore sources for each actor in-vivo coding motivations using the detailed codes developed for data analysis
Motivation Code System
Data Collection - Actor Evidence
• For each actor, locate evidence documents to identify motives for nefarious act conducted
• Summarize evidence and apply motivational codes to evidence
Analyze and Code Evidence Summaries
• Read, summarize, and consolidate evidence into summary documents
• Load summary documents into MAXQDA for analysis
• Use MAXQDA's lexical search and in-vivo code capability applying themes and detail codes to summaries
• Conduct top down and bottom up coding
• Validate coding with third party source
Consolidated Motivational Themes

*Figure 4.* Data Collection and Analysis Overview.
*Source:* Created by author.

After identifying and loading the literature (documents) for the content analysis into the MAXQDA software by document group (terrorist, spy, or hacker), the researcher used the software to identify the motivation keywords in the literature automatically and then manually reviewed the validity of the identified words. Next, the researcher set the software to code automatically the motivation source documents. However, MAXQDA's automatic coding was unsuccessful because many of the Portable Document Format (PDF) document formats were incompatible with MAXQDA's ability to search the PDF. The incompatibility with MAXQDA's functionality was due to the age of some of the PDFs and an inability to recreate the PDFs using PDF file formats MAXQDA could consistently read. The result was inconsistent automatic coding of motivation variables within PDFs.

To overcome this challenge, instead of auto coding, the researcher used MAXQDA's lexical search capability on each PDF to in-vivo code and tag motivation keywords using both deductive and inductive reasoning to build the coding system. Using this approach, the researcher created and then verified the coding system with a third party consultant versed in MAXQDA. Following code system verification, the researcher loaded case study summary evidence data sources into MAXQDA for in-vivo coding, creating the consolidated and converged motivational theme typology. Finally, the researcher used the MAXQDA software to perform data analysis and visualizations, and develop presentations of the data for display in the results chapter.

The data collection and qualitative content analysis approach, although not difficult, required the researcher to spend time learning the MAXQDA software. The researcher purchased the software and consulting services to achieve proficiency in the shortest time possible. Working with the consultant, the researcher took individual instructional courses including software setup, function use, and analysis techniques. Once proficient, the researcher was able to make explicit observations and interpret the resulting data.

**Interviews**

The case study research in this dissertation established a proposed model of converging motivations. The researcher has no experience as a terrorist, spy, or hacker. To improve the validity and help judge the appropriateness of the proposed model and extend the research, in consultation with the researcher's dissertation Committee Chair and the doctoral program Dean, the interviewer chose to conduct interviews as a second method of inquiry, extending the research as described in Chapter 1. Using interviews improves study validity because it enables triangulation of data obtained in the case study method (Lincoln & Guba, 1985).

The researcher used semi-structured interviews to investigate the motives of terrorists, spies, and hackers. Interviews are a common data collection technique to gather insights from a small number of people (Creswell, 2013; 2014; Merriam & Tisdell, 2016; Robinson, 2014).

Typically, interviewees can provide opinions and analysis, and are rich sources of information about the phenomena under study and are advantageous when the researcher cannot directly observe participants in action (Creswell, 2014). In this study, interviewees helped the researcher validate or refute the researcher’s interpretation of the consolidated and converged motivational typology model derived using the case study data.

According to Patton (2015), researchers cannot observe the feelings, thoughts, behaviors, and past actions of others in retrospect, therefore, the interview method “allow[s] us to enter into the other person’s perspective” (p. 426). The researcher use the “interpretive interactionism” (p. 436) interview to learn about interviewees’ experiences and perspectives with these actors using the “interview guide approach” (p. 437) to explore the motivations identified. Interviews took place using the telephone because of its convenience and low cost in comparison to the cost of arranging face-to-face interviews across multiple states. The critical steps to prepare for interviews in this study included participant selection, sample size, developing the interview guide, planning and managing logistics, conducting the interviews, transcribing the recorded sessions, and evaluating the results.

### ***Participant selection and sample size.***

The researcher obtained interview participants using the convenience sampling method (Bhattacherjee, 2012; Creswell, 2013; Robinson, 2014). The researcher selected this narrowly focused sampling strategy because the population of terrorists, spies, and hackers and the population of experts with knowledge of the motivations of these actors are difficult to access. Although convenience sampling is not strategic and may be biased, researchers primarily use it when it is difficult to identify a population to sample (Bhattacherjee, 2012; Creswell, 2013), as was the case in this study. In addition, because the case study method used previously provided the breadth of data, adding the interview method extended the depth of data the researcher collected. Consistent with the depth of data is the use of a small sample size. According to Bhattacherjee (2012), "convenience samples and small samples are considered acceptable in interpretive research as long as they fit the nature and purpose of the study" (p. 104). Finally, Creswell (2013; 2014) advocates a deep, thick, exploration of the phenomena under study in certain conditions. Conducting interviews enabled this type of deep exploration.

The primary criterion for interviewee selection for this study required the participants to have deep knowledge of the phenomena under study (Creswell, 2013; 2014; Merriam & Tisdell, 2016). Interviewees must have worked in their field of expertise for at least one year. The secondary criterion for selection was that interviewees were willing to reflect upon and to share opinions about the actors' motivations from the interviewee's career perspective. The tertiary criterion was the interviewees were adults. Using the criteria above, the researcher reviewed biographical summaries of NAU's faculty to identify potential interviewees with deep knowledge of counterterrorism, counterespionage, and cybercrimes.

The goal for interviewing was to augment the data derived using the case study method to uncover experts' feedback about the proposed motivational typology model. The researcher required one knowledgeable expert for each actor group—terrorist, spy, and hacker—thus the interview sample size of three. Again, the justification for a small sample size in line with Mason's (2010) assertion that "sample size becomes irrelevant as the quality of data is the measurement of its value" (p. 14). Finally, in-depth interviews may reveal information researchers are unable to collect using other methods such as case studies, thus filling voids in the research.

Since interviews do not provide a broad range of perspectives, for this study, the researcher used the interview feedback to confirm or refute findings about converging motivations, and possibly identify additional motivations not observed in case studies. Due to the small sample size and narrow perspective, the researcher cannot generalize to the population of terrorists, spies, or hackers. The following sections describe the research design for the interview research method and the protections to ensure no harm to study participants.

***Protection of participants.***

While developing the research design for this study, the researcher considered the protection of human subjects paramount. Precautions used in the research complied with Title 45 – Public Welfare, Part 46–Protection of Human Subjects and DHHS' guidance for research on human subjects (DHHS, 2016). The protections included informed consent, protection from harm, disclosure of risks and benefits, limited collection and use of Personally Identifiable Information (PII), analysis of data, and storage of information collected.

The informed consent process included consultation with NAU's IRB to obtain the appropriate wording for inclusion in the invitation to participate in research and the informed consent form interviewees completed prior to any discussion. When interviewees decided to participate, the researcher asked each to sign a consent form permitting taping and transcription by the researcher of the interviews for data analysis. Each interviewee asked for a preview of the interview questions, which the researcher provided prior to interviews. In addition, the researcher provided each interviewee with the proposed motivational topology, definitions used in the study, and the definitions of the motivational themes and sub themes in preparation for the discussion.

Before each interview, the researcher reviewed the interviewee's experience per the selectin criteria, reviewed highlights of the interviewee's resume qualifying him or her as an expert. In addition, the researcher asked for permission to record, reminded the interviewee of the signed consent and reaffirmed consent. Finally, the researcher reminded interviewees they could withdraw consent and stop the interview at any time should the need arise. In summary, each participant received a formal invitation to participate in a one hour taped interview and an informed consent form, along with pre-interview information. See Appendix C: Invitation to Participate and Appendix D: Informed Consent.

The Belmont Report (DHHS, 2016) explains the concept of beneficence as one of the guiding principles for human subjects' research. It is the "obligation" (DHHS, 2016) of the researcher to ensure participants' privacy, confidentiality, and protections from potential harm are in place. Harms may include psychological, embarrassment, or loss of privacy. Although no study is completely risk-free, the researcher did not anticipate harm to participants during the study. Participants had multiple opportunities to ask questions, read about the interview process, and were free to decline or discontinue participation at any time. In addition, via the Informed Consent form, the researcher provided participants the web address to PsychCentral, an independent online mental health resource. The service asserts it is "run by mental health professionals offering reliable, trusted information and over 250 support groups to individuals struggling with a problem in their lives" (PsychCentral, 2019, para. 1).

The proposed risk to the interviewees is they might feel uncertain providing answers to questions. However, this risk is minimal because the researcher limited questioning to the motivations of each actor based on the interviewee's experience. Consequently, the study involved minimal risk to the participants.

While the risk to participants was minimal, the researcher addressed the issue by explicitly informing participants at the beginning of the interview that they may decline to answer any question at any time or halt the interview. The researcher did not judge participants because she was interested in obtaining feedback and rich, thick data, be it positive, negative, neutral, or mixed responses provided by interviewees. Rather, the researcher was only interested in the motivations, feedback on definitions, and the converging motivations model. There were no other known risks or discomforts associated with participating in this study, and there was no cost or payment for participation.

The researcher expected several benefits from participating in this study. Results of this study could increase the understanding policy makers and national security practitioners have about the motivations of terrorists, spies, and hackers. If the interview participants confirmed motivational convergence, it would serve as additional validity to study findings. Furthermore, policy makers and national security practitioners could gain insight into new perspectives they may wish to pursue to advance counterterrorism policy. Academicians could use the findings in this study to develop new research in the strategic security field.

The researcher obtained minimal PII to invite participation and enable the interviewee to complete the consent form. The IRB-mandated informed consent served as evidence the participant understood the nature of the study and risks. The researcher took take steps to protect each interviewee’s identity. Protection involved the use of pseudonyms for each participant, such as Interviewee 1, Interviewee 2, and 3 in the data analysis tables and refrained from referring to any interviewee by his or her name. The researcher conducted the phone-based interviews from her private office, where the researcher’s transcriptions of the conversations remain in a secure file.

***Data collection and instrument.***

To collect data, the researcher used a semi-structured phone call in-depth interview format. During each 60-minute interview, the researcher asked open-ended questions about the motivation definitions and topology developed during the case study analysis. The researcher expected interviewees to select motivations from the typology to discuss. Questions prompted stories that helped the interviewee explain their responses but under no circumstances did the researcher explore any of the work activities or sources and methods. Additionally, the researcher did not ask any questions about PII. The researcher used the Semi-structured Interview Guide illustrated in Appendix F to conduct questioning during interviews.

***Data analysis.***

The analysis and interpretation of data occurred in two phases. The first phase included the researcher's transcription of interviews. Then, the researcher contextually coded transcripts highlighting motivations from the topology as interviewees discussed themes and sub themes. The researcher manually code three transcripts due to the low volume.

The second phase of analysis consisted of moving the hand-coded data from the transcripts by transferring it to the proposed topology using a pre-formatted Semi-structured Interview Guide shown in Appendix F. Once the data were on the analysis form, the researcher proceeded to analysis. The researcher stored coded, transcribed transcripts in filing cabinet in the researcher's office following the completion of the study and destroyed the electronic copy of the transcription and interview recordings following transcription. One-year post analysis, the researcher will destroy the paper transcripts. The results of the interviews appear in Chapter 4 of the researcher's dissertation.

### ***Ethical considerations.***

Before embarking on the interviews, the researcher followed all NAU policies and procedures for conducting research on human subjects. The researcher applied for an IRB approval of the interview method and process, consistent with NAU policies and procedures. NAU's IRB follows all guidelines as prescribed in Title 45 – Public Welfare, Part 46–Protection of Human Subjects and the Belmont Report (DHHS, 2016). The researcher expected no inherent risks to life, limb, stress, embarrassment, or loss of self-esteem of participants in this study; none appeared. Hence, the researcher did not alter methods from those proposed to the IRB. No additional reporting to the IRB was necessary.

### ***Researcher's role.***

A critical factor of data analysis in qualitative studies is that the researcher is the primary means of data collection (Creswell, 2013; 2014). One of the likely challenges resulting from the researcher's dual role in the process—data collector and data interpreter—is researcher bias. Therefore, the researcher must endeavor to limit the impact of any potential biases that may exist. As noted earlier, the researcher provided an opportunity for interviewees to ask questions and clarify comments during interviews. After analysis, the researcher reviewed processes with the researcher's committee chair who raised no additional issues. Finally, the researcher knew of no conflicts of interest that may affect this study.

## **Assumptions, Limitations, and Bias**

No research project is without its assumptions, limitations, and biases. Assumptions are expectations about things believed to be true without evidence to support the belief. In this study, the primary assumptions included obtaining truthful and honest responses to researcher's questions when interviewing participants, assumed truthfulness of the authors' of the references upon which the researcher relied, and the truthful reporting of terrorist, espionage, and hacker events upon which the author based case study coding. Additional assumptions included the interview questionnaire that sparked conversation for the semi-structured interviews.

Limitations included types and sources of historical documents, lack of access to case documentation, small sample sizes, sampling bias, incorrect assumptions, inevitable human error in data gathering, measurement and coding, software limitations, incorrect interpretation and analysis, and researcher bias. To minimize these concerns, the researcher took precautions to validate the authenticity and triangulate data using multiple sources. Limitations also result from the researcher acting as the primary data collector and analyst who relied on her instincts and education throughout the process. Whenever a data collection or analysis dilemma arose, the researcher vetted it with her committee chair before proceeding. In addition, upon completion of coding the case study evidence data, the researcher contacted a third-party strategic security expert to review coding procedures, and in particular, review codes applied to the terrorism cases because terrorism cases presented a unique challenge. See the data analysis section on terrorism for the explanation. Additional limitations may result from the interviewees' perspectives and biases, which the researcher may have been unable to detect.

Due to the qualitative methodology and case study and interview methods, the researcher expects the findings cannot be generalized to the larger population; this is a known limitation of qualitative research, hence the inclusion of multiple case studies and the addition of a second method of inquiry. Finally, complete objectivity is impossible in any study; thus, the accuracy of the study findings may be limiting. Nonetheless, the researcher took the measures noted to mitigate limitations and bias throughout the research process.

To minimize case study sampling bias, the researcher executed a multi-phased sampling technique. Coding bias can result from a misinterpretation of the context of the variables under study. The researcher used MAXQDA software in multiple ways during the research process to minimize coding bias. In addition, the researcher solicited feedback from an external consultant who specialized in MAXQDA software for coding structure and guidelines before setting up the software. After initial execution and identification of the MAXQDA limitation with PDFs, the external consultant suggested using automatic coding to identify keywords only, and to use lexical and in-vivo coding to tag keywords for creating the coding structure. Using this process provided a double check of the content analysis procedures.

**Methodology Summary**

Chapter 3 provided the details of the research conducted for this study, using the methods described to improve the understanding of the motivations of terrorists, spies, and hackers. The researcher integrated into a single study, the analysis of the three actor groups, using a qualitative cases survey approach, and content analysis, followed by interviews with an expert with experience from each of the triple threat actor groups. Using multiple methods of inquiry enabled creating a sample of cases to develop, test, and analyze the convergence of the phenomenon of interest to understand the complex web of interdependencies, which may bind several motivational variables together. As described in the next chapter, the results of the data analysis advanced research on the collective threat while providing policymakers with a new perspective and deeper understanding of the primary actors comprising national security’s triple threat.

# Chapter 4: Results and Discussion

The purpose of this research was to explore and gain an understanding of the collective motivations of national security's triple threat—terrorists, spies, and hackers. This research employed two qualitative methods of inquiry: multiple case studies and semi-structured interviews with experts in counterterrorism, counterespionage, and cybersecurity that have deep knowledge to explore the theme/sub-theme motivational topology. The interviews increased study validity enabling triangulation of data obtained using the case study method (Lincoln & Guba, 1985).

While examining case studies and conducting interviews, the researcher used an iterative and interpretive approach (Taniguchi, 2014) to simultaneously assess the motivations of each actor. The case study method involved two types of data collection prior to analysis: identification of the motivations in the literature reviewed for each actor group and identification of 20 case studies in each group (totaling 60 case studies), to assess the actors' motivations against the motives from the literature. Computer assisted content analysis helped identify the motivations in the literature reviewed for each actor group. The motivations identified became the code system the researcher used to identify and tag the motives in each case study, also referred to as evidence or evidence documents in this study.

Data collected via the semi-structured interviews augmented the case study data by obtaining details and confirming or refuting the motivational themes and sub-themes identified. The researcher followed the method to select participants as described in Chapter 3. Each interviewee confirmed their educational and background in either counterespionage, counterterrorism, or cybercrimes, and their willingness to participate in the study prior to data collection. This enabled the researcher to confirm each interviewee met the criteria established and ensure the interviewee was an expert in their field. During semi-structured interviews, the researcher collected data about the motivational topology, themes, sub-themes, and obtained detailed comments and insights the interviewees were willing to share. Chapter 4 presents the findings and insights based on motives identified in the literature, analysis of the case studies, and the interviews.

### Motivations: Definitions and Discussion

The first finding was the lack of definitional consistency with respect to motives in the literature reviewed for each actor group. While this finding is parallel to the definitional discussions of each actor in the literature review, it was an unanticipated finding with respect to motives. Although the corpus of literature consisted of older literature (1960 to 2010), the authors of current literature (2011 to 2016) neither observed nor commented on the lack of consistent motive definitions, nor did most of these authors define the motives about which they wrote. Thus, readers had to rely on their own interpretations of the definitions and descriptions of the motives mentioned in each piece of literature. Furthermore, lack of definitional consistency highlights a shortcoming of prior research with respect to motivational acronyms or mnemonics—MICE, MEECES, MINCE, MINCES and RASCALS—whichever one chooses to subscribe. The result is many researchers' perpetuated mnemonics and assumed definitions within and across actor groups irrespective of clarity in understanding. To eliminate this shortcoming from the current research, Table 5 presents the discussion the definitions and sources that apply to this research for the 12 motivational themes resulting from the content analysis.[1]

[1] The author purposely placed Table 3 in this section versus in an appendix because of the importance of the definitions to the results and motive discussion and the dissertation Committee Chair approved this placement.

*Table 5.*

*Motivation Definitions, Discussions, and Sources.*

| Motivation | Definition/Discussion | Sources |
|---|---|---|
| Addiction | An addiction is “a strong and harmful need to regularly have something…or do something” to satisfy a human need (Merriam-Webster Online, n.d.). Addiction is a motive cited in the terrorism and hacking literature. It is absent in espionage-related motivation discourse. The medical definition of addiction is outside the scope of this research. | Campbell & Kennedy (2014)<br>Cottee & Hayward (2011)<br>Crenshaw (1986)<br>Taylor, P. (1999)<br>Wade et al. (2011)<br>Wilson (2012) |
| Choice | Choice is “the act of picking or deciding between two or more possibilities” (Merriam-Webster Online, n.d.). It is a motivation primarily cited by terrorist researchers as rational choice, deliberate, willful, intentional, or existential. With respect to hackers, researchers citing choice primarily note it hackers’ lack of the social aspects of moral choices rather than a deliberate decision such as terrorism researchers assert. Choice as a motive is absent in the espionage literature. | Bossler & Burruss (2011)<br>Cottee & Hayward (2011)<br>Crenshaw (1981, 1986, 2000)<br>Özdamar (2008)<br>Post (1988, 2007)<br>Swann et al. (2012)<br>Taylor, M. (2010)<br>Victoroff (2005) |
| Coercion | Coercion is the act of “mak[ing] (someone) do something by using force or threats” (Merriam-Webster Online, n.d.) against one’s will. It is a form of internal or external pressure, which is generally involuntary. Coercion is the subject of discourse in the espionage literature; it is absent in both the terrorism and hacking discourse. | Burkett (2013)<br>Charney (2010)<br>Herbig & Wiskoff (2002)<br>Hitz (2008)<br>Mickolous (2015)<br>Sarbin, Carney, & Eoyang (1994)<br>Wilson (2012) |
| Curiosity | Curiosity is “the desire to learn or know more about something or someone” (Merriam-Webster Online, n.d.). As a motive, curiosity has sub-themes such as continuous learning and exploration, in the form of technical mastery. Curiosity as a motive researchers identify in the hacking literature; it is absent in both the terrorism and espionage literature. | Bossler & Burruss (2011)<br>Campbell & Kennedy (2014)<br>Holt & Bossler (2014)<br>Holt & Kilger (2012)<br>Jaishankar (2011)<br>Post (2009)<br>Post & Berko (2009)<br>Schell & Melnychuk (2011)<br>Schouten (2010)<br>Taylor, P. (1999)<br>Thompson (2013)<br>Turgeman-Goldschmidt (2005)<br>Wade et al. (2011) |
| Ego | Ego is “one of the three divisions of the psyche in psychoanalytic theory that serves as the organized conscious mediator between the person and reality especially by functioning both in the perception of and adaptation to reality — compare id, superego” (Merriam-Webster Online, n.d.). Ego is a self-conscious cognitive state in which a person entertains and reflects on his or her own thoughts, feelings, actions, and behaviors as compared to others. The subconscious self-assessment either restrains or justifies one’s actions to oneself or others, including peer groups. Numerous terrorism, espionage, and hacking researchers cite ego as a motivational theme. Subthemes of ego include entrance to or support of a | Bossler & Burruss (2011)<br>Burkett (2013)<br>Charney (2010)<br>Campbell & Kennedy (2014)<br>Charney (2010)<br>Cottee & Hayward (2011)<br>Crenshaw (1981, 1986, 2000)<br>DCIC (2002)<br>Herbig & Wiskoff (2002)<br>Holt & Bossler (2014)<br>Holt & Kilger (2012)<br>Kilger, Arkin, & Stutzman (2004)<br>Mickolous (2015)<br>Post (2007, 2009)<br>Post, Sprinzak, & Denny (2003) |

| Motivation | Definition/Discussion | Sources |
|---|---|---|
|  | social group, power, recognition, status, thrills, and self-importance. | Rogers, Smoak, & Liu (2006)<br>Sageman (2004)<br>Sarbin, Carney, & Eoyang (1994)<br>Schouten (2010)<br>Schwartz (2007)<br>Sulick (2012)<br>Swann et al. (2012)<br>Taylor, M. (2010)<br>Taylor, P. (1999)<br>Thompson (2013)<br>Turgeman-Goldschmidt (2005)<br>Victoroff (2005)<br>Wade et al. (2011)<br>Weatherston (2003)<br>Wilson (2012) |
| Entertainment | Entertainment is “something diverting or engaging” (Merriam-Webster Online, n.d.) a person does generally for pleasure or relaxation. Researchers studying espionage and hacking cite entertainment as a motive while it is absent in the terrorism literature. Sub-themes of entertainment include adventure, fun, kicks, excitement, and pranks, tricks, and jokes. | Bossler & Burruss (2011)<br>DCIC (2002)<br>Hitz (2008)<br>Holt & Kilger (2012)<br>Jaishankar (2011)<br>Kilger, Arkin, & Stutzman (2004)<br>Mickolous (2015)<br>Sulick (2012)<br>Turgeman-Goldschmidt (2005)<br>Wade et al. (2011)<br>Wilson (2012) |
| Ideology | Ideology is “a manner or the content of thinking characteristic of an individual, group, or culture” (Merriam-Webster Online, n.d.). Researchers cite ideology as a motive in each actor group without defining the term. This becomes problematic because the mix of ideological motives for actor groups differs. For example, anarchy is a motivation terrorism researchers cite however it is absent in the espionage and hacking literature; and, social ideology, while present in the hacking and terrorism literature is absent in the espionage literature. Motives in the ideological theme include hacktivism, nationalist-separatist, economic, social, divided loyalty, ethnocentric, political, and religious. Right wing and left wing, though mentioned in literature, are not ideologies; rather, these are classifications or categorizations of numerous ideologies that fall to one or the other end of a spectrum. | Burkett (2013)<br>Campbell & Kennedy (2014)<br>Charney (2010)<br>Cottee & Hayward (2011)<br>Crenshaw (1981, 1986, 2000)<br>Denning (2011)<br>Herbig & Wiskoff (2002)<br>Hitz (2008)<br>Holt & Kilger (2012)<br>Jaishankar (2011)<br>Kilger, Arkin, & Stutzman (2004)<br>Lizardo & Bergesen (2003)<br>Mickolous (2015)<br>Özdamar (2008)<br>Post (1988, 2005, 2007)<br>Post, Sprinzak, & Denny (2003)<br>Rapoport (2004)<br>Rogers, Smoak, & Liu (2006)<br>Sarbin, Carney, & Eoyang (1994)<br>Schouten (2010)<br>Schwartz (2007)<br>Sulick (2012)<br>Swann et al. (2012)<br>Taylor, M. (2010)<br>Taylor, P. (1999)<br>Thompson (2013)<br>Turgeman-Goldschmidt (2005)<br>Victoroff (2005)<br>Wade et al. (2011)<br>Wilson (2012) |

| Motivation | Definition/Discussion | Sources |
|---|---|---|
| Ingratiation | Ingratiation is the act of seeking “to gain the favor or favorable acceptance for by deliberate effort” (Merriam-Webster Online, n.d.), on the part of an actor. Ingratiation is a motivation cited by espionage researchers who refer to it as a motive driving spies to please someone else to demonstrate commitment. Ingratiation is a motive absent in the literature of terrorists and hackers. | Charney (2010)<br>DCIC (2002)<br>Herbig & Wiskoff (2002)<br>Wilson (2012) |
| Money | Money is “something generally accepted as a medium of exchange, a measure of value, or a means of payment” (Merriam-Webster Online, n.d.). The underlying cause for money as a motive is economic gain, which actors view as payment for services rendered. Money is a motive cited by researchers who study hackers and spies. This motivation is absent in the terrorism literature. | Burkett (2013)<br>Charney (2010)<br>DCIC (2002)<br>Denning (2011)<br>Herbig & Wiskoff (2002)<br>Hitz (2008)<br>Holt & Kilger (2012)<br>Kilger, Arkin, & Stutzman (2004)<br>Mickolous (2015)<br>Sarbin, Carney, & Eoyang (1994)<br>Schwartz (2007)<br>Sulick (2012)<br>Thompson (2013)<br>Wade et al. (2011)<br>Wilson (2012) |
| Psychological | As defined in Gerrig & Zimbardo (2002) and cited in the APA’s online Glossary of Psychological Terms, psychology is “the scientific study of the behavior of individuals and their mental processes” (APA, 2016). The motives in this theme include personality disorders such as introversion, narcissism, and diagnoses that fall into the broad category of Autism Spectrum disorders such as Asperger’s syndrome. Initially researchers studying terrorists sought psychological motives as explanations for terrorism. Researchers studying crime and hacking identified psychological motives to explain behavior. Few researchers cite psychological motives with respect to espionage. | Campbell & Kennedy (2014)<br>Cottee & Hayward (2011)<br>Crenshaw (1981, 1986, 2000)<br>Holt & Bossler (2014)<br>Mickolous (2015)<br>Özdamar (2008)<br>Post & Berko (2009)<br>Post (1988, 2005, 2007, 2009)<br>Rogers, Smoak, & Liu (2006)<br>Sageman (2004)<br>Schell & Melnychuk (2011)<br>Schouten (2010)<br>Schwartz (2007)<br>Seigfried-Spellar, O’Quinn, & Treadway (2015)<br>Swann et al. (2012)<br>Taylor, P. (1999)<br>Zuckerman (2001) |
| Revenge | Revenge is the act of “retaliating in kind or degree” (Merriam-Webster Online, n.d.) as a result of actions or perceived actions thrust upon a person by another person or entity. Numerous terrorism, espionage, and hacking researchers cite revenge as a motivational theme. Sub-themes of revenge include disgruntlement, economic sabotage, harm, blame, and injustice. | Borum (2003)<br>Bossler & Burruss (2011)<br>Campbell & Kennedy (2014)<br>Charney (2010)<br>Crenshaw (1981, 2002)<br>DCIC (2002)<br>Denning (2011)<br>Herbig & Wiskoff (2002)<br>Hitz (2008)<br>Holt & Bossler (2014)<br>Holt & Kilger (2012)<br>Mickolous (2015)<br>Post (1988, 2005, 2007, 2009)<br>Post & Berko (2009)<br>Rogers, Smoak, & Liu (2006)<br>Sarbin, Carney, & Eoyang (1994) |

| Motivation | Definition/Discussion | Sources |
|---|---|---|
| | | Schell & Melnychuk (2011)<br>Schouten (2010)<br>Schwartz (2007)<br>Sulick (2012)<br>Taylor, M. (2010)<br>Thompson (2013)<br>Turgeman-Goldschmidt (2005)<br>Victoroff (2005)<br>Wade et al. (2011)<br>Wilson (2012) |
| Romance | Romance is "an emotional attraction or aura belonging to an especially heroic era, adventure, or activity" (Merriam-Webster Online, n.d.). Many times this motive leads to sexual desires, which espionage and hacking researchers cite. Romance as a motive is absent in the terrorism literature. | Campbell & Kennedy (2014)<br>Herbig & Wiskoff (2002)<br>Hitz (2008)<br>Mickolous (2015)<br>Sulick (2012) |

## Motivations in the Literature Reviewed by Actor

The researcher divided the literature review into three sections—one for each of the actors. Within each section, the researcher surveyed journal articles, books, dissertations, theses, and other publications to present a holistic assessment of scholarly works that attempted to explain the history, definition, categories, and behavioral theories and motivations shaping perceptions of each actor. Since the purpose of the research was to study and advance the understanding of the motivations across actor groups, the literature review sub-section on behavioral theories and motivations was of particular interest. In preparation for executing the content analysis, the researcher reviewed the proposed process, discussing literature selected for content analysis and the process of coding with the Committee Chair and obtained agreement with proposed procedures.

The researcher reviewed the literature in each of these sub-sections selecting 45 significant publications containing motivation discussions for content analysis. The content analysis resulted in tagging and coding 290 motivation segments across all actors. In keeping with the qualitative tradition of data reduction during analysis, the researcher recorded 12 motivational themes as described in the prior section. After establishing the code structure and before beginning analysis of the results, the researcher sought to improve validity by reviewing the process and results with a terrorism, counterterrorism, and strategic security expert previously unfamiliar with the research. Dr. Diane Maye served in this role. The researcher explained the rationale for document selection and demonstrated the coding process using the MAXQDA software. Dr. Maye confirmed the rationale, process, and the resulting code structure (personal communication, September 4, 2016). The following three sections present the results of the analysis of motivation-related literature identified for each of the actor groups. The final section introduces a consolidated motivation typology across all actor groups.

### Terrorist motivations.

From the literature review on terrorists' motivations, the researcher loaded 19 publications (documents) into the MAXQDA content analysis tool. These documents represented both the historic and current assessments about what motivates terrorists to commit the acts they do. The researcher reviewed and tagged motives, such as ideology, ego, and revenge in each of the documents. The coding process resulted in 101 coded segments across the 19 documents. In keeping with the qualitative research tradition, the researcher aggregated the segments, reducing the segments into motivational themes. This process of analysis resulted in identification of six motivational themes for terrorist actions. Figure 6 shows the six motivational themes and the percent represented by each theme in the coding of the terrorism literature reviewed.

Since the literature is replete with ideological discussions, it is not surprising that ideology dominated the coding, appearing nearly three times as often as ego. Although the psychological motive occurred in the literature, researchers concluded terrorists' the relative normalcy of terrorists' psyches. Hence, it is not surprising to see this motive occurring less often than other motives. Choice as a motive centered on individual terrorists rationally choosing to "engage in pro-group behavior" (Swann, 2012, p.451).

That said, when scrutinizing the types of ideology to which researchers referred, eight sub-theme ideologies emerged in addition to a generalized or non-specific category. Sub-themes also emerged for the ego and revenge motives as shown in Figure 7, grouped by theme and sub-theme and displayed in descending order by the percentage the sub-theme contributed to the overall theme in the reviewed literature.

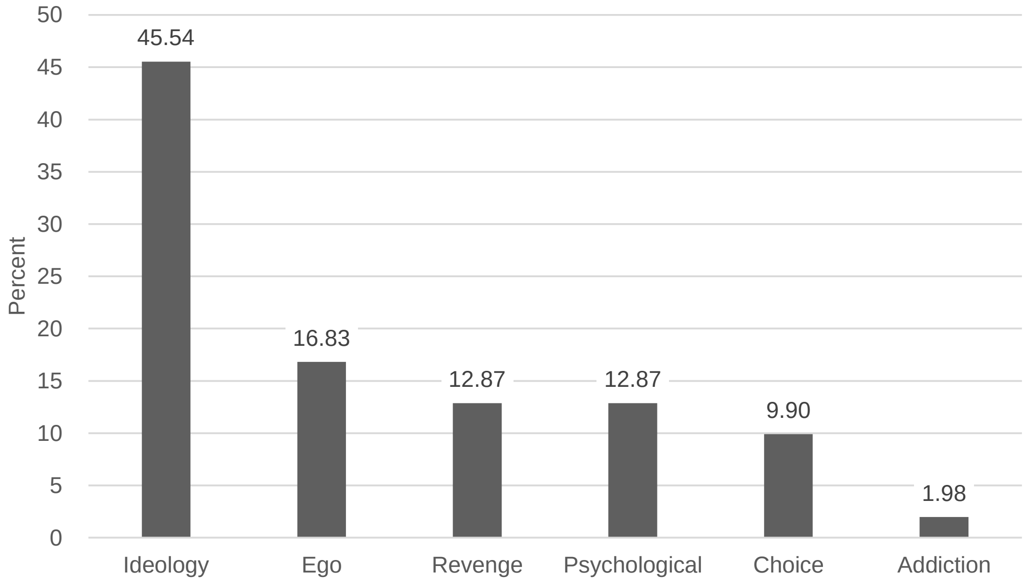


*Figure 5.* Motivation Themes in Terrorism Literature

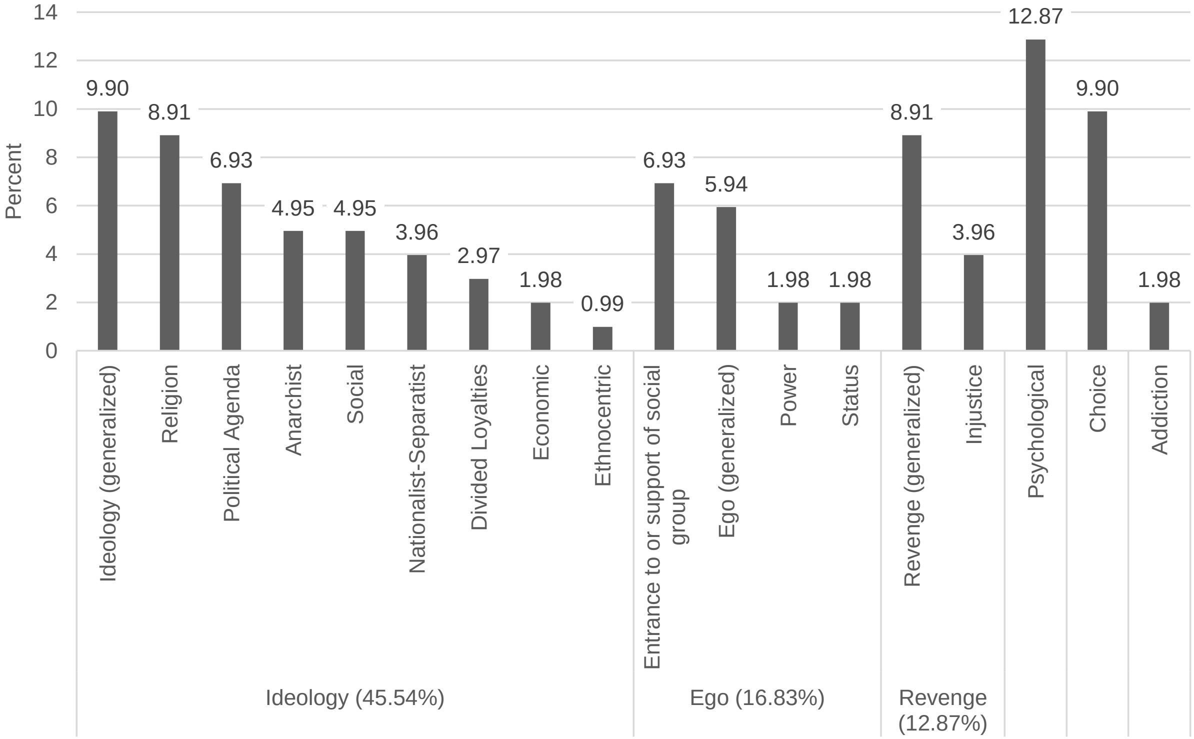


*Figure 6.* Motivation Sub-themes in Terrorism Literature

**Spy motivations.**

Repeating the process of analysis used to review the literature on terrorists, the researcher uploaded 11 espionage documents into the MAXQDA content analysis tool. These documents also represented the historic and current assessments about what motivates spies to commit the acts they do. The researcher reviewed and tagged motives, such as ideology, ego, and revenge in each of the documents. The coding process resulted in 75 coded segments across 11 documents. Again, the researcher aggregated segments into motivational themes. Figure 8 shows the nine motivational themes that emerged from the coding process.

Once again, ideology surfaced as the number one motivational theme—occurring 21.33% of the time. Researchers cited ideology approximately 1.2 times more often than ego. Equally mentioned in the literature, the theme of both money and revenge occurred one and a half times as often as ideology.

Figure 9 shows the sub-themes of each motivational theme. Aside from the generalized category, where researchers did not specify ideological details, predictably, divided loyalties are the most common ideological sub-theme. However, when assessing motivations across sub-themes money rises to the top, followed by ego, and then divided loyalty ties with revenge. Based on the discourse in the literature, this breakdown is not readily apparent; rather the overwhelming discussion and mention of ideology in general conceals this observation. As a result, the breakdown of motivation by sub-themes clarifies espionage motivations and perhaps represents a more effective assessment.

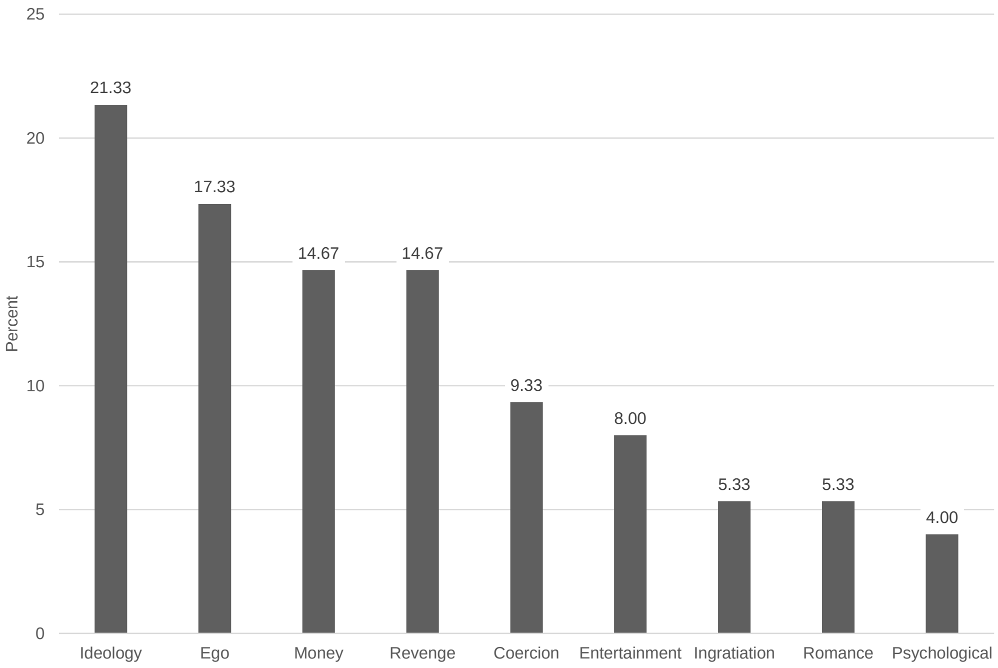


*Figure 7*. Motivation Themes in Espionage Literature

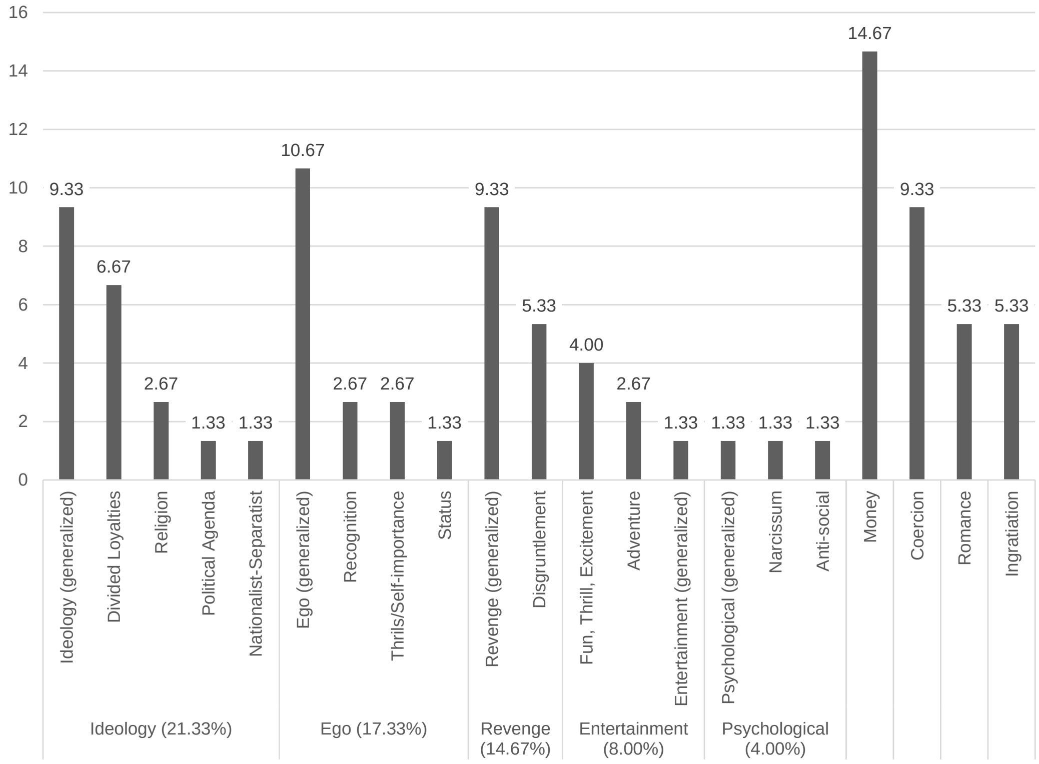


*Figure 8.* Motivation Sub-themes in Espionage Literature

### Hacker motivations.

Again, using the same analysis process to review the literature as with the prior two actors, the researcher loaded 15 hacking documents into the MAXQDA content analysis tool. These documents represented the historic and current assessments about what motivates hackers to commit to the act of hacking. The researcher reviewed and tagged motives in each of the documents. The coding process resulted in 114 coded segments across the 15 documents. Again, the researcher aggregated segments into motivational themes. Figure 10 shows the 10 motivational themes that emerged from this analysis.

For the third time, ideology emerged as the top motive, occurring in 22.81 percent of the coded segments. Ego and curiosity followed ideology with 20.18 percent and 17.54 percent respectively. Collectively, the authors of the literature cite 10 of the 12 motive themes identified by the coding process. This could be an indication of the complexity of the hacker's motivational psyche, which the case study analysis may reveal.

Figure 11 displays the motivational sub-themes clustered by the primary theme. Although ideology was the primary theme, again, looking into the sub-themes of the primary motivation, the sub-theme motivations change as compared with the prior two actors. Excluding the generalized ideology category because it is broad and non-specific, the primary motivational sub-theme in the hacker literature reviewed is political agenda. However, in analyzing the spectrum of sub-themes, the motives recognition and revenge top ideological sub-themes coded in the literature.

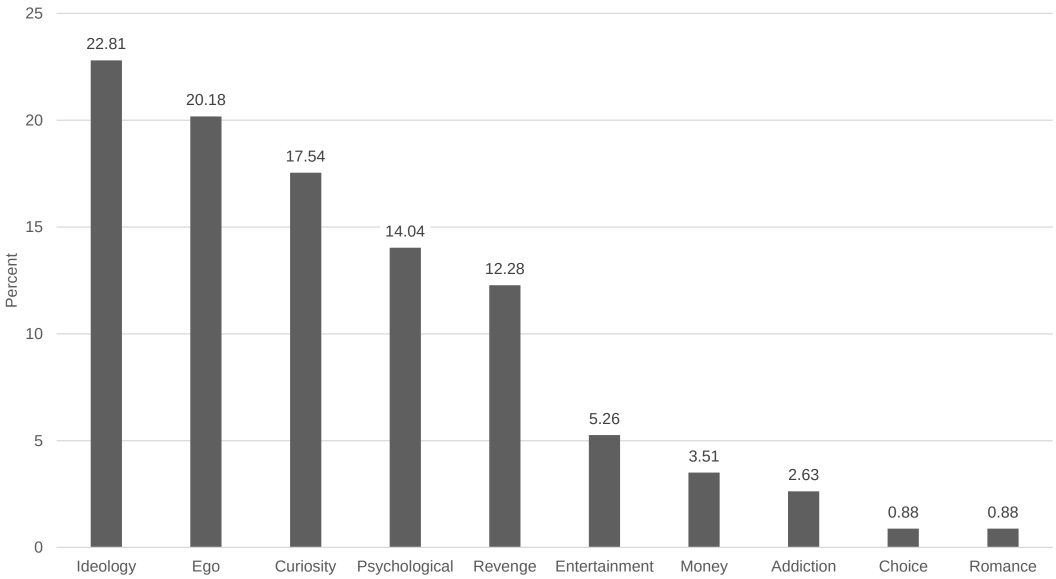


*Figure 9.* Motivation Themes in Hacking Literature

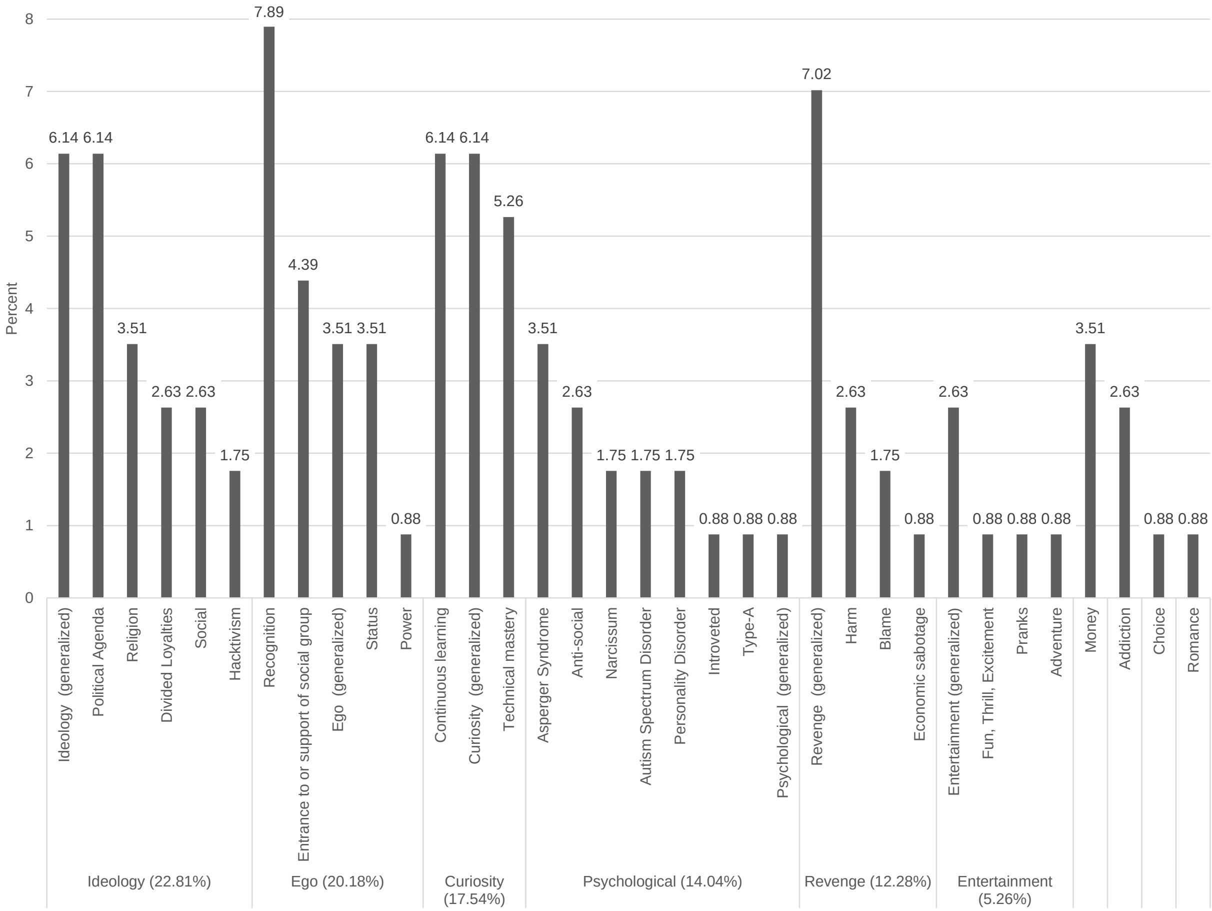


*Figure 10.* Motivation Sub-themes in Hacking Literature

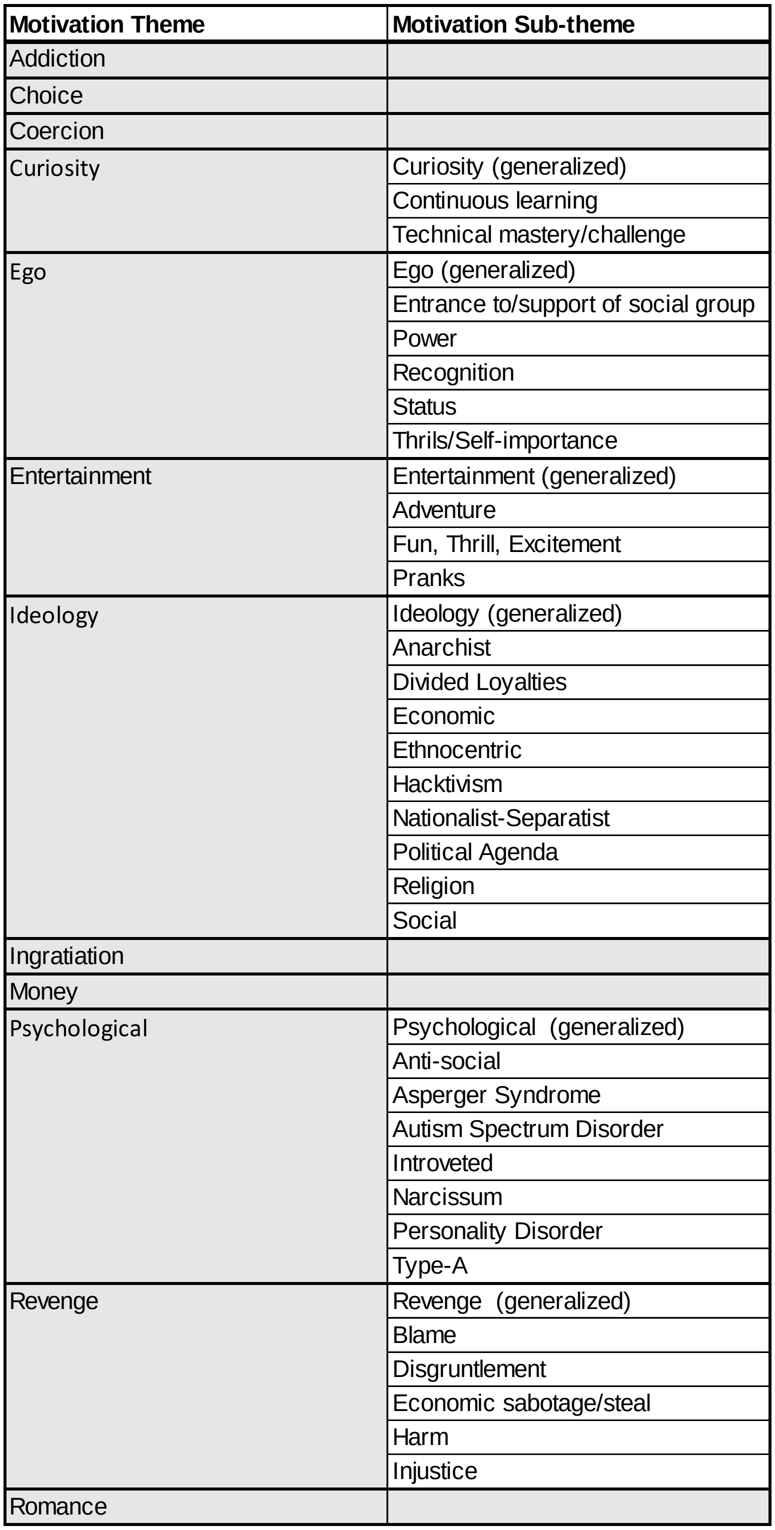
## Proposed Typology

The second finding was the emergence of a motivational typology. It is comprised of broad themes from which sub-themes surfaced thereby illuminating the complexity of motivations. Based on the identification of 12 motivational themes and the surfacing of numerous sub-themes revealed by deeper analysis of the literature, the research indicates motivational acronyms and mnemonics as analytical topologies are too simplistic and superficial from which obtain an understanding of actors' motivations. Researchers must delve deeper into the causes and stimuli underlying human behavior by assessing the sub-themes.

Given the inconsistency of the definitions of motivations amongst academics and researchers, and the surfacing of motivational sub-themes, there is reason to develop a formalized operational typology to categorize more accurately motivations within and between actor groups. The thesis of this research was whether researchers could identify the similarities and differences of the motives of terrorists, spies, and hackers, and develop recognizable patterns, then US counterterrorism and security specialists could develop TTPs to minimize, or thwart, the threat these actors collectively create. The proposed cross-actor motivational typology based on the motivational themes and sub-themes in the literature illustrated in Table 6 is a step toward more consistently identifying patterns based on common definitions.

*Table 6.*

*National Security Threat Actor Typology: Motivation Themes and Sub-themes*



| Motivation Theme | Motivation Sub-theme |
|---|---|
| Addiction | |
| Choice | |
| Coercion | |
| Curiosity | Curiosity (generalized) |
| | Continuous learning |
| | Technical mastery/challenge |
| Ego | Ego (generalized) |
| | Entrance to/support of social group |
| | Power |
| | Recognition |
| | Status |
| | Thrils/Self-importance |
| Entertainment | Entertainment (generalized) |
| | Adventure |
| | Fun, Thrill, Excitement |
| | Pranks |
| Ideology | Ideology (generalized) |
| | Anarchist |
| | Divided Loyalties |
| | Economic |
| | Ethnocentric |
| | Hacktivism |
| | Nationalist-Separatist |
| | Political Agenda |
| | Religion |
| | Social |
| Ingratiation | |
| Money | |
| Psychological | Psychological (generalized) |
| | Anti-social |
| | Asperger Syndrome |
| | Autism Spectrum Disorder |
| | Introveted |
| | Narcissum |
| | Personality Disorder |
| | Type-A |
| Revenge | Revenge (generalized) |
| | Blame |
| | Disgruntlement |
| | Economic sabotage/steal |
| | Harm |
| | Injustice |
| Romance | |

## Motivations in the Case Study Evidence by Actor

To test the applicability of the proposed typology, the researcher developed a case study for each of the actors by collecting evidence of the actor and the nefarious act each actor committed. The researcher developed 20 case studies for each actor group as described in Chapter 3, Methodology. Data for each case included names, dates of arrest, an event overview, triggering event, motives, attack types, target, age, sex marital status, race/ethnicity, education, employer, occupation, charges, convictions, sentence, initial locating source, and confirmatory evidence from at least 3 sources. See Appendix E Case Study Data for the data sheets on each case study.

Following the same process used to code the motivations in the literature the researcher separated the case studies by actor, loaded MAXQDA, and began coding each case. The researcher used the motivational themes and sub-themes to code the actor's motivations as supported by the evidence in the case study. A discussion of the results for each actor group and a summary across actor groups follows.

### Terrorist case studies motivations.

Terrorists subordinate their individual identities to groups and group causes, as described and articulated by the group's leader, effectively leading the individual terrorist to adopt the group's cause as his or her own (Dr. D. Maye, personal communication, September 4, 2016). The group's cause becomes the individual's motive and it becomes nearly impossible to separate the two. This phenomenon is apparent in the multiple case studies of terrorists in this study as evidenced by the lack of individuals claiming responsibility for the terrorist act.

Rather, as the data demonstrate, the majority of terrorists that claimed responsibility claimed it in the name of the terrorist group, not in individual's own name. Hence, the unit of measure for the terrorist actor was the event. This was an unexpected finding with respect to the terrorism case studies and is a limitation due to the absence of named individuals in the START database (START, 2016a) used to identify cases. Although the START database had a Claimed indicator, the database did not identify individuals. For example, if the Animal Liberation Front (ALF) bombed a building and called a newspaper claiming responsibility for the bombing, the START database cited the ALF, not an individual.

The researcher loaded 20 terrorist case studies into the MAXQDA content analysis tool. For each case study, the researcher reviewed and tagged motivational themes and sub-themes as warranted by the motive described in the case study. The coding process resulted in 30 coded segments across the 20 case studies. Figure 11 shows the motivational themes and sub-themes of for the 20 terrorist case studies.

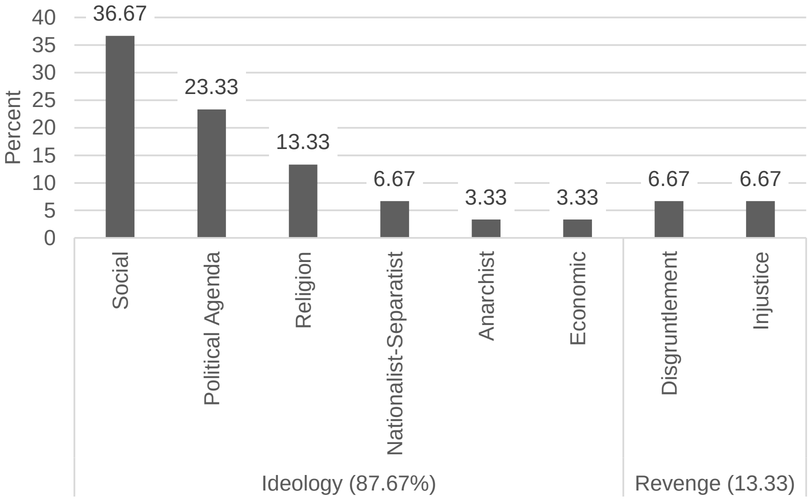


*Figure 11.* Motivations in Terrorist Case Studies

As anticipated, ideology and revenge were motivational themes that emerged. Surprisingly however, no other motivational themes for terrorists surfaced. This is in stark contrast to the motivational themes that appeared in the terrorism literature, which suggested 6 themes and 18 sub-themes as motives. For example, based on the literature, the researcher expected motivations such as ego, psychology, choice, and addiction to come forward.

Instead, what materialized was a preponderance of ideological and revenge motivation sub-themes in percentages that diverged from those in the literature. For example, based on the literature, the expectation was the religion sub-theme would appear most often, however, in the cases assessed the social agenda sub-theme emerged as a motive one and one half time more often than the political agenda motive, occurring 35 percent and just over 23 percent of the time respectively. As expected, revenge and its sub-themes, disgruntlement and injustice occurred in equal proportion.

Perhaps because of the small sample of domestic terrorism cases religion did not emerge. On the other hand, the literature appears biased toward non-domestic terrorism. In either case, researchers should conduct deeper analysis of the motivations of domestic terrorists and write more specifically about it.

**Spy case studies motivations.**

In contrast to the terrorist cases analyzed for this research, the spies in the cases studies reviewed acted independently. Hence, the unit of measure is the individual. Following the same procedures, the researcher loaded 20 espionage case studies into the MAXQDA content analysis tool. For each case study, the researcher reviewed and tagged motivational themes and sub-themes as warranted by the motive described in the case study. The coding process resulted in 28 coded segments. Figure 12 shows the motivational themes and sub-themes of for the 20 espionage case studies.

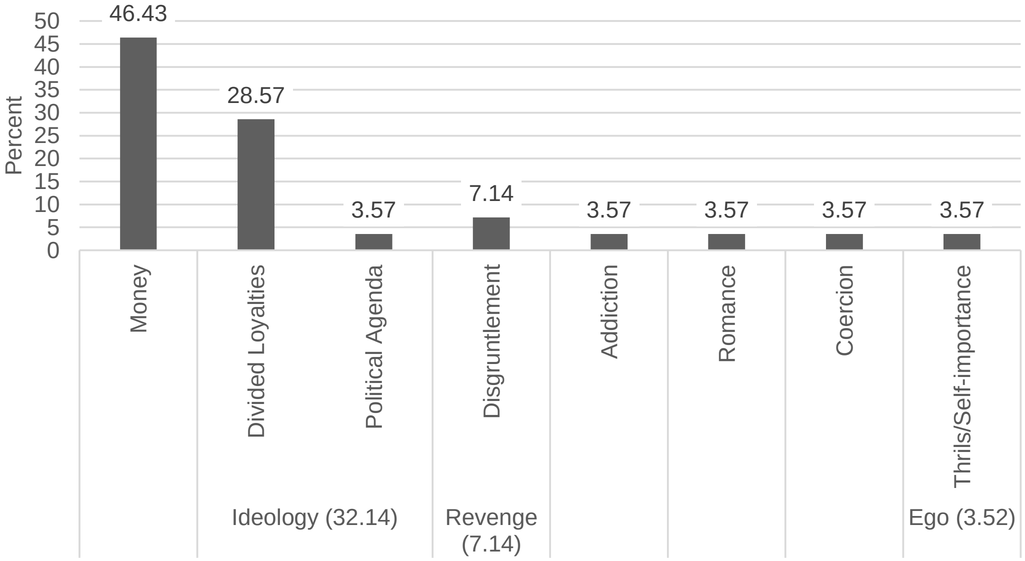


*Figure 12.* Motivations in Espionage Case Studies

Unsurprisingly, money, ideology, and revenge emerged as the top three motivational themes with 46.43 percent, 28.57 percent, and 7.14 percent respectively. Four motivational themes, addiction, romance, coercion, and ego, each appeared 3.57 percent of the time. Money as a motivation was 13 times more prevalent than these least-mentioned themes. In total, seven motivational themes surfaced in the espionage cases studies in contrast to the terrorist cases where only two motivational themes surfaced, an indication that from a cognitive perspective, the motives driving a person toward espionage are more complicated than terrorism.

Although the literature suggested 21 motivational sub-themes, the case studies revealed only eight, most likely due to the small sample. As in the terrorist case study discussion, the motivational sub-themes revealed in the literature were more representative than the themes. This supports the proposed typology based on sub-themes is a more accurate predictive model than one based on higher-level themes. For example, in the case studies, spies cited divided loyalties, an ideology sub-theme, four times more often than disgruntlement, a revenge sub-theme. Nonetheless, submitting more case studies to content analysis coding using the motivational typology would help verify and reinforce the sub-theme premise.

**Hacker case studies motivations.**

Following the same process, the researcher loaded 20 hacker case studies into MAXQDA. The researcher loaded 20 hacker case studies into the MAXQDA content analysis tool. For each case study, the researcher reviewed and tagged motivational themes and sub-themes as warranted by the motive described in the case study. The coding process resulted in 61 coded segments across the 20 case studies. Figure 13 displays the motivational themes and sub-themes of for the hacker case studies.

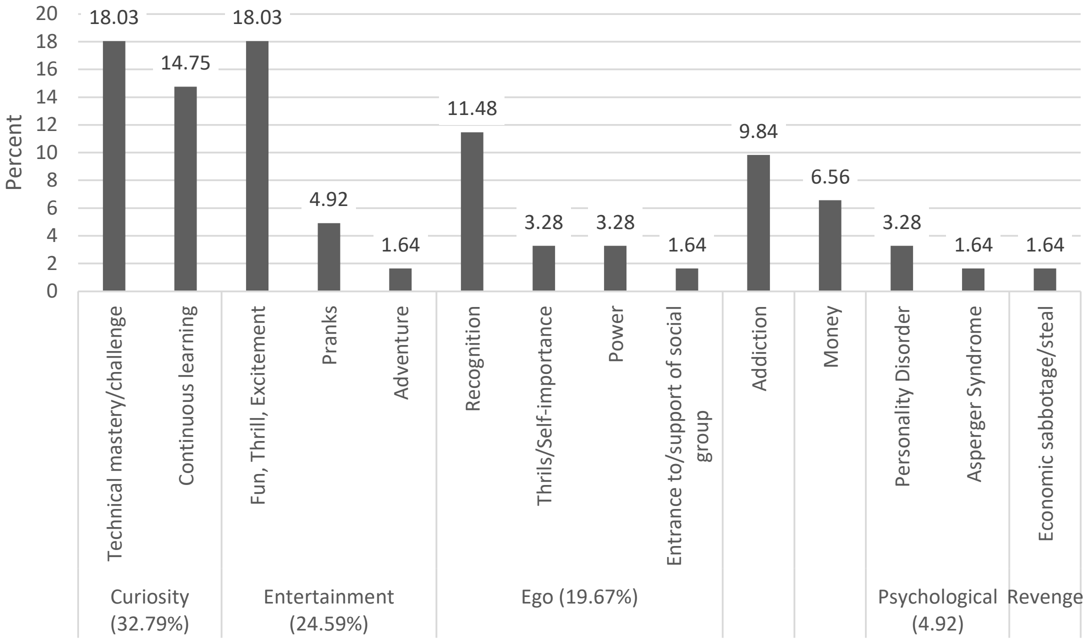


*Figure 13.* Motivations in Hacking Case Studies

The content analysis of the literature on hackers suggested ideology would be the primary motivation; however, this did not prove true based on hacker case studies in this research. Most likely this is because the unit of measure for hackers in this study was the individual. It is possible ideology would emerge as a primary motive if the unit of measure for hacking cases studies was events and evaluated similar to terrorists' events where individuals adopt the group's motivations in carrying out nefarious acts.

Similar to the terrorists and spies, the literature on hackers revealed more motivational sub-themes than the case studies revealed. The literature indicated 34 sub-themes of which, 14 emerge in the case studies. The small sample size may be a factor; however, future research increasing the sample size and coding additional case studies may reveal additional sub-themes. Nonetheless, the 14 motivational sub-themes represent the greatest number of motivations of all actors groups evaluated in this research. This insight leads to an inference that understanding hackers' motivations presents the most difficult challenge amongst national security's triple threat actors.

Once again, the sub-themes presented a more descriptive picture of motivations in contrast to the high-level themes. The curiosity sub-theme technical mastery/challenge and entertainment sub-theme fun, thrill, excitement tied as the top motivations hackers' in the case studies cited as motivations for their actions. Each of these sub-themes appeared 1.2 times as often as the continuous learning, which itself occurred 1.3 times more often than recognition.

## Motivations in the Interview Evidence by Actor

Prior to each interview, the researcher provided each participant with the motivational topology shown in Table 6. In addition, each participant received three documents:

1. The definition of the terms terrorism, espionage, and hacking explained in Chapter 1
2. The definitions of the motivations defined in Table 5, and
3. A preview of interview questions six through 12 shown in Appendix F.

During the interviews, the researcher recorded responses to the interviewee's discussion and comments as each reviewed the motivational topology themes and sub-themes pursuant to the actor for which the interviewee was an expert. In addition, the researcher conducted a content analysis of the researcher-transcribed interviews as part of the data collection effort. Presented in the following sections are the results of the researcher's data collection from each interview.

### Terrorist interview motivations.

Using the criteria described in Chapter 3, the researcher selected the counterterrorism interviewee based on his or her experience, willingness to provide feedback on the topology, and his or her willingness to provide opinions about terrorists' motivations from the interviewee's career perspective. The interviewee's resume stated he or she had over nine years as a counterterrorism analyst role working terrorist threats. The interviewee confirmed he or she reviewed materials sent prior to the interview and was prepared to discuss motivations of terrorists. The counterespionage expert identified 25 sub-themes, which he or she had experienced in the course of his or her career. The counterterrorism interviewee asserted, from his or her experience, the proposed topology, including themes and sub-themes was “on target” because “it’s a mixture of [motivations] that cause terrorists to act the way they do.” Table 7 displays the motivational themes and sub-themes the counterterrorism interviewee identified.

*Table 7.*

*Motivation Themes and Sub-themes—Evidence by Counterterrorism Interviewee*

| Motivation Theme | Motivation Sub-theme | Interviewee #3 | Comments |
|---|---|---|---|
| Addiction | | | |
| Choice | | ✓ | |
| Coercion | | ✓ | |
| Curiosity | Curiosity (generalized) | ✓ | "I have either interviewed or known of interviews of individuals who have stated their motivation as what I would characterize as marked curiosity, or morbid curiosity." |
| | Continuous learning | | |
| | Technical mastery/challenge | ✓ | "Especially individuals who had a military mindset but were not...sworn military. They studied on line and had something to prove-a strategy or strategic or technical ability. When it came to improvised explosive device construction, it was, what kind of IED could we make to have more destructive, more lethal, more technical, in order to get around countermeasures; so they took that as a curious challenge." |
| Ego | Ego (generalized) | ✓ | "It's general and all of the sub-themes. |
| | Entrance to/support of social group | ✓ | |
| | Power | ✓ | |
| | Recognition | ✓ | "The Islamic extremists had the ego of wanting to stand out, wanting to be recognized…as do the Lone Wolves." It was "lack of recognition prior to, and [an event] would give them a recognition." |
| | Status | ✓ | |
| | Thrills/Self-importance | ✓ | |
| Entertainment | Entertainment (generalized) | ✓ | "I would say entertainment in general over fun, thrill or excitement. There was an entertainment value of watching IEDs explode." |
| | Adventure | | |
| | Fun, Thrill, Excitement | ✓ | "Only unless they saw themselves as a mercenary." |
| | Pranks | | |
| Ideology | Ideology (generalized) | ✓ | |
| | Anarchist | | |
| | Divided Loyalties | ✓ | |
| | Economic | ✓ | "Especially to those threatening a terrorist event for economic gain of economic…you know, ransom. I'm either going to do an attack, or you pay me. Usually these were smaller in scope of doing an event." |
| | Ethnocentric | ✓ | "I'm thinking the Balkans in the 90s." |
| | Hacktivism | | |
| | Nationalist-Separatist | ✓ | |
| | Political Agenda | ✓ | |
| | Religion | ✓ | |
| | Social | | |
| Ingratiation | | ✓ | "From a terrorism standpoint, there have been many that have done acts for the sole purpose of ingratiation…[for example] in Afghanistan and Iraq...in order to be part of the organization." "Another example, the tribes within, or the clans within Afghanistan, would offer up the young men to ingratiate the clan itself for the sole purpose of being on the right side of the Taliban." |
| Money | | | |
| Psychological | Psychological (generalized) | | |
| | Anti-social | | |
| | Asperger Syndrome | | |
| | Autism Spectrum Disorder | | |
| | Introverted | | |
| | Narcissism | | |
| | Personality Disorder | | |
| | Type-A | | |
| Revenge | Revenge (generalized) | ✓ | "Both domestic and international terrorism. Get back at a country for example." |
| | Blame | ✓ | "The United States was to blame for the world economic problems, or their own social problems, talking from more Middle-Eastern terrorist groups, like Hezbollah or Hamas, attacking any United States individuals." |
| | Disgruntlement | ✓ | "Disgruntled domestic, IED emplacement. Domestically, disgruntled employees. Disgruntled at the U.S. government for its actions, so federal building attacks, for example." |
| | Economic sabotage/steal | | |
| | Harm | ✓ | "Any terrorist attack or plan has harm involved." |
| | Injustice | ✓ | "Anything against the U.S. government period, has been an injustice." |
| Romance | | | |

Note: A check mark (✓) indicates presence of the motivation theme or sub-theme as identified by interviewee.

### Spy interview motivations.

Again, following the criteria described in Chapter 3, the researcher identified the counterespionage interviewee and invited participation in this study. The counterespionage interviewee confirmed his or her willingness to provide opinions about the motivations of spies based on his or her career perspective. This interviewee confirmed he or she had about 50 years of experience in the areas of intelligence and national security, served as a human intelligence case officer, and manager of an organization in specializing in counterespionage.

In contrast to the counterterrorism expert's experiences, the counterespionage expert saw many more motivations driving spies' behavior than terrorists. As shown in Table 8, the interviewee identified the motivational themes and sub-themes he or she had observed during his or her career. This interviewee made an astute comment that is in line with the convergence hypothesis: "This motivational thing is very complex, and trying to boil it down to simple terms is a challenge….Every individual's motivational package is unique to that person." Therefore, interviewee concluded, "you start looking at a human problem, not a scientific problem, and picking out these different sub-elements as you have in the proposed topology illustrates the complexity." Another point this interviewee made was the actors themselves "may not necessarily understand their own motives" because some of the motivations in the topology are "subconscious behavior traits." In summarizing the interview, the counterespionage expert stated, "the way you organized the topology reflects my experiences in the real world and it supports the case study research you assessed in the earlier phase of your project."

*Table 8.*

*Motivation Themes and Sub-themes—Evidence by Counterespionage Interviewee*

| Motivation Theme | Motivation Sub-theme | Interviewee #1 | Comments |
|---|---|---|---|
| Addiction | | | |
| Choice | | | |
| Coercion | | | |
| Curiosity | Curiosity (generalized) | | |
| | Continuous learning | ✓ | |
| | Technical mastery/challenge | ✓ | |
| Ego | Ego (generalized) | ✓ | |
| | Entrance to/support of social group | | |
| | Power | ✓ | "The higher they stood in their particular, let's say, profession, the more power they had relative to their peers." |
| | Recognition | ✓ | |
| | Status | ✓ | "It tied in with their status, and obviously this was ego-driven." |
| | Thrills/Self-importance | | |
| Entertainment | Entertainment (generalized) | | |
| | Adventure | ✓ | "This particularly is something that deals with double agents. They love the game almost more than anything else." |
| | Fun, Thrill, Excitement | | |
| | Pranks | | |
| Ideology | Ideology (generalized) | ✓ | "During the '40s and '50s, even back into the '30s, the predominant motivation was ideology." |
| | Anarchist | | |
| | Divided Loyalties | | |
| | Economic | | |
| | Ethnocentric | | |
| | Hacktivism | | |
| | Nationalist-Separatist | | |
| | Political Agenda | ✓ | "There were conflicting systems of the West, and capitalism, and Communism, and this political aspect was dominating." |
| | Religion | ✓ | |
| | Social | | |
| Ingratiation | | | |
| Money | | ✓ | "A person like Richard Hanson, it was ego. He was driven by ego, furious that he was not promoted within the FBI as he felt he should be. Aldrich Ames, on the other hand, was solely driven by money – total greed. And he had a lot of personality failures and behavior failures, but the driving motivation for him was money." |
| Psychological | Psychological (generalized) | | |
| | Anti-social | | |
| | Asperger Syndrome | | |
| | Autism Spectrum Disorder | | |
| | Introverted | | |
| | Narcissism | | |
| | Personality Disorder | | |
| | Type-A | ✓ | "This motivation is defined by the medical psychological community. But most of these actors...if they're not outright top of the order type A, have a lot of these characteristics." |
| Revenge | Revenge (generalized) | | |
| | Blame | | |
| | Disgruntlement | | |
| | Economic sabotage/steal | | |
| | Harm | | |
| | Injustice | | |
| Romance | | | |

Note: A check mark (✓) indicates presence of the motivation theme or sub-theme as identified by interviewee.

### Hacker interview motivations.

The interviewee specializing in cybercrimes also met the selection criteria. He or she confirmed experience as an intelligence analyst, intelligence supervisor, and as an instructor teaching cybersecurity analysts. His or her expertise is in cybercriminal activity and he or she has worked on “a number of high exposure cases” over the course of his or her for at least 10 years.

Again, the interviewee confirmed he or she reviewed the preparation materials. Based on the interviewee’s experience, he or she identified 14 motivational themes or sub-themes in the proposed topology. During the interview, the interviewee said the hackers with whom he or she interacted were “were driven mostly by the ego [motivation and its subthemes] of [the topology]” but there “generally is the money aspect as well.” He or she commented that revenge is a motivation mostly in the business world when a worker believes a company wronged the employee. However, revenge, exhibited as hacktivism, is the hacker’s way of protest. An insightful and interesting comment this interviewee made was with respect to differentiating the hacker person from the hacker’s moniker. The interviewee asserted most hackers “want the status of the online moniker, not the person behind it.” Table 9 displays the motivational themes and sub-themes the cybercrime interviewee identified.

*Table 9.*

*Motivation Themes and Sub-themes—Evidence by Cybercrime Interviewee*

| Motivation Theme | Motivation Sub-theme | Interviewee #2 | Comments |
|---|---|---|---|
| Addiction | | | |
| Choice | | | |
| Coercion | | | |
| Curiosity | Curiosity (generalized) | | |
| | Continuous learning | | |
| | Technical mastery/challenge | | |
| Ego | Ego (generalized) | ✓ | |
| | Entrance to/support of social group | ✓ | |
| | Power | ✓ | "They had a very large ego, they wanted to show that they had the power." |
| | Recognition | ✓ | "What you call recognition is what I tend to refer to as more kind of notoriety. In the hacker world, they just tend to use the word notoriety a little bit more, because they want to be seen as somebody, notorious, recognized... but not for themselves, but rather their moniker." |
| | Status | ✓ | "They want the status of the online moniker, not the person behind it." |
| | Thrills/Self-importance | | |
| Entertainment | Entertainment (generalized) | | |
| | Adventure | | |
| | Fun, Thrill, Excitement | ✓ | "Generally they're doing it for the thrills of it…getting the 'cool' points in that community." |
| | Pranks | | |
| Ideology | Ideology (generalized) | | |
| | Anarchist | | |
| | Divided Loyalties | | |
| | Economic | ✓ | |
| | Ethnocentric | | |
| | Hacktivism | ✓ | "It's the hacker way of fighting pack to ideological and political positions they don't like." |
| | Nationalist-Separatist | | |
| | Political Agenda | ✓ | |
| | Religion | | |
| | Social | | |
| Ingratiation | | | |
| Money | | ✓ | "Generally when you're looking at people that are hackers, a lot of them are financially motivated."<br>"With state actors...wouldn't really be into the money." |
| Psychological | Psychological (generalized) | | |
| | Anti-social | | |
| | Asperger Syndrome | | |
| | Autism Spectrum Disorder | | |
| | Introverted | | |
| | Narcissism | | |
| | Personality Disorder | | |
| | Type-A | | |
| Revenge | Revenge (generalized) | ✓ | |
| | Blame | ✓ | |
| | Disgruntlement | ✓ | |
| | Economic sabotage/steal | ✓ | |
| | Harm | ✓ | |
| | Injustice | ✓ | |
| Romance | | | |

Note: A check mark (✓) indicates presence of the motivation theme or sub-theme as identified by interviewee.

## Results and Discussion Summary

Applying Özdamar’s (2008) assertion of terrorism cases to the triple threat actors “there are great insights that we can learn from comparative case studies” (p. 100). The merging of the motivations of nefarious actors is also similar to the illicit network convergence phenomenon described by Miklaucic & Brewer (2013) whereby

> global trends and developments—including dramatically increased trade volumes and velocity, the growth of cyberspace, and population growth, among others—have facilitated the growth of violent non-state actors, the strengthening of organized crime, and the emergence of a new set of transcontinental supply chains as well as the expansion of existing illicit markets. (p. xiv)

Simply stated, convergence is “the merging and blending of an ever-expanding array of illicit actors and networks” (Miklaucic & Brewer, 2013, p. xiv). What then is the motivational difference between a spy who hacks and a hacker that spies, or a terrorist who hacks and a hacker who terrorizes? To answer these questions, studying motivations across actors becomes important as it may provide insights not previously considered. The use of new tools and technologies by each of these actors, such as the internet and social media, is causing a blur between previously and presumably easily differentiated motivations of the actors. “The old paradigm of fighting terrorism[, espionage, and hacking,] and transnational crime separately, utilizing [*sic*] distinct sets of tools and methods, may not be sufficient to meet the challenges posed by the convergence of these networks into a crime-terror-insurgency nexus” (Miklaucic & Brewer, 2013, p. xv). Table 10 presents the consolidated view of the motivational evidence from the case studies and interviews. A check mark in a cell indicates presence of the motivation theme or sub-theme; a blank cell represents the absence of evidence for the associated motivation in the case studies assessed and interviews conducted as part of this study. (See next page.)

*Table 10.*

*Consolidated Motivation Themes and Sub-themes Evidence*

| Motivation Theme | Motivation Sub-theme | Terrorists | | Spies | | Hackers | | Overlap |
|---|---|---|---|---|---|---|---|---|
| | | Case Studies | Interview | Case Studies | Interview | Case Studies | Interview | Overlap |
| Addiction | | | | ✓ | | ✓ | | **Yes** |
| Choice | | | ✓ | | | | | |
| Coercion | | | ✓ | ✓ | | | | **Yes** |
| Curiosity | Curiosity (generalized) | | ✓ | | | | | |
| | Continuous learning | | | | ✓ | ✓ | | **Yes** |
| | Technical mastery/challenge | | ✓ | | ✓ | ✓ | | **Yes** |
| Ego | Ego (generalized) | | ✓ | | ✓ | | ✓ | **Yes** |
| | Entrance to/support of social group | | ✓ | | | ✓ | ✓ | **Yes** |
| | Power | | ✓ | | ✓ | ✓ | ✓ | **Yes** |
| | Recognition | | ✓ | | ✓ | ✓ | ✓ | **Yes** |
| | Status | | ✓ | | ✓ | | ✓ | **Yes** |
| | Thrills/Self-importance | | ✓ | ✓ | | ✓ | | **Yes** |
| Entertainment | Entertainment (generalized) | | ✓ | | | | | |
| | Adventure | | | | ✓ | ✓ | | **Yes** |
| | Fun, Thrill, Excitement | | ✓ | | | ✓ | ✓ | **Yes** |
| | Pranks | | | | | ✓ | | |
| Ideology | Ideology (generalized) | | ✓ | | ✓ | | | **Yes** |
| | Anarchist | ✓ | | | | | | |
| | Divided Loyalties | | ✓ | ✓ | | | | **Yes** |
| | Economic | ✓ | ✓ | | | | | **Yes** |
| | Ethnocentric | | ✓ | | | | | |
| | Hacktivism | | | | | | ✓ | |
| | Nationalist-Separatist | ✓ | ✓ | | | | | **Yes** |
| | Political Agenda | ✓ | ✓ | ✓ | ✓ | | | **Yes** |
| | Religion | ✓ | ✓ | | ✓ | | | **Yes** |
| | Social | ✓ | | | | | | |
| Ingratiation | | | ✓ | | | | | |
| Money | | | | ✓ | ✓ | ✓ | ✓ | **Yes** |
| Psychological | Psychological (generalized) | | | | | | | |
| | Anti-social | | | | | | | |
| | Asperger Syndrome | | | | | ✓ | | |
| | Autism Spectrum Disorder | | | | | | | |
| | Introverted | | | | | | | |
| | Narcissism | | | | | | | |
| | Personality Disorder | | | | | ✓ | | |
| | Type-A | | | | ✓ | | | |
| Revenge | Revenge (generalized) | | ✓ | | | | ✓ | **Yes** |
| | Blame | | ✓ | | | | ✓ | **Yes** |
| | Disgruntlement | ✓ | ✓ | ✓ | | | ✓ | **Yes** |
| | Economic sabotage/steal | | | | | ✓ | ✓ | **Yes** |
| | Harm | | ✓ | | | | ✓ | **Yes** |
| | Injustice | ✓ | ✓ | | | | ✓ | **Yes** |
| Romance | | | | ✓ | | | | |

Note: A check mark (✓) indicates presence of the motivation theme or sub-theme in the case study evidence. See the Appendix for individual case studies for each actor.

Humans are complex beings and rarely would a single motive be the cause of a nefarious action. The analysis of cases generally indicated more than one motive contributed to the respective terrorist, espionage, or hacking event. Discussions with interviewees confirmed this observation, even though bias may be present based upon the interviewees' experiences working from the national security enforcement perspective versus from the internal perspective of an actor and perhaps lacking direct discussions with actors about their motives.[2] Underlying motivations appeared related to situations combining internal and external triggers such as a divorce, notoriety, or in protest to the US' response to domestic or world events. The central question guiding this research asked whether there were commonalities between the motives of non-state sponsored terrorists, spies, and hackers. The sub-questions queried motives, themes, and patterns, seeking to identify similarities and differences between the motives of each of the actors.

Based on the evidence presented in the case studies, terrorists, spies, and hackers share similar motivational themes or sub-themes in at least five instances: (1) addiction, (2) ego's sub-theme of 'thrills/self-importance,' (3) ideology's sub-theme of 'political agenda,' (4) money, and (5) revenge's sub-theme of 'disgruntlement.' Adding the evidence from the counterterrorism, counterespionage, and cybercrime experts' experiences increased the overlap or convergence of similar motivational themes or sub-themes to 25. While the increase in number of converging motivations supports the thesis, the evidence illustrates the limitations of this research—the relatively small sample sizes and interviewee bias. Nonetheless, for the first time in a single study, the evidence directionally confirms overlapping and converging motives amongst actors.

[2] NAU's IRB provided direction to the researcher to limit discussions to the topology and motivations, to remind interviewees to refrain from discussing confidential information, and to honor all non-disclosure agreements an interviewer made during their careers. Therefore, the researcher did not investigate any interviewees' direct discussions an interviewee may have had with actors about an actor's motivations (hearsay or secondary source data). This approach protected the interviewee's privileged and confidential discussions the interviewee may have had with an actor about his or her motives.

Current events also support the findings in this study. In the case of the *United States v. Ferizi*, the US government arrested and convicted someone for providing material support to a terrorist organization through information that came from computer hacking. “According to the defendant, he [was] a hacker since he was a young teenager” (*United States v. Ferizi*, 2016, p. 16). The motive, technological curiosity led Ardit Ferizi to admit “responsibility for hacking more than 20,000 websites” (*United States v. Ferizi*, 2016, p. 16). Although the defendant was not a US citizen, he was the first *terrorist hacker* the US government prosecuted and imprisoned for his actions. Ferizi will not be the only terrorist hacker (*United States v. Ferizi*, 2016, pp. 14-15) to receive this punishment. According to Assistant Attorney General for National Security John P. Carlin, this incident “was a wake-up call not only to those of us in law enforcement, but also to those in private industry” (DOJ, 2016). Carlin’s comment could be foreshadowing things to come. According to Brian Hale, former DNI Clapper’s spokesperson, the IC was “aware that [political] campaigns and related organizations and individuals are targeted by actors with a variety of motivations—from philosophical differences to espionage—and capabilities—from defacements to intrusions” (Volz & Hosenball, 2016, para. 2). Hale also “defer[red] to the FBI for details on specific incidents” (Volz & Hosenball, 2016, para. 2) hinting that the Bureau is aware of domestic cases.

Although it may be difficult for the government to convict actors of nefarious actions and threats to national security, as illustrated by converging motives, the threats are increasing. For example, as is the goal of a terrorist – to cause fear amongst the populous – that same goal is apparent in the cyberterrorist, who instead of using explosives, uses the internet (Cronin, 2019). In other instances, social media outlets such as Twitter and Facebook are now routinely scouring posts and pages of users seeking to suspend the accounts of actors suspected of terrorism, spying, or hacking that threatens national security (Fingas, 2019). According to Carlin (2018), hackers are joining the terrorist top ranks to launch cyber plots. Even Kirstjen Nielsen, the government's former Secretary of Homeland Security, according to Miroff (2018), asserted the agency was "shifting at her direction from a 'counterterrorism posture' to a wider 'counterthreat' approach" (para. 7) indicating recognition for convergence.

With convergence of disruptive actors on the rise, improved countermeasures based on evidence such as the shared motivations revealed through this research will help officials exploit actors' weaknesses to curtail their threats. A cross-actor motivational typology, such as the one proposed here could become a useful analytical tool for the strategic security discipline. It is only a matter of time before a US citizen commits a nefarious act exhibiting motivational convergence.

Chapter 4 reported the findings based on the data collected and analyzed for this study. The case study and interviewee evidence supported the thesis that motivations across national security's triple threat actor groups is converging. The study also highlighted a limitation of this research: the low sample size for case studies within actor groups and potential bias from interviewees. Nonetheless, as the first study of motivations across these three groups, the results support the convergence hypothesis and that a mosaic of motivations exists. The evidence is sufficient evidence to warrant further study. Chapter 5 concludes this research by reviewing its aims, main findings, presenting recommendations, and offering suggestions for future research.

## Chapter 5: Conclusion

Terrorism, espionage, and hacking are ongoing, top-of-mind national security concerns that evolve as globalization and convergence continue to connect people and nations. Simultaneously, forces such as differing worldviews, religious preferences, ideologies, and other aspects of civilization are working to pull people and nations apart (Huntington, 2007). Although Huntington's characterization of fault lines is broader than the research presented here, the basic premise also holds true for the events that precipitate conflicts *within* countries and the premise foreshadows national security's triple threat—an increasing vulnerability the US government must consider.

The historical analysis in the literature review demonstrated the perils against the US posed by national security's triple threat—terrorists, spies, and hackers—are hardly *new* phenomena. Each of these actors and their sinister actions pose a danger and present a risk to the nation's security. The purpose of this study remains to advance the understanding of the stimuli driving terrorists, spies, and hackers by integrating an analysis of each actor's motivations into a single study. Collectively this group of nefarious actors is converging because of the effects of globalization. Hence, it remains important to explore the multi-faceted threat created by the blurring of these actors' despicable actions. No single open-source research prior to this study examined, compared, or contrasted the motives of national security's triple threat.

If researchers identify the similarities and differences between the motives of terrorists, spies, and hackers, and develop recognizable patterns, then US counterterrorism and security specialists could develop tactics, techniques, and procedures to minimize, or thwart, some of the threats these actors collectively create. To gain an understanding of the collective motivations, the central question posited that there were commonalities between the motives of non-state sponsored US terrorists, spies, and hackers. The sub-questions queried the themes, similarities, and differences of the actors' motives.

This research employed the qualitative methodology using multiple case studies and the interview methods to study the motivations of the three actor groups. The researcher employed the content analysis technique to code, in a systematic manner, the text sources in the literature, and the interview data for motivations of terrorists, spies, and hackers. Based on the coding, the researcher developed a proposed topology of motivational themes and sub-themes.

To test the proposed motivational topology and study the motivations, the researcher identified multiple case studies, 20 cases representative of each actor to study motivation. As motivational themes and sub-themes emerged, the researcher created a single database representing motivational convergence of the triple threat actors. By analyzing the case studies, the researcher confirmed the convergence of actor motivations. To substantiate or refute the initial findings and analysis, the researcher interviewed an expert in each field—counterterrorism, counterespionage, and cybersecurity. Using content analysis of the interview transcripts the researcher confirmed a complex web for these actors' motivations and that motivational convergence amongst actors exists. The data from both the multiple case studies and the interviews supported the hypothesis and began to answer the research questions, although limitations surfaced during the study.

This study advanced the research in the field of strategic security through its examination and rigorously executed analysis of national security's triple threat where previously no prior combined study of the three actor groups existed. Indeed, this research illuminated the need for additional inquiry into the combined threats posed by these actors. The following sections summarize the main findings, present recommendations worthy of consideration, and provide suggestions for future research.

## Findings

This study added to the body of research on terrorists, spies, and hackers, and more specifically to the study of motivations—helping researchers understand the motivations that compelled these actors to commit the crimes they committed.

The analysis of data added to the corpus of strategic security in the following ways:

1. It illuminates weaknesses in prior research with respect the definitional inconsistency of motivations. A lack of definitional clarity perpetuated the flaw such that it creates circular intelligence and reinforced confirmation bias in the body of literature.
2. It establishes a database containing cases studies of three actor types to facilitate cross-comparison studies revealing the convergence of motives and actors—the first study of its kind.
3. It increases knowledge by proposing a common motivation typology.
4. It tests that typology to demonstrate the converging motives across three actor groups.
5. The data and analysis of the multiple case studies and interviews support the hypothesis that motivational convergence exists.
6. As new technology becomes available and the use of these technologies by actors to commit crimes becomes increasingly ubiquitous, convergence and a blurring of motivations makes it increasingly difficult to categorize these actors, and
7. Perhaps the most significant finding is the number of motives the actors cite and experts mention they had experienced over their careers increase as the convergence and blurring of motivations transpire.

The researcher expected several benefits from conducting this study that came to fruition. The findings increase policy makers' and national security practitioners' understanding about the motivations of terrorists, spies, and hackers. The interviewees confirmed motivational convergence in addition to the multiple case study findings. Policy makers and national security practitioners gained insight into new perspectives on motivations they can pursue to advance policy. Finally, academicians can build upon the findings to bolster research in the strategic security field.

## Recommendations

National security's triple threat represents a diverse group of actors with a divergent set of worldviews. These actors claim numerous motives to justify the nefarious and illegal actions they commit. This study and its findings confirm a multi-faceted national security threat exists and the line between these actors and their actions is blurring. Ever since Maslow (1943) proposed motivational theory and identified the hierarchy of needs as the force behind a person's modus operandi for altruistic or nefarious purposes, scholars have sought to understand why people behave the way they do. Biologists, sociologists, psychologists, anthropologists, and numerous researchers in various disciplines such as military science, history, political science, and intelligence also seek to understand motives and behavior. There are multiple theories and beliefs about each actor's motivation but no behavioral or motivational theory as to the collective threat. Perhaps the truth lies at the intersection of the various theories—biological, emotional, social, or psychological.

Policymakers face an important challenge to counter the converging threats that comprise a complex, multi-faceted phenomenon. Unfortunately, this threat does not invite a simple, concise, or straightforward solution. Given the multi-faceted challenge, an appropriate response is also multi-faceted. Hence, the recommendation worthy of consideration is for policymakers to recognize taking an offensive position provides a strategic advantage. It is time to adopt a national security strategy that accounts for not only the asymmetric nature of the threat these actors pose, but also the convergence of their motives. Policymakers should establish strategic planning exercises using representatives from agencies, intelligence, law enforcement, academics, and the private sector to develop thorough and scientific studies about motivations and convergence. The human condition is at the heart of understanding the motives driving national security's triple threat.

In conjunction with gaining a deeper understanding of motives, policymakers must develop scenarios, evaluate the plausibility each presents, and devise a long-term strategy to address the threat. The strategy should portray the US's position on threat convergence, and more importantly, it should provide guidance on how the US will maintain its offensive position to thwart the threats from these actors. As President Eisenhower said, "the only way to win World War III is to prevent it" (Eisenhower, 1956, p. 210). In terms of national security's triple threat, the only way to win is to plan and prepare for it. The country and its leaders—in both the public and private sectors—have little time to respond given globalization, technology-enabled instantaneous communication, and the frequency with which combined attacks such as the Ferizi terrorist hacker example noted in the previous chapter present.

A solution to jump-start the process is an historical look at a strategic planning exercise ordered by President Eisenhower at the beginning of his presidency and to execute a similar exercise. *Project Solarium* was the strategic planning exercise President Eisenhower ordered after World War II because he was "concerned that America's national security strategy, as articulated in National Security Council Paper [NSC] 68, committed the country to policies not sustainable in the long term" (Flournoy & Brimley, 2006, pp. 6-7). After heated debate with then-Secretary of State John Foster Dulles and other policy advisors,

> Eisenhower…propose[d] an exercise that would capture analytically the range of options available to the United States while preserving the differences and disagreements between them. 'Project Solarium,' as it became known [*sic*], is a rare and valuable example of useful strategic planning at the highest levels of the executive branch…. Eisenhower…suggested that the administration assemble 'teams of bright young fellows,' that would 'take an alternative and tackle it with a real belief in it just the way a good advocate tackles a law case.' Eisenhower wanted each team to present its findings before the NSC principals, with 'maps, charts, all the basic supporting figures [*sic*] and estimates, just what each alternative would mean in terms of goal, risk, cost in money and men and world relations. (Flournoy & Brimley, 2006, p. 7)

In a matter of six weeks, three teams assembled, each taking different positions and developed alternatives for their points of view. In a one-day session, each team presented its solution and answered questions. Eventually Eisenhower instructed the groups to take the salient components from each of the three presentations to develop a single strategy from which National Security Council (NSC) developed document NSC 162/2—the New Look national security policy (Flournoy & Brimley, 2006).

Project Solarium is the seminal example of strategic planning using structured analysis tools such as Team A/Team B, Outside-In Thinking, and Alternative Futures Analysis in combination with critical thinking (CIA, 2009; Moore, 2007). It demonstrates the government and the private sector can execute a long-term strategic planning process, "although one must look back [66] years to find it. In some ways, President Dwight D. Eisenhower faced a situation in 1953 similar to what the current administration faces today: how to plan for an uncertain future when the stakes are high, and there is no obvious consensus on how to deal with a growing strategic threat" (Flournoy & Brimley, 2006, p. 6).

The strength of a solution such as Project Solarium is a fitting given the multi-faceted asymmetric threat with little consensus on how to explain and counter the motivations of the actors. This type of strategic planning solution has a US precedent. Most notably, it uses recognized analytical tools proven to work when trying to develop solutions for wicked strategic problems (Camillus, 2008) such as national security's triple threat.

**Future research**

No research is without limitations and this study was no exception. While the results demonstrated a convergence across five of the 12 motivational themes, there was insufficient evidence to support or refute the combination of the 43 motivational themes and sub-themes identified in the literature and proposed in the motivational typology from the case studies alone. The data from the interviews however demonstrated convergence across 11 motivational themes and 20 sub-themes, thereby reinforcing the convergence hypothesis. As noted previously, due to sample sizes, this study may not be sufficient to generalize the findings across the population of terrorists, spies, and hackers, yet it is a first step in that direction.

This study did not reach saturation with the number of cases reviewed in the sample or via the interviews. It is likely however, that expanding significantly the number of cases in each actor group would achieve saturation and therefore reveal instances of motives not seen in the current study. For example, the ingratiation motive identified in the espionage literature was absent in the espionage cases, and despite the hacking literature citing status as a typical hacker motive, no hacker in the sample cited status as their motive. To remedy these situations, future research would need to add cases to the combined database by expanding the sample size for each actor group. In addition, due to NAU's IRB concerns, logistics, and interviewer and interviewee protections, the researcher did not obtain first-hand accounts of actors' motivations. Additional research using the interview technique with the actors themselves would overcome the imposed limitation.

The relationship of the findings to the literature review content analysis demonstrated a gap in the study of domestic terrorism. Although US laws and the constitution protect free speech, a carefully constructed study to avoid impropriety yet delve into the motivations of each of the actors may yield significant insights that contrast with those in the international terrorism literature. For example, the literature on each actor cited ideology as the top motivation. Future research should explore specific ideologies to expose the details and qualitatively tell the stories of these actors to gain a greater understanding of how the hate, frustration, and cognitive cycles of each actor differ so the motivational patterns can be broken.

## Summary

Terrorism, spies, and hackers present a mutually inclusive threat that cannot be defeated unilaterally or without a comprehensive and integrated strategy. With convergence of disruptive actors on the rise, improved countermeasures based on evidence such as the shared motivations revealed through this research will help officials exploit actors' weaknesses to curtail their threats. A cross-actor motivational typology, such as the one proposed here, could become a useful analytical tool for the strategic security discipline when combined with other tools to develop a strategic plan to address the threat. The next President and his or her administration should draw upon the lessons of Project Solarium—using a conceptual approach to attack a new complex threat—and immediately undertake a strategic planning exercise by issuing a strategic planning directive. The result of the directive would be to produce an updated national strategy, with an adaptable approach that provides the flexibility necessary to thwart dangers the US faces from national security’s triple threat. It is only a matter of time before a US citizen commits a nefarious act exhibiting convergence of motivations.

## References

4iQ, Inc. (2019, February). *The changing landscape of identities in the wild: The long tail of small breaches: 2019 4iQ identity breach report* [PDF]. Los Altos, CA: 4iQ Inc.

Abel, T. (1937). The pattern of a successful political movement. *American Sociological Review, 2*(3), 347-352. http://dx.doi.org/10.2307/2084866

Ackerman, S. (2012, August 7). DHS crushed this analysis for warning about far-right terror. *Wired*. Retrieved from https://www.wired.com/2012/08/dhs/

Adamski, A. (1998). Crimes related to the computer network. Threats and opportunities: A criminological perspective. In M. Jousten (Ed.), *Five issues in European criminal justice: Corruption, women in the criminal justice system, criminal policy indicators, community crime prevention, and computer crime: Proceedings of the VI European Colloquium on Crime and Criminal Policy, Helsinki 10-12 December 1998* (pp. 214-248). Retrieved from http://www.heuni.fi/material/attachments/heuni/reports/6KdG0RVGx/fiveissu.pdf

Addiction. (n.d.). In Merriam-Webster Online. Retrieved from https://www.merriam-webster.com/dictionary/addiction

Akers, R. L. & Jensen, G. F. (2006). The empirical status of social learning theory of crime and deviance: The past, present, and future. In F. T. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory: Advances in criminological theory, Vol. 15* (pp. 37-76). New Brunswick: Transaction Publishers.

American Psychiatric Association (APA). (2000). *Diagnostic and Statistical Manual of Mental Disorders: DSM-IV-TR* (4th Edition). Washington, D.C.: American Psychiatric Association.

Appel, E. (2003, August 21). *Why are espionage convictions so rare?* PBS Frontline (Interview from episode From China with Love). Retrieved from https://www.pbs.org/wgbh/pages/frontline/shows/spy/interviews/appel.html

Apter, M. J. (1984). Reversal theory and personality: A review. *Journal of Research in Personality, 18*(3), p. 265-288. doi:10.1016/0092-6566(84)90013-8

Apter, M. J., Mallows, R., & Williams, S. (1998). The development of the motivational style profile. *Personality and Individual Differences, 24*(1), 7-18. http://dx.doi.org/10.1016/S0191-8869(97)00148-7

Apter, M. J.; Fontana, D.; Murgatroyd, S. (2014). *Reversal Theory: Applications and Development*. http://dx.doi.org/10.4324/9781315801773

Bandura, A. (1971). *Social learning theory*. Retrieved from http://cogs.indiana.edu/~cogs/spackled/2012readings/bandura.pdf

Barrett, M. J., (1984). Honorable espionage. *Journal of Defense and Diplomacy, 2*(2), 13-25, 36. https://repository.library.georgetown.edu/handle/10822/802393

Bassham, L. E., & Polk, T. (1992, October). *Threat assessment of malicious code and human threats*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4939.pdf

Begin, M. (2013). *The revolt* (Kindle for iPad edition). Retrieved from http://www.amazon.com

Bertucci, P. (2013). Enlightened secrets: Silk, intelligent travel, and industrial espionage in Eighteenth-Century France. *Technology and Culture, 54*(4), 820-852. http://dx.doi.org/10.1353/tech.2013.0123

Best, K. (2003). The hacker's challenge: active access to information, visceral democracy and discursive practice. *Social Semiotics, 13*(3), 263-282. Retrieved from http://dx.doi.org/10.1080/1035033032000167015

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. Retrieved from https://scholarcommons.usf.edu/oa_textbooks/3/

Bjelopera, J. P. (2013). *The domestic terrorist threat: Background and issues for Congress*. Retrieved from https://fas.org/sgp/crs/terror/R42536.pdf

Bolanos, A. (2012). Is there a "new terrorism" in existence today? In R. Jackson & S. J. Sinclair, (Eds.). *Contemporary debates on terrorism* [ebook] (pp. 29-35). Retrieved from http://www.eblib.com

Borum, R. (2003). Understanding the terrorist mind-set. *FBI Law Enforcement Bulletin 72*(7), 7-10. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/201462.pdf

Borum, R. (2004). *Psychology of terrorism*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/208552.pdf?q=psychology-of-terrorism

Borum, R., Shumate, S. R., & Scalora, M. (2006). The psychology of leaking national security secrets: Implications for homeland security, *Homeland Security Review, 1*(2), 97-111. Retrieved from https://scholarcommons.usf.edu/mhlp_facpub/544/

Bossler, A. M. & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 38-67). Retrieved from http://search.ebscohost.com.ezproxy2.apus.edu/login.aspx?direct=true&db=nlebk&AN=310566&site=ehost-live&scope=site&ebv=EB&ppid=pp_38

Bruce, J. B. (2016). Keeping U.S. national security secrets: Why is this so hard? The Intelligencer: Journal of U.S. *Intelligence Studies, 22*(2), 47-54. Retrieved from https://www.afio.com/publications/BRUCE_James_Keeping_US_National_Security_Secrets_from_AFIO_INTEL_FALL2016_Vol22_no2_FINAL.pdf

Budiansky, S. (2005). *Her Majesty's spymaster: Elizabeth I, Sir Francis Walsingham, and the birth of modern espionage*. New York, NY: Viking.

Burkett, R. (2013). Rethinking and old approach: An alternative framework for agent recruitment: From MICE to RASCLS, *Studies in Intelligence, 57*(1), 7-17. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf

Camillus, J. C. (2008). Strategy as a wicked problem. *Harvard Business Review*, *86*(5), 98-106. Retrieved from https://hbr.org/2008/05/strategy-as-a-wicked-problem

Campbell, Q., & Kennedy, D. M. (2014). The psychology of computer criminals. In S. Bosworth, M. E Kabay, & E. Whyne (Eds.). *Computer security handbook* (6th Ed.) [ProQuest eBook] (pp. 12-1 – 12-33). Retrieved from http://ebookcentral.proquest.com

Cardwell, J. M. (1978). Bible lesson on spying. *Studies in Intelligence, 22*(3), 59-63. Retrieved from https://www.cia.gov/library/readingroom/docs/CIA-RDP80-00630A000100040001-5.pdf

Carlin, J. P. (2018, November 21). Inside the hunt for the world's most dangerous terrorist. *Politico.* Retrieved from https://www.politico.com/magazine/story/2018/11/21/junaid-hussain-most-dangerous-terrorist-cyber-hacking-222643

Carr, C. (1996/1997, Winter). Terrorism as warfare: The lessons of military history. *World Policy Journal*, *13*(4), 1-12. https://www-jstor-org.ezproxy.lib.usf.edu/stable/40209499

Carr, C. (2007). "Terrorism:" Why the Definition Must Be Broad. *World Policy Journal, 1(*47). https://doi.org/10.1162/wopj.2007.24.1.47

Caton, J. L. (2009). What do senior leaders need to know about cyberspace? In D. Neal, H. Friman, R. Doghty, & L. Wells (Eds.) *Crosscutting issues in international transformation: Interactions and innovations among people, organizations, processes, and technology*. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Crosscutting-Issues-in-International-Transformation.pdf?ver=2017-06-16-112714-487

Center for Strategic & International Studies (CSIS). (2019). *Significant cyber incidents since 2006*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf

Central Intelligence Agency (CIA). (2009). *A tradecraft primer: Structured analytical techniques for improving intelligence analysis*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

Centre for Counterintelligence and Security Studies (CI CENTRE). (2019). *SPYPEDIA*®, [Data file]. Retrieved from https://cicentre.site-ym.com/?page=membership_features

Chaliand, G., & Blin, A., (Eds.). (2007). *The history of terrorism: From antiquity to al Qaeda* (E. Schneider, K. Pulver, & J. Browner, Trans.). Retrieved from https://ebookcentral.proquest.com/lib/usf/detail.action?docID=293831.

Champion, B. (2008). Spies (look) like us: The early use of business and civilian covers in covert operations. *International Journal of Intelligence & Counterintelligence, 21*(3), 530-564. http://dx.doi.org/10.1080/08850600701651268

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2), 229-251. http://dx.doi.org/10.1006/ijsl.1996.0015

Charney, D. L. & Irvin, J. A. (2016). *A guide to the psychology of espionage. The Intelligencer: Journal of U.S. Intelligence Studies, 22*(1), 71-77. Retrieved from https://www.afio.com/publications/CHARNEY_The_Psychology_of_Espionage_DRAFT_2014Aug28.pdf

Charney, D. L. (2010). True psychology of the insider spy. *Intelligencer: Journal of U.S. Intelligence Studies, Fall/Winter,* 47-54. Retrieved from http://noir4usa.org/wp-content/uploads/2014/02/Charney-True-Psychology-of-Insider-Spy.pdf

Choice. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/choice

Christ, T. (2013). The worldview matrix as a strategy when designing mixed methods research. *International Journal of Multiple Research Approaches, 7*(1), 110-118. http://dx.doi.org/10.5172/mra.2013.7.1.110

Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.) (Kindle for iPad edition). Retrieved from https://www.amazon.com/

Coerce. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/coerce

Commission on the Roles and Responsibilities of the U.S. Intelligence Community (Aspin-Brown Commission). (1996). Appendix A-Evolution of the U.S. Intelligence Community: An historical overview. In Aspin-Brown Commission, *Preparing for the 21st century: An appraisal of U.S. Intelligence* (pp. A-1–A-25). Retrieved from https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-22-1.pdf

Compton-Lilly, C. (2013). Case studies. In A. A. Trainor & E. Graue (Eds.), *Reviewing qualitative research in the social sciences* [e Book] (pp. 54-65). Retrieved from https://ebookcentral.proquest.com

Cottee, S., & Hayward, K. (2011). Terrorist (E)motives: The existential attractions of terrorism. *Studies in Conflict & Terrorism, 34*(12), 963-986. http://dx.doi.org/10.1080/1057610X.2011.621116

Crenshaw, M. (1981). The causes of terrorism. *Comparative Politics*, *13*(4), 379-399. http://dx.doi.org/10.2307/421717

Crenshaw, M. (1986). The psychology of political terrorism. In M. G. Hermann (Ed.), *Political psychology: Contemporary problems and issues* (pp. 379-413). San Francisco, CA: Jossey-Bass Publishers

Crenshaw, M. (1987). Theories of terrorism: Instrumental and organizational approaches. *Journal of Strategic Studies, 10*(4), 13-31. http://dx.doi.org/10.1080/01402398708437313

Crenshaw, M. (1988). Theories of terrorism: Instrumental and organizational approaches. In D. C. Rapoport (Ed.), *Inside terrorist organizations* (pp. 13-31). Retrieved from http://www.stanford.edu/class/polisci243b/readings/crenshaw.pdf

Crenshaw, M. (1995). *Terrorism in context*. University Park, PA: The Pennsylvania State University Press.

Crenshaw, M. (2000). The psychology of terrorism: An agenda for the 21st century. *Political Psychology, 21*(2), 405-420. http://dx.doi.org/10.1111/0162-895X.00195

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.) [Kindle for iPad version]. Retrieved from http://www.amazon.com

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Los Angeles, CA: SAGE Publications, Inc.

Crimes and Criminal Procedure. Title 18 USC § 2331(5) (2012)

Cronin, C. (2019, June 25). The growing threat of cyberterrorism facing the U.S. Retrieved from https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/

Crowe, S., Creswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology, 11*(1), 2-9. https://doi.org/10.1186/1471-2288-11-100

Cullum, G. (1865). Military espionage. *The United States Service Magazine (1864-1866), 3*(1), 150-161. Retrieved from https://babel.hathitrust.org/cgi/pt?id=mdp.39015073424320&view=1up&seq=11

Curiosity. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/curiosity

Davis, J. H. (2015, July 9). Hacking of government computers exposed 21.5 million people. *The New York Times*. Retrieved from https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

Defense Human Resource Activity (DHRA). (2012, April). *Online guide to security responsibilities* (Version 5.1). Retrieved from https://www.dhra.mil/PERSEREC/OSG/

Denning, D. E. (1999). *Information warfare and security*. New York, NY: ACM Press.

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In T. J. Holt & B. H. Schell (Eds.). *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). Retrieved from http://faculty.nps.edu/dedennin/publications/CyberConflict-EmergentSocialPhenomenon-final.pdf

Department of Justice (DOJ). (2016, March 23). *Chinese national pleads guilty to conspiring to hack into U.S. defense contractors' systems to steal sensitive military information* [Press release]. Retrieved from https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

Dictionnaire de l'Académie française [Dictionary of the French Academy]. (1694/1798). Retrieved from http://artfl-project.uchicago.edu/content/artfl-collaborations

Diderot, D. & Alembert, J. L. (Eds.). (1751-1772/2013). *Encyclopédie, ou dictionnaire raisonné des sciences, des arts et des métiers* [Encyclopedia or reasoned dictionary of sciences, arts and crafts (Spring 2013 Ed.)]. Retrieved from http://encyclopedie.uchicago.edu/.

Director of Central Intelligence (DCI). (1990, April 12). *Project Slammer interim report.* Retrieved from https://www.cia.gov/library/readingroom/docs/DOC_0000218679.pdf

Director of Central Intelligence Center (DCIC). (2002, March). *Why people spy: A Project Slammer report* (Report no. CIC CIT 001-93). Retrieved from http://cryptome.org/2013/06/cia-why-spy.pdf

Dulles, A. (1963/1965/2006). *Craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world* [electronic resource]. Retrieved from https://openlibrary.org/books/OL5935886M/The_craft_of_intelligence

Duyvesteyn, I. & Malkki, L. (2012). The fallacy of the new terrorism thesis. In R. Jackson & S. J. Sinclair, (Eds.), *Contemporary debates on terrorism* [ebook] (pp. 50-57). https://www-taylorfrancis-com.ezproxy.lib.usf.edu/books/9781315679785

Duyvesteyn, I. (2004). How new is the new terrorism? *Studies in Conflict & Terrorism, 27*(5), 439-545. http://dx.doi.org/10.1080/10576100490483750

Dvornik, F. (1974). *Origins of intelligence services: The ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy*. New Brunswick, N.J: Rutgers University Press.

Economic Espionage Act, 18 U.S.C. §§ 1831-1837 (1996).

*Economic espionage: Hearing before the Senate Select Committee on Intelligence and Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology, and Government Information*, 104th Cong. 1. (1996) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation). Retrieved from http://www.intelligence.senate.gov/sites/default/files/hearings/economicespionag00unit.pdf

Ego. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/ego

Eisenhower, D. D. (1956). *Public papers of the presidents of the United States: Dwight D. Eisenhower: Containing the public messages, speeches, and statements of the president, January 1 to December 31, 1956*. Retrieved from http://quod.lib.umich.edu/p/ppotpus/4728413.1956.001/825?rgn=full+text;view=image;q1=World+War+III

Eltringham, S. (Ed). (2015). Prosecuting computer crimes. Retrieved from https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Entertainment. (n.d.). Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/entertainment

Eoyang, C. (1994). Models of espionage. In T. R. Sarbin, R. M. Carney; R. M., & C. Eoyang. (Eds.). *Citizen espionage: Studies in trust and betrayal.* Westport, CT: Praeger.

Erişen, C., Erişen, E., & Özkeçeci-Taner, B. (2013). Research methods in political psychology. *Turkish Studies*, *14*(1), 13-33. https://doi.org/10.1080/14683849.2013.766979

Espionage Act, 18 U.S.C. §§ 792–799 (1917).

Federal Bureau of Investigation (FBI). (2006, May 5). The case of the "Zombie King:" Hacker sentenced for hijacking computers for profit. Retrieved from https://archives.fbi.gov/archives/news/stories/2006/may/botnet050806

Federal Bureau of Investigation (FBI). (2016, March 8). Lottery fraud: Scammers target the elderly. Retrieved from https://www.fbi.gov/news/stories/-scammers-target-the-elderly-in-lottery-fraud

Federal Bureau of Investigation. (n.d.). Terrorism Definition. Retrieved from https://www.fbi.gov/investigate/terrorism

Fialka, J. J. (1997, Winter). The new industrial espionage. *The Wilson Quarterly*, *21*(1), 48-63. Retrieved from http://www.jstor.org/stable/40259596

Fingas, J. (2019, January 2). Hackers seize dormant Twitter accounts to push terrorist propaganda. *Edgadget*. Retrieved from https://www.engadget.com/2019/01/02/hackers-seize-dormant-twitter-accounts-for-isis-propaganda/

Fisher, L. F. (2000). Espionage: Why does it happen? *DoD Security Institute*. Retrieved from http://www.au.af.mil/au/awc/awcgate/dod/espionage_whyhappens.pdf

Flournoy, M. A., & S. W. Brimley. (2006). Strategic planning for U.S. national security: A Project Solarium for the 21st century. *The Princeton Project Papers*. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a521724.pdf

Francis, M. D. M. (2016). Why the "sacred" is a better resource than "religion" for understanding terrorism. *Terrorism & Political Violence*, *28*(5), 912–927. http://dx.doi.org/10.1080/09546553.2014.976625

Fromkin, D. (1975). The strategy of terrorism. *Foreign Affairs*, *53*(4), 683-698. http://dx.doi.org/10.2307/20039540

Fusch, P. I. & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss9/3/

Gage, B. (2011). Terrorism and the American experience: A state of the field. The *Journal of American History, 98*(1), 73-94. http://dx.doi.org/10.1093/jahist/jar106

Ganor, B. (2002). Defining terrorism: Is one man's terrorist another man's freedom fighter? *Police Practice & Research, 3*(4), 287-304. http://dx.doi.org/10.1080/1561426022000032060

*General Orders No. 100, Adjutant General's Office*. (1863). Art. 88. Retrieved from http://avalon.law.yale.edu/19th_century/lieber.asp#art100

Gerrig, R. J., & Zimbardo, P. G. (2002). *Psychology and life*. Boston, MA: Allyn and Bacon.

Greenberg, J. (2014, January 10). CNN's Tapper: Obama has used Espionage Act more than all previous administrations. *Tampa Bay Times, Politifact*. Retrieved from https://www.politifact.com/punditfact/statements/2014/jan/10/jake-tapper/cnns-tapper-obama-has-used-espionage-act-more-all-/

Greene, T. (2015, December 2). Biggest data breaches of 2015. *NetworkWorld.* Retrieved from https://www.networkworld.com/article/3011103/biggest-data-breaches-of-2015.html

Halleck, H. W. & Davis, G. D. (1911). Military espionage. *The American Journal of International Law (5)*3, 590-603. http://dx.doi.org/10.2307/2186360

Hartley, J. (2004). Case study research. In C. Cassell & G. Symon (Eds.), *Essential guide to qualitative methods in organizational research* (pp.323-333). Retrieved from https://smpncilebak2011.files.wordpress.com/2011/11/essential-guide-to-qualitative-in-organizational-research.pdf

Hatamleh, H. (2012). A review and comparing of all hacking techniques and domain name system method. *Contemporary Engineering Sciences, 5*(5), 239-250. Retrieved from http://www.m-hikari.com/ces/ces2012/ces5-8-2012/hatamlehCES5-8-2012.pdf

Heberle, R. (1949). Observations on the sociology of social movements. *American Sociological Review, 14*(3), 346-357. http://dx.doi.org/10.2307/2086882

Herbig, K. L. (2008, March). *Changes in Espionage by Americans: 1947-2007* (Technical report no. 08-05). Retrieved from https://fas.org/sgp/library/changes.pdf

Herbig, K. L. (2017, August). *The expanding spectrum of espionage by Americans, 1947 - 2015* (Technical report no. 17-10). Retrieved from https://fas.org/irp/eprint/spectrum.pdf

Herbig, K. L., & Wiskoff, M. F. (2002, July). *Espionage against the United States by American citizens 1947-2001* (Technical report no. 02-5). Retrieved from https://fas.org/sgp/library/spies.pdf

Hiley, N. (1985). The failure of British counter-espionage against Germany, 1907-1914. *Historical Journal, 28*(4), 835-862. http://dx.doi.org/10.1017/S0018246X00005094

Hiley, N. (1986). Counter-espionage and security in Great Britain during the First World War. *English Historical Review, 101*(400), 635-670. http://dx.doi.org/10.1093/ehr/CI.CCCC.635

Hitz, F. P. (2008). *Why spy?: Espionage in an age of uncertainty*. New York, NY: Thomas Dunne Books/St. Martin's Press.

Hitz, F. P., & Weiss, B. J. (2004) Helping the CIA and FBI connect the dots in the War on Terror, *International Journal of Intelligence and CounterIntelligence, 17*(1), 1-41. http://dx.doi.org/10.1080/08850600490252641

Hoffman, B. (2006). *Inside terrorism*. New York, NY: Columbia University Press.

Hoffman, B. (2015). *Anonymous soldiers: The struggle for Israel 1917-1947* [Kindle edition]. https://www.amazon.com/

Holt, T. J. & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. http://dx.doi.org/10.1080/01639625.2013.822209

Holt, T. J. & Kilger, M. (2012, May 28). *Know your enemy: The social dynamics of hacking*. Retrieved from https://stratcomcoe.org/thomas-j-holt-max-kilger-know-your-enemy-social-dynamics-hacking

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171-198. http://dx.doi.org/10.1080/01639620601131065

Hong, S. (2001). *Wireless: From Marconi's black-box to the audion*. Retrieved from http://monoskop.org/images/f/f4/Hong_Sungook_Wireless_From_Marconis_Black-Box_to_the_Audion.pdf

Hsieh, H. & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288. https://doi.org/10.1177/1049732305276687

Hulnick, A. S. (2004). Espionage: Does it have a future in the 21st century? *Brown Journal of World Affairs, 11*(1), 165-173. Retrieved from https://www.jstor.org/stable/24590505

Hunter, R. (1914/2010). *Violence and the labor movement* [Kindle edition]. Retrieved from http://www.gutenberg.org/ebooks/31108

Huntington, S. P. (2007). *The clash of civilizations and the remaking of world order* [Kindle for iPad version]. Retrieved from https://www.amazon.com/

Ideology. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/ideology

Infoplease. (2014). Computer virus timeline. *Sandbox Networks, Inc*. Retrieved from http://www.infoplease.com/ipa/A0872842.html#ixzz20WXIV22R

Ingratiate. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/ingratiate

Inserra, D. (2018, July 3). Terror plot 104 targets the Fourth of July [Commentary]. Retrieved from https://www.heritage.org/terrorism/commentary/terror-plot-104-targets-the-fourth-july

Jaishankar, K. (2011). *Cyber criminology: Exploring internet crimes and criminal behavior* [electronic resource]. http://dx.doi.org/10.1201/b10718

Johnson, C. (1982). *Revolutionary change* (2nd ed.). Stanford, CA: Stanford University Press.

Kainz, H. (1999). Biblical terrorism: With a Platonic deconstruction, *Philosophy & Rhetoric, 32*(1), 40-59. Retrieved from https://www.jstor.org/stable/40238016

Kautilya. (1915). *Arthashastra* (R. Shamasastry, Trans.). Retrieved from https://ia802703.us.archive.org/13/items/Arthasastra_English_Translation/Arthashastra_of_Chanakya_-_English.pdf

Kilger, M., Arkin, O., & Stutzman, J. (2004). Chapter 16: Profiling. In The Honeynet Project (Ed.), *Know your enemy: Learning about security threats (2nd Ed.)* (pp. 505-556). Addison-Wesley Professional. Retrieved from http://old.honeynet.org//book/Chp16.pdf

Kirwan, G., & Power, A. (2013). *Cybercrime: The psychology of online offenders* [electronic resource]. http://dx.doi.org/10.1017/CBO9780511843846

Knightly, P. (1986). *The second oldest profession: Spies and spying in the twentieth century* [eBook]. Retrieved from https://archive.org/details/TheSecondOldestProfession

Kohlbacher, F. (2006). The use of qualitative content analysis in case study research. *Forum: Qualitative Social Research, 7*(1), (n.p.). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/75/153

Kramer, L. A., & Heuer, R. J. (2007). America's increased vulnerability to insider espionage. *International Journal of Intelligence & Counterintelligence, 20*(1), 50-64. http://dx.doi.org/10.1080/08850600600888698

Krebs, B. (2003, February 14). A short history of computer viruses and attacks. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html

Lake, E., & Hudson, A. (2009, April 16). Napolitano stands by controversial report. *The Washington Times*. Retrieved from https://www.washingtontimes.com/news/2009/apr/16/napolitano-stands-rightwing-extremism/

Laqueur, W. (1987). *The age of terrorism*. Boston, MA: Little, Brown and Company.

Laqueur, W. (1996). Postmodern terrorism. *Foreign Affairs, 75*(5), 24-36. http://dx.doi.org/10.2307/20047741

Laqueur, W. (2003). No end to war: Terrorism in the 21st Century. New York, NY: The Continuum International Publishing Group Inc.

Laqueur, W. (2007). Terrorism: A brief history. *Foreign Policy Agenda, 12*(5), 20-23. Retrieved from https://www.hsdl.org/?view&did=473930

Lerner, K. L. & Lerner, B. W. (Eds.) (2004). *Encyclopedia of espionage, intelligence, and security* (Vol. 1, A-E). Detroit, MI: Gale.

Levchenko, S. (1988). *On the wrong side: My life in the KGB* [ebook]. Retrieved from https://archive.org/stream/onwrongsidemylif00levc#page/n5

Lewis, R. C. (2004). Espionage and the war on terrorism: Investigating U.S. efforts. *Brown Journal of World Affairs, 11*(1), 175-18273. Retrieved from https://www.jstor.org/stable/24590506

Lillbacka, R. (2017). The social context as a predictor of ideological motives for espionage. *International Journal of Intelligence & Counterintelligence, 30*(1), 117–146. http://dx.doi.org/10.1080/08850607.2016.1230704

Lincoln, Y. S. & Guba, E. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage Publications, Inc.

Lizardo, O. A., & Bergesen, A. J. (2003). Types of terrorism by world system location. Humboldt *Journal of Social Relations*, *27*(2), 162-192. Retrieved from https://www.jstor.org/stable/23524157

Machiavelli, N. (1515/2006). *The prince* (eBook #1232) (W. K. Marriott, Trans.). Retrieved from https://www.gutenberg.org/files/1232/1232-h/1232-h.htm

Madarie, R. (2017). Hackers' motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology, 11*(1), 78–97. https://doi.org/10.5281/zenodo.495773

Mahoney, J., & Goertz, G. (2006). A tale of two cultures: Contrasting quantitative and qualitative research. *Political Analysis, 14*(3), 227-249. https://dx.doi.org/10.1093/pan/mpj017

Major, D., & Oleson, P. C. (2017). Espionage against America. *The Intelligencer: Journal of U.S. Intelligence Studies, 23*(1), 59-71. Retrieved from https://www.afio.com/publications/MAJOR_and_OLESON_Espionage_Against_America_from_AFIO_INTEL_SUMMER2017_Vol23_no1.pdf

Marks, P. (2011). Dot-dash-diss: The gentleman hacker's 1903 lulz. *New Scientist*, *2844*/45, 48-49. Retrieved from http://www.newscientist.com/article/mg21228440.700-dotdashdiss-the-gentleman-hackers-1903-lulz.html?full=true

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review, 50*(4), 370-396. http://dx.doi.org/10.1037/h0054346

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, 11*(3). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1428/3028

Matusitz, J. A. (2013). *Terrorism & communication: A critical introduction*. Thousand Oaks, CA: SAGE.

Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution.* Retrieved from https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173

McBrayer, J. (2014). *Exploiting the digital frontier: Hacker typology and motivation* (Master's thesis). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 1561364)

McCormack, T. (1950). The motivation of radicals. *American Journal of Sociology, 56*(1), 17-24. https://doi.org/10.1086/220639

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation* [eBook]. Retrieved from https://ebookcentral.proquest.com.

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* [eBook]. Retrieved from https://ebookcentral.proquest.com

Mickolus, E. F. (2015). *The counterintelligence chronology: Spying by and against the United States from the 1700s through 2014* [Kindle for iPad version]. Retrieved from https://www.amazon.com/

Miklaucic, M., & Brewer, J. (2013). *Convergence: Illicit networks and national security in the age of globalization*. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/Books/convergence.pdf

Miller, G. D. (2007). Confronting terrorisms: Group motivation and successful state policies, *Terrorism and Political Violence, 19*(3), 331-350. http://dx.doi.org/10.1080/09546550701424059

Miroff, N. (2018, September 5). Hacking, cyberattacks now the biggest threat to U.S., Trump's Homeland Security chief warns. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/hacking-cyberattacks-now-the-biggest-threat-to-us-trumps-homeland-security-chief-warns/2018/09/05/d0045800-b119-11e8-a20b-5f4f84429666_story.html?noredirect=on

Mitnick, K. D., & William, L. S. (2002). *The art of deception: Controlling the human element of security* [Kindle for iPad version]. Retrieved from http://www.amazon.com

Money. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/money

Moore, D. T. (2007). *Critical thinking and intelligence analysis: Occasional paper number fourteen* (2nd printing with revisions). Retrieved from http://permanent.access.gpo.gov/lps93921/Critical-Thinking.pdf

Moreira, A., & Costa, A. P. (2016). Introduction: Qualitative analysis: Quantifying quality and qualifying quantity. *The Qualitative Report, 21*(13), 1-5. Retrieved from https://nsuworks.nova.edu/tqr/vol21/iss13/1/

Morgan, D. (1993). Qualitative content analysis: A guide to paths not taken. *Qualitative Health Research,* 3(1), 112-121. https://doi.org/10.1177/104973239300300107

National American University (NAU). (2019). Which type of IRB do I need? [Class lecture]. https://online.national.edu/d2l/le/content/58070/viewContent/2882130/View

National Commission on Terrorist Attacks upon the United States (9/11 Commission). (2004). *The 9/11 Commission report: Final report of the National Commission on terrorist attacks upon the United States*. Retrieved from http://www.9-11commission.gov/report/911Report.pdf

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016a, June). Global Terrorism Database [Data file]. Retrieved from http://www.start.umd.edu/gtd

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016b, June). Annex of statistical information: Country reports on terrorism 2015. Retrieved from https://www.start.umd.edu/publication/annex-statistical-information-country-reports-terrorism-2016

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016c, June). *Codebook: Inclusion criteria and variables*. Retrieved from https://www.start.umd.edu/gtd/

National Cybersecurity and Communications Integration Center (NCCIC). (2018, April). *Fiscal year 2017 NCCIC year in review*. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_Year_in_Review_2017_Final.pdf

National High Magnetic Field Laboratory (National MagLab). (2014, December 10). Transatlantic Telegraph Cable-1858. Retrieved from https://nationalmaglab.org/education/magnet-academy/history-of-electricity-magnetism/museum/transatlantic-telegraph-cable

National Institute of Standards and Technology (NIST). (2019, April 13). *National vulnerability database* (under CVE List Home). Retrieved from https://cve.mitre.org/cve/

National Security Act, 50 U.S.C. § 401 (1947)

Naval Postgraduate School (NPS). (2017, November 20). *Self-plagiarism/reuse in NPS theses and dissertations*. Retrieved from https://my.nps.edu/documents/105790666/106471207/Self_Plagiarism.pdf/

Nobel Media AB. (n.d.). Guglielmo Marconi facts. Retrieved from https://www.nobelprize.org/prizes/physics/1909/marconi/facts/

Nolan, F. (2014). *Espionage and espionage-related offenses under the U.S. Code* (USC). Unpublished manuscript, Henley-Putnam University, San Jose, CA.

O'Toole, G. J. A. (1988). *The encyclopedia of American intelligence and espionage: From the Revolutionary War to the present*. New York, NY: Facts on File Publications.

O'Donoghue, T. (2018). Planning your qualitative research thesis and project: An introduction to interpretivist research in education and the social sciences (2nd Ed.). [eBook]. https://doi-org.ezproxy.lib.usf.edu/10.4324/9781351165563

Office of the Director of National Intelligence (ODNI). (2009, February 12). *Annual threat assessment of the Intelligence Community for the Senate Select Committee on Intelligence: Statement for the record* (testimony of Dennis C. Blair). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/20090212_testimony.pdf

Office of the Director of National Intelligence (ODNI). (2010, February 2). *Annual threat assessment of the Intelligence Community for the Senate Select Committee on Intelligence: Statement for the record* (testimony of Dennis C. Blair). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf

Office of the Director of National Intelligence (ODNI). (2011, February 16). *Statement for the record on the worldwide threat assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence* (testimony of James R. Clapper). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/20110216_testimony_sfr.pdf

Office of the Director of National Intelligence (ODNI). (2012, January 31). *Unclassified statement for the record on the worldwide threat assessment of the US Intelligence Community for the Senate Select Committee on Intelligence* (testimony of James R. Clapper). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/20120131_testimony_ata.pdf

Office of the Director of National Intelligence (ODNI). (2013, March 12). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of James R. Clapper). Retrieved from https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

Office of the Director of National Intelligence (ODNI). (2014, January 29). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of James R. Clapper). Retrieved from https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

Office of the Director of National Intelligence (ODNI). (2015a, February 26). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of James R. Clapper). Retrieved from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Office of the Director of National Intelligence (ODNI). *Remarks as delivered by the Honorable James R. Clapper Director of National Intelligence: Opening statement to Worldwide Threat Assessment Hearing*. Senate Armed Services Committee, 114th Cong. 1 (2015b) (testimony of James R. Clapper). Retrieved from http://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf

Office of the Director of National Intelligence (ODNI). (2016, February 9). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of James R. Clapper). Retrieved from https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Office of the Director of National Intelligence (ODNI). (2017, May 11). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of Daniel R. Coats). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

Office of the Director of National Intelligence (ODNI). (2018, February 13). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of Daniel R. Coats). Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Office of the Director of National Intelligence (ODNI). (2019, January 29). *Statement for the record: Worldwide threat assessment of the US Intelligence Community; Senate Select Committee on Intelligence* (testimony of Daniel R. Coats). Retrieved from https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Oleson, P. C. (2015). Assessing Edward Snowden: Whistleblower, traitor, or spy? *The Intelligencer: Journal of U.S. Intelligence Studies, 21*(2), 15-23. Retrieved from https://www.afio.com/publications/OLESON%20Snowden%20Pages%20from%20INTEL_SUMMER2015_Vol21_No2.pdf

Onomatopoeia. (n.d.). In Merriam-Webster Online. Retrieved from https://www.merriam-webster.com/dictionary/onomatopoeia

Orth, M. (1971, October 31). For whom Ma Bell tolls not. *Los Angeles Times*. Retrieved from http://www.historyofphonephreaking.org/docs/orth1971.pdf

Özdamar, O. (2008). Theorizing terrorist behavior: Major approaches and their characteristics. *Defence Against Terrorism Review, 1*(2), 89-101. Retrieved from http://www.coedat.nato.int/publication/datr/volume2/05-Theorizing_Terrorist_Behavior_Major_ApproachesandTheir_Characteristics.pdf

PATRIOT Act of 2001, 18 USC § 2331.

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th Ed.) [Kindle for iPad edition]. Retrieved from https://www.amazon.com

Personnel and Security Research Center (PERSEREC). (2009a). *Espionage and other compromises of national security: Case summaries from 1975 to 2008* [Data file]. Retrieved from https://www.dhra.mil/PERSEREC/espionage-cases/

Personnel and Security Research Center (PERSEREC). (2009b). *Espionage and other compromises of national security: Case summaries from 1975 to 2008*. Retrieved from https://fas.org/irp/eprint/esp-summ.pdf

Personnel and Security Research Center (PERSEREC). (n.d.). History. Retrieved from https://www.dhra.mil/PERSEREC/History/

Polmar, N., & Allen, T. B. (2004). *Spy book: The encyclopedia of espionage*. New York, NY: Random House Reference.

Ponemon Institute LLC. (2018, June). *Separating the truths from the myths in cybersecurity.* Retrieved from https://www.ponemon.org/local/upload/file/BMC%20Consolidated%20Report%20Final.pdf

Post, J. M. (1998). Terrorist psycho-logic: Terrorist behavior as a product of psychological forces. In W. Reich (Ed.). *Origins of terrorism: Psychologies, ideologies, theologies, states of mind* (pp. 25-40). Washington, DC: Woodrow Wilson Center Press.

Post, J. M. (2005). When hatred is bred in the bone: Psycho-cultural foundations of contemporary terrorism, *Political Psychology, 26*(4), 615-636. http://dx.doi.org/10.1111/j.1467-9221.2005.00434.x

Post, J. M. (2007). Collective identity: Hatred bred in the bone. In George Clack (Ed.). *Countering the terrorist mentality* (pp. 12-15). Retrieved from http://photos.state.gov/libraries/amgov/30145/publications-english/EJ-terror-0507.pdf

Post, J. M. (2015). Terrorism and right-wing extremism: The changing face of terrorism and political violence in the 21st century: The virtual community of hatred. *International Journal of Group Psychotherapy, 65*(2), 242-271. https://doi.org/10.1521/ijgp.2015.65.2.242

Post, J. M., & Berko, A. (2009). Talking with terrorists. *Democracy & Security, 5*(2), 145-148. https://doi.org/10.1080/17419160903044486

Post, J. M., Sprinzak, E., & Denny, L. M. (2003). The terrorists in their own words: Interviews with 35 incarcerated Middle Eastern terrorists. *Terrorism & Political Violence, 15*(1), 171-184. https://doi.org/10.1080/09546550312331293007

Protection of Human Subjects. Title 45 USC § 46.104 (2018)

PsychCentral. (2019, May 25). About. Retrieved from https://psychcentral.com/about/

Radcliff, D. (1997, October). Hackers, terrorists, and spies. *Software Magazine, 17*(11), 36-47. Retrieved from https://dl.acm.org/citation.cfm?id=284133.284139

Rafalko, F. J. (Ed.). (2004). *A counterintelligence reader: Volume 3: Post-World War I to closing the 20th century*. Retrieved from https://fas.org/irp/ops/ci/docs/ci3/

Rankin, N. (2009). *A genius for deception: How cunning helped the British win two world wars*. Oxford, England: Oxford University Press.

Rapoport, D. C. (1984). Fear and trembling: Terrorism in three religious traditions. *The American Political Science Review, 78*(3), 658-677. http://dx.doi.org/10.2307/1961835

Rapoport, D. C. (1999). Terrorism. In L. Kurtz & J. Turpin (Eds.), *Encyclopedia of violence, peace & conflict* (Vol. 3) (pp. 497-510). San Diego, CA: Academic Press.

Rapoport, D. C. (2001). The fourth wave: September 11 in the history of terrorism. *Current History, 100*(650), 419-424. Retrieved from http://www.currenthistory.com/Article.php?ID=226

Rapoport, D. C. (2004). The four waves of modern terrorism. In A. K. Cronin & J. Ludes (Eds.), *Attacking terrorism: elements of a grand strategy* (pp. 46-73). Washington, D.C.: Georgetown University Press.

Raymond, E. (2002). *The new hacker's dictionary*. Retrieved from http://www.proselex.net/documents/the%20new%20hacker's%20dictionary.pdf

RCW39RJ. (2013, May 20). *Hackers the history of hacking – phone phreaking, Cap.Crunch, Wozniak, Mitnick* [Video file]. Retrieved from https://www.youtube.com/watch?v=FufYSx2_6Bg

Reagan, M. L. (2014, June 9). *Counterintelligence glossary: Terms & definitions of interest for CI professionals.* Retrieved from https://fas.org/irp/eprint/ci-glossary.pdf

Revenge. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/revenge

Richelson, J. (1995). *A century of spies: Intelligence in the twentieth century*. New York, NY: Oxford University Press.

Riley, M. & Robertson, J. (2015, February 5). Chinese state-sponsored hackers suspected in Anthem attack. *Bloomberg News.* Retrieved from https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack

Robinson, O. (2014). Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide. *Qualitative Research in Psychology, 11*(1), 25–41. https://doi-org.ezproxy.lib.usf.edu/10.1080/14780887.2013.801543

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study* (Doctoral dissertation, University of Manitoba, Winnipeg, Manitoba, Canada). Retrieved from ProQuest Dissertations & Theses Global. (Order No. NQ79886)

Rogers, M. K. (2005). The development of a meaningful hacker taxonomy: A two dimensional approach. *CERIAS Technical Report, 43*, 1–9. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-43.pdf

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, *3*97-102. http://dx.doi.org/10.1016/j.diin.2006.03.001

Rogers, M. K., Smoak, N. D., & Liu, J. (2006). Self-reported deviant computer behavior: A Big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior, 27*(3), 245-268. http://dx.doi.org/10.1080/01639620600605333

Romance. (n.d.). In Merriam-Webster Online. Retrieved from http://www.merriam-webster.com/dictionary/romance

Rose, A. (2006). *Washington's spies: The story of America's first spy ring*. New York, NY: Bantam Books.

Rosenbaum, R. (1971). Secrets of the little blue box. *Esquire, 76*(5-6), 116-125, 222-226. Retrieved from http://www.historyofphonephreaking.org/docs/rosenbaum1971.pdf

Rothenberg, G. (1992). Military intelligence gathering in the second half of the eighteenth century, 1740-1792. In K. Neilson, & B. J. C. McKercher,  (Eds.), (pp. 99-113). *Go* spy the land: Military intelligence in history. Westport, CT: Praeger.

Rubin, B. & Rubin, J. C. (2008). *Chronologies of modern terrorism*. Armonk, NY: M.E. Sharpe, Inc.

Ruby, C. L. (2002). The definition of terrorism. *Analyses of Social Issues & Public Policy, 2*(1) 9-14. http://dx.doi.org/10.1111/j.1530-2415.2002.00021.x

Russell, F. S. (1999). *Information gathering in classical Greece.* Ann Arbor, MI: The University of Michigan Press. Retrieved from https://www.press.umich.edu/pdf/0472110640.pdf

Rutkowski, A. M. (2010). Lessons from the first great cyberwar era. *Info, 12*(1), 5-9. http://dx.doi.org/10.1108/14636691011015330

Sageman, M. (2004). *Understanding terror networks.* Philadelphia, PA: The University of Pennsylvania Press.

Sarbin, T. R, Carney; R. M., & Eoyang, C. (Eds.). (1994). *Citizen espionage: Studies in trust and betrayal*. Westport, CT: Praeger.

Schell, B. H., & Melnychuk, J. (2011). Female and male hacker conferences attendees: Their Autism-Spectrum Quotient (AQ) scores and self-reported adulthood experiences. In B. H. Schell & T. J. Holt, (Eds.), *Corporate hacking and Technology-driven crime: Social dynamics and implications* [eBook Collection, EBSCOhost] (pp. 144-168). Retrieved from https://faculty.nps.edu/dedennin/publications/CyberConflict-EmergentSocialPhenomenon-final.pdf

Schmid, A. (2004). Terrorism—The definitional problem. *Case Western Reserve Journal of International Law, 36*(2/3), 103-147. Retrieved from https://scholarlycommons.law.case.edu/jil/vol36/iss2/8

Schmid, A. (2011). The definition of terrorism. In A. Schmid (Ed.), *Handbook of terrorism research* (pp. 86-87). London, England: Routledge.

Schmid, A., & Jongman, A. J. (1988). *Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature.* Piscataway, NJ: Transaction Books

Schmidt, M. S., & Apuzzo, M. (2015, March 3). Petraeus reaches plea deal over giving classified data to his lover. *The New York Times.* Retrieved from http://www.nytimes.com/2015/03/04/us/petraeus-plea-deal-over-giving-classified-data-to-lover.html

Schouten, R. (2010). Terrorism and the behavioral sciences. *Harvard Review of Psychiatry, 18*(6), 369-378. http://dx.doi.org/10.3109/10673229.2010.533005

Schwartz, J. M. (2007). Exploring the mind of a spy. *The Forensic Examiner, 61*(1), 67-68. Retrieved from https://lastsummerwithoscar.com/whitecollarcorruption.com/wp-content/uploads/2012/06/MindofaSpy.pdf

Schwartz, S. H. (2012). An overview of the Schwartz Theory of Basic Values. *Online Readings in Psychology and Culture, 2*(1). https://doi.org/10.9707/2307-0919.1116

Scientificamerican.com. (2001, October 19). When did the term "computer virus' arrive? *Scientific American.* Retrieved from https://www.scientificamerican.com/article/when-did-the-term-compute/

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: a menu of qualitative and quantitative options. *Political Research Quarterly, 61*(2), 294-308. https://doi.org/10.1177/1065912907313077

Seigfried-Spellar, K. C., O'Quinn, C. L., & Treadway, K. N. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour & Information Technology, 34*(5), 533-542. http://dx.doi.org/10.1080/0144929X.2014.978377

Senate Select Committee on Intelligence (SCCI). (1994, November 1). *An assessment of the Aldrich H. Ames espionage case and its implications for U.S. intelligence*. https://www.intelligence.senate.gov/sites/default/files/publications/10390.pdf

Shane, S. (2008, April 20). A spy's motivation: For love of another country. *The New York Times*. Retrieved from Retrieved from https://www.nytimes.com/2008/04/20/weekinreview/20shane.html

Shapiro, F. R. (1987). Etymology of the computer bug: History and folklore. *American Speech, 62*(4), 376-378. http://dx.doi.org/10.2307/455415

Shapiro, W., Willenson, K., & Monroe, S. (1986, January 6). A fitting end to “The year of the spy.” *Newsweek Magazine, 107*(1), 23.

Shaw, E., Ruby, K. G., & Post, J. M. (1998). The insider threat to information systems: The psychology of the dangerous insider [Reprint]. *Security Awareness Bulletin, 2-98.* Retrieved from https://homes.cerias.purdue.edu/~mkr/sab.pdf

Sheldon, M. R. (1997). The ancient imperative: Clandestine operations and covert action. *Journal of Intelligence and Counterintelligence, 10*(3), 299-315. http://dx.doi.org/10.1080/08850609708435352

Smith, M. J. (2006). Realism. In V. Jupp (Ed.), *The Sage dictionary of social research methods* (pp. 376-380). Retrieved from https://ebookcentral.proquest.com.

Stake, R. E. (1978). The case study method in social inquiry. *Educational Researcher, 7*(2), 5-8. https://doi.org/10.3102/0013189X007002005

Stilwell, R. G. (1985). *Keeping the nation’s secrets: A report to the Secretary of Defense by the Commission to review DOD Security Policy and Practices*. Retrieved from https://fas.org/sgp/library/stilwell.html

Stone, G. R. (2003). Judge Learned Hand and the Espionage Act of 1917: A mystery unraveled. *University of Chicago Law School Review, 70*(1), 335-358. Retrieved from http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2969&context=journal_articles

Stone, L. A. (1989). On the psychological makeup of a spy. *Forensic Reports, 2*(3), 215-221. Retrieved from https://psycnet.apa.org/record/1990-20001-001

Strauss, A. (1947). Research in the collective behavior: Neglect and need. *American Sociological Review, 12*(3), 352-354. Retrieved from http://ezproxy.lib.usf.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=12772690&site=eds-live

Strozier, C. B. (2008). The global war on terror, sliced four ways. *World Policy Journal, 24*(4), 90-98. http://dx.doi.org/10.1162/wopj.2008.24.4.90

Sulick, M. J. (2012). *Spying in America: Espionage from the Revolutionary War to the dawn of the Cold War*. Retrieved from http://www.eblib.com

Sulick, M. J. (2013). *American Spies: Espionage against the United States from the Cold War to the present*. Washington, DC: Georgetown University Press Retrieved from http://muse.jhu.edu/books/9781626160095

Sulick, M. J. (2015). Intelligence in the Cold War. *The Intelligencer, Journal of U.S. Intelligence Studies, 21*(1). Retrieved from https://www.afio.com/publications/SULICK_Michael_Guide_to_Intelligence_in_the_Cold_War_from_INTEL_WINTER2014-15_Vol21_No1.pdf

Sun, B. (2003, September 4). Why are espionage convictions so rare? PBS Frontline (Interview from episode From China with Love). Retrieved from https://www.pbs.org/wgbh/pages/frontline/shows/spy/interviews/sun.html

Swann, W. B, Jetten, J., Gómez, Á., Whitehouse, H., & Bastian, B. (2012). When group membership gets personal: A theory of identity fusion. *Psychological Review, 119*(3), 441-456. http://dx.doi.org/10.1037/a0028589

Taniguchi, T. H. (2014). Understanding and the interpretive approach in international relations. *International Journal of Science in Society, 5*(2), 53-64. http://dx.doi.org/10.18848/1836-6236/CGP/v05i02/51423

Taylor, M. (1988). *The terrorist.* London, UK: Brassey's Defence Publishers Ltd.

Taylor, M. (2010). Is terrorism a group phenomenon? *Aggression and Violent Behavior, 15*(2), 121–129. http://dx.doi.org/10.1016/j.avb.2009.09.001

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London, England: Routledge.

Terror. (n.d.). In Merriam-Webster Online. Retrieved from https://www.merriam-webster.com/dictionary/terror

Thomas, G. (2011). A typology for the case study in social science following a review of definition, discourse, and structure. *Qualitative Inquiry, 17*(6) 511–521. https://doi.org/10.1177/1077800411409884

Thompson, T. J. (2013). Toward and updated understanding of espionage motivation. *International Journal of Intelligence and CounterIntelligence, 27*(1) 58-72. http://dx.doi.org/10.1080/08850607.2014.842805

Thompson, T. J. (2018). A psycho-social motivational theory of mass leaking. International *Journal of Intelligence & Counterintelligence, 31*(1), 116-125. http://dx.doi.org/10.1080/08850607.2017.1374800

Thycotic. (2014). *Thycotic black hat 2014 hacker survey executive report.* Retrieved from https://thycotic.com/wp-content/uploads/2014/03/Executive-summary-blackhat-survey-data-2014_PDF.pdf

Tilly, C. (2004). Terror, terrorism, terrorists. *Sociological Theory*, *22*(1), 5-13. http://dx.doi.org/10.1111/j.1467-9558.2004.00200.x

Totty, M. (2011, September 26). The first virus...and other not-so-great moments in the history of computer mischief. *Wall Street Journal (Online)*. Retrieved from https://search.proquest.com/docview/893950257?accountid=14745

Turgeman-Goldschmidt, O. (2005). Hackers' Accounts: Hacking as a Social Entertainment. *Social Science Computer Review*, *23*(1), 8-23. http://dx.doi.org/10.1177/0894439304271529

Tzu, S. (1910). *The art of war* (L. Giles, Trans). Retrieved from http://www.artofwarsuntzu.com/Art%20of%20War%20PDF.pdf

U.S. Const. art. III, § 3.

Uniform Code of Military Justice (UCMJ, 64 Stat. 109, 10 U.S.C. Chapter 47)

United States Department of Defense (DOD). (2010/2016). Dictionary of military and associated terms (as amended through 15 February 2016). Retrieved from https://fas.org/irp/doddir/dod/jp1_02.pdf

United States Department of Defense (DOD). (2019). *Dictionary of military and associated terms* (as of February 2019). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

United States Department of Health and Human Services (DHHS). (2016, March 16). *Belmont report: Ethical principles and guidelines for the protection of human subjects of research.* Retrieved from https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

United States Department of Health and Human Services (DHHS). (n.d.). Self plagiarism. Retrieved from https://ori.hhs.gov/plagiarism-13

United States Department of Homeland Security (DHS). (2009a, January 26). *Leftwing extremists likely to increase use of cyber attacks over the coming decade* (Report No. IA-0141-09). Retrieved from https://fas.org/irp/eprint/leftwing.pdf

United States Department of Homeland Security (DHS). (2009b, April 7). *Rightwing extremism: Current economic and political climate fueling resurgence in radicalization and recruitment* (Report No. IA-0257-09). Retrieved from https://fas.org/irp/eprint/rightwing.pdf

United States Department of Homeland Security (DHS). (2018, November 28). Explore Terms: A Glossary of Common Cybersecurity Terminology. Retrieved from https://niccs.us-cert.gov/about-niccs/glossary#H

United States Department of Justice (DOJ). (2016, September 23). ISIL-linked Kosovo hacker sentenced to 20 years in prison [Press release]. Retrieved from https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison

United States Department of Justice (DOJ). (2019, March 15). *Former defense intelligence officer pleads guilty to attempted espionage* [Press release]. Retrieved from https://www.justice.gov/opa/pr/former-defense-intelligence-officer-pleads-guilty-attempted-espionage

United States Department of Justice (DOJ). (n.d.). *Criminal resource manual 2001-2099.* Retrieved from https://www.justice.gov/jm/criminal-resource-manual-2057-synopses-key-national-defense-and-national-security-provisions

United States v. Ardit Ferizi (a/k/a “Th3Dir3torY”), no. 1:16-cr-042 Document 54 (E.D. Virg. September. 23, 2016).

United States v. Assange, no. 1:18:CR (E.D. Virg. March 6, 2018). Retrieved from https://www.justice.gov/usao-edva/press-release/file/1153481/download

United States v. Assange, no. 1:18:CR-00111-CMH (E.D. Virg. May 23, 2019). Retrieved from https://www.justice.gov/opa/press-release/file/1165556/download

United States v. Hansen, no. 2:18-mj-00324-PMW (D. Utah June 2, 2018).

United States v. Henry, no. 8:19-mj-01151-CBD (D. Maryland April 8, 2019).

United States v. Liew, et al, no. 3-11-cr-00573 (N.D. Cal. July 21, 2014)

United States v. Liew, et al, no. 3-11-cr-00573 (N.D. Cal. September 29, 2015)

United States v. Manning, no. 20120514 (A. Ct. Crim. App. July 30, 2013)

United States v. Petraeus, no. 3-15-cr-00047 (N.D. N. Car. March 3, 2015).

United States v. Snowden, no. 1-13-cr-265 (E.D. Virg. June 14, 2013).

United States v. Sterling, no. 1-10-cr-00485 (E.D. Virg. January 27, 2015).

United States v. Witt et al., no. 1:19-cr-00043-BAH (D. Columbia February 8, 2019). Retrieved from https://www.justice.gov/opa/press-release/file/1131726/download

United States. Congress. House. Committee on Un-American Activities. (1949, August 15). *100 things you should know about Communism in the U.S.A.* (2nd printing). Retrieved from https://archive.org/details/100thingsyoushou1949unit

Victoroff, J. (2005). The mind of the terrorist: A review and critique of psychological approaches. *Journal of Conflict Resolution, 49*(1), 3-42. http://dx.doi.org/10.1177/0022002704272040

Volz, D. (2016, February 8). National Security Agency merging offensive, defensive hacking operations. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-cyber-nsa-idUSKCN0VH21H

Volz, D., & Hosenball, M. (2016, May 18). Hackers target presidential campaigns: U.S. spy chief. *Reuters.* Retrieved from http://www.reuters.com/article/us-usa-election-hackers-idUSKCN0Y929G

Wade, C., Aldridge, J., Hopper, L., Drummond, H., Hopper, R., & Andrew, K. (2011). Hacking into the hacker: Separating fact from fiction. In T. Holt (Ed.), *Crime on-line: Correlates, causes, and context* (pp. 29-55). Durham, NC: Carolina Academic Press.

Watson, J. B. (1913). Psychology as the behaviorist views it. *Psychological Review, 20*(2), 158-177. http://dx.doi.org/10.1037/h0074428

Weatherston, D. & Moran, J. (2003). Terrorism and mental illness: Is there a relationship? *International Journal of Offender Therapy and Comparative Criminology, 47*(6), 698-713. http://dx.doi.org/10.1177/0306624X03257244

Weinberg, L. & Eubank, W. (2010). *An end to the fourth wave of terrorism? Studies in Conflict & Terrorism, 33*(7), 594-602. http://dx.doi.org/10.1080/1057610X.2010.483757

Weiner, R. (2019, April 4). Chelsea Manning pushes for release from jail, with support of Alexandria Ocasio-Cortez. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/legal-issues/chelsea-manning-pushes-for-release-from-jail-with-support-of-alexandria-ocasio-cortez/2019/04/02/6687625c-557c-11e9-8ef3-fbd41a2ce4d5_story.html?noredirect=on&utm_term=.45f34ecd276f

Weiner, T. (1994, July 31). Why I spied: Aldrich Ames. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/1994/07/31/magazine/why-i-spied-aldrich-ames.html

Wheeler, D. L. (2013). Intelligence between the World Wars, 1919-1939. *The Intelligencer Journal of U.S. Intelligence Studies*, *20*(1). Retrieved from https://www.afio.com/publications/WHEELER%20Douglas%20Intelligence%20Between%20the%20War%201919%201939%20from%20AFIO%20INTEL_SPRGSUM2013_Vol20_No1_FINAL.pdf

Wikström, P. (2010). Situational action theory. In F. T. Cullen & P. Wilcox (Eds.), *Encyclopedia of criminological theory* (Vol. 2, pp. 1001-1008). Thousand Oaks, CA: SAGE Publications Ltd. http://dx.doi.org/10.4135/9781412959193.n277

Wikström, P. (2014). Why crime happens: A situational action theory. In G. Manzo (Ed.), *Analytical Sociology*. John Wiley & Sons, Ltd, Chichester, United Kingdom. http://dx.doi.org/10.1002/9781118762707.ch03

Wilshusen, G. C. (2018, December). *Information security: Agencies need to improve implementation of federal approach to security systems and protecting against intrusions* (GAO-19-105). Retrieved from http://www.gao.gov/products/GAO-15-758T

Wilson, L. (2012). Reversal theory: Understanding the motivational styles of espionage. *International Journal of Intelligence Ethics, 3*(1), 76-100. Retrieved from http://journals.fcla.edu/ijie/article/view/83450/wilson

Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision*. Stanford, CA: Stanford University Press.

World Economic Forum. (2018). *The global risks report 2018, 13th edition* (Report no. 09012018). Retrieved from http://wef.ch/risks2018

Xenophon. (1925/1945). Scripta minora. (E. C. Marchant, Trans.). In T. E. Page, E. Capps, W. H. D. Rouse, L. A. Post, & E. H. Warmington (Eds.). *The Loeb Classical Library: Xenophon, Scripta minora* (pp. 233-294). DOI:10.4159/DLCL.xenophon_athens-cavalry_commander.1925

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4), 64-74. http://dx.doi.org/10.1145/2436256.2436272

Yagoda, B. (2014, March 6). A short history of "hack." *The New Yorker*. Retrieved from https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack

Yin, R. K. (2012). A*pplications of case study research* (3rd ed.) [PDF version]. Retrieved from https://www.sagepub.com/sites/default/files/upm-binaries/41407_1.pdf

Yin, R. K. (2014). *Case study research: Design and methods*. Los Angeles, CA: Sage.

Yin, R. K., & Heald, K. A. (1975). Using the case survey method to analyze policy studies. *Administrative Science Quarterly, 20*(3), 371-381. http://dx.doi.org/10.2307/2391997

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281-287. http://dx.doi.org/10.1080/10580530701585823

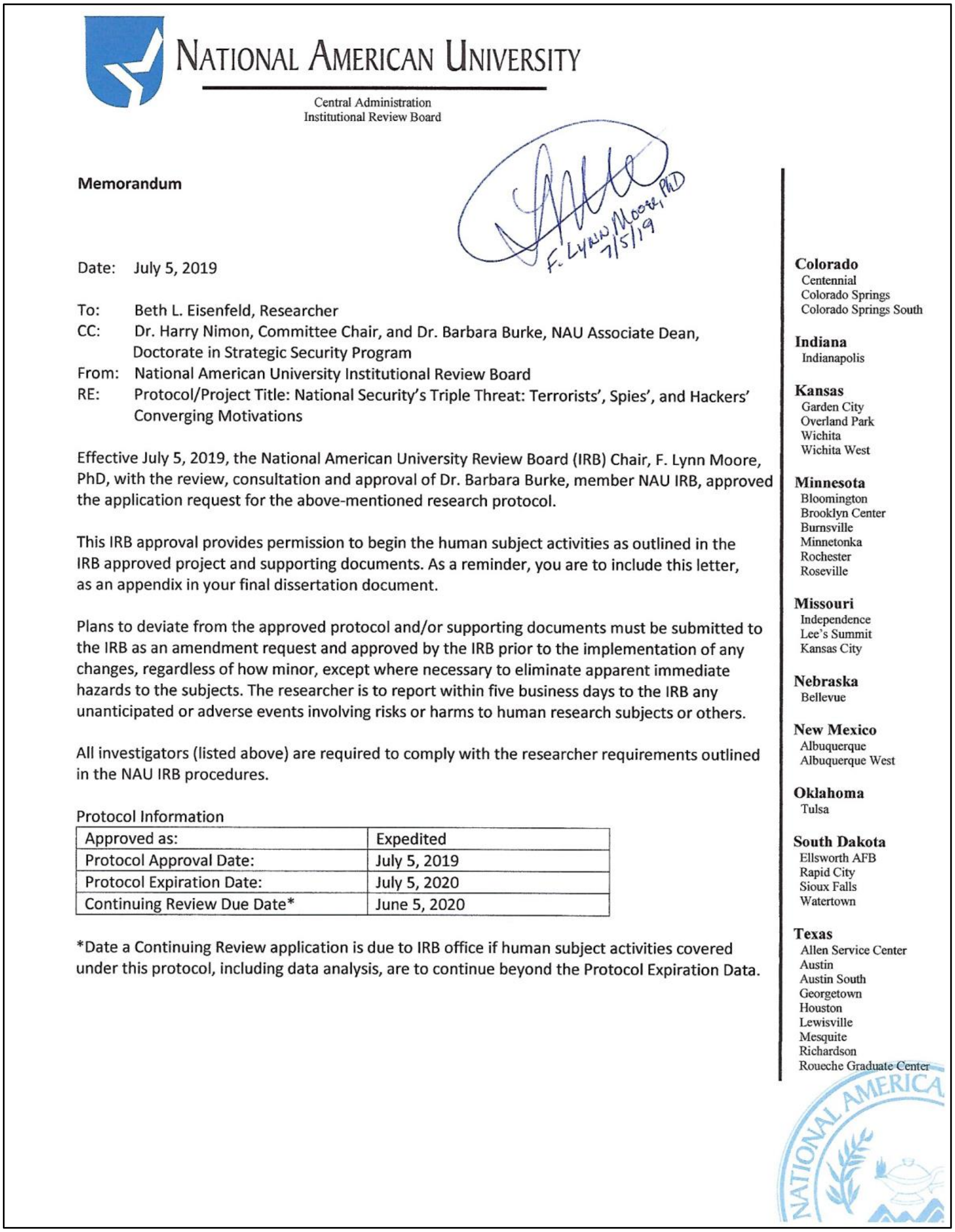
Zapotosky, M. & Barrett, D. (2018, November 15). Julian Assange has been charged, prosecutors reveal inadvertently in court filing. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/julian-assange-has-been-charged-prosecutors-reveal-in-inadvertent-court-filing/2018/11/15/9902e6ba-98bd-48df-b447-3e2a4638f05a_story.html?utm_term=.b755bb9f8abd

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers, 17*(6), 1239–1251. http://dx.doi.org/10.1007/s10796-015-9567-0

Zuckerman, M. J. (2001, March 29). Hacker reminds some of Asperger syndrome. *USA Today*. Retrieved from http://usatoday30.usatoday.com/news/health/2001-03-29-asperger.htm

# Appendices

## Appendix A: National American University IRB Approval



NATIONAL AMERICAN UNIVERSITY

Central Administration
Institutional Review Board

**Memorandum**

F. Lynn Moore, PhD
7/5/19

Date: July 5, 2019

To: Beth L. Eisenfeld, Researcher
CC: Dr. Harry Nimon, Committee Chair, and Dr. Barbara Burke, NAU Associate Dean, Doctorate in Strategic Security Program
From: National American University Institutional Review Board
RE: Protocol/Project Title: National Security's Triple Threat: Terrorists', Spies', and Hackers' Converging Motivations

Effective July 5, 2019, the National American University Review Board (IRB) Chair, F. Lynn Moore, PhD, with the review, consultation and approval of Dr. Barbara Burke, member NAU IRB, approved the application request for the above-mentioned research protocol.

This IRB approval provides permission to begin the human subject activities as outlined in the IRB approved project and supporting documents. As a reminder, you are to include this letter, as an appendix in your final dissertation document.

Plans to deviate from the approved protocol and/or supporting documents must be submitted to the IRB as an amendment request and approved by the IRB prior to the implementation of any changes, regardless of how minor, except where necessary to eliminate apparent immediate hazards to the subjects. The researcher is to report within five business days to the IRB any unanticipated or adverse events involving risks or harms to human research subjects or others.

All investigators (listed above) are required to comply with the researcher requirements outlined in the NAU IRB procedures.

Protocol Information

| | |
|---|---|
| Approved as: | Expedited |
| Protocol Approval Date: | July 5, 2019 |
| Protocol Expiration Date: | July 5, 2020 |
| Continuing Review Due Date* | June 5, 2020 |

*Date a Continuing Review application is due to IRB office if human subject activities covered under this protocol, including data analysis, are to continue beyond the Protocol Expiration Data.

**Colorado**
Centennial
Colorado Springs
Colorado Springs South

**Indiana**
Indianapolis

**Kansas**
Garden City
Overland Park
Wichita
Wichita West

**Minnesota**
Bloomington
Brooklyn Center
Burnsville
Minnetonka
Rochester
Roseville

**Missouri**
Independence
Lee's Summit
Kansas City

**Nebraska**
Bellevue

**New Mexico**
Albuquerque
Albuquerque West

**Oklahoma**
Tulsa

**South Dakota**
Ellsworth AFB
Rapid City
Sioux Falls
Watertown

**Texas**
Allen Service Center
Austin
Austin South
Georgetown
Houston
Lewisville
Mesquite
Richardson
Roueche Graduate Center

NATIONAL AMERICA

## Appendix B: Confidentiality Statement

### NATIONAL AMERICAN UNIVERSITY
### Confidentiality Statement

Student Name: **Beth L. Eisenfeld**

Research Study Title: **National Security's Triple Threat: Terrorists', Spies', and Hackers' Converging Motivations**

I, the undersigned student, am the primary researcher working on the above-named research study at National American University. I understand that I must maintain the confidentiality of all information concerning all research participants as required by law. Only the National American University Institutional Review Board(s) may have access to this information.

Confidential information includes but is not limited to names, characteristics, identifying information, questionnaires, ratings, scores, comments, and other information. To maintain the confidentiality of the information, I agree to refrain from discussing or disclosing any confidential information regarding research participants to any individual who is not part of the above research study or in need of the information for the expressed purposes on the research program. This includes discussing any confidential information in a way that would provide an unauthorized person means to associate (either correctly or incorrectly) an identity with such information.

I will store research records, in any media, securely and with all necessary safeguards. If I use the services of a third party to assist in the research study, which will potentially give the third party access to confidential information of participants, I will enter into an agreement with such third party prior to using any of the services. I will immediately report any known or suspected breach of this confidentiality statement regarding the above research project to the National American University Institutional Review Board.

Beth L. Eisenfeld ______________________ 6/6/2019 ______________________
Researcher Signature Date

Beth L. Eisenfeld ______________________
Printed Name

______________________ ______________________
Witness Signature Date

______________________
Printed Name

## Appendix C: Invitation to Participate

Date: July 6, 2019

Dear [Potential Participant],

My name is Beth L. Eisenfeld. I am a Doctoral student at National American University. Dr. Harry Nimon is my dissertation chairman. I invite you to participate in my research based on your expertise. My dissertation is tentatively titled National Security's Triple Threat: Terrorists', Spies', and Hackers' Converging Motivations.

I am studying the motivations of terrorists, spies, and hackers. In an earlier phase of my research, I reviewed cases studies of terrorists, spies, and hackers seeking to understand the motivations of each actor. I developed a motivational topology and identified 12 themes and 37 sub-themes. For the next phase of research, I would like your feedback on the topology. In particular, I am interested in your perception of the motivations for the actors under study. I want to stress that I am only interested in feedback on the motivations and the topology and no other facet of your work.

I am inviting you to participate in a one-hour phone interview. During the interview, you are not required to answer any questions you do not want to answer. If at any time you do not want to continue with the interview, you may decline. The entire interview will take approximately one hour. In preparation for the interview, I will send you definitions and the motivation topology for review. Those items will be the topic of our discussion during the interview.

The interview will be tape-recorded and I will take notes in preparation for data analysis. I will transcribe the tape and remove all personally identifying information as I create the paper copy of the transcript. Once transcribed, I will destroy the recording and the electronic transcription. Participant identity and confidentiality will be concealed using coding procedures; only a paper copy of the transcript will survive locked in my office.

Excerpts from the interview may be included in the final dissertation report or other later publications. However, under no circumstances will your name or identifying characteristics appear in these writings.

If you agree to assist, please sign, date this letter in the spaces below, and return it to me. I will contact you to set up a mutually agreeable time to call you for the phone interview. Remember, your participation is voluntary and there is no payment for participating. Thank you in advance for agreeing to assist.

Sincerely,
Beth L. Eisenfeld

I, ___________________________________________, have read the above invitation to participate in research and understand the terms and conditions of participations. My signature below confirms my participation.
____________________________________________Signed or electronically signed
____________________________________________Printed Name
Please return the signed page by email to me at beisenfeld@national.edu. If you have problems with the electronic signature or any questions with the contents of this invitation, please call me at 813-258-4673.

## Appendix D: Informed Consent

### NATIONAL AMERICAN UNIVERSITY
### Confidentiality Statement

---

Name of NAU Student/Researcher: **Beth L. Eisenfeld**
Degree Sought: **Doctor of Strategic Security**
Title of Research Project/Study: **National Security's Triple Threat: Terrorists', Spies', and Hackers' Converging Motivations**
Purpose of Research: **The purpose of this qualitative study using case studies and interviews is to explore the motivations of terrorists, spies, and hackers.**

Your participation in the above-named researcher's project is appreciated and will consist of an hour-long interview where the researcher will ask questions about the motivations of terrorists, spies, and hackers. You can choose whether to participate, and you may withdraw from the study at any time with no penalty. The researcher may terminate any interview to protect participants from harm or distress, and may exclude portions of your interview that deviate from study objectives. If you would like to talk to professionals for any reason, you may contact PsychCentral (PsychCentral.com) at any time. The results of the research study may be published but your identity will remain confidential and your name will not be made known to any outside party.

With this research, there are no foreseeable risks to you; however if for any reason you have questions about the research study or your rights as a participant, please contact the researcher at 813-258-4673 or via email at beisenfeld@national.edu. If you have any concerns or complaints, please contact the National American University Institutional Review Board via email at IRB@national.edu or Protocol Director, Dr. Barbara Burke bburke@national.edu.

As a participant in this study, you understand and agree to the following:

1. You may choose not to be part of this study and you may withdraw from the study at any time.
2. Your identity is confidential.
3. You must give permission for the researcher to record the interviews. You understand that the information from the recorded interviews will be transcribed. The researcher will develop a way to code the data to assure that your name is protected.
4. Data will be kept in a secure and locked area. The data will be kept for three years and then destroyed.
5. The results of this study may be published.
6. The researcher has fully explained the nature of the research study and has answered all questions and concerns about the research study.

By checking "I accept the above terms" below and signing this form below, you agree that you understand the nature of the study, the possible risks to you as a participant, and the extent to which your identity will be kept confidential. You confirm that you are at least 18 years of age and that you are willing to volunteer as a participant in the study described above.

**CHECK ONE:** [__] I accept the above terms.     [__] I do not accept the above terms.

Participant Signature: ________________________________ Date: __________________

Print Name: ________________________________________

Researcher Signature ________________________________ Date: __________________

Print Name: ________________________________________

## Appendix E: Case Study Data

| | |
|---|---|
| **Random** | 0.058812 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Army of God |
| **Arrest/Event Date** | 1989 |
| **Event Overview** | 9/6/1989: Perpetrators claiming to be members of the Army of God set fire to the front door of the building housing the Allegheny Reproductive Health Center in Pittsburgh, Pennsylvania, United States. There were no casualties, but the building sustained $10,000 in damages. |
| **Triggering Event** | |
| **Motive 1** | To protest the practice of abortion and to sabotage abortion facilities operating in Pennsylvania. |
| **Motive 2** | Anti-abortion; Extremist right-wing |
| **Motive 3** | Religious |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Abortion Related |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | An unidentified woman called to television stations after the incident claiming that the Army of God perpetrated the attack. The abortion clinic had previously been the target of many protests. |
| **Initial Locating Source** | GTD; Anti-Abortion Project 2010 |
| **Evidence 1** | Sheila Mullan, "'Army of God' Says It Set Abortion Clinic Fires," United Press International, September 6, 1989. |
| **Evidence 2** | "Clinic's New Home Burns," Associated Press, September 7, 1989. |
| **Evidence 3** | http://infoweb.newsbank.com/resources/doc/nb/news/0EB76115F8D43D76?p=AWNB "Fire Caused $3,000 to $5,000 damage: Abortion Clinic Fire," Orlando Sentinel, September 7, 1989. |

| | |
|---|---|
| **Random** | 0.046377 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Aryan Liberation Front |
| **Arrest Date** | 1993 |
| **Event Overview** | 10/5/1993: Richard Joseph Campos, the sole member of the Aryan Liberation Front, threw a Molotov cocktail into the Sacramento, California, United States home of Asian American city council member Jimmie Yee. The firebomb landed in an unoccupied bedroom. No casualties but bedroom damaged. |
| **Triggering Event** | |
| **Motive 1** | Richard Joseph Campos adopted the racist ideology of the White Aryan Resistance (WAR) and wanted to create an all-White society. |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Private Citizens & Property |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Richard Joseph Campos bombed four other buildings in the Sacramento area including the NAACP headquarters, a synagogue, the Japanese American Citizens League, and the state Office of Fair Employment and Housing building. Campos claimed responsibility by calling the Sacramento TV station |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/news/0EB4F55F5474CDA8?p=AWNB<br>Ann Bancroft, "Councilman's Home Attacked In Sacramento," San Francisco Chronicle, October 6, 1993. |
| **Evidence 2** | "Man Convicted Of 2 Bombings Tied to Racism," New York Times, August 31, 1994. |
| **Evidence 3** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/news/0FC29140CDDC52D5?p=AWNB<br>Mareva Brown, "Racist's Rampage Was 'Wake-Up Call.' The White Supremacist Convicted in '93 Bombings is Out of Prison," Sacramento Bee, July 7, 2003. |

| | |
|---|---|
| **Random** | 0.005601 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Aryan Nation |
| **Arrest/Event Date** | 1987 |
| **Event Overview** | 04/19/1987: A bomb explosion destroyed a 1984 unmarked, unoccupied police car, parked outside Missoula City Hall in Missoula, Montana. The blast also shattered windows in City Hall and other nearby buildings, but no injuries resulted from the incident. About five minutes after the explosion, a male caller, claiming to be a member of the Aryan Nation white supremacist group, phoned an emergency number and claimed responsibility for the incident, stating that the group was tired of harassment from law enforcement agencies. |
| **Triggering Event** | |
| **Motive 1** | Tired of being harassed by law enforcement agencies |
| **Motive 2** | Social - racism/racial tension |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Police |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Three phone calls made to emergency numbers, all from the same male caller stating he was a member of the Aryan Nation and claiming responsibility for the bombing on behalf of the group. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | https://news.google.com/newspapers?nid=1314&dat=19870420&id=MVpWAAAAIBAJ&sjid=fu8DAAAAIBAJ&pg=3836,2039999&hl=en "Bomb Destroys Police Car," The Associated Press, April 19, 1987. |
| **Evidence 2** | https://news.google.com/newspapers?nid=1345&dat=19870420&id=II5OAAAAIBAJ&sjid=yfoDAAAAIBAJ&pg=5095,752147&hl=en "Team hunts bomb clues in Missoula," Spokane Chronicle, Washington, April 20,1987. |
| **Evidence 3** | https://news.google.com/newspapers?nid=1314&dat=19870420&id=MVpWAAAAIBAJ&sjid=fu8DAAAAIBAJ&pg=5222,2018631&hl=en "Bomb rips police car in Missoula," The Spokesman-Review, Spokane, Washington, April 20, 1987. |

| | |
|---|---|
| **Random** | 0.040395 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Boricua Revolutionary Front |
| **Arrest Date** | 12/10/1992: |
| **Event Overview** | Three members of the Boricua Revolutionary Front placed two explosive devices at a USMC Recruiting Office in Chicago, Illinois, United States. One pipe bomb located in the doorway of the office failed to explode and another bomb underneath a military vehicle at the facility failed to detonate but did ignite on fire. There were no casualties but the military vehicle damaged. |
| **Triggering Event** | To promote Puerto Rican Independence from the United States; To call for the release of Puerto Rican political prisoners from United States jails |
| **Motive 1** | Nationalist - Separatist |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Military |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Two communiqués by the Boricua Revolutionary Front left at the scene, a communiqué sent to Chicago's Puerto Rican Cultural Center, and the next day Solis anonymously called UPI claiming the incident on behalf of the BRF. Incident purposely scheduled to coincide with International Human Rights Day. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | "Terrorism in the United States 1982-1992," Terrorist Research and Analytical Center, Counterterrorism Section Intelligence Division, FBI, 1992. |
| **Evidence 2** | http://openjurist.org/223/f3d/676/united-states-of-america-v-jose-solis-jordan "223 F3d 676 United States of America v. Jose Solis Jordan," United States Court of Appeals For the Seventh Circuit, August 17, 2000. |
| **Evidence 3** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/news/0EB373E8349D9AF8?p=AWNB Phillip J. O'Connor, "2 Bombs Planted At Marine Office," Chicago Sun-Times, December 11, 1992. |

| | |
|---|---|
| **Random** | 0.010203 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Chicano Liberation Front/Army |
| **Arrest Date** | 1971 |
| **Event Overview** | 7/6/1971: The Chicano Liberation Front threw a firebomb into Montebello High School in Montebello, California, United States. There were no casualties; one classroom destroyed, other classrooms damaged. |
| **Triggering Event** | To protest the treatment of Mexican-Americans |
| **Motive 1** | Social - protesting treatment |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Educational Institution |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | The firebombing occurred at 12:19 AM. Minutes after the fire broke out, a spokesperson for the Chicano Liberation Front called the Los Angeles Times claiming responsibility the attack. The Chicano Liberation Army also claimed credit for the incident in a tape recording sent to the Los Angeles Free Press. The CLF stated that they were "fed up with our people being treated like dogs." |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | "Montebello High Hit by Firebomb," Los Angeles Times, July 6, 1971. |
| **Evidence 2** | Paul Houston and Franz Rodriguez, "Chicano Militants Reportedly Claim 28 Bombings in L.A.," Los Angeles Times, August 14, 1971. |
| **Evidence 3** | Did not find a third source. |

| | |
|---|---|
| **Random** | 0.106803 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Christian Liberation Army |
| **Arrest/Event Date** | 1991 |
| **Event Overview** | 2/14/1991: Members of the Christian Liberation Army threw two firebombs into the Central Ohio Women's Clinic housed in a building owned by the Planned Parenthood of Central Ohio in Columbus, Ohio, United States. There were no casualties, but the abortion clinic sustained $75,000 in damages. |
| **Triggering Event** | To protest the practice of abortion and to sabotage abortion facilities operating in Ohio. |
| **Motive 1** | Pro Life/anti-abortion |
| **Motive 2** | Religious |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Abortion Related |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Nine days after this incident, a firebomb thrown through another abortion clinic in Columbus, Ohio. The Christian Liberation Army claimed both attacks in a letter sent to another abortion clinic. |
| **Initial Locating Source** | GTD; Anti-Abortion Project 2010 |
| **Evidence 1** | http://www.nytimes.com/1991/02/17/us/firebomb-in-columbus-ohio-damages-an-abortion-clinic.html<br>"Firebomb in Columbus, Ohio, Damages an Abortion Clinic," New York Times, February 17, 1991. |
| **Evidence 2** | "Clinic Damaged by Firebomb," The Bryan Times, February 25, 1991. |
| **Evidence 3** | "Second Columbus, Ohio, Abortion Clinic Firebombed Within Two Weeks," Associated Press, February 25, 1991. |

| | |
|---|---|
| **Random** | 0.061332 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Coalition to Save the Preserves (CSP) |
| **Arrest/Event Date** | 2001 |
| **Event Overview** | 06/12/2001: Members of the group Coalition to Save the Preserves (CSP) are suspected in the $2 million arson of four luxury homes being constructed in upscale Pima Canyon Estates outside of Tucson, AZ. |
| **Triggering Event** | |
| **Motive 1** | The specific motive is unknown. Ecoterrorism |
| **Motive 2** | Terrorism and the Lone Wolf, Environmental Terrorist Groups |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Business |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Letters sent to media, homeowners and contractors, and messages on construction sites of several of the arsons claimed responsibility in the name of CSP, stating, "God's work had to be done." |
| **Initial Locating Source** | GTD; Eco Project 2010 |
| **Evidence 1** | https://news.google.com/newspapers?nid=894&dat=20020612&id=WiALAAAAIBAJ&sjid=yFIDAAAAIBAJ&pg=6539,1533941&hl=en<br>"Trail cold in Catalina Foothills arsons," Associated Press State & Local Wire, June 12, 2002. |
| **Evidence 2** | "Ignition device found in one of four Tucson arsons," Associated Press State & Local Wire, June 17, 2001. |
| **Evidence 3** | Ecoterrorism: Radical Group Linked to Arizona Fires," Greenwire, June 13, 2001. |
| **Evidence 4** | http://tucsoncitizen.com/morgue2/2001/06/16/24177-ignition-device-is-clue-in-4-home-fires/<br>"Ignition device is clue in 4 home fires" Tucson Citizen, Jun 16, 2001 |

| | |
|---|---|
| **Random** | 0.101961 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Earth First! |
| **Arrest/Event Date** | 1994 |
| **Event Overview** | 07/31/1994: Earth First! Members claimed responsibility for setting arson to logging equipment at Dave Littlejohn Logging Company near Olympia, Washington in the United States. The arson caused damage to a log skidder, a bulldozer and two fire prevention trucks. There were no casualties in the incident. This incident was one in a series of two; the first arson occurred four days earlier at the same logging company, damaging more equipment. Nine days later, both incidents were claimed in a phone call to the contract logging association |
| **Triggering Event** | "To protect planet Earth from loggers" |
| **Motive 1** | Disaffected environmentalists; ecoterrorism |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Business |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | This incident was one of two arsons at the Dave Littlejohn Logging Company, which were 4 days apart, and both claimed by Earth First! |
| **Initial Locating Source** | GTD; Eco Project 2010 |
| **Evidence 1** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/news/0F0FBF44DD10704E?p=AWNB<br>Rob Tucker, "The In Basket: Loggers worry 'monkey wrenchers' could be headed this way," The News Tribune, September 9, 1994. |
| **Evidence 2** | James L. Outman and Elisabeth M. Outman, "Terrorism Almanac," The Gale Group, Inc., 2003. (Book at the HCPLC). |
| **Evidence 3** | Did not find a third source. |

| | |
|---|---|
| **Random** | 0.065965 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Jewish Armed Resistance |
| **Arrest/Event Date** | 1972 |
| **Event Overview** | 3/11/1972: The Jewish Armed Resistance Assault Team claimed credit for firebombing the home of Robert Ambrose in Queens, New York, United States. Bomb intended for the home of Anna Harmione Ryan, a suspected Nazi. No casualties; house sustained slight damages. |
| **Triggering Event** | |
| **Motive 1** | Revenge |
| **Motive 2** | Religious/anti-Semitism; To intimidate a suspected Nazi. |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Private Citizens & Property |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | The Jewish Resistance Assault Team is likely an offshoot of the Jewish Defense League and/or the Jewish Armed Resistance. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | http://www.nytimes.com/1972/03/12/archives/fire-bombers-said-to-pick-wrong-home.html?_r=0<br>"Fire Bombers Said To Pick Wrong Home," New York Times, March 12, 1972. |
| **Evidence 2** | Christopher Hewitt, "Political Violence and Terrorism in Modern America: A Chronology," Praeger Security International, 2005. |
| **Evidence 3** | Did not find a third source. |

| | |
|---|---|
| **Random** | 0.184623 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Jewish Defense League (JDL) |
| **Arrest/Event Date** | 1985 |
| **Event Overview** | 09/06/1985: A bomb exploded at the home of Elmars Sprogis in Brentwood, New York, United States, a residential community in Suffolk County, about 40 miles east of Manhattan. Sprogis, and American citizen, was a former police chief in Nazi-occupied Latvia during World War II, and had been previously been accused of war crimes, but in deportation proceedings, all charges against him were dismissed. At the time of the incident, suspected that a fire was set at Sprogis' home in order to have him evacuate the home via the front door, where an explosive planted on his front steps. Sprogis' neighbor Robert Seifried, saw the fire, and went to alert Sprogis, but inadvertently set off the bomb (meant for Sprogis), resulting in serious burns to his Seifried's right foot, leg and shoulder. Damage to the home included shattered windows, destroyed aluminum siding, and other minor damage. After the incident, two calls made to Newsday newspaper from an unknown male, stating, and “Listen carefully, Jewish Defense League, Nazi war criminal. Bomb. Never again." Though the JDL denied involvement in the incident, authorities believe the group was responsible. |
| **Triggering Event** | Elmars Sprogis was a former police chief in Nazi occupied Latvia during WWII and accused of war crimes against Jews; the FBI brought a deportation case against him years prior, but all charges dismissed due to lack of evidence. Members of the JDL and other militant Jewish organizations were critical of the decision. |
| **Motive 1** | Extremist Right Wing Terrorist Groups; In the 80s, JDL changed its primary cause to the plight of Soviet Jews |
| **Motive 2** | Revenge - Injustice |
| **Motive 3** | NOTE: Scholars differ on interpretation of right wing as right wing group. Doesn't think JDL is a right Wing terrorist group (Diane Maye) |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion/Incendiary |
| **Target of Event** | Police |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | The incident occurred at about 4:30am, and the calls to Newsday were |

| | |
|---|---|
| **Random** | 0.184623 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Jewish Defense League (JDL) |
| | Even though the callers claimed responsibility in the name of the JDL, leaders of the group denied the group's responsibility or involvement in the fire and explosion. Sprogis, and American citizen not injured in the incident, and never convicted of the alleged war crimes; charges dismissed due to lack of evidence. Members of the JDL and other militant Jewish organizations were critical of the decision. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | http://www.higginsctc.org/terrorism/FBI%201985.pdf<br>"FBI Analysis of Terrorist Incidents and Terrorist Related Activities in the United States: 1985," Terrorist Research and Analytical Center, Terrorism Section, Criminal Investigative Division, FBI, 1985. |
| **Evidence 2** | http://www.nytimes.com/1985/09/07/nyregion/blast-at-home-of-ex-war-crimes-suspect-injures-one.html<br>Robert D. McFadden, "Blast at Home of Ex-War Crimes Suspect Injures One; Bystander Hurt by Blast at Home Of a Onetime War Crimes Suspect," New York Times, September 7, 1985. |
| **Evidence 3** | http://www.apnewsarchive.com/1985/Police-Suspect-Link-In-Blasts-At-Homes-Of-Men-Tied-to-War-Crimes/id-a7272be9f9b890093fad6d02187e6d35<br>"Police Suspect Link In Blasts At Homes Of Men Tied to War Crimes," The Associated Press, September 7, 1985. |

| | |
|---|---|
| **Random** | 0.128995 |
| **Actor** | Terrorist |
| **Last Name** | Snider; Roberts; one unidentified man |
| **First Name** | Timothy Wayne; Richard Lee; one unidentified man |
| **Affiliation/Group Name** | Ku Klux Klan |
| **Arrest/Event Date** | 1981 |
| **Event Overview** | 02/13/1981: Three members of the Ku Klux Klan, Timothy Wayne Snider and Richard Lee Roberts and one unidentified man, kidnapped a former KKK chaplain William Seward from his home and forced him into their van, hand cuffed him, and held Seward at gun point for a two hour ride to east Memphis in Tennessee, United States, before leaving him near a hotel after they poured yellow paint on him and feathered him. Seward stated that the men attempted to collect debts they believed he owed them after accusing Seward of being a government agent and traitor. The men cut Seward's hair, threatened his life and the lives of his family members, and told him they knew where he "cashed his government paycheck," all of which was untrue. Timothy Wayne Snider and Richard Lee Roberts arrested and charged with kidnapping. One day prior to the incident, a Klansman called the Commercial Appeal newspaper and stated that a traitor to the Klan would be disciplined the next day, and then after the incident, another call came through notifying that the deed was done and the man could be found near the east Memphis area, where Seward was released. |
| **Triggering Event** | |
| **Motive 1** | Establishing political and economic equality for blacks. |
| **Motive 2** | Racial component - social issue |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Hostage Taking (Kidnapping)/Firearm |
| **Target of Event** | Private Citizens & Property |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | This was a case of inner-party conflict where the goal was to intimidate a former KKK member, believed to be working with the government in some capacity, and send a larger message to anyone who betrays or goes against the Klan. The perpetrators called the victim a "traitor." The attack claimed both the day before and after it occurred, through telephone calls to Commercial Appeal newspaper. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/ |

| | |
|---|---|
| **Random** | 0.128995 |
| **Actor** | Terrorist |
| **Last Name** | Snider; Roberts; one unidentified man |
| **First Name** | Timothy Wayne; Richard Lee; one unidentified man |
| **Affiliation/Group Name** | Ku Klux Klan |
| | news/15574C0CD2FE59B8?p=AWNB<br>"Ex-Klansman abducted, painted and feathered," United Press International, February 15, 1981. |
| **Evidence 2** | Christopher Hewitt, "Political Violence and Terrorism in Modern America: A Chronology," Praeger Security International, 2005. |
| **Evidence 3** | https://news.google.com/newspapers?nid=1356&dat=19810216&id=-YlPAAAAIBAJ&sjid=AQYEAAAAIBAJ&pg=3237,102168&hl=en<br>"Peers suspected ex-klandsmen" Ocala Star Banner, Feb, 16, 1981 |

| | |
|---|---|
| **Random** | 0.100108 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Macheteros |
| **Arrest/Event Date** | 1998 |
| **Event Overview** | 6/9/1998: The Macheteros bombed a Banco Popular branch in Rio Piedras, Puerto Rico. No casualties. Front of the bank was damaged. Macheteros released a communiqué stating bombing was to protest the impending sale of the Puerto Rican Telephone Company to a United States conglomerate. |
| **Triggering Event** | To protest the impending sale of the Puerto Rican Telephone Company to a United States conglomerate |
| **Motive 1** | Separatist / New Regime Nationalist / Ethnic Nationalist, Transnational Crime and Terrorism / Organized Crime |
| **Motive 2** | Revenge - unhappy with sale |
| **Motive 3** | Revenge - unhappy with sale |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Business |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | It is unknown how the Macheteros released their communiqué claiming responsibility for the incident. Believed the Macheteros also bombed a Banco Popular branch in Santa Isabel two weeks later. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | https://www.fbi.gov/file-repository/stats-services-publications-terror_98.pdf<br>"Terrorism in the United States 1998," Counterterrorism Threat Assessment and Warning Unit, National Security Division, FBI, 1998. |
| **Evidence 2** | Eviedo De la Cruz, "Explota Bomba en Banco Popular de Rio Piedras," El Diario La Prensa, June 10, 1998. |
| **Evidence 3** | Christopher Hewitt, "Political Violence and Terrorism in Modern America: A Chronology," Praeger Security International, 2005. |

| | |
|---|---|
| **Random** | 0.13561 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | New World Liberation Front (NWLF) |
| **Arrest/Event Date** | 1976 |
| **Event Overview** | 12/14/1976: Suspected members of the New World Liberation Front (NWLF) attempted to bomb the home of San Francisco Supervisor and acting mayor, Diane Feinstein in San Francisco, California, in the United States. The powerful bomb could have been lethal according to police; however, the bomb misfired (the detonator went off, but the bomb did not ignite), and thus, caused no damage or casualties at the Lyon Street home. NWLF claimed responsibility for the attack, but it is uncertain if claims confirmed. |
| **Triggering Event** | |
| **Motive 1** | Political agenda |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Government (General) |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | http://pqasb.pqarchiver.com/washingtonpost_historical/doc/146588774.html?FMT=ABS&FMTS=ABS:AI&type=historic&date=Dec+16%2C+1976&author=&pub=The+Washington+Post++%281974-Current+file%29&edition=&startpage=A32&desc=Bomb+Is+Found+at+Home+Of+San+Francisco+Aide<br>"Bomb Is Found at Home Of San Francisco Aide," The Washington Post, December 16, 1976. |
| **Evidence 2** | http://www.sfgate.com/bayarea/article/Bomb-targets-Feinstein-2839872.php<br>Laura Perkins, "Bomb Targets Feinstein," The San Francisco Chronicle, December 14, 2001. |
| **Evidence 3** | Christopher Hewitt, "Political Violence and Terrorism in Modern America: A Chronology," Praeger Security International, 2005. |

| | |
|---|---|
| **Random** | 0.060811 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | People's Brigade For A Healthy Genetic Future |
| **Arrest/Event Date** | 1981 |
| **Event Overview** | 05/29/1981: In Toledo, OR, two women, claiming to be part of the People's Brigade For A Healthy Genetic Future set fire to a 1977 Hiller 12-E helicopter leased at the time by Publishers Paper Company to spray herbicides on 100 acres of forest nearby. The women said the arson was a protest against the use of herbicides, and claimed responsibility for the incident in phone calls to various news organizations, including Coast News Service, as well as in a written statement left at the Newport Post Office. |
| **Triggering Event** | As a protest against the use of herbicides, which the perpetrators believed were "poison"  As a message to companies who profit from spraying poisons indiscriminately, without regard to human and animal life |
| **Motive 1** | Ecoterrorism |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Facility/Infrastructure Attack/Incendiary |
| **Target of Event** | Airports & Aircraft |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | |
| **Initial Locating Source** | GTD; Eco Project 2010 |
| **Evidence 1** | "Anti-Herbicide Group Takes Responsibility For Copter Fire," Associated Press, June 2, 1981. |
| **Evidence 2** | "Herbicide Foes torch Helicopter," The Bulletin, May 29, 1981. |
| **Evidence 3** | https://news.google.com/newspapers?nid=1243&dat=19810603&id=KLVYAAAAIBAJ&sjid=Q_cDAAAAIBAJ&pg=5448,5271929&hl=en<br>Company sprays despite copter loss," The Bulletin, June 3, 1981. |
| **Evidence 4** | https://news.google.com/newspapers?nid=1310&dat=19810601&id=xEkVAAAAIBAJ&sjid=UuIDAAAAIBAJ&pg=6048,213476&hl=en<br>"Herbicide foes say they burned copter" Eugene Register Gurard, June 2, 1981 |

| | |
|---|---|
| **Random** | 0.120386 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Revolutionary Cells-Animal Liberation Brigade |
| **Arrest/Event Date** | 2003 |
| **Event Overview** | 09/26/2003: The "Revolutionary Cells Animal Liberation Brigade" claimed responsibility for two explosive devices that detonated at the headquarters of the Shaklee Corporation. |
| **Triggering Event** | The group stated it attacked Shaklee because of its connections to Huntingdon Life Sciences (HLS), which tests products on animals. |
| **Motive 1** | Environmental Terrorist Groups animal liberationists |
| **Motive 2** | Revenge for not stopping doing business |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Business |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | The explosion kept hundreds of people who work in the Hacienda Business Park from reporting to their offices that morning, while police and federal agents combed the area for clues. The same group may have been responsible for bombings at Chiron Corp earlier in the year. |
| **Initial Locating Source** | GTD; CETIS |
| **Evidence 1** | Bryant, "Activists: We won't stop our terrorism; Animal rights group says they set off bomb at Shaklee in Pleasanton," Alameda Times-Star, October 1, 2003. |
| **Evidence 2** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/news/0FDEAC235C381761?p=AWNB<br>Stacy Finz, "Militants say they planted Shaklee bomb; Animal activists attacking clients of research firm," San Francisco Chronicle, October 1, 2003. |
| **Evidence 3** | http://infoweb.newsbank.com.martians.thpl.lib.fl.us/resources/doc/nb/news/1064A16C9886125D?p=AWNB Guy Ashley and Scott Marshall, "Animal Militants say bomb was theirs; revolutionary cells says it left the device at Shaklee in Pleasanton and threatens more violence," Contra Costa Times, October 1 2003. |

| | |
|---|---|
| **Random** | 0.068441 |
| **Actor** | Terrorist |
| **Last Name** | Leguin |
| **First Name** | Douglas |
| **Affiliation/Group Name** | Sovereign Citizen |
| **Arrest/Event Date** | 2014 |
| **Event Overview** | 08/11/2014: An assailant, Douglas Leguin, opened fire on firefighters and police officers in Dallas, TX. Leguin, armed with an AK-47, propane tanks and bottles containing flammable liquid, approached and intended to occupy a residence with an eight-year-old girl and her nanny trapped inside. After an exchange of fire, police captured Leguin identified as a member of Sovereign Citizen and claimed responsibility for the incident. |
| **Triggering Event** | To get citizens to vote. |
| **Motive 1** | Sovereign citizen ideology modeled on Posse Comitatus. |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Police |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Although Douglas Leguin, a self-identified member of Sovereign Citizen, claimed responsibility for the incident, the attack does not represent Sovereign Citizen ideology. |
| **Initial Locating Source** | GTD; START Primary Collection |
| **Evidence 1** | http://www.cbsnews.com/news/cops-man-fires-ak-47-at-police-firefighters-says-he-meant-no-harm/ "Cops: Man fires AK-47 at authorities; says he meant no harm," CBS News, August 18, 2014. |
| **Evidence 2** | http://www.nbcdfw.com/news/local/Accused-North-Dallas-Shooter-Claims-Incident-was-Get-Out-the-Vote-Publicity-Stunt-271318451.html "Accused North Dallas Shooter Claims Incident was 'Get Out the Vote' Publicity Stunt," NBC Dallas-Fort Worth, August 15, 2014. |
| **Evidence 3** | "Suspect who allegedly shot at first responders made strange 911 call," FOX Dallas - Fort Worth, August 12, 2014. |

| | |
|---|---|
| **Random** | 0.184245 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | United Freedom Front (UFF) |
| **Arrest/Event Date** | 1983 |
| **Event Overview** | 08/21/1983: Two bombs exploded at the Sgt. Joseph E. Muller Army Reserve Center in the Bronx, New York in the United States. No casualties resulted from the incident; heavy damage was caused to the building and some military vehicles. A communiqué left by the United Freedom Front in a Bronx post office box, claiming responsibility for the bombing. |
| **Triggering Event** | |
| **Motive 1** | To get out of El Salvador and Nicaragua and support for locked up freedom fighters and grand jury resisters. |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Military |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | The incident occurred at 10:30pm. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | "Explosion At U.S. Army Reserve Center," The Associated Press, August 22, 1983. |
| **Evidence 2** | Ron Powers, "Bombs Explode at Bronx Army Reserve Center," The Associated Press, August 22, 1983. |
| **Evidence 3** | "Left-Wing Bombers Leave Letter After Blasting Reserve Center," The Associated Press, August 22, 1983. |

| | |
|---|---|
| **Random** | 0.084512 |
| **Actor** | Terrorist |
| **Last Name** | Hicks |
| **First Name** | Dean Harvey |
| **Affiliation/Group Name** | Up the IRS, Inc. |
| **Arrest/Event Date** | 1988 |
| **Event Overview** | 9/19/1988: Dean Harvey Hicks, the sole member of Up the IRS, Inc., parked a car filled with explosives in the basement of the Olympic Plaza Building which housed Internal Revenue Service offices in Los Angeles, California, United States. Only one of the bombs detonated. The where no casualties and damages were limited to the car itself. |
| **Triggering Event** | |
| **Motive 1** | To protest the IRS and the taxation system of the United States government |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Government (General) |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | Hicks pled guilty to committing this attack. |
| **Sentence** | |
| **Additional Notes** | Dean Harvey Hicks claimed this incident on behalf of Up the IRS, Inc. in a letter to City National Bank and a local newspaper. Six months after this incident, Hicks bombed at utility poles that he erroneously believed supplied power to the Olympic Plaza Building. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | http://law.justia.com/cases/federal/appellate-courts/F2/997/594/382210/<br>United States Court of Appeals for the Ninth Circuit, "United States of America v. Dean Harvey Hicks," No. 92-50127, June 28, 1993 |
| **Evidence 2** | https://www.ncjrs.gov/pdffiles1/Digitization/138780NCJRS.pdf<br>"Terrorism in the United States 1988," Terrorist Research and Analytical Center, Counterterrorism Section Criminal Investigative Division, FBI, December 31, 1988. |
| **Evidence 3** | https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf<br>Brent L. Smith and Kelly R. Damphousse, "Pre-Incident Indicators of Terrorist Incidents; The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct," United States Department of Justice, May 2006. |

| | |
|---|---|
| **Random** | 0.184999 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Veterans United for Non-Religious Memorials |
| **Arrest/Event Date** | 2013 |
| **Event Overview** | 08/22/2013: An explosive device placed near the Mingus Park Vietnam War Memorial detonated in Coos Bay city, Oregon state, United States. No one was injured in the blast and it is unknown if the memorial was damaged. Veterans for Non-Religious Memorials claimed responsibility for the incident. The group stated that they were against the existence of religious memorials and felt that they were offensive toward non-Christian families. |
| **Triggering Event** | |
| **Motive 1** | Group stated against the existence of religious memorials and felt that they were offensive toward non-Christian families. |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Private Citizens & Property |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | |
| **Initial Locating Source** | GTD; START Primary Collection |
| **Evidence 1** | "Investigation Continues on Coos Bay IEDs," KDRV.com, September 20, 2013. |
| **Evidence 2** | http://theworldlink.com/news/local/crime-and-courts/explosion-at-mingus-park-memorial-prompts-investigation/article_44e1c662-0c2e-11e3-8a94-001a4bcf887a.html<br>"Explosion at Mingus Park memorial prompts investigation," Coos Bay World, August 23, 2013. |
| **Evidence 3** | http://theworldlink.com/news/local/letter-claims-responsibility-for-bombings-threatens-further-violence/article_79c1bd16-1a60-11e3-b2be-001a4bcf887a.html<br>"Letter claims responsibility for bombings, threatens further violence," TheWorldlink.com, September 11, 2013. |
| **Evidence 4** | https://archives.fbi.gov/archives/portland/press-releases/2013/fbi-offers-reward-of-up-to-10-000-in-coos-bay-ied-investigation |

| | |
|---|---|
| **Random** | 0.140518 |
| **Actor** | Terrorist |
| **Last Name** | |
| **First Name** | |
| **Affiliation/Group Name** | Weather Underground, Weathermen |
| **Arrest/Event Date** | 1970 |
| **Event Overview** | 2/21/1970: The Weathermen claimed credit for bombing the residence of State Supreme Court Justice John Murtagh New York, United States. The attack caused no casualties but the house sustained minor damages. Judge Murtagh was presiding over a trial of thirteen Black Panther members at the time. Anti-Vietnam war and pro-Black Panther graffiti left at the scene of the attack. |
| **Triggering Event** | |
| **Motive 1** | Protest Vietnam War and show support for Black Panthers. |
| **Motive 2** | Started as opposition to Viet Nam War. Promote social change. |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Bombing/Explosion |
| **Target of Event** | Private Citizens & Property |
| **Age (at arrest)** | |
| **Sex** | |
| **Marital Status** | |
| **Race/ Ethnicity** | |
| **Education** | |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | |
| **Rank** | |
| **Charges/Convictions** | |
| **Sentence** | |
| **Additional Notes** | Weathermen claimed credit for this attack in a letter to the New York Times. Written in front of the house was graffiti stating "Free Panther 21" and "Vietcong Have Won." The bombs placed on the front doorway, next to a window, and under the Murtagh's car. Murtagh and his family placed in the protection of the police due to the attack. |
| **Initial Locating Source** | GTD; Hewitt Project |
| **Evidence 1** | https://ia802205.us.archive.org/25/items/riotscivilcrimin00unit/riotscivilcrimin00unit.pdf<br>Committee on Government Operations United States Senate, "Riots, Civil, and Criminal Disorders," U.S. Government Printing Office, August 6, 1970. |
| **Evidence 2** | Emanuel Perlmutter, "Justice Murtagh's Home Target of 3 Fire Bombs," New York Times, February 22, 1970. |
| **Evidence 3** | http://www.nytimes.com/1971/01/19/archives/an-end-to-violence-a-message-from-the-weathermen-indicates-a-shift.html?_r=0<br>Bernardine Dohrn, "An End to Violence?" New York Times, January 19, 1971. |

| | |
|---|---|
| **Random** | 0.018375 |
| **Actor** | Spy |
| **Last Name** | Ames |
| **First Name** | Aldrich Hazen |
| **Affiliation/Group Name** | CIA |
| **Arrest Date** | 1994 |
| **Event Overview** | Sold names of 2 FBI officers for $50K |
| **Triggering Event** | Divorce and Financial Problems |
| **Motive 1** | Monetary |
| **Motive 2** | Once started, had to protect himself so continued |
| **Motive 3** | Arrogance |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 52 |
| **Sex** | M |
| **Marital Status** | Divorced |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | CIA |
| **Occupation** | CI Officer |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Conspiracy to commit espionage on behalf of Russia and the former Soviet Union. |
| **Sentence** | Life in prison without the possibility of parole. |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001; http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://fas.org/irp/congress/1994_rpt/ssci_ames.htm |
| **Evidence 2** | http://www.nytimes.com/1994/07/31/magazine/why-i-spied-aldrich-ames.html?pagewanted=all |
| **Evidence 3** | http://www.washingtonpost.com/wp-srv/local/longterm/tours/scandal/ames.htm |
| **Evidence 4** | https://www.fbi.gov/history/famous-cases/aldrich-ames |

| | |
|---|---|
| **Random** | 0.029581 |
| **Actor** | Spy |
| **Last Name** | Bishop |
| **First Name** | Benjamin |
| **Affiliation/Group Name** | Navy retired |
| **Arrest Date** | 2014 |
| **Event Overview** | E-mailed classified information to a  woman with whom he had a romantic relationship |
| **Triggering Event** | |
| **Motive 1** | Romance/Love |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 59 |
| **Sex** | M |
| **Marital Status** | Divorced |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | Defense contractor |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | LTC Army reserve retired |
| **Charges/Convictions** | Willfully communicating classified national defense information to a person not authorized to receive it and unlawfully retaining classified national defense information at his home. |
| **Sentence** | 87 months imprisonment and three years' supervised release |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.ncis.navy.mil/PubNewsRoom/PublishingImages/Overwatch/Oct%202015/Overwatch%20October%202015_low.pdf |
| **Evidence 2** | https://www.justice.gov/nsd/pr/hawaii-man-sentenced-87-months-improsonment-communicating-classified-national-defense |
| **Evidence 3** | http://www.cicentre.com/?BISHOP_Benjamin |
| **Evidence 4** | http://www.cbsnews.com/news/us-defense-contractor-benjamin-bishop-to-fess-up-in-secrets-case-lawyer/ |
| **Evidence 5** | https://fas.org/irp/ops/ci/index.html |

| | |
|---|---|
| **Random** | 0.074981 |
| **Actor** | Spy |
| **Last Name** | Clark |
| **First Name** | James |
| **Affiliation/Group Name** | Government Contractor |
| **Arrest Date** | 1997 |
| **Event Overview** | Passed Microfiche to German handlers while spying for East Germany |
| **Triggering Event** | |
| **Motive 1** | Ideology - Communist sympathizer |
| **Motive 2** | Received $ |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 49 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College drop out |
| **Employer** | |
| **Occupation** | Private investigator |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Title 18 United States Code, Section 794(c): Conspiracy to commit espionage; convicted on a charge of conspiracy to commit espionage |
| **Sentence** | 12 years and seven months in prison. |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001; http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.dhra.mil/perserec/espionagecases/1997-99.html#JamesMichaelClark |
| **Evidence 2** | http://www.cnn.com/US/9710/06/spying/ |
| **Evidence 3** | http://www.cicentre.com/?page=CLARK_James |
| **Evidence 4** | http://articles.latimes.com/print/1998/jun/04/news/mn-56581 |

| | |
|---|---|
| **Random** | 0.008994 |
| **Actor** | Spy |
| **Last Name** | Gold |
| **First Name** | Harry |
| **Affiliation/Group Name** | |
| **Arrest Date** | 1950 |
| **Event Overview** | Theft of atomic secrets. |
| **Triggering Event** | |
| **Motive 1** | Soviet Sympathy |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 40 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College graduate |
| **Employer** | |
| **Occupation** | Biochemist |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Wartime espionage; serving as a courier between a British scientist who stole top-secret info and his Soviet contact; delivered information on the atomic bomb |
| **Sentence** | Sentenced to 30 years in prison; paroled in 1966. |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.history.com/this-day-in-history/harry-gold-sent-to-prison-for-his-role-in-atomic-espionage/print |
| **Evidence 2** | http://www.cicentre.com/?GOLD_Harry |
| **Evidence 3** | http://www.fjc.gov/history/home.nsf/page/tu_rosenberg_bio_gold.html |

| | |
|---|---|
| **Random** | 0.039003 |
| **Actor** | Spy |
| **Last Name** | Grunden |
| **First Name** | Oliver Everett |
| **Affiliation/Group Name** | Air Force Enlisted |
| **Arrest Date** | 1973 |
| **Event Overview** | Attempting to sell tape recordings to Soviets |
| **Triggering Event** | |
| **Motive 1** | Money |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 20 |
| **Sex** | M |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Graduate |
| **Employer** | Air Force |
| **Occupation** | |
| **Civilian/ Military** | Military |
| **Rank** | Airman First Class |
| **Charges/Convictions** | Attempted espionage |
| **Sentence** | Military court martial; five years in prison, reduction to Airman Basic, forfeiture of all pay and allowances in excess of $300 a month; dishonorably discharged; initial conviction overturned on technicality, reconvicted and sentenced to time served. |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.cicentre.com/?GRUNDEN_Oliver |
| **Evidence 2** | https://books.google.com/books?id=l_ZTCgAAQBAJ&pg=PA173&lpg=PA173&dq=Oliver+Everett+grunden+espionage&source=bl&ots=VNyoEjrHZt&sig=epznHjLm-sHJqWObcXLYuI1mUdk&hl=en&sa=X&ved=0ahUKEwiVmLqc0aLOAhVGJCYKHd1RAmwQ6AEIHzAB#v=onepage&q=Oliver%20Everett%20grunden%20espionage&f=false |
| **Evidence 3** | https://fas.org/irp/ops/ci/docs/ci3/ |

| | |
|---|---|
| **Random** | 0.075869 |
| **Actor** | Spy |
| **Last Name** | Harper, Jr. |
| **First Name** | James Durward |
| **Affiliation/Group Name** | Government Contractor |
| **Arrest Date** | 1983 |
| **Event Overview** | Acquired classified materials from wife; subsequently sold to Polish intelligence. |
| **Triggering Event** | |
| **Motive 1** | Money |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 50 |
| **Sex** | M |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | Self employed |
| **Occupation** | Electrical Engineer |
| **Civilian/ Military** | Civilian |
| **Rank** | Former USMC |
| **Charges/Convictions** | Selling classified documents to Polish intelligence for a reported sum of $250,000; eventually pleaded guilty to six counts of espionage |
| **Sentence** | Life sentence |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001; http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.dhra.mil/perserec/espionagecases/1983.html#JamesDurwardHarper |
| **Evidence 2** | http://www.cicentre.com/?page=HARPER_JAMES |
| **Evidence 3** | http://www.nytimes.com/1984/05/15/us/californian-gets-life-sentence-in-espionage-case.html |

| | |
|---|---|
| **Random** | 0.01667 |
| **Actor** | Spy |
| **Last Name** | Harris |
| **First Name** | Ulysses Leonard |
| **Affiliation/Group Name** | Army Enlisted |
| **Arrest Date** | 1967 |
| **Event Overview** | Delivering info to unauthorized personnel |
| **Triggering Event** | |
| **Motive 1** | Monetary |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 38 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Black |
| **Education** | Unknown |
| **Employer** | Army |
| **Occupation** | |
| **Civilian/ Military** | Military |
| **Rank** | SGT 1st Class |
| **Charges/Convictions** | Conspiring to deliver to unauthorized individuals information pertaining to the national defense |
| **Sentence** | 7 years of hard labor. |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001;<br>http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | https://books.google.com/books?id=3zSSCgAAQBAJ&pg=PA73&lpg=PA73&dq=Ulysses+Leonard+harris+espionage&source=bl&ots=kM1ez6Yp82&sig=Gh6PIPz5smJvSncyDxW9IkmILB0&hl=en&sa=X&ved=0ahUKEwiJw_Of_5vOAhWCNSYKHdpoCsYQ6AEIHDAA#v=onepage&q=Ulysses%20Leonard%20harris%20espionage&f=false |
| **Evidence 2** | https://www.fas.org/sgp/library/spies.pdf |
| **Evidence 3** | https://news.google.com/newspapers?nid=757&dat=19671214&id=KbZNAAAAIBAJ&sjid=nkQDAAAAIBAJ&pg=3910,3006114&hl=en |

| | |
|---|---|
| **Random** | 0.007247 |
| **Actor** | Spy |
| **Last Name** | Hernandez |
| **First Name** | Linda |
| **Affiliation/Group Name** | Wasp Network - Cuban spy ring |
| **Arrest Date** | 1998 |
| **Event Overview** | Spied for the Cuban government on US military installations and Cuban exile organizations |
| **Triggering Event** | |
| **Motive 1** | Threats against family |
| **Motive 2** | Loyalty to adopted country |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 46 |
| **Sex** | F |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Charged with attempting to collect information for the Cuban Intelligence Service by infiltrating a right-wing Cuban exile group called Alpha 66 |
| **Sentence** | Pled guilty to acting as an unregistered agent of a foreign government. Sentenced to seven years in prison; spared treason charge because info was in the public domain |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 – 2001<br>http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.dhra.mil/perserec/espionagecases/1997-99.html |
| **Evidence 2** | https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/intelligence-officers-bookshelf.html |
| **Evidence 3** | http://webcache.googleusercontent.com/search?q=cache:ebMCpFPd4zAJ:thomas.loc.gov/cgi-bin/query/z%3Fr105:S24SE8-544:&num=1&hl=en&gl=us&strip=1&vwsrc=0 |
| **Evidence 4** | http://www.jonathanpollard.org/2000/022400.htm |
| **Evidence 5** | http://www.cicentre.com/?page=HERNANDEZ_LINDA |

| | |
|---|---|
| **Random** | 0.023085 |
| **Actor** | Spy |
| **Last Name** | Hoffman |
| **First Name** | Robert Patrick |
| **Affiliation/Group Name** | Navy Enlisted |
| **Arrest Date** | 2012 |
| **Event Overview** | Provided Russians information on methods and technology to track US submarines and procedures required |
| **Triggering Event** | |
| **Motive 1** | Monetary |
| **Motive 2** | "Help" both countries |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 39 |
| **Sex** | M |
| **Marital Status** | Divorced |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Graduate |
| **Employer** | Unemployed at time of espionage |
| **Occupation** | Cryptologic Technician-Technical |
| **Civilian/ Military** | Military |
| **Rank** | Petty Officer First Class |
| **Charges/Convictions** | Espionage by attempting to hand over closely held military secrets |
| **Sentence** | 30 years in prison |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | https://archives.fbi.gov/archives/norfolk/press-releases/2014/former-sailor-sentenced-to-30-years-in-prison-for-attempted-espionage |
| **Evidence 2** | http://www.ca4.uscourts.gov/Opinions/Unpublished/144136.U.pdf |
| **Evidence 3** | http://pilotonline.com/news/robert-hoffman-the-spy-who-struck-out/article_bd898a94-259a-5f08-a611-5df12ba462b6.html |
| **Evidence 4** | http://www.cicentre.com/?HOFFMAN_Robert |

| | |
|---|---|
| **Random** | 0.015556 |
| **Actor** | Spy |
| **Last Name** | Irene |
| **First Name** | Dale Vern |
| **Affiliation/Group Name** | Civilian |
| **Arrest Date** | 1984 |
| **Event Overview** | Selling cryptographic cards |
| **Triggering Event** | |
| **Motive 1** | Monetary |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 24 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Pled guilty to two counts of receiving stolen property. |
| **Sentence** | Two-year confinement |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001;<br>http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.dhra.mil/perserec/espionagecases/1985.html#MichaelTimothyTobias |
| **Evidence 2** | http://www.cicentre.com/?page=IRENE_DALE |
| **Evidence 3** | https://news.google.com/newspapers?nid=1755&dat=19840824&id=ly4eAAAAIBAJ&sjid=5r4EAAAAIBAJ&pg=2277,2956030&hl=en |

| | |
|---|---|
| **Random** | 0.064659 |
| **Actor** | Spy |
| **Last Name** | Kadish |
| **First Name** | Ben-Ami |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2008 |
| **Event Overview** | Provided classified documents related to US missile defense systems to an agent of Israel |
| **Triggering Event** | |
| **Motive 1** | Help Israel |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 84 |
| **Sex** | M |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | Retired government employee |
| **Occupation** | Mechanical engineer |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Initially 4 charges. Plead to one: Conspiracy to act as unregistered agent of Israel; Count One: Title 18, USC, Section 794; Count Two: Title 18, USC, Section 951; Count Three: Title 18, USC, Section 1001(a) (2); Count Four: Title 18, USC, Section 1512 (b) (3) |
| **Sentence** | Fined. No prison time. |
| **Additional Notes** | |
| **Initial Locating Source** | PERSEREC (2009) 1975 to 2008; http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.dhra.mil/perserec/espionagecases/2005-08.html#BenAmiKadish |
| **Evidence 2** | http://www.cicentre.com/?page=KADISH_Ben |
| **Evidence 3** | http://www.nytimes.com/2009/05/30/nyregion/30kadish.html?_r=0 |
| **Evidence 4** | https://www.justice.gov/archive/usao/nys/pressreleases/May09/kadishsentencingpr.pdf |

| | |
|---|---|
| **Random** | 0.008205 |
| **Actor** | Spy |
| **Last Name** | King |
| **First Name** | Donald Wayne |
| **Affiliation/Group Name** | Navy Enlisted |
| **Arrest Date** | 1989 |
| **Event Overview** | Delivered classified docs to undercover agent |
| **Triggering Event** | |
| **Motive 1** | Money |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 23 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | USAF |
| **Occupation** | Aviation storekeeper at the Naval Air Station in Belle Chasse |
| **Civilian/ Military** | Military |
| **Rank** | Airman |
| **Charges/Convictions** | Conspiracy to commit espionage and larceny of government property; Charged with espionage, theft of government property, sale of classified aircraft parts, and selling cocaine |
| **Sentence** | Ten years, reduction in rank to E-1, forfeiture of all pay and a dishonorable discharge |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001; http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://articles.orlandosentinel.com/1989-03-06/news/8903070312_1_storekeeper-espionage-graf |
| **Evidence 2** | http://www.cicentre.com/?page=KING_Donald |
| **Evidence 3** | http://www.dhra.mil/perserec/espionagecases/1989.html#DonaldWayneKing |
| **Evidence 4** | http://www.nytimes.com/1989/03/06/us/2-at-new-orleans-base-accused-of-espionage.html |

| | |
|---|---|
| **Random** | 0.034204 |
| **Actor** | Spy |
| **Last Name** | Lieber |
| **First Name** | Donald |
| **Affiliation/Group Name** | Bureau of African Affairs |
| **Arrest Date** | 1995 |
| **Event Overview** | Passing documents and diplomatic cables to the African National Congress |
| **Triggering Event** | |
| **Motive 1** | Ideology - against apartheid |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 33 |
| **Sex** | M |
| **Marital Status** | Unknown |
| **Race/ Ethnicity** | |
| **Education** | College graduate |
| **Employer** | Bureau of African Affairs |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Title 18 USC, theft of government property |
| **Sentence** | 10 months in prison and 3 years' probation |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.cicentre.com/?LIEBER_Donald |
| **Evidence 2** | https://books.google.com/books?id=3zSSCgAAQBAJ&pg=PA177&lpg=PA177&dq=donald+charles+lieber&source=bl&ots=kM1ezfPnf_&sig=3nQwmlNvgkMg1qDz32-YpeoW62k&hl=en&sa=X&ved=0ahUKEwjV2_y_rJ7OAhVGeCYKHZhMAM4Q6AEIPzAI#v=onepage&q=donald%20charles%20lieber&f=false |
| **Evidence 3** | Did not find a third source. |

| | |
|---|---|
| **Random** | 0.01102 |
| **Actor** | Spy |
| **Last Name** | Lindauer |
| **First Name** | Susan |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2004 |
| **Event Overview** | Conspiring with two sons of a former Iraqi diplomat acting as an unregistered agents of the Iraqi government |
| **Triggering Event** | |
| **Motive 1** | Anti-war activist |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 41 |
| **Sex** | F |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Graduate School (Master's degree) |
| **Employer** | Government |
| **Occupation** | Congressional Aide |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Two counts of conspiracy to act as unregistered agent of a foreign government; Engaging in financial transaction with government of a country; Indicted for accepting money from the Iraqis and traveling to Baghdad, meeting  with Iraqi intelligence agents |
| **Sentence** | Declared incompetent for trial; Government dropped prosecution stating it would no longer be in the interests of justice. |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.cicentre.com/?page=lindauer_susan |
| **Evidence 2** | http://www.nytimes.com/2004/08/29/magazine/susan-lindauer-s-mission-to-baghdad.html?pagewanted=all&src=pm&_r=0 |
| **Evidence 3** | http://www.foxnews.com/story/2004/03/12/american-charged-with-being-paid-iraqi-intel-agent.html |
| **Evidence 4** | http://news.findlaw.com/usatoday/docs/iraq/uslindauer31004ind.pdf |

| | |
|---|---|
| **Random** | 0.033003 |
| **Actor** | Spy |
| **Last Name** | Nicholson |
| **First Name** | Harold James |
| **Affiliation/Group Name** | CIA |
| **Arrest Date** | 1996/2009 |
| **Event Overview** | Personal problems |
| **Triggering Event** | Failing marriage |
| **Motive 1** | Money |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 47 |
| **Sex** | M |
| **Marital Status** | Divorced |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Masters |
| **Employer** | CIA |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | Army CPT retired |
| **Charges/Convictions** | Two counts of conspiracy, one count of acting as an agent of a foreign government and four counts of money laundering. In 1997 convicted on charges of conspiring to commit espionage for the Russian Federation. |
| **Sentence** | 23 years 7 months of imprisonment |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001; http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | https://archives.fbi.gov/archives/news/stories/2009/february/familyspies_020209 |
| **Evidence 2** | http://www.cicentre.com/?page=NICHOLSON_Jim |
| **Evidence 3** | http://www.nytimes.com/1997/06/06/us/cia-traitor-saying-he-wanted-cash-for-family-gets-23-years.html?ref=haroldjnicholson |
| **Evidence 4** | http://www.gq.com/story/my-father-and-me-spy-story-russia |

| | |
|---|---|
| **Random** | 0.040811 |
| **Actor** | Spy |
| **Last Name** | Nozette |
| **First Name** | Stewart David |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2009 |
| **Event Overview** | Provided classified info to suspected Israeli intel officer |
| **Triggering Event** | |
| **Motive 1** | Money |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 52 |
| **Sex** | M |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Ph.D. MIT |
| **Employer** | Alliance for Competitive Technology |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | 4 charges of attempted espionage. Pled guilty today to attempted espionage for providing classified information to a person he believed to be an Israeli intelligence officer. (Attempted Espionage, in violation of Title 18, United States Code, Section 794(a)) |
| **Sentence** | Plea agreement 13 years in prison |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | https://www.justice.gov/opa/pr/noted-scientist-pleads-guilty-attempted-espionage |
| **Evidence 2** | http://www.cicentre.com/default.asp?page=NOZETTE_Stewart |
| **Evidence 3** | http://c.ymcdn.com/sites/www.cicentre.com/resource/resmgr/spycase_docs/nozette_ind211009.pdf |

| | |
|---|---|
| **Random** | 0.073055 |
| **Actor** | Spy |
| **Last Name** | Pelton |
| **First Name** | Ronald William |
| **Affiliation/Group Name** | NSA |
| **Arrest Date** | 1985 |
| **Event Overview** | Provided classified info to Soviets on collection programs targeting Soviets for 5 years |
| **Triggering Event** | |
| **Motive 1** | Money - Financial difficulties |
| **Motive 2** | Angry with employer/position dissatisfaction |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 44 |
| **Sex** | M |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Graduate |
| **Employer** | NSA |
| **Occupation** | Communications intelligence and cryptology |
| **Civilian/ Military** | Civilian |
| **Rank** | Retired Air Force |
| **Charges/Convictions** | Convicted on one count of conspiracy and two counts of espionage. |
| **Sentence** | 3 concurrent life sentences. |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001;<br>http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | https://www.fbi.gov/history/famous-cases/year-of-the-spy-1985 |
| **Evidence 2** | http://www.cicentre.com/?page=PELTON_Ronald |
| **Evidence 3** | http://www.dhra.mil/perserec/espionagecases/1985.html#RonaldWilliamPelton |
| **Evidence 4** | http://www.nytimes.com/1986/06/03/us/pelton-tells-spy-jury-he-admitted-he-might-have-jeopardized-lives.html?pagewanted=all |
| **Evidence 5** | http://law.justia.com/cases/federal/appellate-courts/F2/835/1067/296623/ |

| | |
|---|---|
| **Random** | 0.048669 |
| **Actor** | Spy |
| **Last Name** | Pitts |
| **First Name** | Earl Edwin |
| **Affiliation/Group Name** | FBI |
| **Arrest Date** | 1996 |
| **Event Overview** | Conspired with officers of the KGB and SVRR to commit espionage |
| **Triggering Event** | |
| **Motive 1** | Money |
| **Motive 2** | Revenge; "payback" against employer. |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 43 |
| **Sex** | M |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Caucasian |
| **Education** | JD |
| **Employer** | FBI |
| **Occupation** | Supervisory Special Agent |
| **Civilian/ Military** | Civilian |
| **Rank** | Retired Army |
| **Charges/Convictions** | Conspiracy to commit espionage, attempted espionage, communication of classified information, and conveyance of government property; Conspiracy to commit espionage, Title 18, United States Code, Section 794 (c) |
| **Sentence** | 27 years in prison by a Federal judge who stated that the former agent was guilty of "the most egregious abuse of trust." |
| **Additional Notes** | |
| **Initial Locating Source** | Herbig & Wiskoff (2002) 1947 - 2001;<br>http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://fas.org/irp/offdocs/pitts_nr.htm |
| **Evidence 2** | http://www.dhra.mil/perserec/espionagecases/1996.html#EarlEdwinPitts |
| **Evidence 3** | http://noir4usa.org/resources/inside-the-mind-of-a-spy/ |

| | |
|---|---|
| **Random** | 0.037898 |
| **Actor** | Spy |
| **Last Name** | Slack |
| **First Name** | Alfred Dean |
| **Affiliation/Group Name** | Government contractor |
| **Arrest Date** | 1950 |
| **Event Overview** | Courier, passing |
| **Triggering Event** | |
| **Motive 1** | Money/financial gain |
| **Motive 2** | Sympathy with USSR |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 44 |
| **Sex** | M |
| **Marital Status** | Divorced |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | Kodak |
| **Occupation** | Chemist |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Conspiracy to commit espionage during wartime |
| **Sentence** | 15 years in prison. |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.tned.uscourts.gov/docs/0906history.pdf |
| **Evidence 2** | http://www.cicentre.com/?page=SLACK_ALFRED |
| **Evidence 3** | https://vault.fbi.gov/rosenberg-case/harry-gold/harry-gold-part-51-of |

| | |
|---|---|
| **Random** | 0.077268 |
| **Actor** | Spy |
| **Last Name** | Velazquez |
| **First Name** | Marta Rita |
| **Affiliation/Group Name** | Federal Employee |
| **Arrest Date** | 2014 |
| **Event Overview** | Conspired to transmit US national defense information and recruiting US citizens to spy for Cuba. |
| **Triggering Event** | |
| **Motive 1** | Sympathetic to Cuba |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Espionage |
| **Target of Event** | Government |
| **Age (at arrest)** | 55 |
| **Sex** | F |
| **Marital Status** | Married |
| **Race/ Ethnicity** | Latino |
| **Education** | JD |
| **Employer** | Federal Employee |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Title 18, U.S.C., Section 794(a) and (c): Conspiracy to Commit Espionage. |
| **Sentence** | |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.cicentre.com/?page=case_spies |
| **Evidence 1** | http://www.cicentre.com/?VELAZQUEZ_Marta |
| **Evidence 2** | https://archives.fbi.gov/archives/washingtondc/press-releases/2013/unsealed-indictment-charges-former-u.s.-federal-employee-with-conspiracy-to-commit-espionage-for-cuba |
| **Evidence 3** | http://www.thelocal.se/20130426/47574 |
| **Evidence 4** | https://www.justice.gov/iso/opa/resources/441201342515915732615.pdf |

| | |
|---|---|
| **Random** | 0.060026 |
| **Actor** | Hacker |
| **Last Name** | Abene |
| **First Name** | Mark |
| **Affiliation/Group Name** | Independent; Legion of Doom and Masters of Deception |
| **Arrest Date** | 1991 |
| **Event Overview** | Hack into SW Bell |
| **Triggering Event** | |
| **Motive 1** | Prestige/show off |
| **Motive 2** | Enhance image in view of others |
| **Motive 3** | Exploration |
| **Motive 4** | Challenge |
| **Motive 5** | |
| **Attack Type** | Hacking |
| **Target of Event** | Business |
| **Age (at arrest)** | 20 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Drop out |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Charges of computer tampering and conspiracy computer fraud, wire fraud, illegal wiretapping, and conspiracy. |
| **Sentence** | Plea agreement to a lesser misdemeanor charge, and was sentenced to 35 hours of community service. |
| **Additional Notes** | |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | https://vimeo.com/6578941 |
| **Evidence 2** | http://www.textfiles.com/news/modbust.txt |
| **Evidence 3** | http://www.wired.com/1994/04/phiber-optik-goes-to-prison/ |
| **Evidence 4** | https://www.youtube.com/watch?v=hkQ0BOrFTJk  Phiber Optik - Last Interview Before 1 Year In Prison (1993) Joseph Turner Published on Apr 15, 2013 |
| **Evidence 5** | http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/accidental-hacker-wsj-7-11-97.txt |

| | |
|---|---|
| **Random** | 0.283419 |
| **Actor** | Hacker |
| **Last Name** | Ancheta |
| **First Name** | Jeanson James |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2005 |
| **Event Overview** | Network of Bots |
| **Triggering Event** | |
| **Motive 1** | Money |
| **Motive 2** | Boasting/Advertising |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Botnets |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | 20 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School equivalency |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Conspiracy, fraud and other crimes in connection with a 14-month crime spree that started in June 2004; four felony charges for crimes, including infecting machines at two U.S. military sites, that earned him more than $61,000 |
| **Sentence** | Plea agreement will receive from 4 years to 6 years in prison, forfeit a 1993 BMW and more than $58,000 in profit and pay $19,000 in restitution to the federal government |
| **Additional Notes** | |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | http://news.bbc.co.uk/2/hi/technology/4642566.stm |
| **Evidence 2** | http://articles.latimes.com/2005/nov/04/business/fi-hacker4 |
| **Evidence 3** | http://archive.wired.com/science/discoveries/news/2006/01/70069 |
| **Evidence 4** | https://books.google.com/books?id=NsWgBgAAQBAJ&pg=PA44&lpg=PA44&dq=Jeanson+James+Ancheta+hacker&source=bl&ots=SnLRUmaXY2&sig=7G4O2mAWayrGx_Z-3i9M_qzKb8k&hl=en&sa=X&ved=0ahUKEwiA_46ZgIrOAhULLB4KHexrDh04ChDoAQg1MAQ#v=onepage&q=Jeanson%20James%20Ancheta%20hacker&f=false |
| **Evidence 5** | https://www.justice.gov/archive/criminal/cybercrime/press-releases/2005/anchetaArrest.htm |

| | |
|---|---|
| **Random** | 0.159167 |
| **Actor** | Hacker |
| **Last Name** | Auernheimer |
| **First Name** | Andrew |
| **Affiliation/Group Name** | “the organization,” Goatse Security, Gay Nigger Association of America |
| **Arrest Date** | 2010 |
| **Event Overview** | Hack into ATT and stole email addresses |
| **Triggering Event** | |
| **Motive 1** | Fun |
| **Motive 2** | Mischief |
| **Motive 3** | Self-promotion |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Hacking |
| **Target of Event** | Business |
| **Age (at arrest)** | 24 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College drop out |
| **Employer** | Self employed |
| **Occupation** | Security Researcher |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Identity theft and conspiracy to gain unauthorized access to computers; charged under the Computer Fraud and Abuse Act. |
| **Sentence** | Jury found him guilty of identity theft and conspiracy to gain unauthorized access to computers. Sentenced to 41 months in prison for collecting thousands of email addresses from AT&T’s servers and disclosing them to a reporter, also ordered to serve an additional three years of probation and pay more than $73,000 in restitution. Conviction overturned after serving 36 months. |
| **Additional Notes** | |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | https://www.justice.gov/sites/default/files/usao-nj/legacy/2014/09/02/Spitler,%20Daniel%20et%20al.%20Complaint.pdf |
| **Evidence 2** | https://www.law.berkeley.edu/article/court-to-sentence-att-hacker-andrew-auernheimer/ |
| **Evidence 3** | https://www.justice.gov/sites/default/files/usao-nj/legacy/2014/09/02/Spitler,%20Daniel%20et%20al.%20Complaint.pdf |

| | |
|---|---|
| **Random** | 0.311564 |
| **Actor** | Hacker |
| **Last Name** | Bentley |
| **First Name** | Robert Matthew |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2007 |
| **Event Overview** | Bot installations ad sales |
| **Triggering Event** | |
| **Motive 1** | Money/Profit |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Attack Type** | Botnet |
| **Target of Event** | Business |
| **Age (at arrest)** | 21 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Conspiracy to commit computer fraud and computer fraud. Pled guilty to two felony counts related to his botnet activities, counts related to his botnet activities, which inflicted more than $150,000 worth of damage. Pled guilty to conspiracy to commit computer fraud, contrary to Title 18 United States Code, Section 1030. Sentenced to 41 months imprisonment, and told to pay fines amounting to US $65,000. |
| **Sentence** | 41 months in jail for breaking into corporate computers in Europe and making them part of a money-generating botnet; three years of supervised release once his prison time is over and to pay $65,000 in restitution |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.networkworld.com/article/2349880/security/fbi--bot-roast-ii--1-million-infected-pcs---20-million-in-losses-and-8-indictments.html |
| **Evidence 1** | http://www.darknet.org.uk/2008/06/botmaster-robert-matthew-bentley-aka-lsdigital-sentenced/ |
| **Evidence 2** | https://nakedsecurity.sophos.com/2013/01/04/lsdigital-botnet-downfall/ |
| **Evidence 3** | https://www.justice.gov/archive/criminal/cybercrime/press-releases/2008/bentleyPlea.pdf |

| | |
|---|---|
| **Random** | 0.238819 |
| **Actor** | Hacker |
| **Last Name** | Corley |
| **First Name** | Eric (Emmanuel Goldstein) |
| **Affiliation/Group Name** | |
| **Arrest Date** | 1984/2000 |
| **Event Overview** | Hacking phones/distributed a program that breaks the security code on DVDs so they could copy onto computers. a program called DeCSS, which cracks the encryption code, |
| **Triggering Event** | |
| **Motive 1** | Curiosity/discovery/learn/explore |
| **Motive 2** | Fun |
| **Motive 3** | Challenge |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Decryption program |
| **Target of Event** | Business |
| **Age (at arrest)** | 41 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College graduate |
| **Employer** | 2600 Magazine |
| **Occupation** | Writer |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Committed piracy by posting the program on the Web site in violation of the Digital Millennium Copyright Act |
| **Sentence** | |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/groupsites.html |
| **Evidence 1** | https://web.archive.org/web/20060519071519/http://edition.cnn.com/TECH/specials/hackers/qandas/goldstein.html |
| **Evidence 2** | https://www.mied.uscourts.gov/PDFFIles/01-71685RHC.pdf |
| **Evidence 3** | http://www-bcf.usc.edu/~hantran/3pov.html |
| **Evidence 4** | http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1391&context=btlj |
| **Evidence 5** | http://broom02.revolvy.com/main/index.php?s=Eric%20Corley |

| | |
|---|---|
| **Random** | 0.346954 |
| **Actor** | Hacker |
| **Last Name** | Draper |
| **First Name** | John T. (later nicknamed Captain Crunch) |
| **Affiliation/Group Name** | Homebrew Computer Club |
| **Arrest Date** | 1971/2 |
| **Event Overview** | Used a Captain Crunch cereal whistle to make free phone calls. |
| **Triggering Event** | Bullying; unhappy life |
| **Motive 1** | Technical curiosity |
| **Motive 2** | Intellectual |
| **Motive 3** | Diagnosed Psychotic |
| **Motive 4** | Attention |
| **Motive 5** | Obsessive |
| **Attack Type** | Hacking |
| **Target of Event** | Business |
| **Age (at arrest)** | 29 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College drop out |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian/USAF |
| **Rank** | AFC/SGT |
| **Charges/Convictions** | Charges of wire fraud |
| **Sentence** | 3 jail terms; received a five-year probation; He was sentenced to prison for phone fraud in 1976 and again in 1978, and again in 1979 |
| **Additional Notes** | |
| **Initial Locating Source** | http://webcache.googleusercontent.com/search?q=cache:2bpgoF0VX0kJ:www.wonderslist.com/top-10-hackers-who-wrote-history/+&cd=8&hl=en&ct=clnk&gl=us |
| **Evidence 1** | http://www.computerworld.com/article/2470109/endpoint-security/interview-with-iconic-hacker-captain-crunch.html |
| **Evidence 2** | http://search.proquest.com.ezproxy.lib.usf.edu/docview/398985584?accountid=14745 |
| **Evidence 3** | http://www.barbalet.net/crunch/ |
| **Evidence 4** | http://csrc.nist.gov/publications/secpubs/hacker.txt |

| | |
|---|---|
| **Random** | 0.02463 |
| **Actor** | Hacker |
| **Last Name** | Goldstein |
| **First Name** | Ryan Brett |
| **Affiliation/Group Name** | Taunet |
| **Arrest Date** | 2007 |
| **Event Overview** | Botnet |
| **Triggering Event** | |
| **Motive 1** | Steal |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Botnet/DDOS |
| **Target of Event** | Business |
| **Age (at arrest)** | 21 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College student |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | For botnet related activity which caused a distributed denial of service (DDoS) attack at a major Philadelphia area university |
| **Sentence** | |
| **Additional** | |
| **Initial Locating Source** | http://www.networkworld.com/article/2349880/security/fbi--bot-roast-ii--1-million-infected-pcs---20-million-in-losses-and-8-indictments.html |
| **Evidence 1** | https://archives.fbi.gov/archives/news/pressrel/press-releases/bot-roast-ii-nets-8-individuals |
| **Evidence 2** | https://books.google.com/books?id=nmgK7KcibSUC&pg=PA48&lpg=PA48&dq=Ryan+Brett+goldstein+hacker&source=bl&ots=xdrBJyqiJY&sig=6Q2KcuRlZ9GeuJKnytMmB3ZTMoA&hl=en&sa=X&ved=0ahUKEwjVhYiLvoDOAhWIGh4KHZr2C0sQ6AEIPzAF#v=onepage&q=Ryan%20Brett%20goldstein%20hacker&f=false |
| **Evidence 3** | https://nakedsecurity.sophos.com/2007/12/03/botmasters-herded-up-by-the-fbi/ |
| **Evidence 4** | http://www.computerworld.com/article/2538356/security0/crime-and-punishment--the-botnet-barons.html |

| | |
|---|---|
| **Random** | 0.159151 |
| **Actor** | Hacker |
| **Last Name** | Gonzalez |
| **First Name** | Albert |
| **Affiliation/Group Name** | Shadowcrew |
| **Arrest Date** | 2008 |
| **Event Overview** | SQL Injection Credit card theft |
| **Triggering Event** | |
| **Motive 1** | Intellectual Curiosity |
| **Motive 2** | Money |
| **Motive 3** | Show off/boasting |
| **Motive 4** | Addiction/substance abuse (drugs) |
| **Motive 5** | Thrill |
| **Motive 6** | Asperger's syndrome |
| **Attack Type** | SQL Injection |
| **Target of Event** | Business |
| **Age (at arrest)** | 27 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College drop out |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Three federal indictments - one count of wire fraud conspiracy |
| **Sentence** | On March 25, 2010, Gonzalez was sentenced to 20 years in federal prison |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/<br>http://www.businessinsider.com/the-10-most-infamous-hackers-of-all-time-2015-4?op=1<br>http://content.time.com/time/business/article/0,8599,1917345,00.html |
| **Evidence 1** | https://www.wired.com/2010/03/tjx-sentencing/ |
| **Evidence 2** | http://www.ismlab.usf.edu/isec/files/HackerSentencedto20YearsinMassiveDataTheft-WSJ.pdf |
| **Evidence 3** | https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail |

| | |
|---|---|
| **Random** | 0.546882 |
| **Actor** | Hacker |
| **Last Name** | Googins |
| **First Name** | Chris (AKA: Erik Bloodaxe) |
| **Affiliation/Group Name** | Legion of Doom |
| **Arrest Date** | 1984 |
| **Event Overview** | Hacking |
| **Triggering Event** | |
| **Motive 1** | Fun |
| **Motive 2** | Challenge |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Hacking |
| **Target of Event** | Business |
| **Age (at arrest)** | 21 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Goggins was raided by the US Secret Service on March 1, 1990, but was not charged |
| **Sentence** | |
| **Additional Notes** | |
| **Initial Locating Source** | Sterling, Bruce (1994). "Part 2: The Digital Underground". The Hacker Crackdown<br>Law and Disorder on the Electronic Frontier. Project Gutenberg.<br>http://www.computerworld.com/article/2536061/cybercrime-hacking/six-hours-to-hack-the-fbi--and-other-pen-testing-adventures-.html |
| **Evidence 1** | http://www.gutenberg.org/files/101/101-h/101-h.htm |
| **Evidence 2** | https://joi.ito.com/weblog/2002/10/29/drinks-with-chr.html |
| **Evidence 3** | https://www.youtube.com/watch?v=D6mXYNbVj_U |

| | |
|---|---|
| **Random** | 0.069108 |
| **Actor** | Hacker |
| **Last Name** | Hotz |
| **First Name** | George |
| **Affiliation/Group Name** | Individual; possibly associated with “fail0verflow” |
| **Arrest Date** | 2007/2010 |
| **Event Overview** | Unlock iPhone/Crack Sony PlayStation |
| **Triggering Event** | |
| **Motive 1** | Fun, Entertainment (curb boredom) |
| **Motive 2** | Challenge |
| **Motive 3** | Power |
| **Motive 4** | Curiosity |
| **Motive 5** | Competitiveness |
| **Attack Type** | Hacking |
| **Target of Event** | Business |
| **Age (at arrest)** | 17 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | College graduate |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Violating the Computer Fraud and Abuse Act and facilitating copyright infringement, such as downloading pirated games |
| **Sentence** | Sony announced that it had reached an agreement with Hotz, who denied wrongdoing but consented to a permanent injunction barring him from reverse engineering any Sony product in the future. |
| **Additional Notes** | |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | https://web.archive.org/web/20071014041013/http://northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXk4NDgmZmdiZWw3Zjd2cWVlRUV5eTcxODU2MTMmeXJpcnk3ZjcxN2Y3dnFlZUVFeXkz |
| **Evidence 2** | http://news.bbc.co.uk/2/hi/technology/8478764.stm |
| **Evidence 3** | http://thetartan.club.cc.cmu.edu/2015/8/24/news/hack |
| **Evidence 4** | http://www.newyorker.com/magazine/2012/05/07/machine-politics |

| | |
|---|---|
| **Random** | 0.331433 |
| **Actor** | Hacker |
| **Last Name** | James |
| **First Name** | Jonathan |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2000 |
| **Event Overview** | Hacking/sniffer |
| **Triggering Event** | |
| **Motive 1** | Learning |
| **Motive 2** | Drugs |
| **Motive 3** | Power |
| **Motive 4** | Computer enthusiast |
| **Motive 5** | |
| **Attack Type** | Sniffer |
| **Target of Event** | Government (DOD) |
| **Age (at arrest)** | 16 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Two counts of juvenile delinquency; invaded 13 computers of the National Aeronautics and Space Administration at the agency's Marshall Space Flight Center in Huntsville, Ala., on June 29 and 30, 1999. Among other things, he downloaded software and stole data, leading to a three-week shutdown of some computers. |
| **Sentence** | Six months in juvenile detention. |
| **Additional Notes** | James committed suicide in May 2008. Self-inflicted gunshot. |
| **Initial Locating Source** | http://www.itsecurity.com/features/top-10-famous-hackers-042407/<br>http://list25.com/25-most-notorious-hackers-to-ever-get-caught/<br>https://hacked.com/hackers/<br>http://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/ |
| **Evidence 1** | http://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html |
| **Evidence 2** | https://www.wired.com/2009/07/hacker-3/ |
| **Evidence 3** | http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/anon.html |
| **Evidence 4** | http://www.pcmag.com/article2/0,2817,2164176,00.asp |

| | |
|---|---|
| **Random** | 0.403069 |
| **Actor** | Hacker |
| **Last Name** | Lacroix |
| **First Name** | Cameron |
| **Affiliation/Group Name** | Individual and possible links to Defonic Team Screen Name Club |
| **Arrest Date** | 2005/2014 |
| **Event Overview** | Hacked into Paris Hilton's phone and LexisNexis; into LE and college |
| **Triggering Event** | Unhappy home life |
| **Motive 1** | Computer obsessive - "Gave him a high"/also addicted to drugs |
| **Motive 2** | A game/challenge |
| **Motive 3** | Recognition |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Hacking |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | 16/25 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Drop out |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Convicted federally of aggravated identity fraud, computer fraud, wire fraud, and making a false bomb threat; 18 counts of computer related crimes |
| **Sentence** | Received 11 months in a federal juvenile detention facility; violated release and got four-year sentence |
| **Additional Notes** | |
| **Initial Locating Source** | https://www.justice.gov/usao-ma/pr/man-charged-computer-hacking-and-credit-card-theft |
| **Evidence 1** | http://www.nbcnews.com/news/investigations/ex-teen-hacker-tells-paris-hilton-hes-sorry-n239601 |
| **Evidence 2** | https://www.justice.gov/opa/pr/massachusetts-man-sentenced-four-years-prison-computer-hacking-involving-stolen-credit-card |
| **Evidence 3** | http://www.bizjournals.com/boston/news/2014/06/02/hacker-whose-exploits-included-invading-paris.html |

| | |
|---|---|
| **Random** | 0.005471 |
| **Actor** | Hacker |
| **Last Name** | Levin |
| **First Name** | David Michael |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2016 |
| **Event Overview** | Hacked into Lee County, FL elections website |
| **Triggering Event** | |
| **Motive 1** | Helping cybersecurity |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Hacking |
| **Target of Event** | Government (General) |
| **Age (at arrest)** | 31 |
| **Sex** | M |
| **Marital Status** | Unknown |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | Vanguard Security |
| **Occupation** | Consultant |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Three third-degree-felony counts of property crimes |
| **Sentence** | Pending |
| **Additional Notes** | Levin logged in to the Lee County Elections Office website using the pilfered credentials of Sharon Harrington, the county's supervisor of elections. |
| **Initial Locating Source** | http://thehackernews.com/2016/05/hack-an-election.html |
| **Evidence 1** | http://webcache.googleusercontent.com/search?q=cache:rSOFkbvh-WcJ:www.news-press.com/story/news/crime/2016/05/04/estero-man-arrested-hacking-into-state-lee-elections-website-david-levin-dan-sinclair/83921672/+&cd=2&hl=en&ct=clnk&gl=us |
| **Evidence 2** | http://www.activistpost.com/2016/05/hacker-jailed-after-exposing-flaws-in-election-website.html |
| **Evidence 3** | http://arstechnica.com/security/2016/05/how-a-security-pros-ill-advised-hack-of-a-florida-elections-site-backfired/ |

| | |
|---|---|
| **Random** | 0.544496 |
| **Actor** | Hacker |
| **Last Name** | Mitnick |
| **First Name** | Kevin |
| **Affiliation/Group Name** | |
| **Arrest Date** | 1994 |
| **Event Overview** | Social engineering/hacking |
| **Triggering Event** | |
| **Motive 1** | Pursuit of knowledge |
| **Motive 2** | Adventure |
| **Motive 3** | Fun/ Hobby |
| **Motive 4** | Addiction |
| **Motive 5** | Personality disorder |
| **Attack Type** | Hacking |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | 31 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Graduate |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | 25-count indictment that includes charges of wire fraud and illegal possession of computer files stolen from such companies; charged with computer and wire fraud |
| **Sentence** | Signed a plea agreement that reportedly will set him free after serving another year in prison. |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.itsecurity.com/features/top-10-famous-hackers-042407/<br>http://www.makeuseof.com/tag/5-of-the-worlds-most-famous-hackers-what-happened-to-them/<br>http://www.businessinsider.com/the-10-most-infamous-hackers-of-all-time-2015-4?op=1<br>https://hacked.com/hackers/<br>http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | http://www.forbes.com/sites/singularity/2013/04/11/kevin-mitnick-the-hacking-hamburglar/#64a517024057 |
| **Evidence 2** | http://www.cnn.com/SPECIALS/1999/mitnick.background/ |
| **Evidence 3** | https://www.justice.gov/archive/opa/pr/Pre_96/February95/89.txt.html |
| **Evidence 4** | http://www.recode.net/2015/3/26/11560712/why-kevin-mitnick-the-worlds-most-notorious-hacker-is-still-breaking |
| **Evidence 5** | https://www.hsgac.senate.gov/download/?id=6ff169ff-94ab-4b24-90f7-e0a642619e69. |
| **Evidence 6** | Mitnick, K. D., & William, L. S. (2002). The art of deception: Controlling the human element of security [Kindle for iPad version]. Retrieved from http://www.amazon.com |

| | |
|---|---|
| **Random** | 0.054884 |
| **Actor** | Hacker |
| **Last Name** | Moore |
| **First Name** | Robert |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2006 |
| **Event Overview** | Steal VOIP services |
| **Triggering Event** | |
| **Motive 1** | Fun |
| **Motive 2** | Money |
| **Motive 3** | Challenge |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Brute force attacks |
| **Target of Event** | Business |
| **Age (at arrest)** | 22 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Drop out |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | conspiracy to commit computer fraud |
| **Sentence** | two-year sentence |
| **Additional Notes** | |
| **Initial Locating Source** | http://www.informationweek.com/interview-with-a-convicted-hacker-robert-moore-tells-how-he-broke-into-routers-and-stole-voip-services/d/d-id/1059631? |
| **Evidence 1** | http://www.informationweek.com/interview-with-a-convicted-hacker-robert-moore-tells-how-he-broke-into-routers-and-stole-voip-services/d/d-id/1059631? |
| **Evidence 2** | https://www.computer.org/csdl/mags/it/2007/06/mit2007060004.pdf |
| **Evidence 3** | http://www.nytimes.com/2006/06/08/technology/08voice.html?_r=0 |
| **Evidence 4** | https://www.linkedin.com/in/robert-moore-74a38016 |

| | |
|---|---|
| **Random** | 0.556943 |
| **Actor** | Hacker |
| **Last Name** | Moran |
| **First Name** | Dennis |
| **Affiliation/Group Name** | |
| **Arrest Date** | 2000 |
| **Event Overview** | Website defacement; DDOS attacks |
| **Triggering Event** | |
| **Motive 1** | Part of a joke that got out of hand |
| **Motive 2** | Addiction (cough syrup) |
| **Motive 3** | Show off/boasting |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | DDOS |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | 17 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School Drop out |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Moran was charged as an adult with 7 counts of Class A felony unauthorized access of a computer; Pleaded guilty to 4 counts of misdemeanor unauthorized access of a computer and was sentenced to 12 months in jail with 3 months suspended as well as ordered to pay $15,000 USD in restitution; pleaded guilty in January to misdemeanor charges of hacking. |
| **Sentence** | Sentenced to nine months behind bars — and was ordered to help program the jail's computers |
| **Additional Notes** | Moran died of a heroin overdose on April 14, 2013 at age 30. |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | http://www.zdnet.com/article/coolio-arrested-for-defacing-site/ |
| **Evidence 2** | http://usatoday30.usatoday.com/tech/news/2001-03-09-coolio.htm |
| **Evidence 3** | http://www.foxnews.com/story/2001/08/31/teen-hacker-coolio-gets-fresh-start-as-head-computer-services-company.html |
| **Evidence 4** | http://articles.latimes.com/keyword/dennis-m-moran |

| | |
|---|---|
| **Random** | 0.451398 |
| **Actor** | Hacker |
| **Last Name** | Morris |
| **First Name** | Robert Tappan |
| **Affiliation/Group Name** | |
| **Arrest Date** | 1988 |
| **Event Overview** | Morris worm |
| **Triggering Event** | |
| **Motive 1** | Juvenile act |
| **Motive 2** | Unfocused intellectual meandering |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Worm |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | 23 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Graduate School |
| **Employer** | |
| **Occupation** | Student |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Violating the computer Fraud and Abuse Act (Title 18); Prosecuted under 1986 Computer Fraud and Abuse Act. |
| **Sentence** | Three years of probation, 400 hours of community service, a fine of $10,050 plus costs of supervision |
| **Additional Notes** | First person convicted under the Computer Fraud and Abuse Act. |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/<br>http://www.itsecurity.com/features/top-10-famous-hackers-042407/<br>http://www.telegraph.co.uk/technology/6670127/Top-10-most-famous-hackers.html |
| **Evidence 1** | http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html |
| **Evidence 2** | http://www.cs.cornell.edu/courses/cs1110/2009sp/assignments/a1/p706-eisenberg.pdf |
| **Evidence 3** | https://louisville.edu/faculty/ddking01/cecs311/cases/morris.htm |
| **Evidence 4** | https://archives.fbi.gov/archives/news/testimony/cyber-security |

| | |
|---|---|
| **Random** | 0.541284 |
| **Actor** | Hacker |
| **Last Name** | Murphy |
| **First Name** | Ian (Captain Zap) |
| **Affiliation/Group Name** | |
| **Arrest Date** | 1981 |
| **Event Overview** | Hacked into ATT, Broke into White House computers |
| **Triggering Event** | |
| **Motive 1** | Curiosity |
| **Motive 2** | Love of technology |
| **Motive 3** | Entertainment (curb boredom) |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Hacking |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | High School |
| **Employer** | |
| **Occupation** | |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Guilty of felony fraud and theft |
| **Sentence** | 1,000 hours of community service and 2 1/2 years' probation; because there were no federal computer-crime laws at that time, he got off with a third-degree felony count. |
| **Additional Notes** | First hacker to be convicted of a crime |
| **Initial Locating Source** | http://www.symantec.com/region/sg/homecomputing/library/cybercrime.html |
| **Evidence 1** | http://attrition.org/errata/charlatan/ian_murphy/threat_profile/ |
| **Evidence 2** | http://hackstory.net/Captain_Zap |
| **Evidence 3** | http://www.people.com/people/archive/article/0,,20108863,00.html |

| | |
|---|---|
| **Random** | 0.137807 |
| **Actor** | Hacker |
| **Last Name** | Rose |
| **First Name** | Leonard |
| **Affiliation/Group Name** | Legion of Doom |
| **Arrest Date** | 1991 |
| **Event Overview** | Hack into ATT |
| **Triggering Event** | |
| **Motive 1** | Testing boundaries |
| **Motive 2** | |
| **Motive 3** | |
| **Motive 4** | |
| **Motive 5** | |
| **Attack Type** | Trojan Horse |
| **Target of Event** | Business |
| **Age (at arrest)** | 32 |
| **Sex** | M |
| **Marital Status** | Unknown |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | Consultant |
| **Occupation** | |
| **Civilian/ Military** | Civilian/US Army (per his linked in profile.) |
| **Rank** | |
| **Charges/Convictions** | Five-count indictment alleging that he and other computer hackers schemed to steal source codes for AT&T's widely used UNIX program; pleaded guilty in March to two counts of wire fraud. |
| **Sentence** | Sentenced to a year and a day in federal prison and three years of probation |
| **Additional Notes** | |
| **Initial Locating Source** | http://list25.com/25-most-notorious-hackers-to-ever-get-caught/ |
| **Evidence 1** | http://pqasb.pqarchiver.com/latimes/doc/281357071.html?FMT=ABS&FMTS=ABS:FT&type=current&date=Mar%2023,%201991&author=HENRY%20WEINSTEIN&pub=Los%20Angeles%20Times%20(pre-1997%20Fulltext)&edition=&startpage=2&desc=Hacker%20Enters%20Guilty%20Plea%20in%20Theft%20of%20Computer%20Data |
| **Evidence 2** | http://articles.baltimoresun.com/1991-06-11/news/1991162105_1_hacker-computer-fraud-rose |
| **Evidence 3** | http://articles.latimes.com/keyword/leonard-jr-rose |
| **Evidence 4** | http://www.worldlibrary.org/articles/leonard_rose_(hacker) |
| **Evidence 5** | http://cd.textfiles.com/secretsubjects/UNDERGRD/VOL_2/CUD200C.TXT |

| | |
|---|---|
| **Random** | 0.05755 |
| **Actor** | Hacker |
| **Last Name** | Smith |
| **First Name** | David L. |
| **Affiliation/Group Name** | |
| **Arrest Date** | 1999 |
| **Event Overview** | Melissa virus |
| **Triggering Event** | |
| **Motive 1** | Show off |
| **Motive 2** | Kicks |
| **Motive 3** | Evade anti-virus programs |
| **Motive 4** | Prank |
| **Motive 5** | |
| **Attack Type** | Virus |
| **Target of Event** | Business; Government |
| **Age (at arrest)** | 30 |
| **Sex** | M |
| **Marital Status** | Single |
| **Race/ Ethnicity** | Caucasian |
| **Education** | Unknown |
| **Employer** | subcontractor for CGS Computer Associates |
| **Occupation** | Programmer |
| **Civilian/ Military** | Civilian |
| **Rank** | |
| **Charges/Convictions** | Computer-related crimes |
| **Sentence** | 20-month jail term. |
| **Additional Notes** | The sentence, originally ten years (of a maximum forty-year sentence) in a US federal prison reduced to twenty months and a $5,000 fine when Smith began working undercover with the FBI shortly after his capture. |
| **Initial Locating Source** | http://www.telegraph.co.uk/technology/6670127/Top-10-most-famous-hackers.html<br>https://hacked.com/hackers/ |
| **Evidence 1** | https://nakedsecurity.sophos.com/2009/03/26/memories-melissa-virus/ |
| **Evidence 2** | https://www.soldierx.com/hdb/David-Smith-Kwyjibo-VicodinES-Alt-F11 |
| **Evidence 3** | http://www.cnn.com/TECH/computing/9903/31/melissamarine.idg/index.html |
| **Evidence 4** | http://webcache.googleusercontent.com/search?q=cache:_TivUx7Sg3gJ:www.people.vcu.edu/~dbromley/melissavirusLink.htm+&cd=4&hl=en&ct=clnk&gl=us |
| **Evidence 5** | https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/melissaSent.htm |

## Appendix F: Semi-structured Interview Guide

**Introduction:**

Thank you for agreeing to participate in my research on the motivations of terrorists, spies, and hackers. In an earlier phase of my research, I reviewed cases studies of terrorists, spies, and hackers seeking to understand the motivations of each actor. I developed a motivational topology and identified 12 themes and 37 sub-themes. For this phase of research, I would like your feedback on the topology. In particular, I am interested in hearing your perspective on the motivations of the actors with whom you have experience. I want to stress, I am only interested in feedback on the motivations and the topology, and no other facet of your work. In preparation for today's discussion, I sent you definitions of themes and sub-themes, and the motivation topology for review. Those items will be the topic of our discussion.

Please remember, you are not required to answer any questions you do not want to answer. If at any time you do not want to continue with the interview let me know and we will stop. The entire interview will take approximately one hour.

I selected you based on your experience and your willingness to provide your opinions about the actors' motivations from your career perspective. Your resume states [review highlights of resume, including years of experience].

1. Is this correct.
2. Are you willing to reflect upon and share opinions about the actors' motivations from your career perspective?

Great.

I want to remind you that I will record this conversation.

3. Do I have your permission to record?

Thank you.

Before today's call, you signed a consent form.

4. Do you still consent?

Great. Thanks.

Just a reminder, you can withdraw your consent or stop the interview at any time. Just let me know.

I will also take notes during the discussion so if you hear me pause, I am taking notes.

5. Finally, do you have any questions for me before we begin? (Answer questions or begin).

Ok, let’s begin with the first question:

**Semi-structured interview questions:**

6. Did you understand the definitions of the motivations I sent you before the call?
7. Do you have any questions about any of the definitions? If need time to review, OK.
8. Looking through the list of motivation themes and subthemes, please list the motivations about which you have experience.
9. For **each motivation listed**, is this list similar to your experiences?

   Ask probing questions based on responses.

   Be sure to use active listening techniques

   Repeat words such as “Wow!, Tell me more about that!” or “That is really interesting.” to prompt additional discussion and discovery.

   Ask probing questions such as  “Could you say some more about that…?”or “What do you mean by that . . .?”

10. In reviewing the topology, do you see any motivations you think are missing? If so, what, and please explain.

11. Is there anything you think I should consider that I’ve not considered?

**Conclusion:**

12. Before we wrap things up and talk about next steps, do you have any questions for me or comments you’d like to make?

As I mentioned at the beginning of our call, I’ll be transcribing the interview and then destroying the recording.

I’m hoping to finish up the interviews in the next month or so and then begin analysis. Thank you for your participation and feedback. And, please feel free to call or e-mail if you think of additional motivations or other comments that I should include or if you have any questions. My phone number is: 813-258-4673 and if you’d prefer to email, my email is: beisenfeld@national.edu.

Again, thanks so much for your time today.

Bye.

## Appendix G: Interview Data Analysis Guide

| Motivations | | Interviewees | | | Quotation/Comments |
|---|---|---|---|---|---|
| **Theme** | **Sub-theme** | **1** | **2** | **3** | |
| Addiction | | ✓ | | ✓ | If interviewee mentioned theme or sub-theme, researcher inserted a check mark and inserted quotes, if any. |
| Choice | | | | | |
| Coercion | | | | | |
| Curiosity | Curiosity (generalized) | | | | |
| | Continuous learning | | | | |
| | Technical mastery/challenge | | | | |
| Ego | Ego (generalized) | | | | |
| | Entrance to/support of social group | | | | |
| | Power | | | | |
| | Recognition | | | | |
| | Status | | | | |
| | Thrills/Self-importance | | | | |
| Entertainment | Entertainment (generalized) | | | | |
| | Adventure | | | | |
| | Fun, Thrill, Excitement | | | | |
| | Pranks | | | | |
| Ideology | Ideology (generalized) | | | | |
| | Anarchist | | | | |
| | Divided Loyalties | | | | |
| | Economic | | | | |
| | Ethnocentric | | | | |
| | Hacktivism | | | | |
| | Nationalist-Separatist | | | | |
| | Political Agenda | | | | |
| | Religion | | | | |
| | Social | | | | |
| Ingratiation | | | | | |
| Money | | | | | |
| Psychological | Psychological (generalized) | | | | |
| | Anti-social | | | | |
| | Asperger Syndrome | | | | |
| | Autism Spectrum Disorder | | | | |
| | Introverted | | | | |
| | Narcissism | | | | |
| | Personality Disorder | | | | |
| | Type-A | | | | |
| Revenge | Revenge (generalized) | | | | |
| | Blame | | | | |
| | Disgruntlement | | | | |
| | Economic sabotage/steal | | | | |
| | Harm | | | | |
| | Injustice | | | | |
| Romance | | | | | |

Source: Author