AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBER-TERRORORISM AND CYBER-CRIME:

THERE IS A DIFFERENCE

By

Craig Gong, Major, USAFR

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Mary Hittmeier and Dr. Richard L. Smith

Maxwell Air Force Base, Alabama

August 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

DISCLAIMER ii
TABLE OF CONTENTS iii
LIST OF TABLES iv
PREFACE v
ABSTRACT vii
INTRODUCTION 1
BACKGROUND 2
The Various Definitions 3
  Department of Defense (DOD) 4
  Federal Bureau of Investigation (FBI) 5
  Department of Justice (DOJ) 8
  Industry Example – Symantec 8
  International Example – United Kingdom (UK) 9
  International Example – Interpol 11
  Scholarly Examples – Cyber-Terrorism 12
  Scholarly Examples – Cyber-Crime 13
United States Code References 14
Investigating Cyber-Terrorism and Cyber Crime 17
Potential Definition Parameters 19
Alternatives 24
Conclusions 27
Recommended Definition Parameters 28
CONCLUSION 34
ENDNOTES 35
BIBLIOGRAPHY 40

LIST OF TABLES

Page

Table 1: Potential Parameters for Distinguishing Cyber-Terrorism 20
Table 2: Potential Parameters for Distinguishing Cyber-Crime 23
Table 3: Recommended Parameters for Distinguishing Cyber-Terrorism 29
Table 4: Recommended Parameters for Distinguishing Cyber-Crime 33

PREFACE

During the initial days of the 2016 Democratic National Convention (DNC) email hacking incident, before Russia was named the likely suspect, it reminded me of the Sony Pictures email hacking event two years prior. While the latter event fell quickly from media attention the former continues to this day. In the simplest of terms, it made me wonder, when these two events initially occurred, why one was considered a major event like a terrorist attack and the other just a minor inconvenience? While selecting a topic for this research paper, I came across the following topic title from Joint Special Operations University's *Special Operations Research Topics 2017*, "Cyberterrorism: Is it real or hyperbole?"[1] Considering the two previously mentioned events, the question became: What is "cyber-terrorism" versus "cyber-crime" and how it is defined? While it might seem like a simple exercise in attaching the word "cyberspace" to an established definition of "terrorism," cyberspace does not entirely behave in the same manner as any physical domain. Such a solution would also have been implemented years ago were the case so simple. Therefore, this research seeks to examine the parameters that would make up a definition for "cyber-terrorism" and "cyber-crime" by examining the various definitions developed by various organizations and authors to find commonalities to assemble these parameters. I hope this research paper will encourage further research into the implications and complications of cyberspace operations to ensure the United States military remains strong in this new domain.

First and foremost, I would like to express gratitude to my family, whose support enabled me the time necessary to write this paper. I would also like to acknowledge my advisors, Dr. Mary Hittmeier and Dr. Richard Smith, and my fellow Air Command and Staff College (ACSC)

Online Master's Program (OLMP) Research Elective classmates for their feedback, who helped formulate this research paper and its thesis.

ABSTRACT

The terms “cyber-terrorism” and “cyber-crime” have many varying definitions depending on who is defining them. For example, individuals with expertise in law enforcement will have a different perspective than persons with expertise in information security. While many definitions exist, there is no universally single accepted definition for either. Defining these two terms allows for distinction, which is important as each has different legal considerations and, when investigating a cyber-attack, procedural considerations. By examining the strengths and weaknesses of several definitions offered by national security, law enforcement, industry, law, and scholars, this research constructs a list of parameters to consider when formulating definitions for cyber-terrorism and cyber-crime.

A crucial element in distinguishing both terms is the intent of the cyber-attack and its link to a long-term goal. With cyber-terrorism, the intent is generally to influence the behaviors and decisions of a population and/or government toward a political, social, religious, or ideological agenda. In contrast, the intent of cyber-crime is personal gain or gratification. Lastly, both cyber-terrorism and cyber-crime definitions should consistently represent the technology and avoid limiting it to only a single component of cyberspace such as the Internet. Cyberspace is an expansive domain consisting of the Internet, telecommunications networks, computer systems, mobile networks, and embedded processors and controllers.[2]

INTRODUCTION

This research employs a problem/solution framework to study distinguishing between acts of terrorism in cyberspace between acts of crime in cyberspace, determining the appropriate response, and recommending parameters to create a distinction. The first obstacle in assessing cyber-terrorism is the various proposed definitions with no universally accepted single definition.[3] Responses to such events, in turn, have various legal ramifications, depending on the legal system involved. Some people may counter cyber-terrorism is a myth, as no lives have yet been lost as a result, and no evidence terrorist organizations are pursuing such capabilities.[4] Regardless, the human spirit and imagination should never be underestimated, as cyberspace becomes increasingly a significant part of every aspect of human lives. For instance, in 2015 automotive security researchers Charlie Miller and Chris Valasek successfully hacked a 2014 Jeep Cherokee through its network and paralyzed it on a highway.[5] If done during heavier, high-speed traffic conditions, such an attack could harm or take a human life. Vehicle computer systems also affect other aspects of driving, such as steering and acceleration, which have potential life-threatening implications should those systems become compromised. In this manner, cyber-attacks and cyber-crimes in cyberspace become acts of terror.

The research begins with the background of the problem regarding cyber-attacks and cyber-terrorism, to include recent attacks. The research then explores the various existing definitions for cyber-crimes and cyber-terrorism, as well as the differences and the inconsistencies within these definitions. The research then reviews the general procedures involved in responding to cyber events while considering the differences in cases of cyber-terrorism versus cyber-crimes. Alternatives considered include removal of the term "cyber-terrorism" and alternative parameters for both cyber-terrorism and cyber-crime. Finally, the research provides recommended parameters for distinguishing cyber-terrorism and cyber-crime to stimulate further analysis toward comprehensively accepted definitions.

BACKGROUND

Cyber-attacks generally follow two forms.[6] The first involves attacks against the data, where theft and corruption of data renders them unusable to the service they support. The service, in turn, becomes unavailable to users because it is unable to function correctly. Stolen data may also be used to reveal and exploit information related to service users, such as relationships, financial, and identity information. The second form of attack focuses on a control system. In this form, the focus of the attack is to gain control of the systems commanding the behavior of a service and altering its behavior to the will of the attacker. An often used scenario is an attacker gaining control of a nation's power grid and switching the system off, with potentially devastating results.

The last decade has witnessed several high-profile attacks in the cyberspace domain. In 2006, the non-profit organization *WikiLeaks* began publishing to the Internet classified information from anonymous sources.[7] In 2014, a hacker group known as the "Guardians of Peace" acquired and leaked documents and emails from Sony Pictures' employees to the Internet.[8] The most recent attack occurred during the United States (US) 2016 Presidential elections, where Democratic National Convention (DNC) emails were leaked, revealing the organization's interactions with the media, between party leaders, the campaigns of candidates Hilary Clinton and Bernie Sanders, and financial contributions and perks provided to donors.[9] While there might be general agreement such events represented crimes in cyberspace, whether they are acts of terrorism is less consistent. A significant reason for this situation is the definitions for cyber-terror originate from a variety of different backgrounds and fields of expertise such as “law enforcement, international studies, anti-terror, information security, and information operations.”[10] Also adding to the confusion is the general use of cyber-terror to describe all cyberspace activities by terrorists and terror groups, such as command and control, recruitment, fundraising, and propaganda, which might be merely crimes rather than acts of terror.[11]

Understanding these differences provide two primary benefits. First, the research offers insights concerning the elements of cyber-attacker’s intent and goal to distinguish cyber-terrorism from cyber-crime and why such a distinction is important when considering the potential responses. Finally, the research provides an improved understanding of the two concepts, which have yet to be uniformly established in the understanding of cyberspace within the DOD.

The Various Definitions

As mentioned before, the variety of interpretations of cyber-crime and cyber warfare is inconsistent within the variety of organizations dealing with them. Each organization approaches topics from differing perspectives based on areas such as mission, expertise, and culture, which then subsequently influence the emphasis placed within their definitions. The time and context also influence how the definitions are applied. The research also examines the definitions offered by authors through their own scholarly work. The analysis identifies inconsistencies present within the definitions and demonstrates how the intent and goals of the attacker is crucial to distinguishing acts of cyber-terrorism from those of cyber-crime. From these definitions, the research develops the parameters for defining cyber-terrorism and cyber-crime, as well as distinguishes them from each other.

Department of Defense (DOD)

Cyberspace has only recently been considered a separate domain. Organizational, occupational, and cultural changes are still in planning phases and early execution, as the DOD strives to develop its cyberspace missions, knowledge, expertise, and capabilities in the rapidly evolving nature of this domain. Thus, DOD should establish a formal definition for either cyber-terrorism or cyber-crime. Searches of the Joint Doctrine, Education, and Training Electronic Information System (JDEIS) and *DOD Dictionary of Military and Associated Terms*, revealed no related entries for either term. Similar searches through JDEIS for DOD instructions, manuals, and directives also provided few references to the terms. While reasonable, it does demonstrate an inconsistency in knowledge and understanding of these concepts crucial for the DOD to develop its cyberspace missions, knowledge, expertise, and capabilities. The absence of the term "cyber-crime" is also plausible because of the law enforcement element the name suggests, which is distinct from the national security responsibilities of the DOD.

DOD does provide a definition for terrorism, which is "the unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political."[12] Within this definition are potential elements for developing parameters for defining cyber-terrorism. While the act of violence, or threat of, is undoubtedly significant, the most important distinction for terrorism is the intent[13] of the acts in relation to a long-term goal. In this case, fear and coercion of governments and societies is the intent supporting an often political long-term goal. This is also generally consistent with Title 22, Chapter 38, Section 2656f of the US Code terrorism definition as, "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[14] In both definitions the intent and motivation are both present, which are important features of terrorism and defining it.

DOD also provides a definition for "cyberspace" within *DOD Dictionary of Military and Associated Terms*, which defines cyberspace as, "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[15] This definition is also consistent with and uses the same verbiage posed by the National Initiative for Cybersecurity Careers and Studies (NICCS), an effort by the US government to develop an effective workforce of cyberspace professionals. The NICCS defines cyberspace as "The interdependent network of information technology infrastructures, which includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[16] Like the definition on terrorism, there are also characteristics related to the type of networks possibly targeted in a cyber-attack. However, even this list is limited as mobile technology and networks like those in cellphones and vehicles are becoming a larger presence, which should also be considered.

Federal Bureau of Investigation (FBI)

The FBI has attempted to create a definition for cyber-terrorism and cyber-crime from the 1980s to the early 2000s. The evolution of their definition of cyber-terrorism provides an example of how the changes in understanding cyberspace and terrorism molded the definition. This research examines some of those definitions.

The term "cyber-terrorism" was first used in the 1980s by Barry Collins, of the Institute of Security and Intelligence, who called it a "dynamic of terrorism as transcendence from the physical to the virtual realm and "the intersection, the convergence of these two worlds...."[17]

While an initial definition, it was general and more focused on the intersection of cyberspace and the physical world. It also lacked the specificity necessary to make a clear distinction with terms like "cyber-crime."[18] Disciplines and technology related to cyberspace were also at early stages of development, especially when compared to the number of individuals who currently have access to personal computers and mobile devices to regularly utilize cyberspace for work and personal affairs.

In 1997, the FBI updated this definition to "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents."[19] This definition was more specific as it begins to identify the targets and attackers, motives of the attackers, and what are the targets. However, the definition lack the attacker's intent for the attack, such as use of fear, threat of violence, or damage to aspects like the economy or infrastructure toward the attacker's ends.[20] With the absence of the intent is also the absence of a long-term goal associated with it, such as influencing government decisions toward areas like political, religious, social, and/or ideological beliefs, which encompass more than violence against non-combatants. Using the US 2016 Presidential Election as an example, the attackers would have sought to influence the outcome of the election and discredit the election system with their actions, both of which did not directly result in violence against non-combatants.

The FBI definition was updated in 2004 as, "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda."[21] This definition reflects a more complete view of cyber-terrorism by addressing the agenda of the attackers and their intent to create fear through confusion and uncertainty. A problem with the definition could be in its effort to cover more aspects of terrorism by using the terms "purpose" and "goal", which are similar enough to be confusing. Attacking computer systems and telecommunications to cause fear is also a limiting factor as mobile technology in cellphones, tablets, vehicles, and medical equipment may also become targets.[22] As an example, the evolution of this definition has made significant progress since it was first established and it is likely to continue to evolve as cyberspace itself evolves. From this point, the research will look to current definitions of cyber-terrorism and/or cyber-crimes from various organizations and authors.

Regarding cyber-crime, the FBI categorizes cyber-crime into four areas: 1) computer intrusions, 2) theft of intellectual property and personal information, 3) child pornography and exploitation, and 4) online fraud.[23] In this first example of a cyber-crime definition, there are apparent notable differences from cyber-terrorism. While both encompass cyberspace, the motivations, intent, and goals of the cyber-attacker are less critical than the criminal act themselves. The act of cyber-crime may be conducted by terrorist; however, these will still be performed in support of a long-term goal. The motivation for attackers within cyber-crime, except those acts committed in support of cyber-terrorism, are often self-serving and may be done for 'bragging rights', corporate espionage, and criminal organizations looking to steal information for black market sales.[24]

Department of Justice (DOJ)

The DOJ defines cyber-crime as "the use of the Internet to commit or facilitate the commission of, a crime, including the communication of false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, employment/business opportunity schemes and so-called 'Phishing' schemes."[25] This definition generally includes most types of cyber-crimes potentially encountered, as well as the intent of the attacker to commit a crime or facilitate commissioning one. A potential inconsistency is the current issue of identity theft might appear excluded. In this case, the false representation is happening to both the consumer and the product or service provider.

Lastly, the definition is limited to only crimes committed through the Internet, which is a significant portion of cyberspace, but not the only one. The NICCS definition of cyberspace, discussed in the earlier section relating to DOD, includes telecommunications networks, computer systems, and embedded processors and controllers in addition to the Internet. Likewise, mobile technology, such as those used in cellphones and vehicles, utilize carrier networks separate from the Internet.

Industry Example – Symantec

Symantec Corporation provides a concise definition of cyber-crime as, "any crime that is committed using a computer network or hardware device."[26] For educating the general population, this is an appropriate definition because it is easily understood by those who are less familiar with such areas as information technology (IT), law enforcement, and national security. This definition inadequately distinguishes cyber-crime from cyber-terrorism because it limits cyber-crimes to computer networks and hardware devices. The term "computer networks" is limiting because mobile networks must also be considered, which are different from computer networks. The term "hardware device" is limiting because the definition should also consider software means of committing crimes, like viruses and worms, which still may be spread using portable storage devices (e.g., flash drives, external hard drives, etc.) and optical and magnetic storage media (e.g., CDs, DVDs, tape media, etc.). While hardware has a role in developing the virus or worm, and is also infected during the attack, the virus or worm is ultimately a software entity used to perpetrate the cyber-crime.

International Example – United Kingdom (UK)

The UK definition for terrorism is found in their Terrorism Act 2000, later revised and divided into the Terrorism Act 2006 and Counter-Terrorism Act 2008. Terrorism is defined as, "the use or threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public, and the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause."[27] The acts of terrorism are further defined as, "1) involves serious violence against a person, 2) involves serious damage to property, 3) endangers a person's life, other than that of the person committing the action, 4) creates a serious risk to the health or safety of the public or a section of the public, or 5) is designed seriously to interfere with or seriously to disrupt an electronic system."[28] This is a complete definition intended to cover all types of terrorism. It contains the elements relating to the intention of the terrorist act (i.e., influence the government or an international governmental organization or to intimidate the public, or a section of the public), its motive (i.e., advancing a political, religious, social or ideological cause), and the harm it caused (e.g., Serious violence against a person).[29]

The final line of this definition relates to cyber-terrorism in the statement, "is designed seriously to interfere with or seriously to disrupt an electronic system." An inconsistency in this definition is the cyberspace attack is considered only a result of an act of terrorism instead of as a means; more a nuisance or inconvenience than a danger to the affected population. The words "disruption" and "interference" both suggest the attack is what causes the electronic system to stop functioning properly or as the attacker intended. This definition also should account for attacks meant to steal or access data on the system, but avoid interfering or disrupting the electronic system. In this case, the actions are undetected because the system is behaving normally as the attacker accesses subsystems and networks using a system administrator's credentials and privileges. The attacker may even use the credentials and privileges of a user who, instead of being an administrator, possess just the right amount of authority to get to the intended data.

In 2001, the Council of Europe adopted the Convention on Cybercrime Treaty, also known as the Budapest Convention.[30] The treaty identifies several cyber-crime offenses including:

> 1) Intentional access without right to the whole part of any computer system;
>
> 2) Intentional interception, without right, of non-public transmissions of computer data;
>
> 3) Intentional damage, deletions, deterioration, alteration, or suppression of computer data without right;
>
> 4) Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering, or suppressing computer data;
>
> 5) The production, sale, procurement for use, importation, or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems, with the intent of committing any of the above crimes;

> 6) Producing, offering or making available, distributing, procuring, and possessing child pornography;
>
> 7) Infringement of copyrights and related rights; 8) Intentional attempting to commit, aid or abet the commission of cyber-crime identified offences.[31]

In 2003, the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems was introduced.[32] The treaty criminalized computer system use intended to: disseminate racist and xenophobic material; make threats and insults of the same nature; deny, grossly minimize, approve or justify genocide or crimes against humanity; and aiding and abetting of any such offenses.

Both the treaties are very detailed examples of defining cyber-crime and the US ratified them in August 2006.[33] The article about data suppression is also becoming more relevant in the recent ransomware incidents where cyber attackers restrict a victim's data by encrypting files or locking screens until ransom, paid in cryptocurrency (e.g., Bitcoin), is sent to the attacker. While it is thorough from a cyberspace perspective, legal issues could raise questions such as the US Constitutional right to free speech regarding the articles in the 2003 treaty.[34] These matters should be considered when developing cyber-crime parameters.

International Example – Interpol

Interpol defines cyber-crime in two major categories. The first is, "Advanced cybercrime (or high-tech crime) – sophisticated attacks against computer hardware and software."[35] The second type is, "Cyber-enabled crime – many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism."[36] In this definition, the relation to terrorism is stated, supporting the idea acts of cyber-terrorism are also cyber-crimes, while cyber-crimes are less certainly acts of terrorism. It is a simple definition fitting most situations, and more specific compared to Symantec Corporation's definition. The definition, as in several earlier examples, is limited to Internet-related crimes, where the NICCS definition of cyberspace clarifies the Internet is just one part of the cyberspace whole. Mobile technology is also left out of the definition through this limiting terminology. Finally, a cyber-attacker's target may also be the network medium, while using an attack on computer hardware and software toward the same end. A common example of this is a distributed denial of service (DDOS) attack where malware is hidden within an email attachment. Opening the attachment causes the infected data processing devices, such as a cellphone or virtual computer, to continuously send data across the network and Internet until they become saturated and unable to process further data. The attack took place on a data processing device but ultimately the target was the network medium the data crosses and preventing it from being used.

Scholarly Examples – Cyber-Terrorism

Thomas Chen, Lee Jarvis, and Stuart Macdonald suggest in their book, *Cyberterrorism-Understanding, Assessment, and Response*, "'Cyberterrorism' means conduct involving computer or Internet technology that 1) is carried out for the purpose of advancing a political, religious, racial, or ideological cause; 2) is intended to intimidate a section of the public, or compel a government to do or abstain from doing any act; and 3) intentionally causes serious interference with an essential service, facility or system, if such interference is likely to endanger life or cause significant economic or environmental damage."[37] This definition limits itself to only computer and Internet technology, which is only a partial representation of cyberspace, as stated in earlier examples. A positive aspect of the definition, which is based on legal definitions of terrorism from the UK, Australia, New Zealand, and Canada, is it incorporates the intention and goal of cyber-terrorism, which is important in distinguishing it from cyber-crime.

Maurice Dawson and Marawn Omar in their book, *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, defines cyber-terrorism as, “Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies.”[38] This definition primarily focuses on the cyber-attack aspect, while ignoring the intentions of the attacks to affect the behavior of a targeted group, such as a nation’s government. Disruption of the network is also only a single method terrorists may employ in a cyber-attack, which may also include stealing data without disrupting the network with the intent of causing embarrassment or distrust. Also missing is the long-term goal of the attacker toward a political, religious, social, or ideological cause. This definition would be closer to a cyber-crime definition, though it would still contain inconsistencies.

Scholarly Examples – Cyber-Crime

Andrew Colarik and Lech Janczewski in their book, *Cyber Warfare and Cyber Terrorism*, suggest defining cyber-crime as, “any illegal act involving a computer and all activities done with criminal intent in cyberspace or which are computer-related.”[39] The definition’s focus on computers and computer-related criminal intent limits its ability to adequately define cyber-crime. When this book was published in 2008, the computer was generally the primary device in cyberspace. Soon after, mobile technology and networking capabilities would begin to experience a substantial expansion, ultimately changing the concept of personal computing and information access. Criminal intent might also be a limiting term because some cyber-crimes may be carried out unintentionally.[40] A modern example of a growing area of concern is the use of mobile phones to send sexually explicit images, known as 'sexting.' When the senders and receivers are underage, this can unintentionally become a case of child pornography possession and distribution; a cyber-crime.[41] Even accessing an establishment's wireless network as anyone other than an actual customer could be an offense resulting in incarceration, as it may violate computer security laws in certain US states.[42] Bullying, harassing, and stalking in cyberspace can also be unintentional cyber-crimes, depending on both the laws of the states they occurred in and the intensity of the activities.[43]

In his book, "*Cybercrime and Cyberwarfare,"* Igor Bernik provides a less-complex definition for cyber-crime, "Cybercrime is the use of ICTs [information and communication technology] to carry out criminal, harmful and immoral acts in cyberspace." Though it is a short definition, it is quite effective through its broader terminology such as "information and computer technology."[44] The simplicity also applies across multiple legal systems, as it avoids specifying criminal activities, which may potentially differ between nations and states within nations. The definition also provides some characteristics of cyber-crime, which may be used in building parameters to distinguish it from cyber-terrorism.

United States Code References

Title 18 of the *US Code* (USC), "Crimes and Criminal Procedures," provides the legal context for distinguishing cyber-terrorism and cyber-crime. Although there is no separate definition for cyber-terrorism, USC Title 18 does provide a definition for "terrorism." This definition, located under Part I, "Chapter 113B-Terrorism", "Section 2331-Definitions," states that "international terrorism" are activities that[45]:

> (A) Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
>
> (B) Appear to be intended-
>
> > (i) to intimidate or coerce a civilian population;
> > (ii) to influence the policy of a government by intimidation or coercion; or
> > (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
>
> (C) Occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum….

This section also defines "domestic terrorism," as activities that[46]:

> A) Involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
>
> (B) Appear to be intended-
>
> > (i) to intimidate or coerce a civilian population;
> > (ii) to influence the policy of a government by intimidation or coercion; or
> > (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
>
> (C) Occur primarily within the territorial jurisdiction of the United States.

Both definitions identify the key element of a terrorist's intent to intimidate, coerce, influence, and affect the US civilian population and government. However, there is an inconsistency in this definition. It omits the link of the terrorist's intent to a political, religious, social, or ideological long-term goal. This demonstrates the inconsistency of defining terrorism, and cyber-terrorism, at one of the highest levels of documentation, the laws of the nation.

Cyber-crime is partially defined in Title 18, Part I, "Chapter 47-Fraud and False Statements", "Section 1030 - Fraud and related activity in connection with computers." Example criminal activities under this section include: [47]

(1) …Knowingly accessed a computer without authorization or exceeding authorized access…obtained information that has been determined…to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in…the Atomic Energy Act of 1954,…that…could be used to the injury of the United States, or to the advantage of any foreign nation…;

(2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-

> (A) Information contained in a financial record of a financial institution, or of a card issuer…;
>
> (B) Information from any department or agency of the United States; or
>
> (C) Information from any protected computer;

(3) Intentionally, without authorization…access any nonpublic computer of a department or agency of the United States, accesses such a computer…that is exclusively for the use of the Government of the United States or…is used by or for the Government of the United States and…affects that use by or for the Government of the United States;

(4) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and…furthers the intended fraud and obtains anything of value…;

(5)(A) Knowingly causes the transmission of a program, information, code, or command, and as a result…, intentionally causes damage without authorization, to a protected computer…;

(6) Knowingly and with intent to defraud traffics…in any password or similar information through which a computer may be accessed without authorization, if-

> (A) Such trafficking affects interstate or foreign commerce; or
>
> (B) Such computer is used by or for the Government of the United States;

(7) With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any-

> (A) Threat to cause damage to a protected computer;
>
> (B) Threat to obtain information…or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

> (C) Demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion….

The term "computers" is also defined as, "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."[48] These descriptions provide important differences in cyber-crimes. Instead of intimidation, coercion, influence, and affecting the US civilian population and government, cyber criminals' intent is generally the unauthorized access of computers, data, and obtaining a valued gain from the activity. Terrorists may perform these activities, but it will be intended to influence a population or government toward their long-term goals.

Investigating Cyber-Terrorism and Cyber Crime

The authors of *Cyber Crime and Cyber Terrorism Investigator's Handbook* present the Cyber Investigators Staircase Model (CISM), a logical approach to cyber incident investigations. The six steps of the CISM are: Step 1) Define the Objective, Step 2) Collect as much information as possible and check the accuracy and validity of the information, Step 3) Develop various options and alternatives, Step 4) Evaluate and decide which is the most compelling, Step 5) Make and implement decision, and Step 6) Monitor and evaluate the consequences.[49] Because cyber-terrorism and cyber-crime share similarities concerning investigating incidents and implementing countermeasures, the CISM is applied to both types of investigations. The research also examines additional considerations for investigating cyber-terrorism cases.

In Step 1, the investigation's objective is defined to guide the decision making. Some example objectives may be: 1) Act in the interests of justice, 2) Rigorously pursue all reasonable lines of enquiry, 3) Conduct a thorough investigation, 4) Identify, arrest and charge offenders, 5) Present all evidence to prosecuting authorities.[50] During Step 2, information regarding an incident is gathered such as identifying the victim, the type of attack, when the attack took place, where the attack took place in cyberspace, physical regions involved in the attack, the motivation for the attack, the perpetrator, how the attack took place, the extent of damage, and severity based on Cyber Incident Severity Schema[51] and the *National Cyber Incident Response Plan*. Cyber-terrorism cases would also identify any relations between the perpetrator and a known terrorist organization and/or sponsoring nation. In Step 3, which is similar to course of action (COA) development during Joint Operation Planning Process (JOPP), investigators develop and list out all potential options to respond, recover, and counter a cyber incident, such as implementing tighter security controls, closing network ports, additional training, implementing policy changes, and patching system vulnerabilities.

Like COA analysis, COA comparison, and COA approval within JOPP, Step 4 examines and selects the appropriate alternative or combination of alternatives. Selected alternatives may undergo additional modification as a provision to them being selected, to improve their ability to resolve the incident. Step 5 involves implementing the selected alternatives to execute the selected response/recovery/countermeasures and prosecute the perpetrator(s) to the extent of the applicable laws, and, if required, coordinate with regional partners. Cyber-terrorism cases would also consider appropriate use of instruments of US national power to disrupt cyberspace operations of terrorists linked to the cyber incident. Finally, Step 6 monitors and evaluates the results the selected alternatives and their effectiveness in resolving the incident. Findings during this step, as well as new information uncovered about the cyber incident, could result in plan adjustments.

Potential Definition Parameters

As previously discussed, there are distinctive characteristics between cyber-terrorism and cyber-crime acts. The first is the intent of the cyber-attack. The cyber-crime perpetrator intends to commit a crime in cyberspace for some personnel gain, such as identity information theft to make fraudulent transactions. Alternatively, cyber-terrorists intend to intimidate, coerce, and/or affect the behavior and decisions of a targeted population and its government. Furthermore, the intentions of cyber-terrorists, which may include causing or inciting violence, are linked to a long-term goal related to political, religious, social, or ideological beliefs. Finally, the cyberspace aspect of both terms needs to be inclusive to account for current technologies and capabilities a perpetrator may use to commit these acts. Table 1 and Table 2 respectively, list potential parameters for distinguishing cyber-terrorism and cyber-crime, based on the definitions examined in this research.

Potential Cyber-terrorism Parameter	**Source/Derived From**
The legal context (Intent, conspiracy, just the threat or act?)	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*
Intent, conspiracy, just the threat or act	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*
Cyberspace being either as a weapon or a target (Integrity, Confidentiality, Availability, Process Control)	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*
Violence, or threat of, with far-reaching psychological effects to the targeted group	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*

Coercion/intimidation of government and/or population	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*
The intent combined with the long-term goal	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*
Serious interference with or disruption to an electronic system	UK, Terrorism Act 2000
The long-term goal of the attacker to advance a cause related to political, racial, religious, or ideological cause	UK, Terrorism Act 2000
Attribution to a group with a known terrorist agenda	US DHS *National Cyber Incident Response Plan*
Observed activity by state and non-state actors amounts to degradation or disruption of service	Thomas Chen, Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*
Significant disruption/interference/shutdown of critical infrastructure and essential services to endanger life or cause significant economic or environmental damage	Thomas Chen, Lee Jarvis, and Stuart Macdonald suggest in their book, *Cyberterrorism-Understanding, Assessment, and Response*
The use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services	FBI
Purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda	FBI

Table 1: Potential Parameters for Distinguishing Cyber-Terrorism

Source(s):

[a] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (Waltham, MA: Syngress Publishing, 2014) under “Chapter 2, Definitions of Cyber Terror,” http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680#

[b] Department of Homeland Security (DHS), *National Cyber Incident Response Plan*, December 2016, 38

[c] Federal Bureau of Investigation (FBI), “Cyber Crime,” https://www.fbi.gov/investigate/cyber (accessed 04 July 2017)

[d] Terrorism Act 2000, *UK Legislation*: London, UK, 2000, part I, chapter 11, section 1 http://www.legislation.gov.uk/ukpga/2000/11/section/1 (accessed 08 July 2018)

[e] Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*, (New York, Heidelberg, Dordrecht, London: Springer, 2014), under “Chapter 3 – Understanding, Assessment, and Response,” http://viewer.books24x7.com/assetviewer.aspx?bookid=76631&chunkid=884399569

Potential Cyber-Crime Parameter	Source/Derived From
Criminal use of computer network and/or Internet systems	Convention on Cybercrime Treaty
Computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud	Convention on Cybercrime Treaty
Intentional access without right to the whole part of any computer system	Convention on Cybercrime Treaty
Intentional interception, without right, of non-public transmissions of computer data	Convention on Cybercrime Treaty
Intentional damage, deletions, deterioration, alteration, or suppression of computer data without right	Convention on Cybercrime Treaty
Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering, or suppressing computer data	Convention on Cybercrime Treaty
A crime that has some kind of computer or cyber aspect to it	Convention on Cybercrime Treaty
Use of computer systems to store and distribute racist and xenophobic material	Convention on Cybercrime Treaty
The production, sale, procurement for use, importation, or distribution of devices designed to commit any of the above crimes, or of passwords or similar data used to access computer systems	Convention on Cybercrime Treaty
Use of the Internet to commit or facilitate the commission of a crime, including the communication of false or fraudulent representations to consumers	US DOJ
Sophisticated attacks against computer hardware and software	Interpol
Traditional crime utilizing the Internet	Interpol
Any crime that is committed using a computer network or hardware device	Symantec Corporation

Knowingly accessed a computer without authorization or exceeding authorized access…obtained information that has been determined…to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in…the Atomic Energy Act of 1954,…that…could be used to the injury of the United States, or to the advantage of any foreign nation	*US Code*
Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains- (A) Information contained in a financial record of a financial institution, or of a card issuer…; (B) Information from any department or agency of the United States; or (C) Information from any protected computer;	*US Code*
Intentionally, without authorization…access any nonpublic computer of a department or agency of the United States, accesses such a computer…that is exclusively for the use of the Government of the United States or…is used by or for the Government of the United States and…affects that use by or for the Government of the United States	*US Code*
Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and…furthers the intended fraud and obtains anything of value…;	*US Code*
Knowingly causes the transmission of a program, information, code, or command, and as a result…, intentionally causes damage without authorization, to a protected computer…;	*US Code*

Knowingly and with intent to defraud traffics…in any password or similar information through which a computer may be accessed without authorization, if- (A) Such trafficking affects interstate or foreign commerce; or (B) Such computer is used by or for the Government of the United States;	*US Code*
With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any- (A) Threat to cause damage to a protected computer; (B) Threat to obtain information…or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or (C) Demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion….	*US Code*

Table 2: Potential Parameters for Distinguishing Cyber-Crime

Source(s):

[a] Council of Europe, Convention on Cybercrime, Treaty No. 185, 23 November 2001, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[b] Department of Justice, "Cybercrime," https://www.fbi.gov/investigate/cyber (accessed 04 July 2017)
[c] Fraud and False Statements Act, *US Code*, Part I, Chapter 47, secs. 1030, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim
[d] Interpol. "Cybercrime," https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime# (accessed 05 July 2017)
[e] Symantec Corporation, "What is Cybercrime?," https://us.norton.com/cybercrime-definition (accessed 04 July 2017)

Alternatives

Rather than distinguish between cyber-terrorism and cyber-crime, there is the suggestion to remove the term "cyber-terrorism" all together. A perspective on this focuses on the common understanding terrorism involves acts or threats of violence, which has not occurred as a result of any recent cyber-attacks. Joshua Green in his *Washington Monthly* article, "The myth of cyberterrorism: there are many ways terrorists can kill you—computers aren't one of them," states, "There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying."[52] Though much of this statement was true in 2002, when many households were still on dial-up Internet access connections while cable and digital subscriber line (DSL) access were still in development, it does make some incorrect assumptions. The first is the Internet is no longer the only means of connecting to cyberspace, highlighted often in this research, along with the advent of mobile technology. The article also did not foresee the extent cyberspace continues to become a major part for nearly all aspects of human life. Likewise, hackers have evolved from simply flooding servers with emails or defacing web pages, to stealing identity information and corporate data. Ultimately, this article considerably underestimated human imagination. For instance, similar to the 2014 Jeep Cherokee hacking experiment, One Worlds Labs security researcher, Chris Roberts, was reported to be under investigation by the FBI for hacking an airline aircraft in-flight entertainment (IFE) system enabling him to overwrite code to the Thrust Management System, allowing him to issue a climb command and briefly alter the aircraft's course.[53] While the circumstances of the events are still under investigation, the vulnerability in the system is still real and presents a potential means for cyber-terrorism to create acts of, or threats of, violence against human lives.

Symantec Corporation researchers in their white paper, *Cyberterrorism?*, similarly questions the use of the term "to describe just any sort of threat or crime carried out with or against computers in general."[54] The authors' reason it is unnecessary to create a special name for a target or tool of terrorist attack. The example provided in the paper is the term "icepick terrorism" is not used to define bombings against icepick factories or terrorist acts carried out using icepicks. They also state the term would create a situation where cyber-terrorism would be handled separately from regular terrorism, fragmenting defenses to the terrorist's advantage. This is also echoed by Michael Stohl in his paper "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?," by stating the need to, "restrict cyber terrorism to activities which in addition to their cyber component have the commonly agreed upon components of terrorism."[55] In this way, a separate definition is not necessary because cyber terrorist attacks already come under the definition as a means of terrorism.

Regarding this recommendation, there are three issues that may not have been considered by the researchers. First, cyberspace is more than a tool like a bomb a terrorist uses for an attack; it is a domain, encompassing unique dynamics and interactions requiring specialized skill to fully utilize. The terrorist may use it as a weapon with little technical skill, but greater technical skill is required to create comprehensive countermeasures to respond to attacks and preemptive capabilities to prevent them from happening. For example, a terrorist may acquire a user's password through a spear phishing email formatted exactly like one sent from a system administrator. The amount of technical skill needed to recreate this format is minimal since it is just a matter of formatting an email message. However, preventing and countering may be accomplished through technically intricate behavioral-based firewalls, which learn a user's standard behavior and generate alerts during any variations. Understanding the intricacies of the technical aspects of cyber-terrorism makes it "qualitatively different"[56] from terrorism.

Consider the general definition of terrorism, which involves acts of violence, or threats of, to affect a group toward a long-term goal. Cyber-terrorism may involve acts or threats of violence; however, non-violent cyber-attacks may have equally strong effects on a population or government, such as an attack, or threat to attack, infrastructure (e.g., power grid) or economic centers (e.g., stock exchange). Neither situatiuon directly involves violence but the psychological aspects alone could be enough to cause the panic desired to affect behavioral change. In this way, cyber-terrorism becomes distinct from terrorism. A real-world example of a non-violent cyber-attack currently being investigated involved operatives planting "reports that that the Qatari emir had praised Hamas and called Iran 'an Islamic power,' and that Qatar had paid nearly a billion dollars in ransom to al Qaeda for the release of a Qatari hunting party."[57] This "fake news" ultimately damaged the image and reputations of Qatar and its government, straining relations with the US and Gulf nations.

Finally, as demonstrated in the previous examples, the term "cyber-terrorism" is already in the vocabulary of the US general population and government. It is being and will continue to be used to describe acts of terrorism in cyberspace. Opting to not use the term could create a knowledge and language gap between communities who should be united in countering and preventing acts of terror in cyberspace. All elements involved should use the same language and terminology. The optimal time to stop the use of the term "cyber-terrorism" would have been in the 1980s when it was first being conceptualized, 2017 is too late. Instead, efforts should focus on building a universal understanding of the terminology in existence.

Conclusions

This research presented a variety of definitions for both cyber-terrorism and cyber-crime, from organizations and individuals within and outside the US. An essential key element in distinguishing between cyber-terrorism from cyber-crime is the long-term goal of the cyber-attacker. Cyber-terrorism intends to influence the decisions and actions of its target, often involving a nation's government and population. Cyber-attacks may cause confusion, fear, and distrust through data manipulation to create narratives favoring the terrorist's cause, accessing and revealing non-public data, or controlling data to affect a nation's way of life, such as disrupting infrastructure. All of the activities are subsequently linked to the terrorist's long-term political, religious, social, or ideological goals. Cyber-crime, on the hand, may involve similar cyber-attacks; however, the long-term impacts, if any, tend to achieve some form of personal profit or gratification to the perpetrator.[58]

This distinction is important when responding to cyber-attacks because it involves different aspects of US law, which includes Title 18 of the *US Code*. In cyber-crime investigations, law enforcement agencies like the FBI will play a leading role in catching and prosecuting perpetrators, as is their responsibility. However, cyber-crime activities supporting terrorists' long-term goals will involve organizations like the DOD who are charged with protecting the nation's security.

Finally, definitions of cyber-terrorism and cyber-crime often contain inconsistencies in the technology involved. In several definitions, attacks were limited to computers and the Internet. However, these definitions only partially represent cyberspace, which includes Internet, telecommunications networks, computer systems, and embedded processors and controllers.[59]

Mobile technology and networks are often missed by these definitions, which continue to increase in significance in the everyday lives of humans.

Recommended Definition Parameters

Based on the conclusions, this research recommends the US Air Force and DOD pursue further studies into cyber-terrorism and cyber-crime to increase their understanding. The Joint Staff would lead and coordinate these studies with the military Services, US government agencies, academic institutions, and industry partners to ensure a suitable mix of perspectives to aid forging a DOD definition for "cyber-terrorism" for improved communication. In the interest of developing this definition, the research recommends the following parameters for defining cyber-terrorism (Table 3) and cyber-crime (Table 4), which have been adjusted to address the inconsistencies recognized during the analysis.

Recommended Cyber-terrorism Parameter	Derived From
Intent to cause fear, uncertainty, and distrust to coerce a population and/or government.	FBI Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*
Intent advances a long-term political, social, religious, or ideological agenda.	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook* UK, Terrorism Act 2000 FBI
Uses information technology infrastructure to disrupt, interfere, control, or shutdown critical infrastructure and essential services to endanger life or cause significant economic or environmental damage.	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook* Thomas Chen, Lee Jarvis, and Stuart Macdonald suggest in their book, *Cyberterrorism-Understanding, Assessment, and Response*

Uses information technology infrastructures to illegally compromise non-public data integrity, confidentiality, and availability to coerce a population and/or government.	Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook* FBI
Information technology includes: an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.	Title 18, Part I, "Chapter 47-Fraud and False Statements", "Section 1030 - Fraud and related activity in connection with computers."
Information technology infrastructure includes Internet, telecommunications networks, mobile networks, computer systems, and embedded processors and controllers.	NICCS

Table 3: Recommended Parameters for Distinguishing Cyber-Terrorism

Source(s):

[a] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (Waltham, MA: Syngress Publishing, 2014) under "Chapter 2, Definitions of Cyber Terror," http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680#

[b] Department of Homeland Security (DHS), *National Cyber Incident Response Plan*, December 2016, 38

[c] Fraud and False Statements Act, *US Code*, Part I, Chapter 47, secs. 1030, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim

[d] Federal Bureau of Investigation (FBI), "Cyber Crime," https://www.fbi.gov/investigate/cyber (accessed 04 July 2017)

[e] National Initiative for Cybersecurity Careers and Studies (NICCS). "Glossary." https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017)

[f] Terrorism Act 2000, *UK Legislation*: London, UK, 2000, part I, chapter 11, section 1 http://www.legislation.gov.uk/ukpga/2000/11/section/1 (accessed 08 July 2018)

[g] Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*, (New York, Heidelberg, Dordrecht, London: Springer, 2014), under "Chapter 3 – Understanding, Assessment, and Response," http://viewer.books24x7.com/assetviewer.aspx?bookid=76631&chunkid=884399569

Table 3 contains some adjustments to the proposed parameters from Table 1. Several parameters examined in this research contain redundant elements, allowing them to be combined in Table 3, such as those relating to intent and long-term goal of terrorists. Regarding the long-term goal of terrorism, the word “social” replaced the word “racial” to widen the scope to include issues such as economic and wealth distribution alongside racial issues. Table 3 also uses the term “information technology,” which is adapted from the *US Code* definition for “computers.” The term “computer” generally brings to mind the desktop and laptop computers. The term “information technology” is more inclusive of new technologies found in mobile devices, vehicles, medical equipment, etc. Table 3 also uses the term “information technology infrastructure,” to align with “information technology” and the NICCS definition of cyberspace. Finally, parameters related to “attributing cyber-attacks to terrorist groups or organizations” was removed as it is unnecessary in distinguishing the “acts” of cyber-terrorism from those of cyber-crime. A cyber-attacker performing an attack as an operative of a terrorist organization or a sympathetic non-member motivated by the group’s goals to independently act would still be considered acts of cyber-terrorism. Even an anonymous cyber-attack threatening further attacks if certain conditions are not met would still be considered cyber-terrorism, if those conditions relate to a long-term political, social, religious, or ideological goal.

Recommended Cyber-Crime Parameter	Derived From
Information technology intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.	Convention on Cybercrime Treaty
Intentional interception, without right, of non-public transmissions of information technology data.	Convention on Cybercrime Treaty
Intentional damage, deletions, deterioration, alteration, or suppression of information technology data without right.	Convention on Cybercrime Treaty

Intentional and serious hindering, without authorization, the function of or damaging an information technology system by inputting, transmitting, damaging, deleting, deterioration, altering, or suppressing information technology data.	Convention on Cybercrime Treaty *US Code*
Use of information technology to store and distribute racist and xenophobic material.	Convention on Cybercrime Treaty
The production, sale, procurement for use, importation, or distribution of devices designed to commit cyber-crimes, or of passwords or similar data used to access information technology systems with intent to defraud and without authorization.	Convention on Cybercrime Treaty *US Code*
Use of the information technology and/or information technology infrastructure to commit or facilitate the commission of a crime, including the communication of false or fraudulent representations to consumers and producers of goods and services.	Convention on Cybercrime Treaty US DOJ
Knowingly accessed information technology without authorization or exceeding authorized access any information technology system obtained information that has been determined…to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in the Atomic Energy Act of 1954, that could be used to the injury of the United States, or to the advantage of any foreign nation.	*US Code*
Intentionally accesses information technology without authorization or exceeds authorized access, and thereby obtains- (A) Information contained in a financial record of a financial institution, or of a card issuer…; (B) Information from any department or agency of the United States; or (C) Information from any protected information technology.	*US Code*

Intentionally, without authorization access any nonpublic computer of a department or agency of the United States, accesses information technology that is exclusively for the use of the Government of the United States or is used by or for the Government of the United States and affects that use by or for the Government of the United States.	*US Code*
Knowingly and with intent to defraud, accesses a protected information technology without authorization, or exceeds authorized access, and furthers the intended fraud and obtains anything of value.	*US Code*
With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any- (A) Threat to cause damage to protected information technology; (B) Threat to obtain information…or to impair the confidentiality of information obtained from protected information technology without authorization or by exceeding authorized access; or (C) Demand or request for money or other thing of value in relation to damage to a protected information technology, where such damage was caused to facilitate the extortion.	*US Code*
"Information technology" includes: an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.	Title 18, Part I, "Chapter 47-Fraud and False Statements", "Section 1030 - Fraud and related activity in connection with computers."
"Protect information technology" includes: (A) Exclusively for the use of a financial institution or the United States Government, or, in the case of information technology not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the	Title 18, Part I, "Chapter 47-Fraud and False Statements", "Section 1030 - Fraud and related activity in connection with computers."

offense affects that use by or for the financial institution or the Government; or (B) Which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.	
"Information technology infrastructures" includes: Internet, telecommunications networks, mobile networks, computer systems, and embedded processors and controllers.	NICCS

Table 4: Recommended Parameters for Distinguishing Cyber-Crime

Source(s):

[a] Council of Europe, Convention on Cybercrime, Treaty No. 185, 23 November 2001, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[b] Department of Justice, "Cybercrime," https://www.fbi.gov/investigate/cyber (accessed 04 July 2017)
[c] Fraud and False Statements Act, *US Code*, Part I, Chapter 47, secs. 1030, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim
[d] National Initiative for Cybersecurity Careers and Studies (NICCS). "Glossary." https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017)

Table 4 removes the Symantec Corporation's cyber-crime definition because of its simplified content, and limitation to computer networks and hardware devices. As stated in the analysis, this definition omitted mobile networks and software means of committing crimes in cyberspace, such as viruses, worms, and ransomware. Similarly, the Interpol cyber-crime definition was removed from the table because of its limit to the Internet and computer hardware and software. As previously stated in the research analysis, the Internet is one part of the cyberspace whole, which also includes telecommunications networks, mobile networks, computer systems, and embedded processors and controllers.[60] The term "computer" generally brings to mind the desktop and laptop computers. As in Table 3, the term "information technology" is utilized in Table 4 because it is more inclusive of new technologies, such as mobile devices, vehicles, and medical equipment. Table 4 also uses the term "information technology infrastructure," to align with this terminology and the NICCS definition of cyberspace. Finally, the redundant parameters were combined or eliminated between the remaining proposed parameters.

CONCLUSION

This research presented various definitions for both cyber-terrorism and cyber-crime, from organizations and individuals within and outside the US. The research also identified inconsistencies among these definitions such as missing key elements and technical terminology, along with an examination of the distinctions involved in investigating cyber-attacks within the legal context of US and international law. The research then assessed the alternative of removing the term "cyber-terrorism" while advocating continued efforts to define the term. Finally, the study developed potential parameters to distinguish cyber-terrorism and cyber-crime based on sources identified in the analysis to create a list of recommended parameters. The expectation is this research and the recommended parameters will stimulate further efforts toward comprehensively accepted definitions of both terms.

ENDNOTES

[1] Joint Special Operations University (JSOU), *Special Operations Research Topics 2017*, JSOU Press, (MacDill AFB: FL, 2017), 2

[2] National Initiative for Cybersecurity Careers and Studies (NICCS), "Glossary," https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017).

[3] Thomas M. Chen, *Cyberterrorism after Stuxnet*, (Carlisle Barracks, PA: Strategic Studies Institute and the U.S. Army War College Press, June 2014), 2.

[4] Joshua Green, "The myth of cyberterrorism: there are many ways terrorists can kill you—computers aren't one of them," *Washington Monthly*, 01 November 2002, https://www.thefreelibrary.com/The+myth+of+cyberterrorism%3A+there+are+many+ways+terrorists+can+kill...-a094775087.

[5] Andy Greenberg. "The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse," *Wired*, 01 August, 2016, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

[6] Andrew M. Colarik and Lech Janczewski, *Cyber Warfare and Cyber Terrorism*, (Hershey, PA and London, United Kingdom: Information Science Reference (an imprint of IGI Global), 2008) 2.

[7] Jonathan Zittrain and Molly Sauter, "Everything You Need to Know About Wikileaks," *MIT Technology Review*, 09 December 2010, "https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks/"

[8] Robb David, "The Sony Hack One Year Later: Just Who Are The Guardians Of Peace?," *ABC*, 24 November 2015.

[9] Tom Hamburger and Karen Tumulty, "WikiLeaks releases thousands of documents about Clinton and internal deliberations", *The Washington Post*, 22 July 2016.

[10] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (Waltham, MA: Syngress Publishing, 2014) under "Chapter 2, Definitions of Cyber Terror," http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680#.

[11] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (Waltham, MA: Syngress Publishing, 2014) under "Chapter 2, Definitions of Cyber Terror," http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680#.

[12] Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-07.2: Antiterrorism, 14 March 2014, I-1.

[13] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 2: Definitions of Cyber Terrorism, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680&resume=yes&resumebookmarkid=57901e94-2b5c-e711-a4ad-00505686029a).

[14] Declaratory Judgement Act, *US Code*, Vol. 22, secs 2656f (1952).

[15] Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, July 2017, https://jdeis.js.mil/jdeis/new_pubs/dictionary.pdf.

[16] National Initiative for Cybersecurity Careers and Studies (NICCS), "Glossary," https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017).

[17] William L. Tafoya, Ph.D. "Cyber Terror," FBI Law Enforcement Bulletin, November 2011, https://leb.fbi.gov/2011/november/cyber-terror

[18] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 2: Definitions of Cyber Terrorism, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680&resume=yes&resumebookmarkid=57901e94-2b5c-e711-a4ad-00505686029a).

[19] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 2: Definitions of Cyber Terrorism, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680&resume=yes&resumebookmarkid=57901e94-2b5c-e711-a4ad-00505686029a).

[20] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 2: Definitions of Cyber Terrorism, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680&resume=yes&resumebookmarkid=57901e94-2b5c-e711-a4ad-00505686029a).

[21] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 2: Definitions of Cyber Terrorism, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680&resume=yes&resumebookmarkid=57901e94-2b5c-e711-a4ad-00505686029a).

[22] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 2: Definitions of Cyber Terrorism, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=444787680&resume=yes&resumebookmarkid=57901e94-2b5c-e711-a4ad-00505686029a).

[23] Federal Bureau of Investigation (FBI), "Cyber Crime," https://www.fbi.gov/investigate/cyber (accessed 04 July 2017).

[24] Federal Bureau of Investigation (FBI), "Cyber Crime," https://www.fbi.gov/investigate/cyber (accessed 04 July 2017).

[25] Department of Justice, "Cybercrime," https://www.fbi.gov/investigate/cyber (accessed 04 July 2017).

[26] Symantec Corporation, "What is Cybercrime?," https://us.norton.com/cybercrime-definition (accessed 04 July 2017).

[27] Terrorism Act 2000, *UK Legislation*: London, UK, 2000, part I, chapter 11, section 1 http://www.legislation.gov.uk/ukpga/2000/11/section/1 (accessed 08 July 2018).

[28] Terrorism Act 2000, *UK Legislation*: London, UK, 2000, part I, chapter 11, section 1 http://www.legislation.gov.uk/ukpga/2000/11/section/1 (accessed 08 July 2018).

[29] Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*. New York, Heidelberg, Dordrecht, London: Springer, 2014, under "Chapter 1 - What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions

of Terrorism" under "1.2 Cyberterrorism in Legal Definitions of Terrorism http://viewer.books24x7.com/assetviewer.aspx?bookid=76631&chunkid=385190652&resumebookmarkid=065130d5-0061-e711-a4ad-00505686029a

[30] Babak Akhgar, Andrew Staniforth, and Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Waltham, MA: Syngress Publishing, 2014), under "Chapter 12 - Cybercrime Classification and Characteristics," http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=776274446&resumebookmarkid=df2c2ae3-255c-e711-a4ad-00505686029a#.

[31] Council of Europe, Convention on Cybercrime, Treaty No. 185, 23 November 2001, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[32] Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Treaty No. 189, 28 January 2003, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f.

[33] Declan McCullagh, "Senate ratifies controversial cybercrime treaty," *CNET*, 2006, https://www.cnet.com/news/senate-ratifies-controversial-cybercrime-treaty/.

[34] Declan McCullagh, "Senate ratifies controversial cybercrime treaty," *CNET*, 2006, https://www.cnet.com/news/senate-ratifies-controversial-cybercrime-treaty/.

[35] Interpol. "Cybercrime," https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime# (accessed 05 July 2017).

[36] Interpol. "Cybercrime," https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime# (accessed 05 July 2017).

[37] Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*, (New York, Heidelberg, Dordrecht, London: Springer, 2014), under "Chapter 3 – Understanding, Assessment, and Response," http://viewer.books24x7.com/assetviewer.aspx?bookid=76631&chunkid=884399569.

[38] Maurice Dawson and Marwan Omar, *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, (Hershey, PA: Information Science Reference (an imprint of IGI Global), 2015), under "Key Terms and Definitions", http://viewer.books24x7.com/assetviewer.aspx?bookid=83474&chunkid=864402330&resume=yes&resumebookmarkid=fd8cc4c3-282f-e711-81ef-00505686029a.

[39]Andrew M. Colarik and Lech Janczewski, *Cyber Warfare and Cyber Terrorism*, (Hershey, PA and London, United Kingdom: Information Science Reference (an imprint of IGI Global), 2008), 438.

[40] Law Offices of Edwards & Mason, "5 Cyber Crimes You May be Committing Without Knowing it," https://www.lawfl.net/5-cyber-crimes-you-may-be-committing-without-knowing-it.html, (accessed 20 July 2017).

[41] Law Offices of Edwards & Mason, "5 Cyber Crimes You May be Committing Without Knowing it," https://www.lawfl.net/5-cyber-crimes-you-may-be-committing-without-knowing-it.html, (accessed 20 July 2017).

[42] Law Offices of Edwards & Mason, "5 Cyber Crimes You May be Committing Without Knowing it," https://www.lawfl.net/5-cyber-crimes-you-may-be-committing-without-knowing-it.html, (accessed 20 July 2017).

[43] Law Offices of Edwards & Mason, "5 Cyber Crimes You May be Committing Without Knowing it," https://www.lawfl.net/5-cyber-crimes-you-may-be-committing-without-knowing-it.html, (accessed 20 July 2017).

[44] Igor Bernik, *Cybercrime and Cyberwarfare*, (London, United Kingdom: ISTE Ltd), (New Jersey, United States: John Wiley and Sons, Inc.), 2014, under "Chapter 1 – Cybercrime", "Overview," http://viewer.books24x7.com/assetviewer.aspx?bookid=62616&chunkid=885755298&rowid=17#.

[45] Terrorism Act, *US Code*, Part I, Chapter 113B, secs. 2331, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter113B&edition=prelim.

[46] Terrorism Act, *US Code*, Part I, Chapter 113B, secs. 2331, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter113B&edition=prelim.

[47] Fraud and False Statements Act, *US Code*, Part I, Chapter 47, secs. 1030, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim.

[48] Fraud and False Statements Act, *US Code*, Part I, Chapter 47, secs. 1030, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim.

[49] Babak Akhgar, Andrew Staniforth, Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (Waltham, MA: Syngress Publishing, 2014), under "Chapter 4 - Police Investigation Processes—Practical Tools and Techniques for Tackling Cyber Crimes, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=940755909&resumebookmarkid=c1d08b4d-fd71-e711-a4ad-00505686029a.

[50] Babak Akhgar, Andrew Staniforth, Francesca Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook*, (Waltham, MA: Syngress Publishing, 2014), under "Chapter 4 - Police Investigation Processes—Practical Tools and Techniques for Tackling Cyber Crimes, http://viewer.books24x7.com/assetviewer.aspx?bookid=70001&chunkid=940755909&resumebookmarkid=c1d08b4d-fd71-e711-a4ad-00505686029a.

[51] Department of Homeland Security (DHS), *National Cyber Incident Response Plan*, December 2016, 38

[52] Joshua Green, "The myth of cyberterrorism: there are many ways terrorists can kill you—computers aren't one of them, " *Washington Monthly*, 01 November 2002. https://www.thefreelibrary.com/The+myth+of+cyberterrorism%3A+there+are+many+ways+terrorists+can+kill...-a094775087.

[53]Kim Zetter. "Feds Say That Banned Researcher Commandeered a Plane," *Wired*, 15 May 2015 https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

[54] Sarah Gordon and Richard Ford, Ph.D., *Cyberterrorism?*, Symantec Corporation white paper. Cupertino, CA: Symantec Corporation, 2003, 13, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

[55] Michael Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?," (Netherlands: Springer Science + Business Media B.V., 2007), 231, https://link.springer.com/content/pdf/10.1007/s10611-007-9061-9.pdf.

[56] Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*, (New York, Heidelberg, Dordrecht, London: Springer, 2014), under "Chapter 9 - The Criminalisation of Terrorists' Online Preparatory Acts," http://viewer.books24x7.com/assetviewer.aspx?bookid=76631&chunkid=884399569

[57] Robert Windrem and William M. Arkin, "Who Planted the Fake News at Center of Qatar Crisis?," *NBC*, 18 July 2017, http://www.nbcnews.com/news/world/who-planted-fake-news-center-qatar-crisis-n784056.

[58] Maria Manuela Cruz-Cunha and Irene Maria Portela. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, under "Chapter 13- Cybercrimes Technologies

and Approaches. Hershey, PA: Information Science Reference (an imprint of IGI Global), 2015, http://viewer.books24x7.com/assetviewer.aspx?bookid=73011&chunkid=734082718.

[59] National Initiative for Cybersecurity Careers and Studies (NICCS), "Glossary," https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017).

[60] National Initiative for Cybersecurity Careers and Studies (NICCS). "Glossary." https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017).

BIBLIOGRAPHY

Akhgar, Babak, Andrew Staniforth, Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Waltham, MA: Syngress Publishing, 2014.

Bernik, Igor. *Cybercrime and Cyberwarfare*, (London, United Kingdom: ISTE Ltd), (New Jersey, United States: John Wiley and Sons, Inc.), 2014.

Chairman of the Joint Chiefs of Staff. Joint Publication (JP) 3-07.2: *Antiterrorism*. 14 March 2014.

Chairman of the Joint Chiefs of Staff. *DOD Dictionary of Military and Associated Terms*. July 2017, https://jdeis.js.mil/jdeis/new_pubs/dictionary.pdf.

Chen, Thomas M. *Cyberterrorism after Stuxnet*. Carlisle Barracks, PA: Strategic Studies Institute and the U.S. Army War College Press, June 2014, 2.

Chen, Thomas M., Lee Jarvis, and Stuart Macdonald, ed. *Cyberterrorism-Understanding, Assessment, and Response*. New York, Heidelberg, Dordrecht, London: Springer, 2014.

Colarik, Andrew M. and Lech Janczewski. *Cyber Warfare and Cyber Terrorism*. Hershey, PA and London, United Kingdom: Information Science Reference (an imprint of IGI Global), 2008.

Council of Europe. Convention on Cybercrime. Treaty No. 185, 23 November 2001. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

Council of Europe. Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. Treaty No. 189, 28 January 2003. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f.

Cruz-Cunha, Maria Manuela and Irene Maria Portela. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, under "Chapter 13- Cybercrimes Technologies and Approaches. Hershey, PA: Information Science Reference (an imprint of IGI Global), 2015.

David, Robb. "The Sony Hack One Year Later: Just Who Are The Guardians Of Peace?" *ABC*, 24 November 2015.

Dawson, Maurice and Marwan Omar. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. Hershey, PA: Information Science Reference (an imprint of IGI Global), 2015.

Department of Homeland Security (DHS). *National Cyber Incident Response Plan*. December 2016.

Department of Justice. "Cybercrime." https://www.fbi.gov/investigate/cyber (accessed 04 July 2017).

Federal Bureau of Investigation (FBI). “Cyber Crime.” https://www.fbi.gov/investigate/cyber (accessed 04 July 2017).

Fraud and False Statements Act, *US Code*, Part I, Chapter 47, secs. 1030, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter47&edition=prelim.

Gordon, Sarah and Richard Ford, Ph.D. *Cyberterrorism?*. Symantec Corporation white paper. Cupertino, CA: Symantec Corporation, 2003, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.

Green, Joshua. “The myth of cyberterrorism: there are many ways terrorists can kill you—computers aren't one of them.” *Washington Monthly*, 01 November 2002. https://www.thefreelibrary.com/The+myth+of+cyberterrorism%3A+there+are+many+ways+terrorists+can+kill...-a094775087.

Greenberg, Andy. “The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse.” *Wired*. 01 August, 2016. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

Hamburger, Tom Hamburger and Karen Tumulty. “WikiLeaks releases thousands of documents about Clinton and internal deliberations.” *The Washington Post*, 22 July 2016.

Interpol. “Cybercrime,” https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime# (accessed 05 July 2017).

Joint Special Operations University (JSOU). *Special Operations Research Topics 2017*. JSOU Press. MacDill AFB: FL, 2017.

Law Offices of Edwards & Mason. “5 Cyber Crimes You May be Committing Without Knowing it.” https://www.lawfl.net/5-cyber-crimes-you-may-be-committing-without-knowing-it.html, (accessed 20 July 2017).

McCullagh, Declan. “Senate ratifies controversial cybercrime treaty.” *CNET*, 2006, https://www.cnet.com/news/senate-ratifies-controversial-cybercrime-treaty/.

National Initiative for Cybersecurity Careers and Studies (NICCS). “Glossary.” https://niccs.us-cert.gov/glossary#C (accessed 14 July 2017).

Stohl, Michael. “Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?” Netherlands: Springer Science + Business Media B.V., 2007 https://link.springer.com/content/pdf/10.1007/s10611-007-9061-9.pdf.

Symantec Corporation. “What is Cybercrime?” https://us.norton.com/cybercrime-definition (accessed 04 July 2017).

Tafoya, William L., Ph.D. “Cyber Terror.” *FBI Law Enforcement Bulletin*, November 2011, https://leb.fbi.gov/2011/november/cyber-terror.

Terrorism Act 2000, *United Kingdom Legislation*: London, UK, 2000. http://www.legislation.gov.uk/ukpga/2000/11/section/1 (accessed 08 July 2018).

Terrorism Act, *US Code*, Part I, Chapter 113B, secs. 2331, (1948), http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter113B&edition=prelim.

Windrem, Robert and William M. Arkin. “Who Planted the Fake News at Center of Qatar Crisis?.” *NBC*, 18 July 2017, http://www.nbcnews.com/news/world/who-planted-fake-news-center-qatar-crisis-n784056.

Zetter, Kim. “Feds Say That Banned Researcher Commandeered a Plane,” Wired, 15 May 2015 https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.