Cyber-Terrorism: Finding a Common Starting Point

By
Jeffrey Thomas Biller
B.A., March 1998, University of Washington
M.H.R., June 2004, University of Oklahoma
J.D., May 2007, University of Kansas

A Thesis submitted to
The Faculty of
The George Washington University Law School
in partial satisfaction of the requirements
for the degree of Master of Laws
May 20, 2012

Thesis directed by
Gregory E. Maggs
Professor of Law, Co-director, National Security and U.S. Foreign Relations Law Program

Acknowledgements
The author appreciates the generous support of the U.S. Air Force JAG Corps for the opportunity to study; Professor Gregory Maggs, for the excellent feedback and guidance; and the author’s family, for the time and occasional solitude to complete this Article.

Disclaimer
Major Jeffrey T. Biller serves in the U.S. Air Force Judge Advocate General’s Corps. This paper was submitted in partial satisfaction of the requirements for the degree of Master of Laws in National Security and Foreign Relations at The George Washington University Law School. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the U.S. Air Force, Department of Defense or the U.S. Government.

Abstract
Cyber-Terrorism: Finding a Common Starting Point
Attacks on computer systems for both criminal and political purposes are on the rise in both the United States and around the world. Foreign terrorist organizations are also developing information technology skills to advance their goals. Looking at the convergence
Cyber-Terrorism: Finding a Common Starting Point

By
Jeffrey Thomas Biller
B.A., March 1998, University of Washington
M.H.R., June 2004, University of Oklahoma
J.D., May 2007, University of Kansas

A Thesis submitted to
The Faculty of
The George Washington University Law School
in partial satisfaction of the requirements
for the degree of Master of Laws
May 20, 2012

Thesis directed by
Gregory E. Maggs
Professor of Law, Co-director, National Security and U.S. Foreign Relations Law Program

Acknowledgements
The author appreciates the generous support of the U.S. Air Force JAG Corps for the opportunity to study; Professor Gregory Maggs, for the excellent feedback and guidance; and the author’s family, for the time and occasional solitude to complete this Article.

Disclaimer
Major Jeffrey T. Biller serves in the U.S. Air Force Judge Advocate General’s Corps. This paper was submitted in partial satisfaction of the requirements for the degree of Master of Laws in National Security and Foreign Relations at The George Washington University Law School. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the U.S. Air Force, Department of Defense or the U.S. Government.

Abstract
Cyber-Terrorism: Finding a Common Starting Point
Attacks on computer systems for both criminal and political purposes are on the rise in both the United States and around the world. Foreign terrorist organizations are also developing information technology skills to advance their goals. Looking at the convergence
of these two phenomena, many prominent security experts in both government and private industry have rung an alarm bell regarding the potential for acts of cyber-terrorism. However, there is no precise definition of cyber-terrorism under U.S. law or in practice among cyber-security academicians. The lack of a common starting point is one of the reasons existing law fails to directly address cyber-terrorism.

This Article furnishes a lexicon of cyber-related malicious activities and argues for a common working definition of cyber-terrorism. This definition can be both incorporated into current counter-terror legislation and used by government agencies to fight cyber-terrorism. This paper arrives at the various definitions proposed by security experts and those in use by governmental organizations. This Article builds on these definitions to arrive at a new definition that is broad while narrow enough to exclude computer network attacks that are attacks this Article finds that, while we have not yet faced a 9/11," and becoming increasingly complex.

Second, analyzing several recent cyber-attacks, this Article finds that, while we have not yet faced a "cyber 9/11," computer network attacks for political purposes are on the rise and becoming increasingly complex. Third, this Article analyzes current law related to both cyber-crimes and terrorism, finding that while these laws are applicable in many instances, they fall short in adequately focusing on the most important factor when addressing cyber-terrorism: prevention. This Article concludes by recommending that cyber-terrorism, as defined in this paper, be incorporated into some of our most frequently used laws to combat terrorism.

INTRODUCTION

"If I had an hour to save the world I would spend 59 minutes defining the problem and one minute finding solutions."1

On January 5, 2012, an Eastern District of Virginia grand jury indicted seven individuals and two corporations, Megaupload Limited and Vestor Limited, with "racketeering conspiracy, conspiring to commit copyright infringement, conspiring to commit money laundering and two substantive counts of criminal copyright infringement." The government based the indictment on the alleged conspirators' business of profiting from users illegally sharing copyrighted music and video files on their website, Megaupload.com.2 The website was one of the most popular on the Internet with approximately 150 million registered users, 50 million hits daily, and endorsements from music superstars earning its founder, Kim Dotcom ("Dotcom"), $42 million in 2011.3

On January 19, 2012, New Zealand police arrived at Dotcom's mansion to arrest him.4 Dotcom retreated into a "safe room" where he had stored weapons, including a sawed-off shotgun.5 The police eventually cut their way into the room and arrested him.6 Following Dotcom's arrest, police arrested three other indicted co-conspirators in Auckland, New Zealand at the United States' request.7 Additionally, police executed more than twenty search warrants in the United States and eight other countries and seized approximately fifty million dollars in assets.8 The action was "among the largest criminal copyright cases ever brought by the United States and directly targets the misuse of a public content storage and distribution site to commit and facilitate intellectual property crime.9 In apparent dissatisfaction with the Megaupload arrests, the hacker group Anonymous launched cyber-attacks against

3. Id. ("[F]or more than five years the conspiracy has operated websites that unlawfully reproduce and distribute infringing copies of copyrighted works . . . on a massive scale.").
5. See Kevin J. O'Brien et al., Flashy Promoter of File-Sharing Captured in New Zealand Raid, INT'L HERALD TRIB., Jan. 21, 2012, at 1 (explaining how Dotcom was arrested).
6. Id.
7. Id.
8. See DOJ Megaupload, supra note 2 ("Dotcom, Batato, Ortmann, and van der Kolk were arrested today in Auckland, New Zealand, by New Zealand authorities, who executed provisional arrest warrants requested by the United States.").
9. Id. (explaining the additional searches and seizures resulting from the Megaupload conspiracy).
10. Id.
11. O'Brien et al., supra note 5.
of these two phenomena, many prominent security experts in both
government and private industry have rung an alarm bell regarding
the potential for acts of cyber-terrorism. However, there is no precise
definition of cyber-terrorism under U.S. law or in practice among
cyber-security academicians. The lack of a common starting point is
one of the reasons existing law fails to directly address cyber-
terrorism.

This Article furnishes a lexicon of cyber-related malicious
activities and argues for a common working definition of cyber-
terrorism. This definition can be both incorporated into current
counter-terror legislation and used by government agencies to
counter cyber-terrorism. This paper arrives at
the various definitions proposed by security experts and those in use
by governmental organizations. This Article builds on these
definitions to arrive at a new definition that is at once broad enough
to cover the potentially unique effects of a weapon of cyber-terrorism,
while narrow enough to exclude computer network attacks that are
relatively minor in nature. Second, analyzing several recent cyber-
attacks, this Article finds that, while we have not yet faced a
“cyber 9/11,” computer network attacks for political purposes are on the rise
and becoming increasingly complex. Third, this Article analyzes
current law related to both cyber-crimes and terrorism, finding that
while these laws are applicable in many instances, they fall short in
adequately focusing on the most important factor when addressing
cyber-terrorism: prevention. This Article concludes by recommending
that cyber-terrorism, as defined in this paper, be incorporated into
some of our most frequently used laws to combat cyber-terrorism.

INTRODUCTION

“If I had an hour to save the world I would spend 59 minutes defining the
problem and one minute finding solutions.”

On January 5, 2012, an Eastern District of Virginia grand jury
indicted seven individuals and two corporations, Megaupload Limited
and Vestor Limited, with “racketeering conspiracy, conspiring to
commit copyright infringement, conspiring to commit money
laundering and two substantive counts of criminal copyright
infringement.” The government based the indictments on the alleged
conspirators’ business of profiting from users illegally sharing

1. Albert Einstein.
2. See Justice Department Charges Leaders of Megaupload with
Widespread Online Copyright Infringement, U.S. DEPT OF JUSTICE
-074.html [hereinafter DOJ Megaupload] (identifying the seven
individuals and two corporations’ charges).

3. Id. (“For more than five years the conspiracy has operated websites
that unlawfully reproduce and distribute infringing copies of copyrighted works . . . on a massive scale.”).
4. See Nick Perry, Popular file-sharing website Megaupload shut down,
USA TODAY (Jan. 20, 2012, 1:00 PM), http://www.usatoday.com/tech/news/story/2012-01-19/megaupload-shuts-down/52675526/1
(“infringement”).
5. Id.
6. Id.
7. Id.
8. See DOJ Megaupload, supra note 2 (“Dotcom, Batato, Ortmann, and
van der Kolk were arrested today in Auckland, New Zealand, by New
Zealand authorities, who executed provisional arrest warrants requested
by the United States.”).
9. Id. (explaining the additional searches and seizures resulting from the
Megaupload conspiracy).
10. Id.
11. O’Brien et al., supra note 5.
the websites of the White House, the U.S. Department of Justice ("DoJ"), the U.S. Copyright Office, and several entertainment companies and trade groups. Across the globe, similar network attacks were up twenty-four percent immediately following the arrests. These actions were crimes, but neither money nor other traditional criminal motives motivated the perpetrators. Anonymous' cyber-attacks were likely politically motivated and geared toward influencing both government and civilian opinion. Should the motivations of such an attack affect how it is classified under the law? Was this a cyber-crime that the law should treat like it an act of civil disobedience? Or, did its political motivations make it a unique form of terrorism? Cyber-crime is now a part of everyday life, and in 2009, caused estimated losses of up to one trillion dollars globally. Given the potential criminal rewards, law enforcement is as unlikely to eliminate cyber-crimes as they are traditional crimes. Lawmakers have attempted to keep pace by enacting statutes such as the Computer Fraud and Abuse Act ("CFAA"), which has been continually updated. Such statutes criminalize offenses that are committed through computers or other information systems located in the United States. However, the Internet's inherent anonymity makes it easy for criminals to act in cyberspace without being caught.

13. See id. (arguing that the FBI may have goaded Anonymous into attacking their website with the arrests following debates about new legislation on Internet piracy in an attempt to turn public support away from Anonymous and similar hacking groups).

14. Id. (identifying the effects of the Megaupload conspiracy).


17. See, e.g., id.

18. See, e.g., Thomas Crampton, Nigeria to battle Internet scams that target its image, N.Y. TIMES (Jan. 23, 2004), http://www.nytimes.com/2004/01/23/business/worldbusiness/23htl-416_0.html (reporting on the infamous Nigerian Internet fraud schemes); accord Semmi Sengupta & Jenna Wortham, U.S. Charges 7 in Online Ad Fraud Scheme, N.Y. TIMES, Nov. 10, 2011, at B1 (describing a recent Internet fraud scheme that diverted marketing revenue to fraudulent sites by replacing real ads with fraudulent ones).

the websites of the White House, the U.S. Department of Justice ("DoJ"), the U.S. Copyright Office, and several entertainment companies and trade groups. Across the globe, similar network attacks were up twenty-four percent immediately following the arrests. These actions were crimes, but neither money nor other traditional criminal motives motivated the perpetrators. Anonymous cyber-attacks were likely politically motivated and geared towards influencing both government and civilian opinion. Should the motivations of such an attack affect how it is classified under the law? Was this a cyber-crime that the law should treat like any other? Was it an act of civil disobedience? Or, did its political motivations make it a unique form of terrorism?

Cyber-crime is now a part of everyday life, and in 2009, caused estimated losses of up to one trillion dollars globally. Given the potential criminal rewards, law enforcement is as unlikely to eliminate cyber-crimes as they are traditional crimes. Lawmakers have attempted to keep pace by enacting statutes such as the Computer Fraud and Abuse Act ("CFAA"), which has been continually updated. Such statutes criminalize offenses that are committed through computers or other information systems located in the United States. However, the Internet's inherent anonymity makes it easy for criminals to act in cyberspace without being caught.

13. See id. (arguing that the FBI may have goaded Anonymous into attacking their website with the arrests following debates about new legislation on Internet piracy in an attempt to turn public support away from Anonymous and similar hacking groups).

14. Id. (identifying the effects of the Megaupload conspiracy).


17. See, e.g., id.

18. See, e.g., Thomas Crampton, Nigeria to battle Internet scams that taint its image, N.Y. TIMES (Jan. 23, 2004), http://www.nytimes.com/2004/01/23/business/worldbusiness/23hit-410_0.html (reporting on the infamous Nigerian Internet fraud schemes); accord Sumnti Senapata & Jenna Wortham, U.S. Charges 7 in Online Ad Fraud Scheme, N.Y. TIMES, Nov. 10, 2011, at B1 (describing a recent Internet fraud scheme that diverted marketing revenue to fraudulent sites by replacing real ads with fraudulent ones).

suggested by academics or in use by government agencies. Section III examines several recent, major cyber-attacks to determine whether they fit this suggested definition of cyber-terrorism. Section IV is an overview of current domestic laws relating to both cyber-crimes and terrorism, and a discussion of the major complications in fighting cyber-terrorism: attribution. Finally, Section V of this Article discusses incorporation of cyber-terrorism into several current counter-terrorism statutes that could be effectively used to prevent cyber-terrorism.

SECTION I: THE CURRENT SITUATION

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy." 24

Attacks on information systems and networks have exponentially increased in the last two decades. 25 A 1996 U.S. Government Accounting Office report found that the Department of Defense (“DOD”) faced 250,000 attempted attacks on its networks in 1995; 26 in 2006 the number had risen to 6 million, 27 and in 2008 the number was more than 300 million. 28 These numbers become staggering when looking beyond the government to other cyber-attacks victims. Seventy-four million people in the United States were victims of cyber-crime in 2010, resulting in an estimated thirty-two billion dollars in financial loss. 29 This Section examines the current threats to information systems and explores how the current approach will be inadequate in preventing a major cyber-attack on the United States.

A. The Current Threat

President Barack Obama has labeled computer network attacks "one of the most serious economic and national security risks we face.

24. President Barack Obama, Remarks by the President on Securing Our Nation’s Cyber Infrastructure, 1 PUB. PAPERS 751 (May 29, 2009).
26. Id. at 3.
28. Id.

JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 4 • NO. 2 • 2013
Cyber-Terrorism: Finding a Common Starting Point

as a nation," 30 and stated, “America’s economic prosperity in the 21st century will depend on cybersecurity." 31 The gravity expressed in these statements, although serious, is mild compared to the fears of cyber-security experts. The leading force among cyber-security experts has been the former chief cyber-security adviser on the National Security Council, Richard Clarke. 32 In his book Cyber War, Clarke describes the potential for “a massive cyberattack on civilian infrastructure that downs power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fire to refineries.” 33 Former Director of National Intelligence and Director of the National Security Agency Mike McConnell stated, “the warnings are over. It could happen tomorrow.” 34 McConnell described the potential for such an attack as impacting the global economy on “an order of magnitude surpassing” the 9/11 attacks. 35

Whether cyber-attacks have the potential to rise to the level just described is certainly debatable. 36 However, cyber-attacks motivated by reasons other than money 37 are becoming more and more

31. Id.
35. Id.
36. See, e.g., Joshua Green, The Myth of Cyberterrorism, WASH. MONTHLY (Nov. 2002), http://www.washingtonmonthly.com/features/2001/0211.green.html (arguing the threat of cyber-terrorism is overhyped and focusing too heavily on cyber-attack will have a negative effect on the information technology industry); see also Derek E. Bambauer, Conundrum, 96 MINN. L. REV. 584, 604, 621 (2011) [hereinafter Bambauer] (arguing that scenes of “cyber-apocalypse” are overblown, but cyber threats are real and that information, not systems should be the focus of cyber-security); but see Richard Clarke, Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks, 12 DEPAUL BUS. L.J. 33, 36-38 (1999-2000) (arguing that large scale cyber-attacks are a distinct possibility and that the best way to respond to cyber-threats is through the development of public-private partnerships).
suggested by academics or in use by government agencies. Section III examines several recent, major cyber-attacks to determine whether they fit this suggested definition of cyber-terrorism. Section IV is an overview of current domestic laws relating to both cyber-crimes and terrorism, and a discussion of the major complication in fighting cyber-terror: attribution. Finally, Section V of this Article discusses incorporation of cyber-terrorism into several current counter-terrorism statutes that could be effectively used to prevent cyber-terrorism.

SECTION I: THE CURRENT SITUATION

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy."

Attacks on information systems and networks have exponentially increased in the last two decades.25 A 1996 U.S. Government Accounting Office report found that the Department of Defense ("DOD") faced 250,000 attempted attacks on its networks in 1995;26 in 2006 the number had risen to 6 million,27 and in 2008 the number was more than 300 million.28 These numbers have staggering when looking beyond the government to other cyber-attacks victims. Seventy-four million people in the United States were victims of cyber-crime in 2010, resulting in an estimated thirty-two billion dollars in financial loss.29 This Section examines the current threats to information systems and explores how the current approach will be inadequate in preventing a major cyber-attack on the United States.

A. The Current Threat

President Barack Obama has labeled computer network attacks "one of the most serious economic and national security risks we face as a nation,"30 and stated, "America’s economic prosperity in the 21st century will depend on cybersecurity."31 The gravity expressed in these statements, although serious, is mild compared to the fears of cyber-security experts. The leading force among cyber-security experts has been the former chief cyber-security adviser on the National Security Council, Richard Clarke.32 In his book Cyber War, Clarke describes the potential for “a massive cyberattack on civilian infrastructure that downs power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fire to refineries."33 Former Director of National Intelligence and Director of the National Security Agency Mike McConnell stated, "[t]he warnings are over. It could happen tomorrow]."34 McConnell described the potential for such an attack as impacting the global economy on an "order of magnitude surpassing" the 9/11 attacks.35 Whether cyber-attacks have the potential to rise to the level just described is certainly debatable.36 However, cyber-attacks motivated by reasons other than money are becoming more and more

25. Id.
29. Id.
30. See, e.g., Joshua Green, The Myth of Cyberterrorism, WASH. MONTHLY (Nov. 2002), http://www.washingtonmonthly.com/features/2001/0211.green.html (arguing the threat of cyber-terrorism is over-hyped and focusing too heavily on cyber-security will have a negative effect on the information technology industry); see also Dorek E. Bambauer, Comandrum, 96 MINN. L. REV. 584, 604, 621 (2011) [hereinafter Bambauer] (arguing that scenes of “cyber-apocalypse” are overblown, but cyber threats are real and that information, not systems should be the focus of cyber-security); but see Richard Clarke, Threats to U.S. National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks, 12 DEPAUL BUS. L.J. 31, 36-38 (1999-2000) (arguing that large scale cyber-attacks are a distinct possibility and that the best way to respond to cyber-threats is through the development of public-private partnerships).
prevalent. The years 2006 to 2010 saw a 650% increase in cyber-attacks on federal agencies. The rise in politically-active hacking groups, such as Anonymous, demonstrates that. The increasing platform for dissenters, both domestic and foreign, to express their disagreement with the government. Espionage on information systems are not immune, as the DOD's classified network was compromised in 2008 by an attack using flash drives. Politically-motivated cyber-attacks are not limited to government websites. Hacking groups have increasingly attacked corporations that have policies with which the groups disagree. Examples of such corporate attacks include a "highly sophisticated" attack on Google in 2010 that originated from China, and numerous coordinated attacks


41. "Air gapped" networks are those physically, electrically, and electromagnetically isolated from other networks such as the Internet. See Oliver Rist, Hack Tales: Air-gap networking for the price of a pair of sneakers, INFOWORLD (May 29, 2006, 2:00 AM), http://www.infoworld.com/d/networking/hack-tales-air-gap-networking-price-pair-sneakers-610 (describing how an "air gap" network works and why certain companies choose to utilize them).


44. Id. (discussing Google's reaction to network attacks it says were aimed at curtailing free speech in China).
against the music and motion picture industries due to the industry's support of anti-copyright infringement legislation. Other attacks have had widespread effects on foreign states, such as the 2007 attack on Estonia, allegedly conducted by Russian hacking groups “that crippled dozens of government and corporate sites[,]” and the 2009 cyber-attacks against South Korea, which targeted several leading web pages.

Every day, new components of U.S. infrastructure are connected to computer networks, which allows for more efficient operation, but also opens these components to network attacks. The development of smart grid technology is such an example. By placing controls of the power grid on interconnected information systems, power can be efficiently controlled and distributed. The security of these systems should be made a national priority. However, no amount of security spending will completely eliminate vulnerabilities, and those vulnerabilities will eventually be exploited.

38. U.S. GOVT ACCOUNTABILITY OFFICE, GAO-11-463T, CONTINUED ATTENTION NEEDED TO PROTECT OUR NATION'S CRITICAL INFRASTRUCTURE AND FEDERAL INFORMATION SYSTEMS (2011) (stating that from 5,503 incidents reported in FY 2006 to 41,770 reported in FY 2010).


41. “Air gapped” networks are those physically, electrically, and electromagnetically isolated from other networks such as the Internet. See Oliver Reis, Back Tales: Air-gap networking for the price of a pair of sneakers, INFOWORLD (May 29, 2006, 2:00 AM), http://www.infoworld.com/d/networking/hack-tales-air-gap-networking-price-pair-sneakers-610 (describing how an “air gap” network works and why certain companies choose to utilize them).


44. Id. (discussing Google's reaction to network attacks it says were aimed at curbing free speech in China).
The dramatic rise in both attacks and vulnerabilities has led governments to recognize the enormity of the issue, resulting in a push for increasing mandated cyber-security covering both government and private networks. At a 2011 hearing, U.S. House Representative Dan Lungren, Chairman of the Subcommittee on Infrastructure Protection, Cybersecurity and Security Technologies, stated that one of the top concerns for American lawmakers, intelligence officials, and military leaders is the rapidly growing cyber-threat. He cited the belief that “a successful cyber attack on [the Nation’s] power grid or communications networks could cripple the economy and threaten national security.” The President has established multiple task forces to evaluate and make recommendations for the future of cyber-security. British Foreign Secretary William Hague convened a conference on security and technology firm computers, the U.K. convened a conference with world leaders and cyber-security experts to discuss a coordinated global response to cyber-attacks).


57. Id.


60. Id. at 3.


62. Id.


The dramatic rise in both attacks and vulnerabilities has led governments to recognize the enormity of the issue, resulting in a push for increasing mandated cyber-security covering both government and private networks. At a 2011 hearing, U.S. House Representative Dan Lungren, Chairman of the Subcommittee on Infrastructure Protection, Cybersecurity and and Technology, stated that one of the top concerns for American lawmakers, intelligence officials, and military leaders is the rapidly growing cyber-threat. He cited the belief that the Nation’s power grid or economy and threaten national security.

The President has established multiple task forces to evaluate and make recommendations for the future of cyber-security. British Foreign Secretary William Hague convened a conference on cyber-attacks after receiving criticisms for failing to take cyber-threats to his country seriously. Secretary Hague stated a “global coordinated response” is required to combat cyber-threats. In 2005, the European Council adopted the European Program for Critical Infrastructure Protection to focus on strengthening information systems and enhancing preparedness for attacks on “critical infrastructure.”

If, as suggested by these experts, cyber-attacks that equate to terrorism are possible, then there are multiple reasons to believe terrorist groups will use information systems as weapons of terror. The Internet and other information systems have attributes that terrorists might appropriate to achieve their goals. The Internet is global, anonymous, and allows collaboration by people around the world on a single project. Cyber-terrorism may be the next logical step in the evolution of terrorism. Given that possibility, preventive laws should be implemented as soon as possible, not after the first major attack. As Senator Joseph Lieberman introduced the Cybersecurity Act of 2012, he stated his belief that “time is not on our side,” and that the Nation should “act to prevent a cyber 9/11 before it happens.” Senator Lieberman went on to describe how he saw the threat in greater detail, stating:

Every day rival nations, terrorist groups, criminal syndicates and individual hackers probe the weaknesses in our most critical computer networks, seeking to steal government and industrial secrets or to plant cyber agents in the cyber systems that control our most critical infrastructure and would enable an enemy to seize control of a city’s electric grid or water supply system with the touch of a key from a world away.

What if cyber-terrorism were currently planning a major attack? What laws could be used to combat this threat? Certainly there are existing laws, such as the CFIAA, under which an attack could be prosecuted, but these laws may be of little consequence in attempting to prevent such an attack.

B. The Inadequacy of the Current Approach

This Article does not suggest that a cyber-apocalypse is just around the corner; the author will leave that judgment to intelligence and industrial security experts. If possible, however, the author suggests it would be wise to develop a preventive approach. Recently, the Senate Homeland Security and Governmental Affairs Committee introduced a major piece of legislation, entitled the Cybersecurity Act of 2012. The bill seeks to regulate critical industry cyber-security and promote information sharing between private parties and
government agencies.\textsuperscript{65} On August 2, 2012, the Senate voted down the bill.\textsuperscript{66} However, there have been talks of “resurrecting” the bill.\textsuperscript{67}

Elements essential to prevent cyber-attacks include regulatory oversight, information sharing, and significant financial investment in cyber-security for the components of the U.S. infrastructure that run on information networks. These components include power grids, pipelines, and systems containing economic data.\textsuperscript{68} The government should develop legal tools to prevent acts of cyber-terrorism, similar to those developed to combat terrorism. This is not to say that the traditional law enforcement model has no role to play in catching and prosecuting cyber-attacks. Not all who commit these types of cyber-attacks have escaped punishment. Mitchell Frost was sentenced to thirty months in prison following a 2007 attack against conservative political websites belonging to Ann Coulter and Bill O’Reilly.\textsuperscript{69} A college student who hacked during the 2008 presidential campaign was sentenced to a year and a day in a halfway house.\textsuperscript{70} In a successful prosecution of an early cyber-attack on physical infrastructure, an Australian man was sent to jail for hacking into a waste-management system and dumping millions of liters of raw sewage into parks, rivers, and other properties.\textsuperscript{71}

Perhaps the best example of the use of traditional law enforcement methods was the capture of five Anonymous members in 2012.\textsuperscript{72} Following his 2008 arrest, New York based hacker Hector Monsegur assisted the FBI in tracking other Anonymous members in exchange for sentencing leniency.\textsuperscript{73} His cooperation led to the arrests of five prominent Anonymous members, prompting one cyber-security expert to state, “[t]his is the most important roll-up of hackers ever.”\textsuperscript{74}

Traditional law enforcement work certainly has its place in combating cyber-terrorism. However, the overwhelming majority of cyber-related crimes evade detection and prosecution. There are a number of reasons for this. First, many large corporations are reluctant to report the astounding number of attacks they receive given shareholder concerns over cybersecurity and loss of intellectual property.\textsuperscript{75} Additionally, cyber-crimes continue to receive lower priority than traditional crimes.\textsuperscript{76} However, the primary reason is

\textsuperscript{65} Id.


\textsuperscript{69} Robert McMillan, Bill O'Reilly hacker gets 30 months, CSO (Nov. 8, 2010), http://www.csouonline.com/article/63430/bill-o-reilly-hacker gets-30-months.

\textsuperscript{70} Bill Poovey, Palin e-mail hacker sentenced to 1 year, 1 day, NBC News (Nov. 12, 2010, 7:39 PM), http://www.msnbc.mm.com/id/4015254/m/politics-more_politics/7/palin-e-mail-hacker-sentenced-year-day (stating the defendant had hoped to find information in Palin’s online accounts that could derail her campaign, but found nothing helpful to that effect).

\textsuperscript{71} Tony Smith, Hacker jailed for revenge sewage attacks, REGISTER (Oct. 31, 2001, 3:55 PM), http://www.theregister.co.uk/2001/10/31/hacker_jailed_for报仇_sewage/ (the perpetrator worked for the company that installed the waste management controlling software and had been recently rejected for employment by the local city council).

\textsuperscript{72} Ellen Nakashima, Peter Finn & Sari Horwitz, 5 members of Anonymous hacking group charged, WASH. POST (Mar. 6, 2012), http://www.washingtonpost.com/world/national-security/5-members-of-anonymous-hacking-group-charged/2012/03/06/gIQAJ70FvR_story.html?hpid=4 (explaining the investigation into the hackers group Anonymous).

\textsuperscript{73} Id.

\textsuperscript{74} Id.


\textsuperscript{76} See Ron Condon, Catching Cyber Criminals Yourself, COMPUTER CRIME RESEARCH CTR (Apr. 24, 2006), http://www.crime-research.org/
government agencies. On August 2, 2012, the Senate voted down the bill. However, there have been talks of “resurrecting” the bill.

Elements essential to prevent cyber-attacks include regulatory oversight, information sharing, and significant financial investment in cyber-security for the components of the U.S. infrastructure that run on information networks. These components include power grids, pipelines, and systems containing economic data. The government should develop legal tools to prevent acts of cyber-terrorism, similar to those developed to combat terrorism. This is not to say that the traditional law enforcement model has no role to play in catching and prosecuting those who commit politically-motivated cyber-crimes. Not all who commit these types of cyber-attacks have escaped punishment. Mitchell Frost was sentenced to thirty months in prison following a 2007 attack against conservative political websites belonging to Ann Coulter and Bill O’Reilly. A college student who hacked Sarah Palin’s email account during the 2008 presidential campaign was sentenced to a year and a day in a halfway house. In a successful prosecution of an early cyber-attack on physical infrastructure, an Australian man was sent to jail for hacking into a waste-management system and dumping millions of liters of raw sewage into parks, rivers, and other properties.

Perhaps the best example of the use of traditional law enforcement methods was the capture of five Anonymous members in 2012. Following his 2008 arrest, New York based hacker Hector Monsegur assisted the FBI in tracking other Anonymous members in exchange for sentencing leniency. His cooperation led to the arrests of five prominent Anonymous members, prompting one cyber-security expert to state, “[t]his is the most important roll-up of hackers ever.”

Traditional law enforcement work certainly has its place in combating cyber-terrorism. However, the overwhelming majority of cyber-related crimes evade detection and prosecution. There are a number of reasons for this. First, many large corporations are reluctant to report the astounding number of attacks they receive given shareholder concerns over cybersecurity and loss of intellectual property. Additionally, cyber-crimes continue to receive lower priority than traditional crimes. However, the primary reason is...
that cyber-crimes are extraordinarily difficult to attribute to a particular culprit.\textsuperscript{77}

Current cyber-crime laws, when applied to potential acts of cyber-terrorism, also suffer from another aspect of traditional criminal law: relying on prosecution for deterrence and prevention.\textsuperscript{78} Traditional criminal law seeks to prevent future crimes primarily through successful arrest and prosecution.\textsuperscript{79} When responding to senatorial nomination questions for the position of Commander of the U.S. Cyber Command, (then) Lieutenant General Keith Alexander explained, "The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do."\textsuperscript{80} However, when making the leap from traditional cyber-crime to cyber-terrorism, the stakes become higher and prevention becomes the most important factor.

Overall, the current focus on cyber-terrorism can be compared to pre-9/11 terrorism. The 9/11 Commission Report Executive Summary noted the FBI was "case-specific, decentralized, and geared towards prosecution."\textsuperscript{81} The report went on to note that "significant FBI resources were devoted to after-the-fact investigations of major terrorist attacks, resulting in several prosecutions."\textsuperscript{82} The FBI was very good at doing what it had always done: investigate crimes, make arrests, and then hand over the perpetrators to the U.S. Attorney's Office for prosecution. However, after-the-fact prosecution is ineffective as a deterrent to terrorists. Other methods of prevention are required to prevent terrorist acts, and future laws should reflect this. But before a problem can be prevented, it must be defined.

SECTION II: DEFINING CYBER-TERRORISM

"As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we

\textsuperscript{77} See Bambauer, supra note 36, at 589.


\textsuperscript{79} E.g., id.

\textsuperscript{80} Id.

\textsuperscript{81} NATIONAL COMMISSION ON TERRORISTE ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT, EXECUTIVE SUMMARY 13.

\textsuperscript{82} Id.
that cyber-crimes are extraordinarily difficult to attribute to a particular culprit.77

Current cyber-crime laws, when applied to potential acts of cyber-terrorism, also suffer from another aspect of traditional criminal law: relying on prosecution for deterrence.78 Traditional criminal law seeks to prevent future crimes primarily through successful arrest and prosecution.79 When responding to senatorial nomination questions for the position of Commander of the Cyber Command, (then) Lieutenant General Keith Alexander explained, "The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do."80 However, when making the leap from traditional cybercrime to cyber-terrorism, the stakes become higher and prevention becomes the most important factor.

Overall, the current focus on cyber-terrorism can be compared to pre-9/11 terrorism. The 9/11 Commission Report Executive Summary noted the FBI was "case-specific, decentralized, and geared towards prosecution."81 The report went on to note that "[s]ignificant resources were devoted to after-the-fact investigations of major terrorist attacks, resulting in several prosecutions.82 The FBI was very good at doing what it had always done: investigate crimes, make arrests and then hand over the perpetrators to the U.S. Attorney's Office for prosecution. However, after-the-fact prosecution is ineffective as a deterrent to terrorists. Other methods of prevention are required to prevent terrorist acts, and future laws should reflect this. But before a problem can be prevented, it must be defined.

SECTION II: DEFINING CYBER-TERRORISM

"As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we

know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know."83 The first and often most difficult step with any great problem is properly defining it, and cyber-terrorism is no exception. Cyber-terrorism is a logical sub-category of both terrorism and cyber-crime.84 These categories are very different; one is based on a relatively new phenomena, cyber-crime, and the other encompasses a phenomena that has taken on new historical significance, terrorism.85 The definitions of these categories continue to be unsettled.86 The definition of cyber-crime generally involves some violation of a criminal code through the use of computers or other information systems, usually, but not necessarily, accomplished through the Internet.87 However, the U.S. Government offers multiple definitions of terrorism,88 and internationally, there is even less clarity on a definition of terrorism.89

Given the evolving definition of terrorism, it is no surprise that definitions of cyber-terrorism have been equally divergent.90 Additionally, the United States has yet to see a cyber-attack on the level of a major terrorist attack.91 Without a major event to spark public debate, lawmakers have little incentive to define and address the issue. Nevertheless, to develop a legal framework that helps to prevent, deter, and defend against cyber-terrorism, the appropriate first step must be to develop a practical working definition that

---

77. See Bambauer, supra note 36, at 389.
79. E.g., id.
80. Id.
81. Id.
82. Id.
83. Donald H. Rumsfeld, Sec. of Def., DEPARTMENT OF DEFENSE NEWS BRIEFING (Feb. 12, 2002).
84. See BRUCE HOFFMAN, INSIDE TERRORISM 2-3 (rev. & expanded ed. 2006) (evaluating the historical development of terrorism and why it is so difficult to define).
85. Id.
86. Id.
89. See United States v. Yousef, 327 F.3d 56, 106 (2d Cir. 2003) (“We regretfully are no closer now than eighteen years ago to an international consensus on the definition of terrorism, or even its prescription.”).
precisely defines what type of attacks should be considered cyber-terrorism.

This Section begins by offering a cyber-terrorism definition that Congress and various governmental agencies can use as a common starting point. As this Section will demonstrate, the current definitions of cyber-terrorism are widely divergent in the scope of actions that fall under their definition. This divergence makes it difficult to develop common strategies and tactics to defeat cyber-terrorism. This Article does not intend to suggest that all legislations and agency mission statements use the exact same definition of cyber-terrorism. Nevertheless, these definitions should begin from a common starting point that may be altered to serve a particular legislative or administrative purpose.

This Section will also examine a lexicon of terms that are generically used to describe different aspects of cyber-attacks. Using these definitions, this Section then categorizes the various types of cyber-attacks and explains how they are distinguished from this Article’s definition of cyber-terrorism. Next, this Article’s definition of cyber-terrorism is analyzed in comparison to other definitions by discussing how they differ and why they should yield in favor of this Article’s version.

A. Proposed Definition of Cyber-Terrorism

Following the 9/11 attacks, terrorist organizations have faced a full-court press by the United States and other nations who recognize the threat posed to their national security. Terrorist organizations such as Al-Qaeda have responded, in part, by using the Internet for organizational and propaganda purposes, utilizing online publications such as Inspire.92 The last decade has also seen the rise in politically motivated hacking groups, both in the United States and abroad.93 These groups have become increasingly daring and sophisticated in their attacks.94 It is logical to assume that both these types of organizations will eventually attempt to use the Internet and other information systems as an instrument of terror.95 Using the Internet

93. See Joshua E. Keating, Shots Fired, FOREIGN POLICY (Feb. 27, 2012), http://www.foreignpolicy.com/articles/2012/02/24/shots_fired (listing instances of political hacking attacks).
94. Id. (comparing the attacks from different sources).
95. See, e.g., Clay Wilson, CONG. RESEARCH SERV., RL32114, COMPUTER ATTACK AND CYBERTERORRISM: VULNERABILITIES AND POLICY ISSUES as a weapon of terror is inexpensive, anonymous, and global.96 At the same time, the United States is becoming more reliant on technology to control critical infrastructure, both physical and informational.97 According to the DoD:

Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption. DoD operations—both at home and abroad—are dependent on this critical infrastructure.98

This quote hints at the existence of cyber-terrorism, but how exactly to define it?

Experts base most definitions of cyber-terrorism on one of two general models: effects-based criteria and intent-based criteria.99 Many current definitions focus on one criterion to the exclusion or minimization of the other, making the actions covered by the definition too broad or too narrow.100 This Article combines the effect- and intent-based approaches, and adds a requirement that the attacker be a non-state actor. The proposed definition for cyber-terrorism is as follows:

Premeditated, politically motivated computer network attacks perpetrated against noncombatant targets by subnational groups, designed to cause fear or anxiety in a civilian populace either by: a) inflicting, falsely appearing to inflict, or

for CONGRESS 5 (2005) (arguing that given the confluence of the United States’ overwhelming military superiority, and its reliance on technology, future adversaries are likely to attempt acts of cyber-terrorism).

96. Cf. id. at 2-5 (describing the characteristics of the various types of cyber-attacks).
99. See WILSON, supra note 95, at 7 (describing the intent-based definition as involving deliberate harm, and the effect-based definition as one that intended to cause destruction and disruptions).
100. See, Perry, supra note 88, at 251 (describing how “definers disagree on what should be included in the definition”).
precisely defines what type of attacks should be considered cyber-terrorism.

This Section begins by offering a cyber-terrorism definition that Congress and various governmental agencies can use as a common starting point. As this Section will demonstrate, the current definitions of cyber-terrorism are widely divergent in the scope of actions that fall under their definition. This divergence makes it difficult to develop common strategies and tactics to defeat cyber-terrorism. This Article does not intend to suggest that all legislations and agency mission statements use the exact same definition of cyber-terrorism. Nevertheless, these definitions should begin from a common starting point that may be altered to serve a particular legislative or administrative purpose. This Section will also examine a lexicon of terms that are generically used to describe different aspects of cyber-attacks. Using these definitions, this Section then categorizes the various types of cyber-attacks and explains how they are distinguished from this Article’s definition of cyber-terrorism. Next, this Article’s definition of cyber-terrorism is analyzed in comparison to other definitions by discussing how they differ and why they should yield in favor of this Article’s version.

A. Proposed Definition of Cyber-Terrorism

Following the 9/11 attacks, terrorist organizations have faced a full-court press by the United States and other nations who recognize the threat posed to their national security. Terrorist organizations such as Al-Qaeda have responded, in part, by using the Internet for organizational and propaganda purposes, utilizing online publications such as Inspire.92 The last decade has also seen the rise in politically motivated hacking groups, both in the United States and abroad.93 These groups have become increasingly daring and sophisticated in their attacks.94 It is logical to assume that both these types of organizations will eventually attempt to use the Internet and other information systems as an instrument of terror.95 Using the Internet as a weapon of terror is inexpensive, anonymous, and global.96 At the same time, the United States is becoming more reliant on technology to control critical infrastructure, both physical and informational.97 According to the DoD:

Hackers and foreign governments are increasingly able to launch sophisticated intrusions into the networks and systems that control critical civilian infrastructure. Given the integrated nature of cyberspace, computer-induced failures of power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption. DoD operations—both at home and abroad—are dependent on this critical infrastructure.98

This quote hints at the existence of cyber-terrorism, but how exactly to define it?

Experts base most definitions of cyber-terrorism on one of two general models: effects-based criteria and intent-based criteria.99 Many current definitions focus on one criterion to the exclusion or minimization of the other, making the actions covered by the definition too broad or too narrow.100 This Article combines the effect- and intent-based approaches, and adds a requirement that the attacker be a non-state actor. The proposed definition for cyber-terrorism is as follows:

Premeditated, politically motivated computer network attacks perpetrated against noncombatant targets by subnational groups, designed to cause fear or anxiety in a civilian populace either by: a) inflicting, falsely appearing to inflict, or

for CONGRESS S(2005) (arguing that given the confluence of the United States’ overwhelming military superiority, and its reliance on technology, future adversaries are likely to attempt acts of cyber-terrorism).

96. Cf. id. at 2-5 (describing the characteristics of the various types of cyber-attacks).
99. See WILSON supra note 95, at 7 (describing the intent-based definition as involving deliberate harm, and the effect-based definition as one that intended to cause destruction and disruptions).
100. See, Perry, supra note 88, at 251 (describing how “definers disagree on what should be included in the definition”).
threatening to inflict, widespread damage to critical physical or informational infrastructure, national security related information systems, or critical economic systems; or b) causing, appearing to cause, or threatening to cause any type of severe physical damage or human casualties.

The elements and requirements contained in this definition, as well as an explanation of the technical terms, will be discussed in the Sections below.

This definition intentionally mirrors the definition of terrorism set forth in 22 U.S.C. § 2656, which defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.” However, in adapting this definition to cyber-terrorism, it is necessary to replace the element of “violence” with a more complicated list of effects. While this makes the definition more cumbersome, it necessarily ensures both that the definition of cyber-terrorism is not overly broad and addresses the unique ways in which cyber-attacks can affect a society. Should the legislature enact law that incorporates definitions and evaluations into this definition wherever possible. The remainder of this Section will review the different terms and elements included in the above definition.

B. General Lexicon of Terms

The above-proposed definition includes several terms of art. These terms build upon legal definitions or as used by government agencies.

1. Information System

An information system is any machine, network, or electronic device that contains stored information or is capable of processing data. This intentionally broad term covers hardware and software systems and the networks in which those systems operate. Hardware systems, which are primarily composed of computers, are defined broadly in 18 U.S.C. § 1030(e)(1), 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.]

Cyberspace encompasses any type of network that hardware systems operate on and is defined by the DoD as the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” The Internet is the network most commonly associated with cyberspace, most easily accessed by outside parties and is the predominant world-wide network today. But, the object of a cyber-terrorist attack does not need to use the Internet, or any other network. Many critical infrastructure components are intentionally not connected to the Internet as a security precaution, yet they remain vulnerable to attack. For example, the Agent.btz attack used thumb drives to attack the U.S. Government’s classified networks.

2. Computer Network Attack

Computer network attack (“CNA”) is a term meaning any unauthorized access, or exceeding of one’s permitted access, to an information system that results in damage, enables potential future damage, or allows for future unauthorized access to information, on any information system. CNA is another intentionally broad term, drafted to cover the entire range of malicious activity that a perpetrator may take against an information system. The DoD defines CNA as “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks

106. See, e.g., Ellen Nakashima, A cyber spy is halted, but not a debate, WASH. POST, Dec. 9, 2011, at A1 (describing security precautions that were intended to prevent infection of Government classified computer systems and how those measures were circumvented).
108. § 1030(a) (providing for how a computer network attack may be perpetrated).
109. JOURNAL OF LAW, TECHNOLOGY & THE INTERNET (JLTI) • VOL. 4 • NO. 2 • 2013
Cyber-Terrorism: Finding a Common Starting Point

292
threatening to inflict, widespread damage to critical physical or informational infrastructure, national security related information systems, or critical economic systems; or b) causing, appearing to cause, or threatening to cause any type of severe physical damage or human casualties.

The elements and requirements contained in this definition, as well as an explanation of the technical terms, will be discussed in the Sections below.

This definition intentionally mirrors the definition of terrorism set forth in 22 U.S.C. § 2656, which defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.” However, in adapting this definition to cyber-terrorism, it is necessary to replace the element of “violence” with a more complicated list of effects. While this makes the definition more cumbersome, it necessarily ensures both that the definition of cyber-terrorism is not overly broad and addresses the unique ways in which cyber-attacks can affect a society. Should the legislature enact law that identifies critical infrastructure and economic systems, they should incorporate those definitions and evaluations into this definition wherever possible. The remainder of this Section will review the different terms and elements included in the above definition.

B. General Lexicon of Terms

The above-proposed definition includes several terms of art. These terms build upon legal definitions or as used by government agencies.

1. Information System

An information system is any machine, network, or electronic device that contains stored information or is capable of processing data. This intentionally broad term covers hardware and software systems and the networks in which those systems operate. Hardware systems, which are primarily composed of computers, are defined broadly in 18 U.S.C. § 1030(e)(1), as:

[A]n 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.

Cyberspace encompasses any type of network that hardware systems operate on and is defined by the DoD as the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” The Internet is the network most commonly associated with cyberspace, most easily accessed by outside parties and is the predominant world-wide network today. But, the object of a cyber-terrorist attack does not need to use the Internet, or any other network. Many critical infrastructure components are intentionally not connected to the Internet as a security precaution, yet they remain vulnerable to attack. For example, the Agent.btz attack used thumb drives to attack the U.S. Government’s classified networks.

2. Computer Network Attack

Computer network attack (“CNA”) is a term meaning any unauthorized access, or exceeding of one’s permitted access, to an information system that results in damage, enables potential future damage, or allows for future unauthorized access to information, on any information system. CNA is another intentionally broad term, drafted to cover the entire range of malicious activity that a perpetrator may take against an information system. The DoD defines CNA as “actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks

103. See id.
themselves. The definition excludes using information systems to collect intelligence, which the DoD defines as “Computer Network Exploitation (‘CNE’).” However, this Article will incorporate CNE into CNA to maintain a broad definition that includes all types of cyber-attack.

3. Critical Infrastructure

The Critical Infrastructures Protection Act of 2001 defines critical infrastructure as, “systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.” Although an imprecise definition, examples of critical infrastructure generally include the power grid, telecommunication lines and towers, air traffic control, port controls, and primary repositories of economic data.

The Senate Judiciary Committee Report accompanying the 1996 version of the Computer Fraud and Abuse Act (“CFAA”) recognized the potential for CNA on critical infrastructure: “[a]s [t]he [National Information Infrastructure] and other network infrastructures continue to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control, and will be critical to other systems which we cannot yet anticipate.” As government and private companies seek to increase efficient operation of critical infrastructure, the operation of the components becomes increasingly dependent on computer and network control. The dependency on computer systems results in an increased vulnerability to CNA.

Recently, the U.S. Government, through the Department of Homeland Security, has taken an increased role in protection of critical infrastructure information systems.

4. Terrorism

Generically, cyber-terrorism has been defined as the use of computers and the Internet to engage in terrorist activity. This simple definition, however, begs the question: what is terrorism? In the last half-century, terrorism has become a loaded term with significant legal and moral overtones. Congress has enacted non-traditional legislation, such as criminalizing providing material support to terrorism, which the Supreme Court upheld as constitutional. The crime of terrorism generally holds extended sentences and may have due process implications. Therefore, incorporating the term “terrorism” into another crime should be done carefully as to not inadvertently include lesser acts that are not on the same moral plane.

The U.S. Code contains numerous definitions of terrorism, and this Article will examine those mostly commonly used. In 22 U.S.C. § 021101_risks_of_cyberterror.pdf [hereinafter Lewis] (arguing that attacks against critical infrastructure by cyber-weapons is primarily a business concern, and that the concern to national security is overstated).

116. See id. (describing the “new vulnerabilities” as “a massive electronic Achilles’ heel”).


118. See, e.g., WILSON, supra note 95, at 7 (combining the intent- and effect-based terrorism aspects to establish a working definition of cyber-terrorism).


120. See Holder v. Humitarian Law Project, 130 S.Ct. 2705, 2712 (2010) (holding that 18 U.S.C. § 2339B, Material Support to Designated Terrorist Organizations, was constitutional and not impermissibly vague as applied to plaintiff’s activities in seeking to provide assistance to designated foreign terrorists organizations).


122. See, e.g., Alejandro M. Suárez, American Terrorism Abroad and Due Process, Int’l POLICY DIGEST (Mar. 20, 2012), http://www.internationalpolicydigest.org/2012/03/20/americ...
The definition excludes using information systems to collect intelligence, which the DoD defines as “Computer Network Exploitation (‘CNE’).” However, this Article will incorporate CNE into CNA to maintain a broad definition that includes all types of cyber-attack.

3. Critical Infrastructure

The Critical Infrastructures Protection Act of 2001 defines critical infrastructure as, “systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.” Although an imprecise definition, examples of critical infrastructure generally include the power grid, telecommunication lines and towers, air traffic control, port controls, and primary repositories of economic data.

The Senate Judiciary Committee Report accompanying the 1996 version of the Computer Fraud and Abuse Act (“CFAA”) recognized the potential for CNA on critical infrastructure and other network infrastructures to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control, and will be critical to other systems which we cannot yet anticipate. As government and private companies seek to increase efficient operation of critical infrastructure, the operation of the components becomes increasingly dependent on computer and network control. The dependency on computer systems results in efficient operation of critical infrastructure, the operation of the components becomes increasingly dependent on computer and network control.113 The dependency on computer systems results in


112. See generally HOMELAND SEC. PRNS. DIRECTIVE 7: CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITIZATION, AND PROTECTION (2003) (noting that “[c]ritical infrastructure and key resources provide the essential services that underpin American society”).

113. Cf. id.


terrorism is defined as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.” Title 18 of the U.S. Code, which defines criminal acts and regulates criminal procedure, defines international terrorism as:

[Activities that . . . 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; and] appear to be intended . . . to intimidate or coerce a civilian population; . . . to influence the policy of a government by intimidation or coercion; or . . . to affect the conduct of a government by mass destruction, assassination, or kidnapping; and [which] 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.

The U.S. Code of Federal Regulations defines terrorism as “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”

The basic elements comprising most definitions of terrorism in use by the United States are the same. The commonality in these definitions is a variation on two elements: 1) an act of violence; and 2) the act must be political in nature, seeking to influence governmental decisions. In addition, some definitions also require the act be aimed at civilians or non-belligerents, or be conducted by non-state actors.

The first element, which is common to all definitions of terrorism, requires the presence of some act, violent in nature or dangerous to human life. The definitions do not provide an exact formula to determine what level of violence qualifies, but the definitions generally specify that the act be violent enough to intimidate the population at large, not just the subject of the attack. This intimidation, and the resulting fear or anxiety, is at the heart of terrorism. This intimidation and fear create the “terror” and present an important distinction when examining which type of CNA has sufficiently affected the population to be considered an act of cyber-terrorism.

The second element typically required is that the attack be political in nature, such as seeking to influence a government through violent actions. The political element distinguishes terrorism from other violent crimes with similar results, like murder. Terrorist organizations typically have clear motivations and explicit end-goals; for example, the Provisional Irish Republican Army desired to oust the British government from Northern Ireland, and Al-Qaeda advocates for the withdrawal of western nations from the Middle East and the establishment of a global Islamic caliphate. The terrorist creates “terror” through acts of large-scale violence, such as setting off bombs, using chemical or biological weapons, or perpetrating other violent attacks. It is this fear and threat of further violence that is intended to motivate a nation to change its policy toward the intended aim of the terrorist organization.

The third element, which appears less frequently in terrorism definitions, requires non-belligerents, those outside the scope of a military conflict, to conduct the violence. The law generally does not consider as terrorism violence aimed directly at military personnel...
2656f, terrorism is defined as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.” Title 18 of the U.S. Code, which defines criminal acts and regulates criminal procedure, defines international terrorism as:

[Activities that . . . 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; (and) appear to be intended . . . to intimidate or coerce a civilian population; . . . to influence the policy of a government by intimidation or coercion; or . . . to affect the conduct of a government by mass destruction, assassination, or kidnapping; and [which] 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.

The U.S. Code of Federal Regulations defines terrorism as “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”

The basic elements comprising most definitions of terrorism in use by the United States are the same. The commonality in these definitions is a variation on two elements: 1) an act of violence; and 2) the act must be political in nature, seeking to influence governmental decisions. In addition, some definitions also require the act be aimed at civilians or non-belligerents, or be conducted by non-state actors.

The first element, which is common to all definitions of terrorism, requires the presence of some act, violent in nature or dangerous to human life. The definitions do not provide an exact formula to determine what level of violence qualifies, but the definitions generally specify that the act be violent enough to intimidate the population at large, not just the subject of the attack. This intimidation, and the resulting fear or anxiety, is at the heart of terrorism. This intimidation and fear create the “terror” and present an important distinction when examining which type of CNA has sufficiently affected the population to be considered an act of cyber-terrorism.

The second element typically required is that the attack be political in nature, such as seeking to influence a government through violent actions. The political element distinguishes terrorism from other violent crimes with similar results, like murder. Terrorist organizations typically have clear motivations and explicit end-goals; for example, the Provisional Irish Republican Army desired to oust the British government from Northern Ireland, and Al Qaeda advocates for the withdrawal of western nations from the Middle East and the establishment of a global Islamic caliphate. The terrorist creates “terror” through acts of large-scale violence, such as setting off bombs, using chemical or biological weapons, or perpetrating other violent attacks. It is this fear and threat of further violence that is intended to motivate a nation to change its policy toward the intended aim of the terrorist organization.

The third element, which appears less frequently in terrorism definitions, requires non-belligerents, those outside the scope of a military conflict, to conduct the violence. The law generally does not consider as terrorism violence aimed directly at military personnel

128. See, e.g., § 2331(1).
129. Cf. id. (listing intent to intimidate as a requisite behavior for terrorism).
130. See, e.g., id.; 50 U.S.C. § 1801(c)(2) (2006) (including a requirement the act intends (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping).
by belligerents within the scope of a military conflict.\textsuperscript{137} Examples of attacks on the military outside the scope of a military conflict include the 9/11 attack on the Pentagon\textsuperscript{138} and the 1996 bombing of the Khobar Towers complex in Saudi Arabia.\textsuperscript{139} Acts against the military occurring within the scope of a military conflict and conducted by belligerents are typically considered acts of warfare under the law, even if these acts mimic terrorist attacks.\textsuperscript{140} Thus, the working definition must consider the category of armed attacks in cyberspace,\textsuperscript{141} which occur as part of the broader conflict. This category of CNA will be discussed in the next Section.

\section*{C. \textbf{Definitional Elements}}

This Section will examine the elements contained in the proposed definition of cyber-terrorism and discuss the reasons for inclusion. Like the traditional elements of terrorism discussed above, cyber-terrorism should include an effects element, an element of intent, and a requirement that the cyber-terrorist be a non-state actor.

1. \textbf{The Effects Element: Fear and Anxiety}

The effects element of the cyber-terrorism definition should require that the CNA cause fear or anxiety in a civilian populace through widespread damage to critical physical or informational infrastructure, national security related information systems, and/or critical economic systems, or that the CNA attack result in severe physical damage or human casualties. This result can occur in one of three ways: as a causation of the effects, by causing the appearance or belief in these effects, or threatening to cause these effects. Some definitions of cyber-terrorism focus solely or predominantly on the effects of the act and minimize the intent of the actor. For example, indicative of this approach is the informal, but commonly used,

\textit{definition of cyber-terrorism as “hacking with a body count.”}\textsuperscript{142} The advantage of this definition is that the attacker’s motivation need not be determined. The CNA need only be evaluated based on tangible outcomes, which provides a clear standard for determining when a CNA rises to the level of cyber-terrorism. If the result of the CNA is equivalent to the fear and anxiety caused by traditional terrorist actions, then it will be labeled an act of cyber-terrorism.

When focusing on the effects of a CNA, there is an advantage in distinguishing cyber-terrorists who are a serious threat to national security from online activists who conduct minor CNA without being a serious threat.\textsuperscript{143} An online activist may seek to influence popular or government opinion by defacing a military or government website,\textsuperscript{144} but this does not make him a terrorist. Some commonly used definitions of cyber-terrorism fail to make this distinction. For example, the Office of the Comptroller of the Currency defines cyber-terrorism as “[t]he use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”\textsuperscript{145} This definition contains no indication of the severity a CNA would have to reach before it is defined as cyber-terrorism. Such a definition runs the risk of making the term cyber-terrorism so broad that it becomes inappropriately over-inclusive of misconduct that is not cyber-terrorism.

Along with a tendency to be overbroad, the other problem with most effects elements is that they leave unanswered the question of how to deal with effects that are not traditionally associated with terrorist attacks that can have equally devastating effects on society. For example, by corrupting large amounts of economic data, a CNA could inflict great economic damage on a nation without inflicting civilian casualties.\textsuperscript{146} Definitions of traditional terrorism historically incorporate an element of physical damage or civilian casualties as the method of producing fear and anxiety in society.\textsuperscript{147} However, to

\textsuperscript{137} See, e.g., 22 U.S.C. § 2656f(d)(2) (2006) (defining terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents").


\textsuperscript{140} See ELISA, supra note 136.

\textsuperscript{141} Brenner, supra note 19, at 401.


\textsuperscript{143} Such groups are commonly referred to as “hacktivists” and are discussed in greater detail infra Section II(E)(4).


\textsuperscript{146} See \textit{WILSON}, supra note 95, at 8 (noting that some believe that “because of U.S. dependency on computer technology, such attacks have the potential to create economic damage on a large scale”).

\textsuperscript{147} See supra Section II(C).
by belligerents within the scope of a military conflict.\textsuperscript{137} Examples of attacks on the military outside the scope of a military conflict include the 9/11 attack on the Pentagon\textsuperscript{138} and the 1996 bombing of the Khobar Towers complex in Saudi Arabia.\textsuperscript{139} Acts against the military occurring within the scope of a military conflict and conducted by belligerents are typically considered acts of warfare under the law, even if these acts mimic terrorist attacks.\textsuperscript{140} Thus, the working definition must consider the category of armed attacks in cyberspace,\textsuperscript{141} which occur as part of the broader conflict. This category of CNA will be discussed in the next Section.

C. Definitional Elements

This Section will examine the elements contained in the proposed definition of cyber-terrorism and discuss the reasons for inclusion. Like the traditional elements of terrorism discussed above, cyber-terrorism should include an effects element, an element of intent, and a requirement that the cyber-terrorist be a non-state actor.

1. The Effects Element: Fear and Anxiety

The effects element of the cyber-terrorism definition should require that the CNA cause fear or anxiety in a civilian populace through widespread damage to critical physical or informational infrastructure, national security related information systems, and/or critical economic systems, or that the CNA attack result in severe physical damage or human casualties. This result can occur in one of three ways: as a causation of the effects, by causing the appearance or belief in these effects, or threatening to cause these effects. Some definitions of cyber-terrorism focus solely or predominantly on the effects, while some definitions incorporate an element of physical damage or civilian casualties as the method of producing fear and anxiety in society.\textsuperscript{146} However, to define cyber-terrorism as “hacking with a body count,”\textsuperscript{142} The advantage of this definition is that the attacker’s motivation need not be determined. The CNA need only be evaluated based on tangible outcomes, which provides a clear standard for determining when a CNA rises to the level of cyber-terrorism. If the result of the CNA is equivalent to the fear and anxiety caused by traditional terrorist actions, then it will be labeled an act of cyber-terrorism.

When focusing on the effects of a CNA, there is an advantage in distinguishing cyber-terrorists who are a serious threat to national security from online activists who conduct minor CNA without being a serious threat.\textsuperscript{143} An online activist may seek to influence popular or government opinion by defacing a military or government website,\textsuperscript{144} but this does not make him a terrorist. Some commonly used definitions of cyber-terrorism fail to make this distinction. For example, the Office of the Comptroller of the Currency defines cyber-terrorism as “[t]he use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”\textsuperscript{145} This definition contains no indication of the severity a CNA would have to reach before it is defined as cyber-terrorism. Such a definition runs the risk of making the term cyber-terrorism so broad that it becomes inappropriately over-inclusive of misconduct that is not cyber-terrorism.

Along with a tendency to be overbroad, the other problem with most effects elements is that they leave unanswered the question of how to deal with effects that are not traditionally associated with terrorist attacks that can have equally devastating effects on society. For example, by corrupting large amounts of economic data, a CNA could inflict great economic damage on a nation without inflicting civilian casualties.\textsuperscript{146} Definitions of traditional terrorism historically incorporate an element of physical damage or civilian casualties as the method of producing fear and anxiety in society.\textsuperscript{147} However, to

\textsuperscript{137} See, e.g., 22 U.S.C. § 2656f(d)(2) (2006) (defining terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents”).


\textsuperscript{140} See ELISA, supra note 136.

\textsuperscript{141} Brenner, supra note 19, at 401.
restrict cyber-terrorism to events where there are civilian casualties or large-scale physical destruction ignores a large range of highly malicious CNA. Therefore, physical damage or civilian casualties should solely determine the effects element; it should also focus on the psychological effect the CNA has on the target society.

Under this Article’s definition, the effects element of cyber-terrorism requires that a CNA lead to either of the following. First, the CNA could lead to damage traditionally associated with terrorism, which includes death, injury, water contamination, or release of radiological material. Alternatively, the CNA could cause damage unique to a CNA with an equivalent psychological impact on society, such as pipeline bursts, extended power outages, disruption of air-traffic control systems, or major loss of economic data. However, the intended effects of CNA can often be hard to predict and distinguish. Therefore, it is necessary to have an element of intent in a proper definition of cyber-terrorism.

2. The Intent Element: Motivation

The intent element of the cyber-terrorism definition requires that the CNA be premeditated and politically motivated. Similar to effects-based definitions, there are definitions currently in use that focus solely on the intent of the CNA. An example of a typical intent-based definition of cyber-terrorism is offered by Serge Krasavin, Ph.D., of the Computer Crime Research Center; he defines cyber-terrorism as the “use of information technology and means by terrorist groups and agents.”

This definition offers a drastically different approach because it focuses on the actor (“terrorist groups and agents”), not the act (“use of information technology” is extremely broad and unhelpful). Accordingly, as long as a terrorist is using the information system to forward his or her means, the result of that use does not matter. For example, the use of e-mail to communicate with other terrorists would be an act of cyber-terrorism. However, the Internet’s widespread use likely means there is not a terrorist organization that does not use the Internet and computers for any number of reasons. Thus, the category essentially becomes redundant when considering its application to terrorism. This definition is an excellent description of “terrorist use of the Internet,” but is not helpful in distinguishing cyber-terrorism from other types of CNA.

The advantage of an intent-based definition is that it covers the full range of attacks both unique to CNA, such as damaging economic data, and similar to traditional terrorism, such as releasing poison gas. However, an attack for political motivations can run the entire spectrum of CNA, from basic denial of service attacks and government website defacement to potentially major attacks, such as on Siemens supervisory control and data acquisition (“SCADA”) controlled utilities. Intent-based definitions, like overly broad effects-based definitions, run the risk of making the category of cyber-terrorism so broad it becomes meaningless. We do not classify the graffiti artist who spray-paints “Out of Iraq” on a public wall as a terrorist, partly because the term would lose its meaning. The same should hold for acts of cyber-terrorism.

The most useful approach is to add an element of motivation that requires the CNA be premeditated and politically-motivated, with the effects element discussed above. The term cyber-terrorism should recognize the purpose behind the attack: to undermine a government or motivate it to change its policies. It should only encompass CNA with specific effects: attacks that produce fear or anxiety in the populace. This combination will prevent the definition from being too narrow, allowing the inclusion of certain effects unique to CNA, while also avoiding being too broad—excluding those acts that are of a more trivial nature.

3. The Non-State Actor Requirement

Although not every definition includes a requirement that a non-state actor commit the terrorist acts, most acts with similar effects that are attributed directly to a state are considered acts of armed aggression. The reason is because governmental agencies would
restrict cyber-terrorism to events where there are civilian casualties or large-scale physical destruction ignores a large range of highly malicious CNA. Therefore, physical damage or civilian casualties should solely determine the effects element; it should also focus on the psychological effect the CNA has on the target society.

Under this Article’s definition, the effects element of cyber-terrorism requires that a CNA lead to either of the following. First, the CNA could lead to damage traditionally associated with terrorism, which includes death, injury, water contamination, or release of radiological material. Alternatively, the CNA could cause damage unique to a CNA with an equivalent psychological impact on society, such as pipeline bursts, extended power outages, disruption of air-traffic control systems, or major loss of economic data. However, the intended effects of CNA can often be hard to predict and distinguish. Therefore, it is necessary to have an element of intent in a proper definition of cyber-terrorism.

2. The Intent Element: Motivation

The intent element of the cyber-terrorism definition requires that the CNA be premeditated and politically motivated. Similar to effects-based definitions, there are definitions currently in use that focus solely on the intent of the CNA. An example of a typical intent-based definition of cyber-terrorism is offered by Serge Krasavin, Ph.D., of the Computer Crime Research Center; he defines cyber-terrorism as the “use of information technology and means by terrorist groups and agents.”

This definition offers a drastically different approach because it focuses on the actor (“terrorist groups and agents”), not the act (“use of information technology” is extremely broad and unhelpful). Accordingly, as long as a terrorist is using the information system to forward his or her means, the result of that use does not matter. For example, the use of e-mail to communicate with other terrorists would be an act of cyber-terrorism. However, the Internet’s widespread use likely means there is not a terrorist organization that does not use the Internet and computers for any number of reasons. Thus, the category essentially becomes redundant when considering its application to terrorism. This definition is an excellent description of “terrorist use of the Internet,” but is not helpful in distinguishing cyber-terrorism from other types of CNA.

The advantage of an intent-based definition is that it covers the full range of attacks both unique to CNA, such as damaging economic data, and similar to traditional terrorism, such as releasing poison gas. However, an attack for political motivations can run the entire spectrum of CNA, from basic denial of service attacks and government website defacement to potentially major attacks, such as on Siemens supervisory control and data acquisition (SCADA) controlled utilities. Intent-based definitions, like overly broad effects-based definitions, run the risk of making the category of cyber-terrorism so broad it becomes meaningless. We do not classify the graffiti artist who spray-paints “Out of Iraq” on a public wall as a terrorist, partly because the term would lose its meaning. The same should hold for acts of cyber-terrorism.

The most useful approach is to add an element of motivation that requires the CNA be premeditated and politically-motivated, with the effects element discussed above. The term cyber-terrorism should recognize the purpose behind the attack: to undermine a government or motivate it to change its policies. It should only encompass CNA with specific effects: attacks that produce fear or anxiety in the population. This combination will prevent the definition from being too narrow, allowing the inclusion of certain effects unique to CNA, while also avoiding being too broad—excluding those acts that are of a more trivial nature.

3. The Non-State Actor Requirement

Although not every definition includes a requirement that a non-state actor commit the terrorist acts, most acts with similar effects that are attributed directly to a state are considered acts of armed aggression. The reason is because governmental agencies would...
address such an attack in a much different manner and the public would view it differently. For example, if the intelligence operative of a foreign nation was to set off a bomb in the United States, and it was known that the operative was acting under the control of that foreign nation, the U.S. Government would view it as an act of armed aggression. The same should be true for cyber-terrorism. The exclusion of this element is not fatal to the definition and may be eliminated for certain applications.

One of the prime difficulties in cyber-terrorism is determining whether a state actor is responsible for the attack. Many experts believe that nations such as China and Russia, who have the capability to conduct extensive CNA, use hacking groups not officially related to the state in order to mask state involvement in CNA against foreign powers.155 This is not a new tactic; state sponsors of traditional terrorism, such as Iran, are common.164 However, the built-in anonymity of the Internet and the lack of physical infrastructure required to launch an attack make this tactic even more successful in cyberspace. Whether a CNA is ultimately attributed to a state will depend on the evidence particular to the case and the willingness of political leaders to place blame on state actors. However, because the response options will be entirely different against a state actor, it is more useful to categorize those attacks as something other than cyber-terrorism.

D. Current Definitions of Cyber-Terrorism

Having proposed a common working definition of cyber-terrorism, this Section analyzes the definitions that have either been offered by academics or are in use by the U.S. Government. To start, the original definition of cyber-terrorism came from Barry C. Collin, a senior research fellow at the Institute for Security and Intelligence in California in the 1980s.165 His vision of cyber-terrorism was one in which attacks conducted through computers mirrored the effects of traditional acts of terrorism:


There has been no shortage of cyber-terrorism definitions offered in response to this statement. Many contain similar elements and themes, but the broad divergence in the scope of these definitions signals the need for a definition that can be used as a common starting point. This Section examines these definitions.

1. United States Government Definitions

Though not explicitly defined as cyber-terrorism, a form of cyber-terrorism is contained in the U.S. Code Section 2332b(g)(5) defines the “federal crime of terrorism” and includes as predicate offenses two CFAA provisions: one relating to cyber-espionage and one related to computer damage.158 If one of those two CFAA provisions is violated, and if that CFAA violation “is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct,” then it meets this definition of terrorism.159 The implications of this provision will be covered in greater depth later, but it is important to recognize that Congress has thought fit to include CNA in one definition of terrorism under the U.S. Code.

In the example in the Introduction, where Anonymous attacked a FBI website in retaliation for its arrest of Dotcom and others, Anonymous’s actions meet the definition of the federal crime of terrorism, despite the fact it does not meet traditional concepts of terrorism. This is because the federal definition fails to sufficiently


159. 18 U.S.C. § 2332b(g)(5) (2012); 18 U.S.C. § 1030(a)(1) (2012) (relating to cyber-espionage); § 1030(a)(5)(A) (resulting in damage as defined in 18 U.S.C. § 1030(c)(4)(A)(i)(II) through (VII) (resulting in damage to national security related computers or if the damage involves 10 or more computers)).
address such an attack in a much different manner and the public would view it differently. For example, if the intelligence operative of a foreign nation was to set off a bomb in the United States, and it was known that the operative was acting under the control of that foreign nation, the U.S. Government would view it as an act of armed aggression. The same should be true for cyber-terrorism. The exclusion of this element is not fatal to the definition and may be eliminated for certain applications.

One of the prime difficulties in cyber-terrorism is determining whether a state actor is responsible for the attack. Many experts believe that nations such as China and Russia, who have the capability to conduct extensive CNA, see hacking groups not officially related to the state in order to mask state involvement in CNA against foreign powers. 155 This is not a new tactic; state sponsors of traditional terrorism, such as Iran, are common. 156 However, the built-in anonymity of the Internet and the lack of physical infrastructure required to launch an attack make this tactic even more successful in cyberspace. Whether a CNA is ultimately attributed to a state will depend on the evidence particular to the case and the willingness of political leaders to place blame on state actors. However, because the response options will be entirely different against a state actor, it is more useful to categorize those attacks as something other than cyber-terrorism.

D. Current Definitions of Cyber-Terrorism

Having proposed a common working definition of cyber-terrorism, this Section analyzes the definitions that have either been offered by academics or are in use by the U.S. Government. To start, the original definition of cyber-terrorism came from Barry C. Collin, a senior research fellow at the Institute for Security and Intelligence in California in the 1980s. 157 His vision of cyber-terrorism was one in which attacks conducted through computers mirrored the effects of traditional acts of terrorism:


Like conventional terrorists, Cyber-Terrorists are out for blood. They try to do things like break into subway computer systems to cause a collision or use computers to tamper with power grids or food processing. However, unlike suicide bombers and roof-top snipers, Cyber-Terrorists attack from the comfort of home and can be in more than one place at a time through cyberspace. CyberTerrorism can be far more damaging, and far more violent, than a 55-gallon drum of fuel and fertilizer. Cyber-Terrorists’ isolation from the results of their actions and the consequent lack of personal risk, make them particularly dangerous. [The ease and low cost of CyberTerrorism combine to offer an attractive tool for once-conventional sociopaths.]

There has been no shortage of cyber-terrorism definitions offered in response to this statement. Many contain similar elements and themes, but the broad divergence in the scope of these definitions signals the need for a definition that can be used as a common starting point. This Section examines these definitions.

1. United States Government Definitions

Though not explicitly defined as cyber-terrorism, a form of cyber-terrorism is contained in the U.S. Code Section 2332b(g)(5) defines the “federal crime of terrorism” and includes as predicate offenses two CFAA provisions: one relating to cyber-espionage and one related to computer damage. 158 If one of those two CFAA provisions is violated, and if that CFAA violation “is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct,” then it meets this definition of terrorism. 159 The implications of this provision will be covered in greater depth later, but it is important to recognize that Congress has thought fit to include CNA in one definition of terrorism under the U.S. Code.

In the example in the Introduction, where Anonymous attacked a FBI website in retaliation for its arrest of Dotcom and others, Anonymous’s actions meet the definition of the federal crime of terrorism, despite the fact it does not meet traditional concepts of terrorism. This is because the federal definition fails to sufficiently


159. 18 U.S.C. § 2332b(g)(5) (2012); 18 U.S.C. § 1030(a)(1) (2012) (relating to cyber-espionage); § 1030(a)(5)(A) (resulting in damage as defined in 18 U.S.C. § 1030(c)(4)(A)(ii)); and § 1030(c)(4)(A)(iii) through (VII) (requiring damage to national security related computers or if the damage involves 10 or more computers)).
define the scope of the attack's effects. Almost any denial of service attack against a national security website will fall under the predicate CFAs offenses. Although denial of service attacks are serious and should be investigated, they do not cause fear or anxiety in the populace. Despite the inclusion of cyber-terrorism in the criminal code, most government agencies have developed their own cyber-terrorism definitions. These definitions contain some important differences and an attempt should be made to make them more consistent.

The Federal Emergency Management Agency (“FEMA”) has defined cyber-terrorism as “unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.”161 This definition incorporates an adequate intent element that appears in most definitions of terrorism and cyber-terrorism alike. It requires the attacker’s objective to be political or social coercion against a government or its people.162 However, the weakness of this definition is in the effects element, which has no requirement for the scale of attack. Under this definition, the lone wolf who hacks a webpage to post a political message such as “Stop the War in Iraq,” or who temporarily takes down a DoJ public website to protest an arrest, would be guilty of cyber-terrorism. Thus, as the requirement that a CNA “intimidate or coerce” a government or its people163 is virtually meaningless, this is too vague to be an effective definition.

The National Infrastructure Protection Center defines cyber-terrorism as “a criminal act perpetrated through computers resulting in crime, death and/or destruction and creating terror for the purpose of coercing a government to change its policies.”164 Unlike the other over-broad definitions, this definition focuses on the effects of a test, with the result that it is extremely narrow. The definition excludes all attacks not “resulting in violence, death and/or destruction,”165 which excludes some of the most devastating possibilities of CNA. An argument could be made that this definition is unhelpful because everything it incorporates is already covered by definitions of terrorism. To be useful, a definition of cyber-terrorism must include effects such as a takedown of economic systems or corruption of massive amounts of national security data, as this is where the unique capabilities of cyber-terrorism lie.

William L. Tafoya, Ph.D., writing in the FBI Law Enforcement Bulletin, defines cyber-terrorism as “the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information.”166 Tafoya clarifies this definition by providing the example of wiping out the data of the Library of Congress as compared to wiping out a single academic paper.167 The former would be seen as devastating and certainly affect the people’s quality of life, whereas the latter would have a limited effect on the public’s lives.168 This definition identifies “disabling or deleting critical infrastructure data or information” as the required effect. It is the opposite of the FEMA definition,169 which required an element of violence. Instead, it does not account for physical harms, and focuses solely on data. Recognizing this unique effect of CNA is important, but the definition should not be completely exclusive of other types of harms. Nonetheless, any definition of cyber-terrorism should similarly include attacks on critical data systems.

Any government definition of cyber-terrorism will need to be altered somewhat to fit with the goals of that agency, and this Article does not suggest that all agencies must use the proposed definition. But, as demonstrated above, the currently used definitions are so divergent that they impede the establishment of a common, government-wide strategy to defeat cyber-terrorism. At minimum, there should be consistency among the three basic elements of cyber-terrorism and particularity about the type of effects included.

2. United Nations Definition of Cyber-Terrorism

An internationally consistent definition should also be sought. Although not the focus of this Article, it is useful to examine how the United Nations (U.N.) has defined cyber-terrorism. The UN Counter-Terrorism Implementation Task Force (“CTITF”), although not explicitly using the term cyber-terrorism, recognizes that one of the ways a terrorist organization may make its use of the Internet to perform terrorist attacks is by remotely altering information on

162. Id.
164. Id.
166. Id. at 2-3.
167. Id.
define the scope of the attack's effects. Almost any denial of service attack against a national security website will fall under the predicate of terrorism against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. This definition incorporates an adequate intent element that appears in most definitions of terrorism and cyber-terrorism alike. It requires the attacker's objective to be political or social coercion against a government or its people. However, the weakness of this definition is in the effects element, which has no requirement for the scale of attack. Under this definition, the lone wolf who hacks a webpage to post a political message such as "Stop the War in Iraq," or who temporarily takes down a DoJ public website to protest an arrest, would be guilty of cyber-terrorism. Thus, as the requirement that a CNA "intimidate or coerce" must require a more substantive attack, this is too vague to be an effective definition.

The National Infrastructure Protection Center defines cyber-terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies." Unlike the other over-broad definitions, this definition focuses more on the effects of a test, with the result that it is extremely narrow. The definition excludes all attacks not "resulting in violence, death and/or destruction," which excludes some of the most devastating possibilities of CNA. An argument could be made that this definition is unhelpful because everything it incorporates is already covered by definitions of terrorism. To be useful, a definition of cyber-terrorism must include effects such as a takedown of economic systems or corruption of massive amounts of national security data, as this is where the unique capabilities of cyber-terrorism lie.

William L. Tafoya, Ph.D., writing in the FBI Law Enforcement Bulletin, defines cyber-terrorism as "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information." Tafoya clarifies this definition by providing the example of wiping out the data of the Library of Congress as compared to wiping out a single academic paper. The former would be seen as devastating and certainly affect the public's quality of life, whereas the latter would have a limited effect on the public's lives. This definition identifies "disabling or deleting critical infrastructure data or information" as the required effect. It is the opposite of the FEMA definition, which required an element of violence. Instead, it does not account for physical harms, and focuses solely on data. Recognizing this unique effect of CNA is important, but the definition should not be completely exclusive of all other types of harms. Nonetheless, any definition of cyber-terrorism should similarly include attacks on critical data systems.

Any government definition of cyber-terrorism will need to be altered somewhat to fit with the goals of that agency, and this Article does not suggest that all agencies must use the proposed definition. But, as demonstrated above, the currently used definitions are so divergent that they impede the establishment of a common, government-wide strategy to defeat cyber-terrorism. At minimum, there should be consistency among the three basic elements of cyber-terrorism and particularity about the type of effects included.

2. United Nations Definition of Cyber-Terrorism

An internationally consistent definition should also be sought. Although not the focus of this Article, it is useful to examine how the United Nations (U.N.) has defined cyber-terrorism. The UN Counter-Terrorism Implementation Task Force ("CTITF"), although not explicitly using the term cyber-terrorism, recognizes that one of the ways a terrorist organization may make "[u]se of the Internet to perform terrorist attacks [i]b by remotely altering information on
computer systems or disrupting the flow of data between computer systems.\textsuperscript{169} The CTITF goes on to explain:

\begin{quote}
[A]ny cyber attack qualifying as ‘terrorist’ would ultimately still have to cause damage in the ‘real world’: for example, by interfering with a critical infrastructure system to the extent of causing loss of life or severe property damage. However, as dependence on online data and services increases, an attack that resulted only in widespread interruption of the Internet could, in future, cause sufficient devastation to qualify as a terrorist attack. However, categorizing such attacks as terrorist remains controversial. The damage resulting from such attacks, while potentially economically significant, to date their impact has been more on the level of a serious annoyance.\textsuperscript{170}
\end{quote}

This definition, while a bit unwieldy, does an excellent job of including both violent attacks and attacks on data that are serious enough to rise to the level of terrorism. This definition, however, fails to address the element of intent and does not include a non-state actor requirement.

3. Academic Definitions

Most academic interest in large-scale CNA tends to focus on cyber-warfare and the involvement of state actors. This is logical given the greater size and resources of governments such as China, Russia, and the United States. Some prominent cyber-security experts, however, have focused on cyber-terrorism: the possibility of large scale CNA by non-state actors. One of the earliest and most widely cited academic descriptions of cyber-terrorism comes from security expert Dorothy Denning:

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism.


\textsuperscript{170} Id. at 9.

Although it primarily focuses on violent acts, Denning’s description does include attacks that cause severe economic loss.\textsuperscript{172} She excludes attacks that are minor in nature, steering the definition towards more significant attacks.\textsuperscript{173} Non-violent attacks may also be covered by the phrase “or at least cause enough harm to generate fear,”\textsuperscript{174} but it is difficult to draw clear guidelines from this statement. Denning also did not include whether the attacker must be a non-state actor. Nevertheless, it is an excellent foundation from which to formulate a precise definition that meets the criteria of being broad enough to include unique CNA, such as attacks on data only, and narrow enough to exclude minor activitist attacks.

The Center for Strategic and International Studies defines cyber-terrorism as “the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.”\textsuperscript{175} This definition is both precise (“shut down critical national infrastructures”) and vague (“coerce or intimidate government or civilian populace”). It fails to define what level of coercion or intimidation is required before the act goes from being a protest to an act of terrorism. Although the definition suggests a higher level of attack by explicitly including critical infrastructure, it fails to be more precise beyond that particular category.

In her article, Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, Kelly Gable provides a similar definition, including “efforts by terrorists to use the Internet to hijack computer systems, bring down the international financial system, or commit analogous terrorist actions in cyberspace.”\textsuperscript{176} Gable focuses on the international finance depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

\textsuperscript{171} Cyberterrorism: Testimony before Special Oversight Panel on Terrorism Comm. on Armed Servs. Before U.S. H.R., (2000) (statement of Dorothy E. Denning, Georgetown Univ.) available at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (arguing that a definition of cyber-terrorism should involve a component of violence or harming of critical infrastructure, and that, at the time, it was mostly theoretical but could arise in the future).

\textsuperscript{172} Id.

\textsuperscript{173} Id.

\textsuperscript{174} Id.

\textsuperscript{175} Lewis, supra note 115.

computer systems or disrupting the flow of data between computer systems.\textsuperscript{169} The CTTTF goes on to explain:

\[\text{Any cyber attack qualifying as 'terrorist' would ultimately still have to cause damage in the 'real world': for example, by interfering with a critical infrastructure system to the extent of causing loss of life or severe property damage. However, as dependence on online data and services increases, an attack that resulted only in widespread interruption of the Internet could, in future, cause sufficient devastation to qualify as a terrorist attack. However, categorizing such attacks as terrorist remains controversial. The damage resulting from such attacks, while potentially economically significant, to date their impact has been more on the level of a serious annoyance.}\textsuperscript{170}

This definition, while a bit unwieldy, does an excellent job of including both violent attacks and attacks on data that are serious enough to rise to the level of terrorism. This definition, however, fails to address the element of intent and does not include a non-state actor requirement.

3. Academic Definitions

Most academic interest in large-scale CNA tends to focus on cyber-warfare and the involvement of state actors. This is logical given the greater size and resources of governments such as China, Russia, and the United States. Some prominent cyber-security experts, however, have focused on cyber-terrorism: the possibility of large scale CNA by non-state actors. One of the earliest and most widely cited academic descriptions of cyber-terrorism comes from security-expert Dorothy Denning:

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism.


\textsuperscript{170} Id. at 9.

171. \textit{Cyberterrorism: Testimony before Special Oversight Panel on Terrorism Comm. on Armed Servs. Before U.S. H.R. (2000) (statement of Dorothy E. Denning, Georgetown Univ.) available at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (arguing that a definition of cyber-terrorism should involve a component of violence or harming of critical infrastructure, and that, at the time, it was mostly theoretical but could arise in the future).}

172. Id.

173. Id.

174. Id.

175. Lewis, supra note 115.

system, as opposed to critical infrastructure, but also includes “analogous terrorist actions,”177 which suggests violent acts. This definition is useful because it identifies the need to include CNA, which causes drastic effects on financial systems in any definition.

Susan Brenner, another noted cyber-security expert, posits a basic definition of cyber-terrorism, stating: “[g]enerically, cyberterrorism consists of using computer technology to engage in terrorist activity.”178 Recognizing the broad nature of this definition, Brenner expands on the definition in several important ways. Brenner excludes attacks that originate through the Internet, but have the result of large-scale destruction, which she terms as a “Weapon of Mass Destruction” attack.179 As an example, she provides a scenario of a cyber-terrorist hacking into a nuclear power plant and causing a Chernobyl-style meltdown.180 Although it seems counter-intuitive to exclude this action from cyber-terrorism, Brenner argues that such an attack would primarily be remembered as a nuclear terrorist attack, not a cyber-attack, and therefore should not be considered an act of cyber-terrorism.181 Brenner argues that we do not define an attack that uses a car to deliver bombs to target cites as automotive-terrorism. The logical follow on question is why define an attack that has a cyber-element as cyber-terrorism?182

While Brenner makes a good point that a CNA that produces violence is a “terrorist” attack in the traditional sense, there is still good reason to further classify it as a cyber-terrorist attack, particularly if government agencies will use this as a common working definition. The definition needs a separate classification to gear prevention and response.

Prevention of a traditional terrorist attack on a nuclear plant is vastly different from a CNA, and will require different thought processes, security measures, and, as this Article later argues, changes to the law. Traditional attack prevention involves protection of physical security on the grounds surrounding the plant, whereas CNA prevention involves protection of the plant’s information systems. Similarly, a law enforcement investigation of a traditional terrorist attack would require vastly different techniques and expertise than a CNA on that same plant. In the automotive analogy, law enforcement would use substantially the same techniques to investigate a physical bombing of a power station whether the bomber used a vehicle or a suicide vest to attack the station. However, the same could not be said if the attack was conducted through information systems.

Brenner proposes a second category of cyber-terrorism, which she labels “Weapon of Mass Disruption.”183 This type of CNA would not result in violent, physical effects, but psychological effects that could undermine faith in government.184 Brenner provides the example of a hacked news website that leads people to believe that there was a suitcase nuclear device on a city bus, leading to mass panic and possibly death.185 This may be a more realistic scenario than the attack on the nuclear plant, given the lower level of sophistication required to complete such an attack. For example, in retaliation for airing a WikiLeaks documentary, the hacker group Lulzsec posted a news story on PBS that rapper Tupac Shakur was found alive several years after his actual death.186 As seen above, cyber-terrorists can accomplish this type of attack completely through the Internet, unlike CNA against a nuclear plant, which would probably require introducing the attack from the inside.187

Because of the lower level of sophistication required, Brenner views this type of attack as more than a theoretical possibility. As an increasing amount of information is relayed through Internet news outlets, Facebook, Twitter, instant messaging, and other Internet-based sources, the potential panic that would likely result from a “weapons of mass distraction” attack is high. Any definition of cyber-terrorism should include the major threat of causing the appearance of a terrorist attack through CNA.

Brenner’s final cyber-terrorism category is a “Weapon of Mass Disruption.”188 This type of attack uses CNA against infrastructure components, such as an electrical grid or gas supply.189 The cyber-terrorist’s goal would likely be to undermine the populace’s faith in

---

177. Id.
178. Brenner, supra note 19, at 386 (categorizing cyber-threats and focusing on attribution as the key element to be solved in battling those threats).
179. Id. at 300-91.
180. Id.
181. Id. at 391.
182. Id.
183. Id. at 391-93.
184. Id. at 391.
185. Id. at 392.
188. Brenner, supra note 19, at 393-95.
189. Id.
system, as opposed to critical infrastructure, but also includes "analogous terrorist actions,"\textsuperscript{177} which suggests violent acts. This definition is useful because it identifies the need to include CNA, which causes drastic effects on financial systems in any definition.

Susan Brenner, another noted cyber-security expert, posits a basic definition of cyber-terrorism, stating: "generically, cyberterrorism consists of using computer technology to engage in terrorist activity."\textsuperscript{178} Recognizing the broad nature of this definition, Brenner expands on the definition in several important ways. Brenner excludes attacks that originate through the Internet, but have the result of large-scale destruction, which she terms as a "Weapon of Mass Destruction" attack.\textsuperscript{179} As an example, she provides a scenario of a cyber-terrorist hacking into a nuclear power plant and causing a Chernobyl-style meltdown.\textsuperscript{180} Although it seems counter-intuitive to exclude this action from cyber-terrorism, Brenner argues that such an attack would primarily be remembered as a nuclear terrorist attack, not a cyber-attack, and therefore should not be considered an act of cyber-terrorism.\textsuperscript{181} Brenner argues that we do not define an attack that uses a vehicle to deliver bombs to target cites as "terrorism." The logical follow on question is why define an attack that has a cyber-element as cyber-terrorism?\textsuperscript{182}

While Brenner makes a good point that a CNA that produces violence is a "terrorist" attack in the traditional sense, there is still good reason to further classify it as a cyber-terrorist attack, particularly if government agencies will use this as a common working definition. The definition needs a separate classification to gear policy makers and law enforcement towards appropriate methods of prevention and response.

Prevention of a traditional terrorist attack on a nuclear plant is vastly different from a CNA, and will require different thought processes, security measures, and, as this Article later argues, changes to the law. "Traditional attack prevention involves protection of physical security on the grounds surrounding the plant, whereas CNA prevention involves protection of the plant’s information systems. Similarly, a law enforcement investigation of a traditional terrorist attack would require vastly different techniques and expertise than a CNA on that same plant. In the automotive analogy, law enforcement would use substantially the same techniques to investigate a physical bombing of a power station whether the bomber used a vehicle or a suicide vest to attack the station. However, the same could not be said if the attack was conducted through information systems.

Brenner proposes a second category of cyber-terrorism, which she labels "Weapon of Mass Disruption."\textsuperscript{183} This type of CNA would not result in violent, physical effects, but psychological effects that could undermine faith in government.\textsuperscript{184} Brenner provides the example of a hacked news website that leads people to believe that there was a suitcase nuclear device on a city bus, leading to mass panic and possibly death.\textsuperscript{185} This may be a more realistic scenario than the attack on the nuclear plant, given the lower level of sophistication required to complete such an attack. For example, in retaliation for airing a WikiLeaks documentary, the hacker group Lulzsec posted a news story on PBS that rapper Tupac Shakur was found alive several years after his actual death.\textsuperscript{186} As seen above, cyber-terrorists can accomplish this type of attack completely through the Internet, unlike CNA against a nuclear plant, which would probably require introducing the attack from the inside.\textsuperscript{187}

Because of the lower level of sophistication required, Brenner views this type of attack as more than a theoretical possibility. As an increasing amount of information is relayed through Internet news outlets, Facebook, Twitter, instant messaging, and other Internet-based sources, the potential panic that would likely result from a "weapons of mass distraction" attack is high. Any definition of cyber-terrorism should include the major threat of causing the appearance of a terrorist attack through CNA.

Brenner’s final cyber-terrorism category is a “Weapon of Mass Disruption.”\textsuperscript{188} This type of attack uses CNA against infrastructure components, such as an electrical grid or gas supply.\textsuperscript{189} The cyber-terrorist’s goal would likely be to undermine the populace’s faith in

\textsuperscript{177} Brenner, supra note 19, at 386 (categorizing cyber-threats and focusing on attribution as the key element to be solved in battling those threats).

\textsuperscript{178} Id. at 390-91.

\textsuperscript{179} Id. at 391.

\textsuperscript{180} Id. at 391.

\textsuperscript{181} Id. at 391.

\textsuperscript{182} Id.
government by interrupting essential services. Brenner sees this as a more realistic possibility than an attack that solely produces violent, catastrophic effects. These types of attacks have been attempted with limited success, though they have yet to cause widespread fear or panic. However, this type of attack seems of a different scale from the type of attack included in the “Weapon of Mass Destruction” category. If a hacker could shut down the gas supply, then certainly that same hacker could overload the gas supply and cause an explosion.

Overall, Brenner’s point was that cyber-terrorism should not be treated as war, for the greatest potential harms from cyber-terrorism were either too theoretical or straightforward terrorism, but should instead be treated as crime. This framework changed following the 9/11 attacks, as terrorist attacks have become a legal category unto themselves, and the response has included participation by intelligence agencies, law enforcement, and the military. The threats posed by terrorism have prompted the passage of new laws and the development of new law enforcement techniques in cyber-space. If it is possible that a cyber-terrorist attack could seriously undermine a citizenry’s faith in government, as Brenner suggests, then policy makers should identify cyber-terrorism as unique from cyber-crime, and devote serious attention to prevention and response.

E. Categories of Computer Network Attack

If cyber-terrorism is to be recognized as a unique type of CNA, it is important to distinguish it from other types of CNA. CNA has several sub-categories that this Article will distinguish by using three factors: damage done to the target information system, motivation of the attack, and identity of the attacker. The attack can be categorized and response options determined by identifying each of the three factors in a particular attack.

190. Id. at 393-94 (describing how generally terrorists’ goal is not to destroy but to demoralize).
191. Id. at 394 (stating that urbanized societies are more vulnerable to terrorism aimed at demoralization).
192. See, e.g., Tony Smith, Hacker jailed for revenge sewage attacks, REGISTER (Oct. 31, 2001, 3:55 PM), http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ (describing a cyber-attack that caused annoyance, and stink, but caused little fear or serious damage).

1. Cyber-crime

This Article defines a cyber-crime as any level of CNA, conducted by any party, for any purpose that is considered illegal under domestic or international law. This sub-category is the broadest within CNA and includes every type of CNA outside those that occur in an armed conflict and do not violate the laws of war. Under U.S. domestic law, it is essentially any act that violates the CPA.

Cyber-crimes need not have an information system as a target, as the definition includes those attacks simply using information systems as a tool. A current definition in use by the Computer Crime Research Center defines cyber-crime as “crimes committed on the Internet using the computer as either a tool or a targeted victim.” Although this Article argues a CNA does not have to be conducted through use of the Internet, this definition accurately reflects that information systems can be used to effectuate an attack and not just serve as the target. Those perpetrating CNAs frequently use means other than the Internet to access information systems. The Stuxnet virus, for example, is thought to have spread to information systems through an infected removable drive, as the target system was not connected to the Internet. This is important for a discussion of cyber-terrorism because many critical infrastructure components are not connected to outside networks as a security measure and must be accessed through another means.

2. Cyber-espionage

Cyber-espionage is a type of CNA by a state actor or government contractor, with the purpose of collecting intelligence against another state, which causes minimal damage or disruption to the information system. This definition does not incorporate non-national security related corporate espionage, as that is a more traditional cyber-crime. This is not to say that corporate espionage does not have national security implications. According to the DoD:

Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property

196. See, e.g., Zetter, supra note 107.
197. See id.; see also William J. Broad, John Markoff & David E. Sanger, Israel Tests Called Crucial In Iran Nuclear Setback, N. Y. TIMES, Jan. 16, 2011, at A1 (describing how Stuxnet spread and was solved).
government by interrupting essential services.190 Brenner sees this as a more realistic possibility than an attack that solely produces violent, catastrophic effects.191 These types of attacks have been attempted with limited success, though they have yet to cause widespread fear or panic.192 However, this type of attack seems a different scale from the type of attack included in the “Weapon of Mass Destruction” category. If a hacker could shut down the gas supply, then certainly that same hacker could overload the gas supply and cause an explosion.

Overall, Brenner’s point was that cyber-terrorism should not be treated as war, for the greatest potential harms from cyber-terrorism were either too theoretical or straightforward terrorism, but should instead be treated as crime.193 This framework changed following the 9/11 attacks, as terrorist attacks have become a legal category unto themselves, and the response has included participation by intelligence agencies, law enforcement, and the military. The threats posed by terrorism have prompted the passage of new laws and the development of new law enforcement techniques in cyber-space.194 If it is possible that a cyber-terrorist attack could seriously undermine a citizenry’s faith in government, as Brenner suggests, then policymakers should identify cyber-terrorism as unique from cyber-crime, and devote serious attention to prevention and response.

E. Categories of Computer Network Attack

If cyber-terrorism is to be recognized as a unique type of CNA, it is important to distinguish it from other types of CNA. CNA has several sub-categories that this Article will distinguish by using three factors: damage done to the target information system, motivation of the attack, and identity of the attacker. The attack can be categorized and response options determined by identifying each of the three factors in a particular attack.

190. Id. at 393-94 (describing how generally terrorists’ goal is not to destroy but to demoralize).
191. Id. at 394 (stating that urbanized societies are more vulnerable to terrorism aimed at demoralisation).
192. See, e.g., Tony Smith, Hacker jailed for revenge sewage attacks, REGISTER (Oct. 31, 2001, 3:55 PM), http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ (describing a cyber-attack that caused annoyance, and stink, but caused little fear or serious damage).

1. Cyber-crime

This Article defines a cyber-crime as any level of CNA, conducted by any party, for any purpose that is considered illegal under domestic or international law. This sub-category is the broadest within CNA and includes every type of CNA outside those that occur in an armed conflict and do not violate the laws of war. Under U.S. domestic law, it is essentially any act that violates the CFAA.

Cyber-crimes need not have an information system as a target, as the definition includes those attacks simply using information systems as a tool. A current definition in use by the Computer Crime Research Center defines cyber-crime as “crimes committed on the Internet using the computer as either a tool or a targeted victim.”195 Although this Article argues a CNA does not have to be conducted through use of the Internet, this definition accurately reflects that information systems can be used to effectuate an attack and not just serve as the target. Those perpetrating CNAs frequently use means other than the Internet to access information systems.196 The Stuxnet virus, for example, is thought to have spread to information systems through an infected removable drive, as the target system was not connected to the Internet.197 This is important for a discussion of cyber-terrorism because many critical infrastructure components are not connected to outside networks as a security measure and must be accessed through another means.

2. Cyber-espionage

Cyber-espionage is a type of CNA by a state actor or government contractor, with the purpose of collecting intelligence against another state, which causes minimal damage or disruption to the information system. This definition does not incorporate non-national security related corporate espionage, as that is a more traditional cyber-crime. This is not to say that corporate espionage does not have national security implications. According to the DoD:

Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property

196. See, e.g., Zetter, supra note 107.
197. See id.; see also William J. Broad, John Markoff & David E. Sanger, Israel Tests Called Crucial In Iran Nuclear Setback, N. Y. TIMES, Jan. 16, 2011, at A1 (describing how Stuxnet spread and was solved).
loosely erode both U.S. military effectiveness and national competitiveness in the global economy. 198

However, the tools for dealing with traditional criminal actions, such as corporate espionage, diverge sharply from counter-intelligence.

Cyber-espionage also does not incorporate a CNA by a state actor that causes more than minor damage or degradation to a foreign network, as this would be classified as an armed attack in cyberspace. Whether or not an armed attack in cyberspace rises to the level of an act of war is a complicated calculus that has received considerable analysis from government sources and academics alike. 199 However, foreign governments routinely deny that they participate in armed attacks in cyberspace, as it is generally condemned as an unacceptable practice. 200 Cyber-espionage, on the other hand, is a generally internationally acceptable as a form of espionage, and presents a rising national security concern. 201 Cyber-espionage is neither clearly condoned nor explicitly allowed by international law, 202 but could be considered a covert action, which is generally prohibited by a state's laws.

Cyber-espionage is neither clearly international accepted as a form of espionage, and presents a rising national security concern. 201 Cyber-espionage is neither clearly condoned nor explicitly allowed by international law, 202 but could be considered a covert action, which is generally prohibited by a state's laws.

States criminalize spying under domestic laws and

199. See, e.g., Jorge Benitez, When Is a cyberattack an act of war?, ATLANTIC COUNCIL (Nov. 6, 2012, 1:43 PM), http://www.acus.org/natsource/when-cyberattack-act-war (“If the physical consequences of a cyberattack work the kind of physical damage that dropping a bomb or firing a missile would, that cyberattack should equally be considered a use of force.” If an attack reaches those levels, then a nation has a right to act in self-defense.”).
200. See, e.g., Estonia hit by ‘Moscow cyber war’, BBC (May 17, 2007, 3:21 PM), http://news.bbc.co.uk/2/hi/europe/6601455.stm (discussing Russia's denial of involvement in CNAs, despite the belief of many experts that the Russian Government does partake in CNAs).
202. Harold Hongis Koh, Legal Advisor U.S. Dep’t of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012) (stating the U.S. Government’s position is that international law applies to cyberspace, but that “this view has not been universal in the International community.”)
203. U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence, Part 5: Hearing Before the H. Select Comm. on Intelligence, 94th Cong. 1730 (1975) (defining a covert action as “any clandestine activity designed to influence foreign governments, events, organizations or persons in support of U.S. foreign policy, conducted in such manner that the involvement of the U.S. Government is not apparent”).
205. See Keating, supra note 93 (describing Titan Rain as one of the ten worst cyber-attacks).
207. See Nathan Thornburgh, The Invasion of the Chinese Cyberspies, TIME (Aug. 29, 2005), http://www.time.com/time/printout/0,8816,1058661,00.html (reporting that a civilian, Shawn Carpenter, was able to track the spies to Guangdong while working as a computer security analyst for Sandia National Laboratories).
208. Id.
209. Anthony Townsend, Hacker Attacks in US Linked to Chinese Military, BREITBART (Dec. 12, 2005), available at http://www.mail-archive.com/telecom-cities@forums.nyue.edu/msg00357.html (arguing that the attacks “have been traced to the Chinese province of Guangdong” and due to the techniques used it is “unlikely to come from any other source other than the military.”)
210. Cf. id. (describing the information that was probes, but not noting any disruption of operations).
losses erode both U.S. military effectiveness and national competitiveness in the global economy.198

However, the tools for dealing with traditional criminal actions, such as corporate espionage, diverge sharply from counter-intelligence. Cyber-espionage also does not incorporate a CNA by a state actor that causes more than minor damage or degradation to a foreign network. Whether or not an armed attack in cyberspace rises to the level of an act of war is a complicated calculus that has received considerable analysis from government sources and academics alike.199 However, foreign governments routinely deny that they participate in armed attacks in cyberspace, as it is generally condemned as an unacceptable practice.200 Cyber-espionage, on the other hand, is a generally internationally acceptable as a form of espionage, and presents a rising national security concern.201 Cyber-espionage is neither clearly condoned nor explicitly allowed by a state's internationally acceptable as a form of espionage, and presents a rising national security concern.202 Harold Hongju Koh, Legal Advisor to the President, Office of the Legal Counsel, Department of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012) (stating the U.S. Government's position is that international law applies to cyberspace, but that "this view has not been universal in the international community").

U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence, Part 5: Hearing Before the H. Select Comm. on Intelligence, 94th Cong. 1730 (1975) (defining a covert action as "any clandestine activity designed to influence foreign governments, events, organizations, or persons in support of U.S. foreign policy, conducted in such manner that the involvement of the U.S. Government is not apparent").


205. See Keating, supra note 93 (describing Titan Rain as one of the ten worst cyber-attacks).


207. See Nathan Thornburgh, The Invasion of the Chinese Cyberespionage, TIME (Aug. 29, 2005), http://www.time.com/time/printout/0,8816,1038961,00.html (reporting that a civilian, Shawn Carpenter, was able to track the spies to Guangdong while working as a computer security analyst for Sandia National Laboratories).

208. Id.

209. Anthony Townsend, Hacker Attacks in US Linked to Chinese Military, BREITBART (Dec. 12, 2005), available at http://www.mail-archive.com/telecom-cities@forums.nyu.edu/msg00357.html (arguing that the attacks "have been traced to the Chinese province of Guangdong" and due to the techniques used it is "unlikely to come from any other source other than the military").

210. Cf. id. (describing the information that was probed, but not noting any disruption of operations).
3. Armed Attack in Cyberspace

An armed attack in cyberspace is a CNA by or at the direction of a state actor that causes more than minor destruction, damage, or degradation to an information system itself, or anything outside the information system as a result of the CNA through the use of an information system. This term is often equated with cyber-warfare and is defined by Susan Brenner as follows:

Cyberwarfare is the conduct of military operations by virtual means. It consists of nation-states’ using cyberspace to achieve the same ends that they pursue through the use of conventional military force: achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them.

This close alliance with warfare has led to questioning of what kind of CNA would rise to the level of “use of force” and trigger law of war considerations. The DoD provides a vague standard, “[as in the physical world, a determination of what is a ‘threat or use of force’ in cyberspace must be made in the context in which the activity occurs, and it involves an analysis by the affected states of the effect and purpose of the actions in question.”

Charles Dunlap, former Deputy Staff Judge Advocate of the Air Force and current law professor, argues that a CNA resulting in violent effects is equivalent to an armed attack and therefore constitutes a use of force. As such, CNA that results in violent effects should, according to Dunlap, be governed by the conduct of state actors just as in traditional warfare under the laws of war. However, rarely have states acknowledged any role in cyber-warfare outside of actions taken during a declared conflict, because most actions that are taken by governments in this area are more precisely defined as covert actions. A classic example of a covert action in cyberspace is the infiltration of the Stuxnet computer virus against Iran; assuming that, as most analysts suspect, it was launched by a nation state. This Article identifies these types of cyber-attacks as armed attacks in cyberspace. A good example of armed attack in cyberspace is the 2008 conflict between Russia and Georgia. The conflict was over a province of Georgia, South Ossetia, which sought independence. The Russian government backed the separatists, and on August 8, 2008, the two sides clashed militarily. The Georgians were pushed out of South Ossetia on August 10, after two days of fighting. As the physical military conflict was taking place, a shadow conflict was taking place on the Internet. According to Georgian officials, Russian state-sponsored hackers launched an extensive CNA campaign against Georgian Government websites. The websites of Georgian President Mikheil Saakashvili, the Ministry of Foreign Affairs, and the Ministry of Defense were all forced offline as part of the attack. This CNA was unique in that it occurred in conjunction with a larger military campaign. Although the CNA did not affect the military operations, it did suppress the Georgian government’s ability to spread information to both its people and those abroad. This event likely foretells the increasingly large role that cyber-warfare will play in future military conflicts.

211. See Brenner, supra note 19, at 401 (stating how cyber-warfare is like traditional warfare in that it consists of nation-states “achieving advantages over a competing nation-state”).

212. Id.

213. See generally Charles J. Dunlap Jr., Perspectives for Cyber Strategists on Law for Cyberwar, STRATEGIC STUD. Q., Spring 2011, at 81-99 (arguing that the laws comprising the Law of Armed Conflict as existing are adequate to deal with the new development of cyber-warfare).

214. DEP’T OF DEF., CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 984, 9 (Nov. 2011).


216. Id.
3. Armed Attack in Cyberspace

An armed attack in cyberspace is a CNA by or at the direction of a state actor that causes more than minor destruction, damage, or degradation to an information system itself, or anything outside the information system as a result of the CNA through the use of an information system. This term is often equated with cyber-warfare and is defined by Susan Brenner as follows:

Cyberwarfare is the conduct of military operations by virtual means. It consists of nation-states' using cyberspace to achieve the same ends that they pursue through the use of conventional military force: achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them.

This close alliance with warfare has led to questioning of what kind of CNA would rise to the level of "use of force" and trigger law of war considerations. The DoD provides a vague standard, "as in the physical world, a determination of what is a 'threat or use of force' in cyberspace must be made in the context in which the activity occurs, and it involves an analysis by the affected states of the effect and purpose of the actions in question." Charles Dunlap, former Deputy Staff Judge Advocate of the Air Force and current law professor, argues that a CNA resulting in violent effects is equivalent to an armed attack and therefore constitutes a use of force. As such, CNA that results in violent effects should, according to Dunlap, be governed by the conduct of state actors just as in traditional warfare under the laws of war. However, rarely have states acknowledged any role in cyber-warfare outside of actions taken during a declared conflict, because most actions that are taken by governments in this area are more precisely defined as covert actions. A classic example of a covert action in cyberspace is the infiltration of the Stuxnet computer virus against Iran; assuming that, as most analysts suspect, it was launched by a nation state. This Article identifies these types of cyber-attacks as armed attacks in cyberspace.

A good example of armed attack in cyberspace is the 2008 conflict between Russia and Georgia. The conflict was over a province of Georgia, South Ossetia, which sought independence. The Russian government backed the separatists, and on August 8, 2008, the two sides clashed militarily. The Georgians were pushed out of South Ossetia on August 10, after two days of fighting. As the physical military conflict was taking place, a shadow conflict was taking place on the Internet. According to Georgian officials, Russian state-sponsored hackers launched an extensive CNA campaign against Georgian Government websites. The websites of Georgian President Mikheil Saakashvili, the Ministry of Foreign Affairs, and the Ministry of Defense were all forced offline as part of the attack. This was unique in that it occurred in conjunction with a larger military campaign. Although the CNA did not appear to affect the military operations, it did suppress the Georgian government's ability to spread information to both its people and those abroad. This event likely foretells the increasingly large role that cyber-warfare will play in future military conflicts.

211. See Brenner, supra note 19, at 401 (stating how cyber-warfare is like traditional warfare in that it consists of nation-states "achieving advantages over a competing nation-state").
212. Id.
213. See generally Charles J. Dunlap Jr., Perspectives for Cyber Strategists on Law for Cyberwar, STRATEGIC STUD. Q., Spring 2011, at 81-99 (arguing that the laws comprising the Law of Armed Conflict as existing are adequate to deal with the new development of cyber-warfare).
214. DEP'T OF DEF., CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECT. 834, 9 (Nov. 2011).
215. Siobhan Gorman & Julian E. Barnes, Cyber Combat: Act of War, Wall St. J., May 31, 2011, at A1 (arguing that cyber attacks "that have a violent effect are the legal equivalent of armed attacks").
216. Id.
4. Hacktivism

If these attacks had been conducted by civilians and had occurred completely outside a military conflict, how should the perpetrators be categorized? The answer would likely be as “hacktivists.” “Hacktivism” is often confused with cyber-terrorism, given that what distinguishes the two is, in some ways, only a matter of degree. The term was coined by a group of hackers called the Cult of the Dead Cow, who wished to use computer hacking to foster human rights and free expression. These groups are non-state actors who conduct politically motivated CNAs. However, the level of these attacks is relatively minor, and do not cause effects traditionally associated with terrorism, such as fear or panic in the civilian populace, affect national security, or damage to critical infrastructure. Although these groups do commit crimes, hacktivist groups are primarily distinguished from most cyber-criminals by their motivations. They are motivated by a desire to change a policy, practice or mode of thinking, as opposed to monetary gain or other traditional criminal motivation. Hacktivists have participated in numerous CNAs, opposing, or favoring, various groups or causes, such as attacks on Visa and MasterCard, and supporting WikiLeaks.

226. See Jay Dioxy Riboz, The Difference Between Hacktivism and Cyber Terrorism, InfoBarrel, Tech. (Dec. 18, 2009), http://www.infobarrel.com/The_Difference_Between_Hacktivism_and_Cyberterrorism (explaining that hacktivism is a “fusion of hacking and activism; politics and technology. . . . Cyber terrorism, on the other hand, is a computer-based attack or threat of attack”).


230. Id.

231. See GAO CYBERSECURITY, supra note 228, at 4.

232. Anonymous hacktivists say Wikileaks war to continue, BBC News (last updated Dec. 9, 2010, 4:10 ET), http://www.bbc.co.uk/news/technology-11903553 (reporting that Visa and MasterCard were hit with denial of service attacks after they withdrew their services from Wikileaks).


Hacktivism is certainly a growing phenomenon, but given the limited nature of the attacks as defined, it is probably not a major threat to national security. However, if the damage caused by hacktivists were to substantially increase and pose a threat to national security, then hacktivism would rise to the level of cyber-terrorism.

One of the largest hacktivist operations seen to date was termed the “50 days of Lulz.” In 2011, a group of hackers going by the name of Lulz, or Luizsec, engaged in a concentrated number of CNAs. For example, in May 2011, the popular PBS news show “Frontline” aired a show on Wikileaks that Lulz disagreed with. In response, Lulz hacked into the PBS website and posted a fake news story about Tupac Shakur being alive in New Zealand. Additionally, the group took down the Central Intelligence Agency’s website and released the personal information of millions of Sony PlayStation users. At least one leader of Lulz, known as Topiary, was arrested in the Shetland Islands. The CNA conducted by Lulz was certainly serious, particularly the release of the Sony PlayStation user data. However, in the age of Facebook, it is a stretch to argue that publicly releasing personal data constitutes terrorism. Just as definitions of terrorism require that the act’s effects rise to a certain level, so should a definition of cyber-terrorism in excluding these acts of hacktivism.

5. Terrorist Use of the Internet

When most people think of terrorist use of the Internet, they do not think of taking down the electric grid through a cyber-attack;
4. Hacktivism

If these attacks had been conducted by civilians and had occurred completely outside a military conflict, how should the perpetrators be categorized? The answer would likely be as “hacktivists.” “Hacktivism” is often confused with cyber-terrorism, given that what distinguishes the two is, in some ways, only a matter of degree. The term was coined by a group of hackers called the Cult of the Dead Cow, who wished to use computer hacking to foster human rights and free expression. These groups are non-state actors who conduct politically motivated CNAs. However, the level of these attacks is relatively minor, and do not cause effects traditionally associated with terrorism, such as fear or panic in the civilian populace, affect national security, or damage to critical infrastructure. Although these groups do commit crimes, hacktivist groups are primarily distinguished from most cyber-criminals by their motivations. They are motivated by a desire to change a policy, practice or mode of thinking, as opposed to monetary gain or other traditional criminal motivation. Hacktivists have participated in numerous CNAs, opposing, or favoring, various groups or causes, such as attacks on Visa and MasterCard and supporting WikiLeaks.

226. See Jay Dicky Riba, The Difference Between Hacktivism and Cyber Terrorism, InfoBarrel Tech. (Dec. 18, 2009), http://www.infobarrel.com/The_Difference_Between_Hacktivism_and _Cyberterrorism (explaining that hacktivism is a “fusin of hacking and activism; politics and technology. . . . Cyber terrorism, on the other hand, is a computer-based attack or threat of attack”).


230. Id.

231. See GAO CYBERSECURITY, supra note 228, at 4.

232. Anonymous hacktivists say Wikileaks war to continue, BBC NEWS (last updated Dec. 9, 2010, 4:10 ET), http://www.bbc.co.uk/news/technology-11935330 (reporting that Visa and MasterCard were hit with denial of service attacks after they withdrew their services from Wikileaks).


235. See Lewis, supra note 115.

236. See Riba, supra note 226.

237. See Keating, supra note 93.

238. Id.

239. See Poulsen, supra note 186.

240. Id.

241. See Keating, supra note 93.


Hacktivism is certainly a growing phenomenon, but given the limited nature of the attacks as defined, it is probably not a major threat to national security. However, if the damage caused by hacktivists were to substantially increase and pose a threat to national security, then hacktivism would rise to the level of cyber-terrorism.

One of the largest hacktivist operations seen to date was termed the "50 days of Lulz." In 2011, a group of hackers going by the name of Lulz, or LulzSec, engaged in a concentrated number of CNAs. For example, in May 2011, the popular PBS news show “Frontline” aired a show on Wikileaks that Lulz disagreed with. In response, Lulz hacked into the PBS website and posted a fake news story about Tupac Shakur being alive in New Zealand. Additionally, the group took down the Central Intelligence Agency’s website and released the personal information of millions of Sony PlayStation users. At least one leader of Lulz, known as Topiary, was arrested in the Shetland Islands. The CNA conducted by Lulz was certainly serious, particularly the release of the Sony PlayStation user data. However, in the age of Facebook, it is a stretch to argue that publicly releasing personal data constitutes terrorism. Just as definitions of terrorism require that the act's effects rise to a certain level, so should a definition of cyber-terrorism in excluding these acts of hacktivism.

5. Terrorist Use of the Internet

When most people think of terrorist use of the Internet, they do not think of taking down the electric grid through a cyber-attack;
instead, they picture Al-Qaeda posting a video online or other promotion measures.\textsuperscript{243} Terrorist organization presence on the Internet has thus far been dominated by using the Internet for planning, coordination, propaganda, and recruitment, which is what this Article defines as "terrorist use of the Internet."\textsuperscript{244} One of the earliest terrorist organizations to realize the potential of the Internet was Al-Qaeda, and it quickly became one of its most effective resources in becoming an international terrorist organization.\textsuperscript{245} Former chief of the CIA unit that tracked Osama Bin Laden, Michael Scheuer, stated a terrorist organization's use of the Internet "eroses the ability of our security services to hit them when they're most vulnerable, when they're moving."\textsuperscript{246} In a similar thought, State Department counter-terrorism expert Dennis Puchinsky finds the global jihad movement has become a "[web-directed] phenomenon."\textsuperscript{247}

Cyberspace is an ideal platform upon which to communicate and coordinate activities. Its speed, simplicity, ease of access, and anonymity makes it difficult to monitor and control.\textsuperscript{248} There are also reports that terrorist organizations have turned to traditional cyber-crimes such as theft and fraud to raise funds.\textsuperscript{249} Some experts believe that such activities are the extent of many terrorist organization's capabilities without a state sponsor, or an influx of highly trained computer personnel.\textsuperscript{250} Others, including the FBI, believe Al-Qaeda may try some act of cyber-terrorism.\textsuperscript{251} Either way, international terrorist organizations have learned the power of the Internet and are willing to use it in creative ways to accomplish their objectives. However, using information systems as a tool to further an organization's objectives is distinctly different from using those information systems as a weapon of terror. Al-Qaeda does not need to write malicious code or manipulate SCADA systems to help organize and fund the organization or to spread propaganda. The two categories will certainly connect in some ways, but the tools needed to counter them are fundamentally different.

Having defined cyber-terrorism, examined the elements of that definition, and distinguished it from other types of CNA, the next Section of this Article will examine examples of major acts of CNA to determine whether those attacks could be appropriately categorized as cyber-terrorism.

\textbf{SECTION III. RECENT EXAMPLES OF COMPUTER NETWORK ATTACK}

\textbf{"CIA TANGO DOWN"\textsuperscript{252}}

This Section examines several recent major examples of CNA to determine if they should be classified as cyber-terrorism. Specifically, this Section examines the effects, motives, and targets of the perpetrators of CNA, measuring them against the elements set out in the definition of cyber-terrorism.

\textbf{A. Anonymous}

Anonymous is an affiliation of hackers who have conducted an increasingly large number of attacks since the group's origin around

\textsuperscript{243} See Eben Kaplan, Terrorists and the Internet, COUNCIL ON FOREIGN REL. (Jan. 8, 2009), \texttt{http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005} (discussing the advantages the Internet offers terrorist organizations and how they use it).

\textsuperscript{244} See GABRIEL WEIMANN, TERROR ON THE INTERNET 25 (2006) (discussing how modern terrorist organizations exploit the Internet to raise funds, recruit members, plan and launch attacks, and publicize their results); see also Benjamin R. Davis, Note, Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance, 15 COLUM. INT’L L. REV. 119, 129 (2006-2007) (arguing the U.S. and foreign governments, as well as international bodies like ICANN, have failed to adequately respond to the use of the Internet by terrorist organizations).

\textsuperscript{245} Steve Coll & Susan B. Glasser, Terrorists Turn to the Web as Base of Operations, WASH. POST (Aug. 7, 2009), \texttt{http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR200508051138.html} (charting Al Qaeda’s migration from operating primarily in real space to operating in cyberspace).

\textsuperscript{246} Id.

\textsuperscript{247} Id.

\textsuperscript{248} See WEIMANN, supra note 244, at 25.

\textsuperscript{249} Jon Swartz, Terrorists use of Internet spreads, USA TODAY (Updated Feb. 21, 2005, 12:05 AM), \texttt{http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-ustat_x.htm} (citing examples of terrorist organizations using fraud on the internet to finance operations).

\textsuperscript{250} Mark Ward, Cyber terrorism ‘overhyped’, BBC (Mar. 14, 2003, 2:01 PM), \texttt{http://news.bbc.co.uk/2/hi/technology/2805441.stm} (stating the belief of several security experts that would-be online terrorists lack the technical expertise and resources to engage in cyber-terrorism).


\textsuperscript{252} Anonymous (YourAnonNews), TWITTER (Feb. 10, 2012, 12:25 PM), \texttt{https://twitter.com/YourAnonNews/status/16808014758009552.}
instead, they picture Al-Qaeda posting a video online or other promotion measures. Terrorist organization presence on the Internet has thus far been dominated by using the Internet for planning, coordination, propaganda, and recruitment, which is what this Article defines as "terrorist use of the Internet." One of the earliest terrorist organizations to realize the potential of the Internet was Al-Qaeda, and it quickly became one of its most effective resources in becoming an international terrorist organization. Former chief of the CIA unit that tracked Osama Bin Laden, Michael Scheuer, stated a terrorist organization’s use of the Internet "erodes the ability of our security services to hit them when they’re most vulnerable, when they’re moving." In a similar thought, State Department counter-terrorism expert Dennis Pluchinsky finds the global jihad movement has become a "[web-directed] phenomenon."

Cyberspace is an ideal platform upon which to communicate and coordinate activities. Its speed, simplicity, ease of access, and anonymity makes it difficult to monitor and control. There are also reports that terrorist organizations have turned to traditional cyber-crimes such as theft and fraud to raise funds. Some experts believe that such activities are the extent of many terrorist organization’s capabilities without a state sponsor, or an influx of highly trained computer personnel. Others, including the FBI, believe Al-Qaeda may try some act of cyber-terrorism. Either way, international terrorist organizations have learned the power of the Internet and are willing to use it in creative ways to accomplish their objectives. However, using information systems as a tool to further an organization’s objectives is distinctly different from using those information systems as a weapon of terror. Al-Qaeda does not need to write malicious code or manipulate SCADA systems to help organize and fund the organization or to spread propaganda. The two categories will certainly connect in some ways, but the tools needed to counter them are fundamentally different.

Having defined cyber-terrorism, examined the elements of that definition, and distinguished it from other types of CNA, the next Section of this Article will examine examples of major acts of CNA to determine whether those attacks could be appropriately categorized as cyber-terrorism.

SECTION III. RECENT EXAMPLES OF COMPUTER NETWORK ATTACK

"CIA TANGO DOWN"

This Section examines several recent major examples of CNA to determine if they should be classified as cyber-terrorism. Specifically, this Section examines the effects, motives, and targets of the perpetrators of CNA, measuring them against the elements set out in the definition of cyber-terrorism.

A. Anonymous

Anonymous is an affiliation of hackers who have conducted an increasingly large number of attacks since the group's origin around...
2003. The members of Anonymous are thought to be associated with Lulz. Some of the group's most notable targets include private organizations such as the Church of Scientology and Sony, government organizations including the CIA, and the Tunisian governments of Tunisia and Iran. Although many of their attacks have shown a high degree of coordination, the nature of the organization is somewhat informal.

In a 2011 interview with IT World reporter Dan Tynan, one Anonymous leader, known as Commander Anonymous, stated there were approximately ten thousand Anonymous members. Commander X stated that its targets are selected by considering several factors, including whether: 1) there are already protests in place against the target; 2) the protests are non-violent; 3) the protest has a likelihood of success; and 4) there is a clear moral imperative. Commander X does not define whose "moral imperative" guides their actions.

Clearly, Anonymous sees its actions as civil disobedience, using the language of morality to justify its actions. An example of this moralistic language was the recent launch of a cyber-campaign against Israel. Anonymous purportedly released a video that promised a "crusade" against Israel. The stated aim of Anonymous was "systematically removing [Israel] from the internet." The video cited Israel's "Zionist bigotry" and population displacement as reasons for the promised attacks.

In conjunction with the attack outlined at the beginning of this Article, these attacks raise the issue of whether Anonymous is a hacktivist organization or a cyber-terrorist organization. As already detailed, the group's attacks against justice and national security websites such as the FBI and DoJ, as well as the CIA attack, meet the definition of a federal crime of terrorism. Nevertheless, should the act of temporarily taking down a government website result in labeling a group as "terrorists"?

Examining the elements presented in this Article's definition of cyber-terrorism clarifies the answer. First is the prong of intent, which Anonymous clearly satisfies: Anonymous endeavors to undermine groups and organizations they disagree with, including governments. It also meets the requirement of being a non-state group, as it contains no known ties to a state. The last question is whether the effects of the group's attacks are designed to cause fear or anxiety in a civilian populace. This can be done through effects that cause widespread damage to critical physical or informational infrastructure, national security related information systems, critical economic systems, or that result in severe physical damage or human casualties.
The members of Anonymous are thought to be associated with Lulz. Some of the group's most notable targets include private organizations such as the Church of Scientology and Sony, government organizations including the CIA, and the Tunisian governments of Tunisia and Iran. Although many of their attacks have shown a high degree of coordination, the nature of the organization is somewhat informal. In a 2011 interview with IT World reporter Dan Tynan, one Anonymous leader, known as Commander X, stated there were approximately ten thousand Anonymous members. Commander X stated that its targets are selected by considering several factors, including whether: 1) there are already protests in place against the target; 2) the protests are non-violent; 3) the protest has a likelihood of success; and 4) there is a clear moral imperative. Commander X does not define whose "moral imperative" guides their actions.

Clearly, Anonymous sees its actions as civil disobedience, using the language of morality to justify its actions. An example of this moralistic language was the recent launch of a cyber-campaign against Israel. Anonymous purportedly released a video that promised a "crusade" against Israel. The stated aim of Anonymous was "systematically removing [Israel] from the internet." The video cited Israel's "Zionist bigotry" and population displacement as reasons for the promised attacks.

In conjunction with the attack outlined at the beginning of this Article, these attacks raise the issue of whether Anonymous is a hacktivist organization or a cyber-terrorist organization. As already detailed, the group's attacks against justice and national security websites such as the FBI and DoJ, as well as the CIA attack, meet the definition of a federal crime of terrorism. Nevertheless, should the act of temporarily taking down a government website result in labeling a group as "terrorists"?

Examining the elements presented in this Article's definition of cyber-terrorism clarifies the answer. First is the prong of intent, which Anonymous clearly satisfies: Anonymous endeavors to undermine groups and organizations they disagree with, including governments. It also meets the requirement of being a non-state group, as it contains no known ties to a state. The last question is whether the effects of the group's attacks are designed to cause fear or anxiety in a civilian populace. This can be done through effects that cause widespread damage to critical physical or informational infrastructure, national security related information systems, critical economic systems, or that result in severe physical damage or human casualties.

Given the nature of Anonymous' announcements, it would be easy for anyone to claim action in their name. However, the Author could find no statement repudiating the intended launch of a cyber-campaign against Israel by Anonymous. Donald MacIntyre, hacking group threatens 'crusade' against Israel, INDEPENDENT (Feb. 11, 2012), http://www.independent.co.uk/news/world/middle-east/hacking-group-threatens-crusade-against-israel-6720039.html?

Tyman, supra note 260 (reporting that Commander X stated that by victory, "[dictators on planes to Saudi Arabia works for us"].

See, e.g., Chris Landers, Serious Business, BALTIMORE SUN (Jan. 3, 2011, 12:14 AM), http://gawker.com/5722104/anonymous-attacks-tunisian-government-over-wikileaks-censorship (claiming that Anonymous's attack against the Tunisian Government's website may have been tied to the FBI arrests of the owners Megaupload.com, a popular music downloading service for its popular gaming system).


Nicole Perlroth, Anonymous Says It Knocked C.I.A. Site Offline, N.Y. TIMES Bits BLOG (Feb. 10, 2012, 5:14 PM), http://bits.blogs.nytimes.com/2012/02/10/anonymous-says-it-knocked-cia-site-offline/ (suggesting that Anonymous's attack against the CIA website may have been tied to the FBI arrests of the owners Megaupload.com, a popular music downloading service for its popular gaming system).

See Chris Landers, Serious Business, BALTIMORE SUN (Apr. 2, 2008), http://www2.citypaper.com/columns/story.asp?id=15543 (describing a 2008 dispute between the Church of Scientology and Anonymous that was a response in part to the Church of Scientology's claims of online copyright infringement).

See supra Section II; see also Poulben, supra note 186.
None of the attacks conducted by Anonymous or its affiliates have directly caused physical damage or human casualties, but the attacks have affected web operations for some national security related agencies through denial of service attacks. However, CNNAs that have resulted in the temporary take-down of websites, such as those of the FBI, White House, or CIA, should not be considered widespread damage. The public web pages of these websites, while important, are generally media outlets and general notices to the public. Additionally, the hacked websites are typically down only for a brief period. Should these attacks occur during a public emergency with increased reliance on those sites for vital information, the effects would likely meet the definitional element of cyber-terrorism.

Anonymous has also gone as far as to eavesdrop on the phone calls between the FBI and Scotland Yard. In this CNA, Anonymous was able to listen in on a conference call discussing efforts against hacking groups, raising the question of how deeply the group had infiltrated various law enforcement agencies. This infiltration should be considered more severe than the take-down of a website, as it could affect operations and, potentially, national security. However, the public effects of such actions are limited and should not be considered cyber-terrorism. Anonymous has not limited itself to denial of service attacks and other types of CNA may be a bit different.

In August 2011, the Bay Area Rapid Transit ("BART") administration in San Francisco announced that they would cut cell phone service in tunnels as a response to protests over the shooting of a man by BART police. Following this announcement, Anonymous leaked the names, phone numbers, and passwords of BART riders. Although Anonymous apologized to the riders for the release of their information, they blamed the release on BART for having lax security practices. The Oakland Police Chief responded by labeling the CNA an act of cyber-terrorism.

Loss of private data can be of great concern, and certainly affects these individuals’ lives more than website disruption, but does it rise to the level of fear and anxiety necessary to fit the definition of cyber-terrorism? As personal information placed on information systems becomes more prevalent, it also becomes more vulnerable to theft. An entire generation has become comfortable putting large amounts of personal information on the Internet. Although most people trust that this data is somewhat secure, an entire industry has grown up around information security and identity protection with companies such as Lifelock, Debitx, and TrustedID, which advertise identity-theft protection. There seems to be a constant flow of news stories about government agencies, banks, and other companies losing the private data of their clients or constituents. Is the knowledge that so much of our personal data is located in the hands of third parties limiting the effect of a release such as that of Anonymous? The line is a difficult one to draw, but in the specific case of BART, in which the...
None of the attacks conducted by Anonymous or its affiliates have directly caused physical damage or human casualties, but the attacks have affected web operations for some national security related agencies through denial of service attacks. However, CNAs that have resulted in the temporary takedown of websites, such as those of the FBI, White House, or CIA, should not be considered widespread damage. The public web pages of these agencies, while important, are generally media outlets and general notices to the public. Additionally, the hacked websites are typically down only for a brief period. Should these attacks occur during a public emergency with increased reliance on those sites for vital information, the effects would likely meet the definitional element of cyber-terrorism.

Anonymous has also gone so far as to eavesdrop on the phone calls between the FBI and Scotland Yard. In this CNA, Anonymous was able to listen in on a conference call discussing efforts against hacking groups, raising the question of how deeply the group had infiltrated various law enforcement agencies. This infiltration should be considered more severe than the take-down of a website, as it could affect operations and, potentially, national security. However, the public effects of such actions are limited and should not be considered cyber-terrorism. Anonymous has not limited itself to denial of service attacks and other types of CNA may be a bit different.

In August 2011, the Bay Area Rapid Transit ("BART") administration in San Francisco announced that they would cut cell phone service in tunnels as a response to protests over the shooting of a man by BART police. Following this announcement, Anonymous leaked the names, phone numbers, and passwords of BART riders. Although Anonymous apologized to the riders for the release of their information, they blamed the release on BART for having lax security practices. The Oakland Police Chief responded by labeling the CNA an act of cyber-terrorism.

Loss of private data can be of great concern, and certainly affects these individuals' lives more than website disruption, but does it rise to the level of fear and anxiety necessary to fit the definition of cyber-terrorism? As personal information placed on information systems becomes more prevalent, it also becomes more vulnerable to theft. An entire generation has become comfortable putting large amounts of personal information on the Internet. Although most people trust that this data is somewhat secure, an entire industry has grown up around information security and identity protection with companies such as Lifelock, Debit, and TrustedID, which advertise identity-theft protection. There seems to be a constant flow of news stories about government agencies, banks, and other companies losing the private data of their clients or constituents. Is the knowledge that so much of our personal data is located in the hands of third parties limiting the effect of a release such as that of Anonymous? The line is a difficult one to draw, but in the specific case of BART, in which the...
data release was limited to user names and passwords, the loss was not substantial enough to be considered cyber-terrorism.

Thus, the actions of Anonymous, while troublesome to many, do not yet rise to the level of cyber-terrorism. Its rhetoric may suggest radical or even occasionally violent aims, but its actions do not rise to that level. However, this does not mean that as Anonymous' capabilities increase the likelihood that the group will not attempt a CNA that rises to the level of cyber-terrorism. The National Security Agency ("NSA") has warned that by 2014, Anonymous could have the ability to bring down portions of the U.S. power grid, which should be considered cyber-terrorism as a CNA on critical infrastructure. NSA had been silent regarding Anonymous to this point, making the statement particularly notable. Additionally, Anonymous announced plans to "blackout" the Internet by attacking the Domain Name System to protect "our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun." Time will tell if Anonymous truly has the intention and capability to carry out such attacks. Given the nature of the organization and the manner in which it distributes its messages, it is difficult to determine whether these statements are legitimately from Anonymous. At this point, Anonymous is an example of a hacktivist group that has generally well-defined motivations, but whose attacks are more of nuisance than a true threat to national security. Sometime in the future, however, Anonymous may meet the definition of a cyber-terrorist organization.

Anonymous' actions are a variety of attacks that have resulted in large-scale damage but with less clearly-defined motivation. The ILOVEYOU virus and its variants are a prime example of this type of CNA. The ILOVEYOU virus was estimated to have infected forty-five million users and cost billions of dollars in damage. The suspected creator, Ouel de Guzman, was allegedly motivated by the rejection of his thesis on computer vulnerabilities. If a physical bombing in the United States caused billions of dollars in damage but no injuries, and had political motivation, it would likely meet the definition of an act of terrorism. However, although the ILOVEYOU virus did just that, a different analysis must be used when examining CNA. The effects of CNA are generally much more widespread and lack the shock of that results from a physical attack. Therefore, the working definition of cyber-terrorism should be analyzed to determine whether an act of cyber-terrorism has truly taken place.

The ILOVEYOU virus does not rise to the level of cyber-terrorism under this Article's definition. First, there is insufficient evidence that the attack was politically-motivated. The attacks did not appear to target government or national security institutions. Additionally, no message declaring intent to undermine government authority was left under the ILOVEYOU virus.

Anonymous may meet the definition of a cyber-terrorist organization. The effects of Anonymous' attack may be more serious than the effects of other such attacks. The attacks have been more widespread and more damaging than those of other groups. Additionally, the attacks have been more politically-motivated than those of other groups. Anonymous' attacks have been more successful than those of other groups. Additionally, the attacks have been more politically-motivated than those of other groups.
data release was limited to user names and passwords, the loss was not substantial enough to be considered cyber-terrorism.

Thus, the actions of Anonymous, while troublesome to many, do not yet rise to the level of cyber-terrorism. Its rhetoric may suggest radical or even occasionally violent aims, but its actions do not rise to that level. However, this does not mean that as Anonymous’ capabilities increase the likelihood that the group will not attempt a CNA that rises to the level of cyber-terrorism. The National Security Agency (“NSA”) has warned that by 2014, Anonymous could have the ability to bring down portions of the U.S. power grid, which should be considered cyber-terrorism as a CNA on critical infrastructure. NSA had been silent regarding Anonymous to this point, making the statement particularly notable. Additionally, Anonymous announced plans to “blackout” the Internet by attacking the Domain Name System to protest “our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun. Time will tell if Anonymous’ capabilities increase the likelihood that the group will to this point, making the statement particularly notable. Additionally, Anonymous announced plans to “blackout” the Internet by attacking the Domain Name System to protest “our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun. Time will tell if


282. Kevin Fogarty, NSA: Anonymous may take down U.S. power grid in two years, IT WORLD (Feb. 21, 2012, 2:12 PM), http://www.itworld.com/security/251450/“(nsa-anonymous-may-take-down-us-power-grid-two-years” (stating that the NSA has treated Anonymous “much more even-handed” than other groups).


Anonymous truly has the intention and capability to carry out such attacks. Given the nature of the organization and the manner in which it distributes its messages, it is difficult to determine whether these statements are legitimately from Anonymous. At this point, Anonymous is an example of a hacktivist group that has generally well-defined motivations, but whose attacks are more of nuisance than a true threat to national security. Sometime in the future, however, Anonymous may meet the definition of a cyber-terrorist organization.

B. ILOVEYOU virus

Opposite to Anonymous’ actions are a variety of attacks that have resulted in large-scale damage but with less clearly-defined motivation. The ILOVEYOU virus and its variants are a prime example of this type of CNA. The ILOVEYOU virus was estimated to have infected forty-five million users and cost billions of dollars in damage. The suspected creator, Onel de Guzman, was allegedly motivated by the rejection of his thesis on computer vulnerabilities. If a physical bombing in the United States caused billions of dollars in damage but no injuries, and had political motivation, it would likely meet the definition of an act of terrorism. However, although the ILOVEYOU virus did just that, a different analysis must be used when examining CNA. The effects of CNA are generally much more widespread and lack the shock of that results from a physical attack. Therefore, the working definition of cyber-terrorism should be analyzed to determine whether an act of cyber-terrorism has truly taken place.

The ILOVEYOU virus does not rise to the level of cyber-terrorism under this Article’s definition. First, there is insufficient evidence that the attack was politically-motivated. The attacks did not appear to target government or national security institutions. Additionally, no message declaring intent to undermine government
or influence policy was released in conjunction with the attack. However, under examination of the effects element, the answer is less clear. Although the attack was not aimed at national security systems or infrastructure, it had a significant effect on business and affected the networks of the CIA, Pentagon, and British Parliament. Given the scale of the damage, had these attacks been politically-motivated, they would likely have risen to the level of cyber-terrorism. However, because the attack fails the intent element, the ILOVEYOU should be categorized as a cyber-crime.

C. U.S. Power Grid

In April 2009, U.S. officials discovered hackers from Russia, China, and other countries had gained access to the U.S. power grid and left behind tools that could have destroyed system controls. The intrusions could not be definitively traced to either state or non-state actors. The motivations of the intrusions were not clearly understood as the attacks were never carried out. Speculations include the belief that Russian and Chinese governments gained access so that in the event of a future conflict, the grid could be shut down or otherwise affected. The threat to the various power grids operating in the United States has prompted the Energy Department to launch an initiative into protecting the grid from CNA. Losing control over the power grid could have cascading effects with disastrous consequences for hospitals, emergency responders, defense and law enforcement agencies, and the financial sector, among others. In an armed conflict, the power grid is often among the first targets because it can debilitate a nation's command and control structure. Given the potential effect on society, a CNA that takes down a significant portion of a region's power grid for any extended period passes the effects test element of cyber-terrorism. If a non-state actor committed the 2009 intrusions into the power grid, then they should be considered an act in preparation for a cyber-terrorist attack and treated just as seriously as an attempted attack.

D. Stuxnet

Between June 2009 and May 2010, a type of computer virus known as a worm was discovered to have damaged SCADA systems that controlled centrifuges for the Iranian nuclear program. The worm most likely infected the software using a portable drive, such as a thumb drive. Given the sophistication of the CNA, experts conclude it would have required the resources of a national government to engineer, and the most likely culprit was Israel. Initially, Stuxnet spread indiscriminately, but the virus was designed to target only a very specific type of system, and to only affect intended targets. Although there were no reports of radiation energy to find and contain gaps in the cyber security defenses protecting the nation's electric grid.

290. Id.
291. Id.
292. John Markoff, An "I Love You" Virus Becomes Anything But, N.Y. TIMES, May 7, 2000, WK2 (reporting that the White House, Pentagon, Congress and the British House of Commons were among those affected by the ILOVEYOU virus).
294. Gorman, supra note 293, at A2.
295. Id.
296. Id.
298. Lewis II, supra note 293, at 1.
300. A worm is a type of CNA that replicates itself and sends those copies to other systems it comes in contact with. Worms can carry other computer viruses, or replicate and spread to use bandwidth. See Definition of: Worm, PC MAG ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia_term/0,2542,f%3Dworms&i%3D54874,00.asp (last accessed Feb. 19, 2013).
302. Id.
303. See Broad, Markoff & Sanger, supra note 197 (reporting that some experts point to a secret facility in Israel’s Negev desert where they claim Israel has a set of nuclear centrifuges similar to Iran’s, where they tested Stuxnet).
304. Jonathan Field, Stuxnet virus targets and spread revealed, BBC (last updated Feb. 15, 2011, 8:51), http://www.bbc.co.uk/news/technology-
or influence policy was released in conjunction with the attack.\textsuperscript{290} However, under examination of the effects element, the answer is less clear. Although the attack was not aimed at national security systems or infrastructure, it had a significant effect on business\textsuperscript{291} and affected the networks of the Parliament.\textsuperscript{292} Given the scale of the damage, had these attacks been politically-motivated, they would likely have risen to the level of cyber-terrorism. However, because the attack fails the intent element, the ILOVEYOU should be categorized as a cyber-crime.

C. U.S. Power Grid

In April 2009, U.S. officials discovered hackers from Russia, China, and other countries had gained access to the U.S. power grid and left behind tools that could have destroyed system controls.\textsuperscript{293} The intrusions could not be definitively traced to either state or non-state actors.\textsuperscript{294} The motivations of the intrusions were not clearly understood, as the attacks were never carried out.\textsuperscript{295} Speculations include the belief that Russian and Chinese governments gained access so that in the event of a future conflict, the grid could be shut down or otherwise affected.\textsuperscript{296}

The threat to the various power grids operating in the United States has prompted the Energy Department to launch an initiative into protecting the grid from CNA.\textsuperscript{297} Losing control over the power grid could have cascading effects with disastrous consequences for hospitals, emergency responders, defense and law enforcement agencies, and the financial sector, among others.\textsuperscript{298} In an armed conflict, the power grid is often among the first targets because it can debilitate a nation’s command and control structure.\textsuperscript{299} Given the potential effect on society, a CNA that takes down a significant portion of a region’s power grid for any extended period passes the effects test element of cyber-terrorism. If a non-state actor committed the 2009 intrusions into the power grid, then they should be considered an act in preparation for a cyber-terrorist attack and treated just as seriously as an attempted attack.

D. Stuxnet

Between June 2009 and May 2010, a type of computer virus known as a worm,\textsuperscript{300} was discovered to have damaged SCADA systems that controlled centrifuges for the Iranian nuclear program.\textsuperscript{301} The worm most likely infected the software using a portable drive, such as a thumb drive.\textsuperscript{302} Given the sophistication of the CNA, experts conclude it would have required the resources of a national government to engineer, and the most likely culprit was Israel.\textsuperscript{303} Initially, Stuxnet spread indiscriminately, but the virus was designed to target only a very specific type of system, and to only affect intended targets.\textsuperscript{304} Although there were no reports of radiation energy to find and contain gaps in the cyber security defenses protecting the nation’s electric grid.

290. Id.
291. Id.
292. John Markoff, An “I Love You” Virus Becomes Anything But, N.Y. TIMES, May 7, 2000, WK2 (reporting that the White House, Pentagon, Congress and the British House of Commons were among those affected by the ILOVEYOU virus).
294. Gorman, supra note 293, at A2.
295. Id.
296. Id.
298. Lewis II, supra note 293, at 1.
300. A worm is a type of CNA that replicates itself and sends those copies to other systems it comes in contact with. Worms can carry other computer viruses, or replicate and spread to use up bandwidth. See Definition of: Worm, PC MAG ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia_term/0,2542,t33Dworm&i33D54874,00.asp (last accessed Feb. 19, 2013).
302. Id.
303. See Broad, Markoff & Sanger, supra note 197 (reporting that some experts point to a secret facility in Israel’s Negev desert where they claim Israel has a set of nuclear centrifuges similar to Iran’s, where they tested Stuxnet).
304. Jonathan Fildes, Stuxnet Virus Targets and Spread Revealed, BBC (last updated Feb. 15, 2011, 8:51), http://www.bbc.co.uk/news/technology-
leakage from the affected sites, the NATO ambassador to Russia stated the virus "could lead to a new Chernobyl."305

The Stuxnet virus should not be considered an act of cyber-terrorism because the prevailing opinion was that it was a covert CNA conducted by a nation state.306 Therefore, the appropriate categorization is as an armed attack in cyberspace. However, it is interesting from a cyber-terrorism perspective because it represents the potential for future cyber-terrorist attacks on SCADA software operating critical infrastructure systems. That no deaths or violence resulted from the Stuxnet virus is not a factor weighing against potential classification as cyber-terrorism. Knowing that a nuclear facility has been targeted would be enough to cause a state of fear for those living near an affected facility. Were it to be revealed that this facility for political purposes would rank as a terrorist attack.307 facilities, or similar facilities such as chemical plants that produce weapons as weapons of mass destruction.308

E. Estonia

In April of 2007, Estonia was one of the most wired nations in the world.309 The Estonians had pioneered a system of "e-government," making many government services and functions available through the Internet,310 Estonia prided itself on both its Internet savvy and cyber-security.311

12465688 ("Once on a corporate network, the worm is designed to seek out a specific configuration of industrial control software made by Siemens.").

305. Id.

306. See Broad, Markoff & Sangor, supra note 197.


308. See infra Section V(D), for a discussion of this classification.


310. Clark Boyd, Estonia opens politics to the web, BBC (May 7, 2004, 7:02 PM), http://news.bbc.co.uk/2/hi/technology/3600601.stm (following independence from the Soviet Union, Estonia made a nationwide push to educate citizens in use of the Internet and place as many government functions online as possible).

311. Traynor, supra note 309.

312. Id.

313. Id. (noting the main targets of the attacks included the “Estonian presidency and its parliament[,] almost all of the country’s government ministries[,] political parties[,] three of the country’s six big new organisations[,] two of the biggest banks; and firms specializing in communications[.]”).

314. Id.

315. Id.


317. See Traynor, supra note 309 (noting that Estonia is “highly dependent on computers”).

318. See id. (“With their reputation for electronic prowess, the Estonians have been quick to marshal their defense[,]”).
leakage from the affected sites, the NATO ambassador to Russia stated the virus "could lead to a new Chernobyl." The Stuxnet virus should not be considered an act of cyber-terrorism because the prevailing opinion was that it was a covert CNA conducted by a nation state. Therefore, the appropriate categorization is as an armed attack in cyberspace. However, it is interesting from a cyber-terrorism perspective because it represents the potential for future cyber-terrorist attacks on SCADA software operating critical infrastructure systems. That no deaths or violence resulted from the Stuxnet virus is not a factor weighing against potential classification as cyber-terrorism. Knowing that a nuclear facility has been targeted would be enough to cause a state of fear for those living near an affected facility. Were it to be revealed that this CNA was actually the result of a non-state actor, it should certainly be considered cyber-terrorism.

Under almost any definition of terrorism, an attack on a nuclear facility for political purposes would rank as a terrorist attack. Given the potentially severe consequences of CNA on nuclear facilities, or similar facilities such as chemical plants that produce dangerous gas, these types of attacks should receive particularly close attention. These sophisticated cyber-weapons that have the unique potential for cyber-terrorism, such as Stuxnet, should be classified as weapons as weapons of mass destruction.

E. Estonia

In April of 2007, Estonia was one of the most wired nations in the world. The Estonians had pioneered a system of "e-government," making many government services and functions available through the Internet. Estonia prided itself on both its Internet savvy and cyber-security.

12465689 ("Once on a corporate network, the worm is designed to seek out a specific configuration of industrial control software made by Siemens.").

304. Id.

305. See Broad, Markoff & Sanger, supra note 197.


307. See infra Section V(D), for a discussion of this classification.

308. See infra Section V(D), for a discussion of this classification.


310. Clark Boyd, Estonia opens politics to the web, BBC (May 7, 2004, 7:02 PM), http://news.bbc.co.uk/2/hi/technology/3690661.stm (following independence from the Soviet Union, Estonia made a nationwide push...

...to educate citizens in use of the Internet and place as many government functions online as possible).

311. Traynor, supra note 309.

312. Id.

313. Id. (noting the main targets of the attacks included the "Estonian presidency and its parliament, almost all of the country’s government ministries, political parties, three of the country's six big new organisations, two of the biggest banks; and firms specializing in communications.").

314. Id.

315. Id.


317. See Traynor, supra note 309 (noting that Estonia is “highly dependent on computers”).

318. See id. ("With their reputation for electronic prowess, the Estonians have been quick to marshal their defense.").
ordination committee, believed the attack to be an act of terrorism, and stated:

This is a kind of terrorism, the act of terrorism is not to steal from a state, or even to conquer it. It is, as the word suggests, to sow terror itself. If a highly IT country cannot carry out its every day activities, like banking, it sows terror among the people. 318

Tammet’s use of the word terrorism may have been intended to pressure Russia into investigating the attacks, but it may also have reflected the anxiety of the nation as a whole, given the unique connection, through the Internet, between the Government and people of Estonia. 320 Thus, this attack meets the effects test, not necessarily due to the nature of the attacks, but because of the nature of Estonian society.

The last question when examining the CNA against Estonia is determining the perpetrator. The identity of the attacker as either the Russian Government or a non-state actor was never completely resolved; this situation represents the difficulty of determining attribution even in large-scale attacks. 321 Jaak Aaviksoo, Estonia’s defense minister, stated, “There is not sufficient evidence of a [Russian] governmental role.” 322 Moreover, Estonia estimated at least one million computers were used in the attack. 323 Hackers can easily control this many computers with a bot-net. 324 Additionally, Estonian officials discovered that many of the attacks had been routed through Russian government servers, but again, this was inconclusive. 325 The ambiguity of who conducted the CNA against Estonia is an excellent example of the difficulty attribution creates in classifying a CNA.

SECTION IV. THE CURRENT LAW AND PROBLEMS

“The pessimist sees difficulty in every opportunity. The optimist sees the opportunity in every difficulty.” 326

In the previous Sections, this Article sought to define cyber-terrorism and apply the definition in the context of some recent examples of CNA. Logically, the next issue to address is how to best fight cyber-terrorism. This Section first examines the main hindrance in combating CNA in general and cyber-terrorism specifically: attribution. It then examines current domestic cyber-crime and counter-terror laws to determine how these existing laws might be used to counter cyber-terrorism.

A. The Dilemma of Attribution

Perhaps the greatest challenge in confronting cyber-terrorism is the problem of attribution: identifying the party or parties responsible for a CNA. 327 The problem of attribution in the context of the Internet is, in large part, inherent in the structure of the system. 328 Many hackers are now able to “spoof” Internet Protocol Addresses, which allows them to make their CNA appear to originate from another location. 329 This is an issue common to all cyber-crimes and is recognized by the government and private industry alike. The DoD stated that “[t]he Internet was designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identity authentication was less important than connectivity.” 330 The United
ordination committee, believed the attack to be an act of terrorism, and stated:

This is a kind of terrorism, the act of terrorism is not to steal from a state, or even to conquer it. It is, as the word suggests, to sow terror itself. If a highly IT country cannot carry out its every day activities, like banking, it sows terror among the people.318

Tammet’s use of the word terrorism may have been intended to pressure Russia into investigating the attacks, but it may also have reflected the anxiety of the nation as a whole, given the unique connection, through the Internet, between the Government and people of Estonia.320 Thus, this attack meets the effects test, not necessarily due to the nature of the attacks, but because of the nature of Estonian society.

The last question when examining the CNA against Estonia is determining the perpetrator. The identity of the attacker as either the Russian Government or a non-state actor was never completely resolved; this situation represents the difficulty of determining attribution even in large-scale attacks.321 Jaak Aaviksoo, Estonia’s defense minister, stated, “There is not sufficient evidence of a [Russian] governmental role.”322 Moreover, Estonia estimated at least one million computers were used in the attack.323 Hackers can easily control this many computers with a bot-net.324 Additionally, Estonian officials discovered that many of the attacks had been routed through Russian government servers, but again, this was inconclusive.325 The ambiguity of who conducted the CNA against Estonia is an excellent example of the difficulty attribution creates in classifying a CNA.

SECTION IV. THE CURRENT LAW AND PROBLEMS

“The pessimist sees difficulty in every opportunity. The optimist sees the opportunity in every difficulty.”326

In the previous Sections, this Article sought to define cyber-terrorism and apply the definition in the context of some recent examples of CNA. Logically, the next issue to address is how to best fight cyber-terrorism. This Section first examines the main hindrance in combating CNA in general and cyber-terrorism specifically: attribution. It then examines current domestic cyber-crime and counter-terrorism laws to determine how these existing laws might be used to counter cyber-terrorism.

A. The Dilemma of Attribution

Perhaps the greatest challenge in confronting cyber-terrorism is the problem of attribution: identifying the party or parties responsible for a CNA.327 The problem of attribution in the context of the Internet is, in large part, inherent in the structure of the system.328 Many hackers are now able to “spoof” Internet Protocol Addresses, which allows them to make their CNA appear to originate from another location.329 This is an issue common to all cyber-crimes and is recognized by the government and private industry alike. The DoD stated that “[t]he Internet was designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identity authentication was less important than connectivity.”330 The United Nations in its

321. See Traynor II, supra note 316; but see Robert Coalson, "Behind The Estonia Cyberattacks", RADIO FREE EUR. (Mar. 6, 2009), http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html (describing a remark by a State Duma Deputy from the pro-Kremlin Unified Russia party that his assistant was responsible for coordinating the attack, but clarifying that his assistant acted on his own accord).
322. Traynor II, supra note 316.
323. See Adrian Bloomfield, Estonia calls for Nato cyber­terrorism strategy, TELEGRAPH (May 18, 2007, 12:01 AM) (noting that “hackers used robots to infiltrate hundreds of thousands of computers around the world . . . [which] then flooded Estonian websites”).
324. See Cytus Farivar, What the attacks on Estonia have taught us about online combat, SLATE (May 22, 2007), http://www.slate.com/articles/technology/technology/2007/05/cyberwar.html (defining botnet as “a network of computers that have been surreptitiously infected to run nefarious software”).
325. Traynor, supra note 309.
326. Winston Churchill.
328. See LarSEN & Wheeler, supra note 327, at 2-4; see also Dycus, supra note 327.
329. See Gable, supra note 176, at 102.
States Computer Emergency Readiness Team noted that the "[t]he speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult." The Internet's anonymity has proved remarkably adept at foiling law enforcement attempts at enforcing laws governing and deterring cyber-crime.

Without the ability to catch and prosecute, there is little deterrence for would-be cyber-criminals. For this reason, many jurisdictions place harsh penalties on cyber-crimes, in relation to similar crimes conducted without the use of information systems.

The current head of U.S. Cyber Command, then-Lieutenant General Keith Alexander, articulated, "The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do." Attribution is a necessity to enable traditional deterrence as well as to distinguish between the categories of CNA.

Susan Brenner framed the issue of attribution elegantly, stating, "Cyberspace fractures the crime scene into shards." One shard can be considered the place or places where the attack is felt. In widespread attacks such as the ILOVEYOU virus, there may be millions of shards. Additional shards include the information systems through which the attack was conducted. Expert cyber-criminals tend to route their attack through a maze of servers across the world to maintain anonymity. Finally, there are the shards of the attackers, who may have planned and launched the attack from multiple information systems at multiple locations across the globe. And, as is the case in some distributed denial of service attacks, the attacking computers may be operating without their owner having any knowledge of the attack.

The shattering of the crime scene immensely complicates law enforcement efforts to track the perpetrators. Whereas most traditional crimes require some physical proximity between perpetrator and victim, the same is not true in cyberspace. Law enforcement agents are forced to navigate a web of state, federal, and international jurisdictions to trace an attack to its origin, and then must tie an individual or individuals to an information system from which the attack was launched. A serious result of this fracturing occurs when investigators mistake an intermediary point of transmission for the attack's originating point.

The discussion on how to deal with the attribution dilemma has led to many interesting ideas, including using civilian enforcement to help deter cyber-criminals. These ideas include how to deal with attribution in large-scale attacks. For greater-scale attacks, some

333. Id. (discussing the addition of harsher penalties for organized crime groups that engage in acts of cyber-crime).
335. See Bambauer, supra note 36, at 598 (arguing that information, not systems, should be the focus of cyber-security); cf. Brenner, supra note 19, at 438.
337. ORACLE THINKQUEST EDUC. FOUND., supra note 285 (noting that the attack was thought to have affected forty-five million computers worldwide).
338. Brenner, supra note 19, at 418-19 (noting that "[c]yber variable crime scene shards . . . are the intermediary points of transmission used in the attack").
339. Id. (describing the various locations from which an attack can be launched).
340. Id.
341. See e.g., Franz-Stefan Gady, Africa’s Cyber WMD, FOREIGN POLICY (Mar. 24, 2010), http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd (describing how one could turn Africa’s computer network into a host of “zombie computers”).
342. See Brenner, supra note 19, at 418 ("Aside from anything else, a fractured crime scene can result in false positives-in investigators assuming that an intermediary point of transmission of an attack is the originating point for the attack.").
343. See generally Darrel Mente, Jurisdiction In Cyberspace: A Theory of International Spaces 4 MICH. TELECOMM. & TECH. L. REV. 69 (1998) (examining jurisdictional laws and arguing Internet jurisdiction should be analogized to Antarctica, outer space, and the high seas, and treated as an “international space”).
344. Brenner, supra note 19, at 418.
345. See, e.g., id. at 465–74 (advocating a redistribution of responsibility for the identification of cyber criminals to civilians to improve cybercrime investigations).
States Computer Emergency Readiness Team noted that the “speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult.” The Internet’s anonymity has proved remarkably adept at foiling law enforcement attempts at enforcing laws governing and deterring cyber-crime.

Without the ability to catch and prosecute, there is little deterrence for would-be cyber-criminals. For this reason, many jurisdictions place harsh penalties on cyber-crimes, in relation to traditional deterrence as well as to distinguish between the categories of similar crimes conducted without the use of information systems.

The current head of U.S. Cyber Command, then-Lieutenant General Keith Alexander, articulated, “The bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do.” Attribution is a necessity to enable traditional deterrence as well as to distinguish between the categories of CNA.

Susan Brenner framed the issue of attribution elegantly, stating, “Cyberspace fractures the crime scene into shards.” One shard can be considered the place or places where the attack is felt. In widespread attacks such as the ILOVEYOU virus, there may be millions of shards. Additional shards include the information systems, should be the focus of cyber-security); cf. Brenner, supra note 19, at 438.

332. See Kathryn Stephens, A Review of the Cybersecurity Legislative Proposal, NAT’L SEC. CYBERSPACE INST., 1 (June 15, 2011), http://www.nsci-va.org/WhitePapers/2011-06-15-Federal%20Cyber%20Legislative%20Proposal%20Whitepaper-KS20Stephens.pdf (reviewing the proposed penalties for cyber-crime, but noting “these guidelines are much needed, and will at least send a message to criminals who engage in cyber crime, they are reactional and do little to help prevent cyber-attacks or address the frequently discussed challenge of attribution”).

333. Id. (discussing the addition of harsher penalties for organized crime groups that engage in acts of cyber-crime).


335. See Bambauer, supra note 36, at 588 (arguing that information, not systems, should be the focus of cyber-security); id. at 418.


337. ORACLE THINKQUEST EDUC. FOUND., supra note 285 (noting that the attack was thought to have affected forty-five million computers worldwide).

338. Brenner, supra note 19, at 418-19 (noting that “[c]yber, variable crime scene shards . . . are the intermediary points of transmission used in the attack”).

339. Id. (describing the various locations from which an attack can be launched).

340. Id.

341. See e.g., Frank-Stephan Grady, Africa’s Cyber WMD, FOREIGN POL’Y (Mar. 24, 2010), http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd (describing how one could turn Africa’s computer network into a host of “sombwe computers”).

342. See Brenner, supra note 19, at 418 (“Aside from anything else, a fractured crime scene can result in false positives-in investigators assuming that an intermediary point of transmission of an attack is the originating point for the attack.”).

343. See generally Darrel Menthe, Jurisdiction In Cyberspace: A Theory of International Spaces 4 MICH. TELECOMM. & TECH. L. REV. 69 (1998) (examining jurisdictional laws and arguing Internet jurisdiction should be analogized to Antarctica, outer space, and the high seas, and treated as an “international space”).

344. Brenner, supra note 19, at 418.

345. See, e.g., id. at 465-74 (advocating a redistribution of responsibility for the identification of cyber criminals to civilians to improve cybercrime investigations).
have favored imputing attribution directly to the state where the attack originated, under a strict liability theory.\textsuperscript{346} Some have also suggested that this approach should apply to traditional acts of terrorism.\textsuperscript{347} This theory is difficult to apply to CNA because of the ease of launching a cyber-attack from any state in the world. Would it be unjust to hold Senegal responsible if an Iranian cyber-terrorist traveled to Dakar, connected to the Internet, and launched his attack that he had planned and developed in Tehran? This theory also assumes that governments have the financial or technical capabilities to adequately monitor their networks.

The Chinese government has attempted to solve attribution problems by enacting a series of laws that require Internet users identify themselves.\textsuperscript{348} These laws include mandatory registration requirements, requirements on ISPs to track users' activity, and regulation of cyber cafes.\textsuperscript{349} These steps have resulted in a general feeling among the Chinese people that "every bit of [their] activity" can be attributed back to them.\textsuperscript{350} Even if these legal attempts to eliminate anonymity on the Internet were successful, it is highly unlikely that such methods could be implemented in the western world for constitutional and human rights reasons.\textsuperscript{351} If governments cannot eliminate the problem of attribution entirely, for a variety of reasons governments will also not be able to rely upon attribution as a primary means of prevention.

346. See David E. Graham, Cyber Threats and the Law of War, 4 J. Nat'l Sec. L. & Pol'y 87, 92-93 (2010) (seeking to impute responsibility to states for attacks originating from that state's territory); see also Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 Mil. L. Rev. 1, 6-7 (2000) (arguing that a state's use of cyber-defenses against CNA emanating from states that do not adequately prevent such attacks).


349. Id. at 111-112.

350. Id. at 112.

351. Id. at 110 ("It is not even clear that it would be constitutional to mandate such a requirement in the United States.").

---

B. Current Domestic Law Relating to Cyber-Crimes

The question now becomes what strategies can be implemented to assist in the ultimate goal of preventing cyber-terrorist attacks? To help answer this question, this Section addresses current cyber and terrorism laws to determine their applicability in helping to deter cyber-terrorism. This Section reviews current laws drafted for, or commonly applied to, cyber-crimes. This collection of statutes is not an exhaustive list of cyber-related crimes, but rather the discussion includes those statutes that are most potentially applicable to cyber-terrorism.

1. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA")\textsuperscript{352} proscribes a number of cyber activities.\textsuperscript{353} Originally enacted pursuant to a federal interest in protecting computers, it established criminal liability for the use of computers to commit trespass, making threats to others, damaging computers, and committing espionage and fraud.\textsuperscript{354} The act was broadened significantly through several amendments,\textsuperscript{355} eventually protecting:

- Computers in which there is a federal interest—federal computers, bank computers, and computers used in or effecting interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud.\textsuperscript{356}

Thus, the CFAA now covers every computer that is connected to the internet, a conduit to "interstate and foreign commerce."


353. OFF. LEGAL EDUC.: EXC. OF. FOR. U.S. ATT'YS, PROSECUTING COMPUTER CRIMES, 1 (2d ed. 2010) (noting that "[i]n the CFAA, Congress attempted to strike an appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of States to prescribe and punish such offenses").


355. Id. at iv.

have favored imputing attribution directly to the state where the attack originated, under a strict liability theory. Some have also suggested that this approach should apply to traditional acts of terrorism. This theory is difficult to apply to CNA because of the ease of launching a cyber-attack from any state in the world. Would it be unjust to hold Senegal responsible if an Iranian cyber-terrorist traveled to Dakar, connected to the Internet, and launched his attack?

The Chinese government has attempted to solve attribution problems by enacting a series of laws that require Internet users to identify themselves. These laws include mandatory registration requirements, requirements on ISPs to track users’ activity, and regulation of cyber cafes. These steps have resulted in a general feeling among the Chinese people that “every bit of [their] activity” can be attributed back to them. Even if these legal attempts to eliminate anonymity on the Internet were successful, it is highly unlikely that such methods could be implemented in the western world for constitutional and human rights reasons. If governments cannot eliminate the problem of attribution entirely, for a variety of reasons governments will also not be able to rely upon attribution as a primary means of prevention.

346. See David E. Graham, Cyber Threats and the Law of War, 4 J. Nat’l Sec. L. & Pol’y 87, 92-93 (2010) (seeking to impute responsibility to states for attacks originating from that state’s territory); see also Matthew J. Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 Mil. L. Rev. 1, 6-7 (2009) (arguing that a state’s use of cyber-defenses against CNA emanating from states that do not adequately prevent such attacks).


349. Id. at 111-112.

350. Id. at 112.

351. Id. at 110 (“It is not even clear that it would be constitutional to mandate such a requirement in the United States.”).

B. Current Domestic Law Relating to Cyber-Crimes

The question now becomes what strategies can be implemented to assist in the ultimate goal of preventing cyber-terrorist attacks? To help answer this question, this Section addresses current cyber and terrorism laws to determine their applicability in helping to deter cyber-terrorism. This Section reviews current laws drafted for, or commonly applied to, cyber-crimes. This collection of statutes is not an exhaustive list of cyber-related crimes, but rather the discussion includes those statutes that are most potentially applicable to cyber-terrorism.

1. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") prescribes a number of cyber activities. Originally enacted pursuant to a federal interest in protecting computers, it established criminal liability for the use of computers to commit trespass, making threats to others, damaging computers, and committing espionage and fraud. The act was broadened significantly through several amendments, eventually protecting:

- Computers in which there is a federal interest—federal computers, bank computers, and computers used in or effecting interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud.

Thus, the CFAA now covers every computer that is connected to the internet, a conduit to “interstate and foreign commerce.”


353. OFF. LEGAL EDUC.: EXEC. OFF. FOR U.S. ATT’YS, PROSECUTING COMPUTER CRIMES, 1 (2d ed. 2010) (noting that “[i]n the CFAA, Congress attempted to strike an appropriate balance between the Federal Government’s interest in computer crime and the interests and abilities of States to prescribe and punish such offenses.”).


355. Id. at iv.

There are seven distinct crimes outlawed by the CFAA. Although not originally intended as a counter-terrorism statute, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (commonly

known as the "PATRIOT ACT") added two provisions to the list of

offenses that, if violated in conjunction with a political purpose and

certain violent effects, meet the definition of a federal crime of
terrorism. This Section discusses those provisions and reviews the

various uses of some CFAA provisions for combating cyber-terrorism.

Section C(1) will discuss the implications of the federal crime of
terrorism.

Section 1030(a)(1) prohibits unauthorized access of a computer to
obtain national security related information, including restricted
nuclear data, and using it to harm the United States or to aid an
enemy of the United States. The provision essentially prohibits
cyber-espionage. The substantial penalty for a first time offense, up
to ten years imprisonment, could make this subsection an effective
prosecution tool, if an attack can be attributed.

Section 1030(a)(2) applies to almost any crime involving

computers, as it prohibits intentionally accessing a computer without
authorization or exceeding the user's authorized access to obtain
information from any protected computer. The statute requires a
showing that the subject has obtained information, but this must be read while keeping in mind accompanying legislative history that
states that "the Committee wishes to make clear that 'obtaining
information' in this context includes mere observation of the data." The penalties under §1030(a)(2) are normally misdemeanors that can
be charged as felonies with up to a five-year sentence if "the offense

was committed in furtherance of any criminal or tortious act." This

statute could be used effectively against organizations with
terrorist aspirations that conduct smaller scale CNA or engage in
preparatory CNA for a larger attack.

Section 1030(a)(3) applies to the unauthorized access of U.S.
Government computers. This is a simple trespass statute and is
limited in its applicability; the statute does not require that the

defendant obtain any information in the commission of the crime.
Therefore, if a cyber-terrorist plot involved accessing a Government
computer, and officials caught the cyber-terrorist while exploring that
computer for vulnerabilities, this statute could apply. The downside
to this law for prosecution of large-scale cyber attacks is that it is a
misdemeanor, unless the defendant has a prior §1030 conviction.
Sections 1030(a)(2)-(3) could be used in a manner similar to "spitting
on the sidewalk" offenses used to combat traditional terrorism.

Section 1030(a)(5) deals with using a computer to cause damage
to a protected computer. The Government is most likely to use this
statute following an actual event of cyber-terrorism. It has the
advantage of being very broad in scope and provides increasing
penalties when the CNA causes certain harms. Depending on the
effects of the attack, these penalties can reach up to twenty years
imprisonment or life. Additionally, a violation of §1030(a)(5)(A), if
one "knowingly causes the transmission of a program, information,

336. § 1030(c)(2)(B) (stating that an offense "committed for commercial
advantage or private financial gain" results in a similar range of
penalties).

337. (defining violating acts as intentional, unauthorized access to
"any nonpublic computer of a department or agency of the United
States that is exclusively for the use of the government of the United
States or, in the case of a computer not exclusively for such use, is used
by or for the Government of the United States and such conduct effects
that use by or for the Government of the United States").

338. § 1030(c)(2)(A) (stating the punishment scheme for repeat offenders).

339. Amy Goldstein, A Deliberate Strategy of Disruption, WASH. POST,
Nov. 4, 2001, at A1 (discussing in part Attorney General John Ashcroft's use
of minor crimes to prevent or investigate terrorist crimes. Ashcroft
stated, "Robert Kennedy's Justice Department, it is said, would arrest
mobsters spitting on the sidewalk if it would help in the battle against
organized crime.")

340. § 1030(a)(5) (describing the various damaging effects that qualify under
this provision).

341. § 1030(c)(2)-(F) (stipulating that if the attack causes serious bodily
injury, then the penalty is a maximum of twenty years imprisonment,
and if a death occurs as a result of the attack the penalties range up to
life imprisonment).
There are seven distinct crimes outlawed by the CFAA. Although not originally intended as an anti-terrorism statute, the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (commonly known as the “PATRIOT ACT”) added two provisions to the list of offenses that, if violated in conjunction with a political purpose and certain violent effects, meet the definition of a federal crime of terrorism. This Section discusses those provisions and reviews the various uses of some CFAA provisions for combating cyber-terrorism. Section C(1) will discuss the implications of the federal crime of terrorism.

The offense 1030(a)(1) prohibits unauthorized access of a computer to obtain national security related information, including restricted nuclear data, and using it to harm the United States or to aid an enemy of the United States. The provision essentially prohibits cyber-espionage. The substantial penalty for a first time offense, up to ten years imprisonment, could make this subsection an effective prosecution tool, if an attack can be attributed.

Section 1030(a)(2) applies to almost any crime involving computers, as it prohibits intentionally accessing a computer without authorization or exceeding the user’s authorized access to obtain information from any protected computer. The statute requires a showing that the subject has obtained information, but this must be read while keeping in mind accompanying legislative history that states that “the Committee wishes to make clear that ‘obtaining information’ in this context includes mere observation of the data.” The penalties under §1030(a)(2) are normally misdemeanors that can be charged as felonies with up to a five-year sentence if “the offense was committed in furtherance of any criminal or tortious act . . .” This statute could be used effectcively against organizations with terrorist aspirations that conduct smaller scale CNA or engage in preparatory CNA for a larger attack.

Section 1030(a)(3) applies to the unauthorized access of U.S. Government computers. This is a simple trespass statute and is limited in its applicability; the statute does not require that the defendant obtain any information in the commission of the crime. Therefore, if a cyber-terrorist plot involved accessing a Government computer, and officials caught the cyber-terrorist while exploring that computer for vulnerabilities, this statute could apply. The downside to this law for prosecution of large-scale cyber attacks is that it is a misdemeanor, unless the defendant has a prior §1030 conviction. Sections 1030(a)(2)-(3) could be used in a manner similar to “spitting on the sidewalk” offenses used to combat traditional terrorism.

Section 1030(a)(5) deals with using a computer to cause damage to a protected computer. The Government is most likely to use this statute following an actual event of cyber-terrorism. It has the advantage of being very broad in scope and provides increasing penalties when the CNA causes certain harms. Depending on the effects of the attack, these penalties can reach up to twenty years imprisonment or life. Additionally, a violation of §1030(a)(5)(A), if one “knowingly causes the transmission of a program, information, was committed in furtherance of any criminal or tortious act . . .” This statute could be used effectively against organizations with terrorist aspirations that conduct smaller scale CNA or engage in preparatory CNA for a larger attack.

Section 1030(a)(3) applies to the unauthorized access of U.S. Government computers. This is a simple trespass statute and is limited in its applicability; the statute does not require that the defendant obtain any information in the commission of the crime. Therefore, if a cyber-terrorist plot involved accessing a Government computer, and officials caught the cyber-terrorist while exploring that computer for vulnerabilities, this statute could apply. The downside to this law for prosecution of large-scale cyber attacks is that it is a misdemeanor, unless the defendant has a prior §1030 conviction. Sections 1030(a)(2)-(3) could be used in a manner similar to “spitting on the sidewalk” offenses used to combat traditional terrorism.

Section 1030(a)(5) deals with using a computer to cause damage to a protected computer. The Government is most likely to use this statute following an actual event of cyber-terrorism. It has the advantage of being very broad in scope and provides increasing penalties when the CNA causes certain harms. Depending on the effects of the attack, these penalties can reach up to twenty years imprisonment or life. Additionally, a violation of §1030(a)(5)(A), if one “knowingly causes the transmission of a program, information, was committed in furtherance of any criminal or tortious act . . .” This statute could be used effectively against organizations with terrorist aspirations that conduct smaller scale CNA or engage in preparatory CNA for a larger attack.

Section 1030(a)(3) applies to the unauthorized access of U.S. Government computers. This is a simple trespass statute and is limited in its applicability; the statute does not require that the defendant obtain any information in the commission of the crime. Therefore, if a cyber-terrorist plot involved accessing a Government computer, and officials caught the cyber-terrorist while exploring that computer for vulnerabilities, this statute could apply. The downside to this law for prosecution of large-scale cyber attacks is that it is a misdemeanor, unless the defendant has a prior §1030 conviction. Sections 1030(a)(2)-(3) could be used in a manner similar to “spitting on the sidewalk” offenses used to combat traditional terrorism.

Section 1030(a)(5) deals with using a computer to cause damage to a protected computer. The Government is most likely to use this statute following an actual event of cyber-terrorism. It has the advantage of being very broad in scope and provides increasing penalties when the CNA causes certain harms. Depending on the effects of the attack, these penalties can reach up to twenty years imprisonment or life. Additionally, a violation of §1030(a)(5)(A), if one “knowingly causes the transmission of a program, information, was committed in furtherance of any criminal or tortious act . . .” This statute could be used effectively against organizations with terrorist aspirations that conduct smaller scale CNA or engage in preparatory CNA for a larger attack.

Section 1030(a)(3) applies to the unauthorized access of U.S. Government computers. This is a simple trespass statute and is limited in its applicability; the statute does not require that the defendant obtain any information in the commission of the crime. Therefore, if a cyber-terrorist plot involved accessing a Government computer, and officials caught the cyber-terrorist while exploring that computer for vulnerabilities, this statute could apply. The downside to this law for prosecution of large-scale cyber attacks is that it is a misdemeanor, unless the defendant has a prior §1030 conviction. Sections 1030(a)(2)-(3) could be used in a manner similar to “spitting on the sidewalk” offenses used to combat traditional terrorism.

Section 1030(a)(5) deals with using a computer to cause damage to a protected computer. The Government is most likely to use this statute following an actual event of cyber-terrorism. It has the advantage of being very broad in scope and provides increasing penalties when the CNA causes certain harms. Depending on the effects of the attack, these penalties can reach up to twenty years imprisonment or life. Additionally, a violation of §1030(a)(5)(A), if one “knowingly causes the transmission of a program, information,
code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer," also falls under the § 2332b terrorism statute if one of the following causes damage without authorization, to a protected computer during any one-year period. Of particular interest is subsection (V), which would make attacks on most government websites a terrorist act. Additionally, subsection (VI) virtually ensures that any active hacking group is now guilty of terrorism.

Section 1030(a)(7) deals with the use of computers for extortion and transmitting threats. This section is potentially useful in combating organizations that threaten cyber-terrorism acts when officials lack sufficient evidence to link them to a particular attacks. Overall, the CFCA provides a wide range of tools for law enforcement to charge organizations with crimes pertaining to acts of cyber-terrorism. When viewed through the lens of prevention, the CFCA’s main use may be the prosecution of cyber-terrorists before the terrorists acquire the capabilities to conduct such an attack. The expansive penalties possible under § 1030 may serve to effectively criminalize and punish any act of cyber-terrorism. However, the CFCA is still a very traditional criminal law statute because it is focused on after-the-fact prosecution for particular instances of misconduct in which each act can be attributed to an actor. The CFCA only prevents future misconduct through deterrence, which, as previously discussed, is inadequate in the cyber-crime environment. Congress must enact additional laws that go to the heart of prevention to supplement after-the-fact prosecution.

2. Access Device Fraud

Section 1029, “Fraud and related activity in connection with access devices,” outlaws the production, use, possession, and/or trafficking of unauthorized or counterfeit access devices. The DoJ manual, Prosecuting Computer Crimes, recommends using the statute

372. § 1030(a)(5)(B)(ii)-(v).
373. § 1030(a)(7).
374. 18 U.S.C. § 1029(a) (2012) (listing qualifying access devices, including telecommunications equipment, scanning receivers, software, hardware, and credit card systems).
code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer," also falls under the § 2332b terrorism statute if one of the following elements is met under § 1030(a)(4)(A)(I)(II)-(VI). These elements include: (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or, (VI) damage affecting 10 or more protected computers during any one-year period. Of particular interest is subsection (V), which would make attacks on most government websites a terrorist act. Additionally, subsection (VI) virtually ensures that any active hacking group is now guilty of terrorism.

Section 1030(a)(7) deals with the use of computers for extortion and transmitting threats. This section is potentially useful in combating organizations that threaten cyber-terrorism acts when officials lack sufficient evidence to link them to a particular attacks.

Overall, the CF AL provides a wide range of tools for law enforcement to charge organizations with crimes pertaining to acts of cyber-terrorism. When viewed through the lens of prevention, the CF AL’s main use may be the prosecution of cyber-terrorism before the terrorists acquire the capabilities to conduct such an attack. The expansive penalties possible under § 1030(a)(7) may serve to effectively criminalize and punish any act of cyber-terrorism. However, the CF AL is still a very traditional criminal law statute because it is focused on after-the-fact prosecution for particular instances of misconduct in which each act can be attributed to an actor. The CF AL only prevents future misconduct through deterrence, which, as previously discussed, is inadequate in the cyber-crime environment. Congress must enact additional laws that go to the heart of prevention to supplement after-the-fact prosecution.

2. Access Device Fraud

Section 1029, “Fraud and related activity in connection with access devices,” outlaws the production, use, possession, and/or trafficking of unauthorized or counterfeit access devices. The DoJ manual, Prosecuting Computer Crimes, recommends using the statute to prosecute perpetrators who employ “phishing” emails to obtain passwords and financial information. This statute could be useful for prosecuting groups suspected of intending to commit acts of cyber-terrorism, as gaining access to computer systems would likely be an initial step in the development of any cyber-terrorism scheme.

C. Domestic Counter-Terrorism Law That Relate to Cyber-Terrorism

In addition to laws that specifically pertain to cyber-crime, a number of laws that the Government uses to prosecute terrorism offenses may also be relevant to cyber-terrorism. This Section examines these laws to determine their applicability.

1. The Federal Crime of Terrorism

The federal crime of terrorism is defined as a violation of any offense listed in § 2332b(g)(5)(B), when that violation “is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct.” The federal crime of terrorism has several implications including an increased statute of limitations, increased maximum term of supervised release, and a presumption against release on bail.

Section 2332b provides prosecutors with important tools for preventing cyber-terrorism. Prosecutors can request supervised release for life instead of the traditional five years, which could prevent a convicted terrorist from being able to strike in a more significant manner a second time. A court’s denial of bail for a defendant suspected of trying to launch a cyber-terrorism attack may also help prevent an attack in its early stages. Additionally, the CF AL violations that are included as predicate offenses in § 375, Office of Legal Educ. & Exec. Office for U.S. Att’ys, Prosecuting Computer Crimes 102 (2d ed. 2010) (defining “phishing” as “where a defendant uses fraudulent emails to obtain bank account numbers and passwords”).

376. § 2332b(g)(5) (defining the requisite intent and violations for culpability).

377. § 3286(g)(a) (noting an eight-year statute of limitations for certain offenses and no limitation for others).

378. § 3583(l) (specifying the supervised release terms for convicted terrorists as “any term of years or life”).

379. See § 3142(g)(1) (noting the judicial officer should take into account that the person had been charged with the federal crime of terrorism into account when determining if bail is available); see also Charles Doyle, Cong. Research Serv., RL307102, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws 38-39 (2010) (describing the presumption against bail).
2332b(g)(5)(B), are also included as predicate offenses in the material support to terrorism statutes, 18 U.S.C. §§ 2339A and 2339B.380

2. Material Support to Terrorism Statutes

One of the most successful prosecutorial methods in combating terrorism is the use of the material-support statutes.381 These laws work well as a prevention method because they inhibit the flow of resources to a terrorist group,382 which hampers the ability to carry out attacks. Outlawing material support to terrorists is comprised primarily of two statutes: 18 U.S.C. §§ 2339A and 2339B.383 Section 2339A outlaws providing material support or resources, when the provider knows that the support will be used to carry out of a violation of certain offenses deemed to rise to the level of terrorism.384 Section 2339B outlaws the provision of any support or resources to designated terrorist organizations.385

Section 2339A is applicable to cyber-terrorism in two situations. First, use of a computer to aid a terrorist is technically a qualifying violation of the statute.386 Thus, one who provides computer training or support to a terrorist organization, knowing that the organization intends to use that training to prepare for or perform an act of terrorism, would violate § 2339A, which poses a punishment of up to fifteen years in prison.387 More directly relevant is the second situation. Section 2339A incorporates two CFCA provisions as predicate offenses.388 The statute includes “any offense listed in § 2332(b)(g)(5)(B),” which, as seen above, incorporates §§ 1030(c)(1), and § 1028(a)(5)(A).389 Under § 2339A, providing any kind of material support includes:

[...]

Section 2339B prohibits providing material support to designated foreign terrorist organizations ("FTO").390 This statute prohibits knowingly providing material support and resources to a FTO.391 Additionally, financial institutions that become aware that they have control over accounts of a FTO must freeze those funds and report to the Secretary of State.392 The Secretary of State may designate an FTO if he finds that: first, the organization is foreign based; second, the organization engages in terrorist activity; and, third, this activity threatens the security of the United States or its nationals.393 The U.S. Code primarily defines terrorist activity as premeditated, politically-motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.394

380. Compare the predicate offenses listed in §2332b(g)(5)(B), with the predicate offenses listed in § 2339A, and § 2339B.
382. §§ 2339A, 2339B (prescribing acts of providing resources to terrorists).
383. Id.
384. § 2339A (codifying the offense of providing material support to terrorists).
385. § 2339B (barring providing material support to foreign terrorist organizations).
386. § 2339A (noting the qualifying provisions, including: §§ 32, 37, 81, 175, 220, 351, 831, 842 (m) or (n), 844 (f) or (l), 930 (c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1901, 2155, 2156, 2286, 2288, 2289, 2302, 2302a, 2302b, 2302b, 2340a, or 2442 of title 18, § 236 of the Atomic Energy Act of 1954 (42 U.S.C. § 2284), § 46502 or 60123 (b) of title 49, or any offense listed in § 2332b (g)(5)(B) (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act.).
387. § 2339A(a) (allowing for a life sentence if the death of a person results from the prohibited act).
388. Id.
389. § 2332(b)(g)(5)(B) (listing predicate offenses).
390. § 2339B(b)(1) (defining "support").
392. § 2339B(a)(1) (describing prohibited conduct).
393. § 2339B(a)(2) (stating the conditions under which financial institutions must report possession of funds).
394. 48 U.S.C. § 1189(a)(1) (2006); see also Foreign Terrorist Organizations, U.S. DEPT. OF STATE (Sept. 28, 2012) http://www.state.gov/j/ct/rls/other/des/123085.htm (noting the current list of FTOs and the procedure that the Secretary of State follows to designate them as such).
2332(b)(5)(B), are also included as predicate offenses in the material support to terrorism statutes, 18 U.S.C. §§ 2339A and 2339B.\(^{380}\)

2. Material Support to Terrorism Statutes

One of the most successful prosecutorial methods in combating terrorism is the use of the material-support statutes.\(^{381}\) These laws work well as a prevention method because they inhibit the flow of resources to a terrorist group,\(^{382}\) which hampers the ability to carry out attacks. Outlawing material support to terrorists is comprised primarily of two statutes: 18 U.S.C. §§ 2339A and 2339B.\(^{383}\) Section 2339A outlaws providing material support or resources, when the provider knows that the support will be used to carry out any of certain offenses deemed to rise to the level of terrorism.\(^{384}\) Section 2339B outlaws the provision of any support or resources to designated terrorist organizations.\(^{385}\)

Section 2339A is applicable to cyber-terrorism in two situations. First, use of a computer to aid a terrorist is technically a qualifying violation of the statute.\(^{386}\) Thus, one who provides computer training or support to a terrorist organization, knowing that the organization intends to use that training to prepare for or perform an act of terrorism, would violate § 2339A, which poses a punishment of up to fifteen years in prison.\(^{387}\) More directly relevant is the second situation. Section 2339A incorporates two CFAA provisions as predicate offenses.\(^{388}\) The statute includes “any offense listed in § 2332(b)(5)(B),” which, as above, incorporates § 1030(a)(1), and § 1028(a)(5)(A).\(^{389}\) Under § 2339A, providing any kind of material support includes:

- [Any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials.\(^{390}\)]

Section 2339B prohibits providing material support to designated foreign terrorist organizations ("FTO").\(^{391}\) This statute prohibits knowingly providing material support and resources to a FTO.\(^{392}\) Additionally, financial institutions that become aware that they have control over accounts of a FTO must freeze those funds and report to the Secretary of State.\(^{393}\) The Secretary of State may designate an FTO if he finds that: first, the organization is foreign based; second, the organization engages in terrorist activity; and, third, this activity threatens the security of the United States or its nationals.\(^{394}\) The U.S. Code primarily defines terrorist activity as premeditated, politically-motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.\(^{395}\)

380. Compare the predicate offenses listed in §2332(b)(5)(B), with the predicate offenses listed in §§ 2339A, and § 2339B.


382. §§ 2339A, 2339B (proscribing acts of providing resources to terrorists).

383. Id.

384. § 2339A (codifying the offense of providing material support to terrorists).

385. § 2339B (barring providing material support to foreign terrorist organizations).

386. § 2339A (noting the qualifying provisions, including: §§ 32, 37, 81, 175, 229, 351, 831, 842 (m) or (n), 844 (f) or (i), 930 (c), 929, 1091, 1114, 1116, 1201, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2322, 2332a, 2332b, 2332c, 2340A, or 2443 of title 18, § 236 of the Atomic Energy Act of 1954 (42 U.S.C. § 2284), § 46502 or 60123 (b) of title 49, or any offense listed in § 2332b (g)(5)(B) (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspiracies to do such an act.).

387. § 2339A(a) (allowing for a life sentence if the death of a person results from the prohibited act).

388. Id.

389. § 2332b(g)(5)(B) (listing predicate offenses).

390. § 2339A(b)(1) (defining "support").


392. § 2339B(a)(1) (describing prohibited conduct).

393. § 2339B(a)(2) (stating the conditions under which financial institutions must report possession of funds).

394. 8 U.S.C. § 1189(a)(1) (2006); see also Foreign Terrorist Organizations, U.S. DEPT. OF STATE (Sept. 28, 2012) http://www.state.gov/j/ct/rls/other/des/123085.htm (noting the current list of FTOs and the procedure that the Secretary of State follows to designate them as such).

When looking to prevent cyber-terrorism, the downside of this statute is twofold. First, the statute requires that the organization be foreign-based. It can be difficult to define whether a cyber-terrorist organization is foreign or domestic, given the lack of physical infrastructure required to maintain the organization. Theoretically, no training camps are required and the members do not even need to reside in the same place. However, this could cut both ways, as almost every hacking organization is, at least in part, foreign.

Second, it is unclear whether this definition of terrorist activity could include cyber-terrorism. The statute does not explicitly mention CNA, and the statute’s definition of terrorism requires violence. As previously discussed, CNA may result in fear and anxiety among the populace without producing violent effects.

It remains uncertain how much utility the material support statutes would have in combating cyber-terrorism. CNA is clearly included in § 2339A, but the applicability of § 2339B to cyber-terrorism is much less clear. This Article will discuss in Section V(A) how the material-support statutes can be amended to make them a more valuable tool in preventing cyber-terrorism.

3. Specially Designated Global Terrorist under Executive Order 13224

Under Executive Order 13224 and related regulations, the Executive branch can attach the label of Specially Designated Global Terrorist (“SDGT”) to terrorist groups, individuals acting as part of a terrorist organization, and other entities providing financial support or assistance. The Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, may designate as “Specially Designated Nationals” (“SDN”) individuals or entities that are determined “to be owned or controlled by, or act for or on behalf of” an individual or entity so designated. Further, the Secretary of State may deem it appropriate to add those, with the approval of the Secretary of Treasury, who “assist in, sponsor, or provide financial, material, or technological support for...acts of terrorism” or individuals or entities so designated; or who are found “to be otherwise associated with” certain individuals or entities designated in or under the Order. Most SDGTs and SDNs are foreign persons, but the late Anwar al-Awlaki, a U.S. citizen, was mistakenly designated as an SDGT.

Executive Order 13224 defines terrorism as an activity that involves “a violent act or an act dangerous to human life, property, or infrastructure.” The act must “appear[] to be intended — (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.”

Here the applicability of Executive Order 13224 to cyber-terrorism depends upon the interpretation of its provision that that the attack be “an act dangerous to human life, property, or infrastructure.” If the Government considers data to be property and information systems to be infrastructure, then the Executive Order could certainly apply to cyber-terrorism.

4. Conspiracy

When looking to prevent cyber-terrorism, the downside of this statute is twofold. First, the statute requires that the organization be foreign-based. It can be difficult to define whether a cyber-terrorist organization is foreign or domestic, given the lack of physical infrastructure required to maintain the organization. Theoretically, no training camps are required and the members do not even need to reside in the same place. However, this could cut both ways, as almost every hacking organization is, at least in part, foreign.

Second, it is unclear whether this definition of terrorist activity could include cyber-terrorism. The statute does not explicitly mention CNA, and the statute's definition of terrorism requires violence. As previously discussed, CNA may result in fear and anxiety among the populace without producing violent effects. It remains uncertain how much utility the material support statutes would have in combating cyber-terrorism. CNA is clearly included in § 2339A, but the applicability of § 2339B to cyber-terrorism is much less clear. This Article will discuss in Section V(A) how the material-support statutes can be amended to make them a more valuable tool in preventing cyber-terrorism.

3. Specially Designated Global Terrorist under Executive Order 13224

Under Executive Order 13224 and related regulations, the Executive branch can attach the label of Specially Designated Global Terrorist ("SDGT") to terrorist groups, individuals acting as part of a terrorist organization, and other entities providing financial support or assistance. The Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, may designate foreign individuals or entities that have been determined to have committed, or pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States. Additionally, the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, may designate as "Specially Designated Nationals" ("SDN") individuals or entities that are determined "to be owned or controlled by, or act for or on behalf of" an individual or entity so designated. Further, the Secretary of State may deem it appropriate to add those, with the approval of the Secretary of Treasury, who "assist in, sponsor, or provide financial, material, or technological support for . . . acts of terrorism" or individuals or entities so designated; or who are found "to be otherwise associated with" certain individuals or entities designated in or under the Order. Most SDGTs and SDNs are foreign persons, but the late Anwar al-Awlaki, a U.S. citizen, was mistakenly designated as an SDGT.

Executive Order 13224 defines terrorism as an activity that involves "a violent act or an act dangerous to human life, property, or infrastructure." The act must "appear[] to be intended — (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking." Here the applicability of Executive Order 13224 to cyber-terrorism depends upon the interpretation of its provision that that the attack be "an act dangerous to human life, property, or infrastructure." If the Government considers data to be property and information systems to be infrastructure, then the Executive Order could certainly apply to cyber-terrorism.

4. Conspiracy

There are two conspiracy statutes that are directly applicable to cyber-terrorism: 18 U.S.C. § 371, conspiracy to commit an offense or to defraud the United States, and 18 U.S.C. § 956, conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign

396. § 2339B(a)(1) (noting the "foreign" requirement of the statute).
Although it does not apply directly to terrorism, the Government prosecuted most terrorist crimes under §§ 371 in the ten years following 9/11.\(^{408}\) Given that any act of cyber-terrorism is covered, at a minimum under the CFAA, there are no obstacles in using § 371 to combat cyber-terrorism.

However, it is less apparent how the DoJ may use § 956 to charge a group conspiring to commit an act of cyber-terrorism in a foreign country. Section 956(b) criminalizes any conspiracy:

[T]o damage or destroy specific property situated within a foreign country and belonging to a foreign government or to any political subdivision thereof with which the United States is at peace, or any railroad, canal, bridge, airfield, or other public utility, public conveyance, or public structure, or any religious, educational, or cultural property so situated.[\(^{409}\)]

This statute focuses on property belonging to foreign governments and certain segments of infrastructure.\(^{410}\) It is unclear whether this statute would apply to damage to the data contained on information systems.

**SECTION V. INCORPORATING CYBER-TERRORISM INTO CURRENT LAW**

"Better to be despised for too anxious apprehensions, than ruined by too confident security."\(^{411}\)

Section V examined the applicability of current cyber-crime and counter-terrorism laws to counter cyber-terrorism. This examination revealed several important gaps in those laws that might prevent the Government from using them in the fight against cyber-terrorism. The previous Section also found that these laws do not provide an adequate focus on the prevention of cyber-terrorism. To help remedy this, Section V proposes that this Article’s definition of cyber-terrorism be incorporated into some of the most frequently-used counter-terrorism laws, thereby filling those gaps and providing tools to law enforcement officials for the prevention of cyber-terrorism.


\(^{409}\) § 956(b).

\(^{410}\) Id.

\(^{411}\) EDMUND BURKE, REFLECTIONS ON THE REVOLUTION IN FRANCE 11 (1890).
Although it does not apply directly to terrorism, the Government prosecuted most terrorist crimes under § 371 in the ten years following 9/11.408 Given that any act of cyber-terrorism is covered, at a minimum under the CFAA, there are no obstacles in using § 371 to combat cyber-terrorism.

However, it is less apparent how the DoJ may use § 956 to charge a group conspiring to commit an act of cyber-terrorism in a foreign country. Section 956(b) criminalizes any conspiracy:

To damage or destroy specific property situated within a foreign country and belonging to a foreign government or to any political subdivision thereof with which the United States is at peace, or any railroad, canal, bridge, airport, airfield, or other public utility, public conveyance, or public structure, or any religious, educational, or cultural property so situated.409

This statute focuses on property belonging to foreign governments and certain segments of infrastructure.410 It is unclear whether this statute would apply to damage to the data contained on information systems.

Section V. Incorporating Cyber-Terrorism into Current Law

"Better to be despised for too anxious apprehensions, than ruined by too confident security."411

Section V examined the applicability of current cyber-crime and counter-terror laws to counter cyber-terrorism. This examination revealed several important gaps in those laws that might prevent the Government from using them in the fight against cyber-terrorism. The previous Section also found that these laws do not provide an adequate focus on the prevention of cyber-terrorism. To help remedy this, Section V proposes that this Article's definition of cyber-terrorism be incorporated into some of the most frequently-used counter-terrorism laws, thereby filling those gaps and providing tools to law enforcement officials for the prevention of cyber-terrorism.

A. Material Support to Terrorism Statutes

As previously discussed, the material support statutes have proven to be some of the Government's most effective tools in the counter-terrorism toolkit. The DoJ has referred to the material support to terrorism statute412 as "[o]ne of the cornerstones of our prosecution efforts" in the battle against terrorism.413 As a demonstration of the statute's effectiveness in combating terrorism, the DoJ quoted a defendant charged under the material support statutes, who made the following statement in conversation with an informant:

The reason it was not organized is, couldn't be organized as it should've been, is because we don't have support. Everybody's scared to give up any money to help us. . . . Because of the law that Bush wrote about, you know, supporting terrorism. . . . Everybody's scared. . . . [Bush] made a law that says, for instance, I left out of the country and I fought, right, but I wasn't able to afford a ticket but you bought my plane ticket, you gave me the money to do it. . . . By me going and me fighting and doing that they can, by this new law, they can come and take you and put you in jail for supporting what they call terrorism.414

Given the success of these statutes the Government should be use it in countering cyber-terrorism.415 The gaps previously identified in § 2339B416 should be remedied to allow the proper authority to designate cyber-terrorist organizations. The two main problems preventing this are the definitions of terrorism,417 and the requirement that designated organizations be foreign.418

409. § 956(b).
410. Id.
411. EDMUND BURKE, REFLECTIONS ON THE REVOLUTION IN FRANCE 11 (1890).
The first step is incorporating cyber-terrorism into the definition of terrorism used in the statute regarding designation of a FTO: "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."\(^{419}\) As previously discussed, the violence requirement effectively precludes many potential acts of cyber-terrorism. If the proposed definition of cyber-terrorism were included along with the definition of terrorism, the Secretary of State could then designate foreign organizations that engage in cyber-terrorism activity as terrorist groups. However, identifying cyber-terrorist organizations as foreign is difficult due to the attribution dilemma—hacker organizations such as Anonymous and LulzSec are distributed worldwide with no specific locus.\(^{420}\)

Given the issue of identifying the precise locus of cyber-terrorist organizations, 8 U.S.C. § 1189 should also be amended with respect to cyber-terrorist organizations and the definition of "foreign organizations." If Congress updated the phrase to "the organization is a foreign organization or conducts operations primarily through cyberspace," it would resolve the difficult question of whether a cyber-terrorist group is foreign. However, the inevitable question resulting from this revision would be: Why include domestic cyber-terrorist groups, but not other types of domestic terrorist organizations? One answer is that cyber-terrorist groups operate from different locations around the world with no specific physical center and may include both domestic and foreign members.

In addition to an exception for domestic cyber-terrorist groups, another counter-argument to the proposed change is that outlawing material support would have little effect in stopping a cyber-terrorist organization. Preventing the flow of money and training to a group of advanced computer hackers will not hinder operations the way it does to a traditional terrorist group, which needs travel funds, weapons, and a base of operations. However, one counter to this theory is an advanced cyber-weapon. Stuxnet, the malware that damaged the Iranian nuclear centrifuges, was estimated to have cost one million dollars to produce, and likely needed the backing of nation states.\(^{421}\) If the definition of cyber-terrorism is limited to only those

419. § 2056(d)(2).
420. See Keating, supra note 100.
421. See § 1189.
422. Ben Flanagan, Former CIA Chief speaks out on Iran Stuxnet attack, The NATIONAL (Dec. 15, 2011), http://www.thenational.ae/themationalconversation/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack (referring to statements by General Michael Hayden, former head of the National Security Agency, in which he stated that "the precision with which Stuxnet targeted Iran mean that "responsible nations" could not be excluded").
The first step is incorporating cyber-terrorism into the definition of terrorism used in the statute regarding designation of a FTO: “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.”\textsuperscript{419} As previously discussed, the violence requirement effectively precludes many potential acts of cyber-terrorism. If the proposed definition of cyber-terrorism were included along with the definition of terrorism, the Secretary of State could then designate foreign organizations that engage in cyber-terrorist activity as terrorist groups. However, identifying cyber-terrorist organizations as foreign is difficult due to the attribution dilemma—hacker organizations such as Anonymous and LulzSec are distributed worldwide with no specific locus.\textsuperscript{420}

Given the issue of identifying the precise locus of cyber-terrorist organizations, 8 U.S.C. § 1189 should also be amended with respect to cyber-terrorist organizations and the definition of “foreign organizations.”\textsuperscript{421} If Congress updated the phrase to “the organization is a foreign organization or conducts operations primarily through cyberspace,” it would resolve the difficult question of whether a cyber-terrorist group is foreign. However, the inevitable question resulting from this revision would be: Why include domestic cyber-terrorist groups, but not other types of domestic terrorist organizations? One answer is that cyber-terrorist groups operate from different locations around the world with no specific physical center and may include both domestic and foreign members.

In addition to an exception for domestic cyber-terrorist groups, another counter-argument to the proposed change is that outlawing material support would have little effect in stopping a cyber-terrorist organization. Preventing the flow of money and training to a group of advanced computer hackers will not hinder operations as the way it does to a traditional terrorist group, which needs travel funds, weapons, and a base of operations. However, one counter to this theory is an advanced cyber-weapon. Stuxnet, the malware that damaged the Iranian nuclear centrifuges, was estimated to have cost one million dollars to produce, and likely needed the backing of nation states.\textsuperscript{422} If the definition of cyber-terrorism is limited to only those major attacks with serious effects, then it is false to believe that a portion of these attacks would not require large amounts of financial and logistical support. Preventing the flow of resources to organizations capable of mounting large-scale attacks should be a priority.

B. Amend FISA’s definition of international terrorism

The Government did not pass the Foreign Intelligence Surveillance Act (“FISA”)\textsuperscript{423} as a counter-terrorism tool, but rather as a means to collect intelligence on foreign powers. However, with the rise of international terrorist organizations in the last two decades, and amendments such as “lone wolf” provision,\textsuperscript{424} FISA has become an important counter-terrorism tool.

FISA allows for the electronic surveillance of a foreign power, within the United States, for the purpose of collecting intelligence information without a Title III warrant.\textsuperscript{425} The definition of a foreign power under the statute includes groups that are “engaged in international terrorism or activities in preparation therefor.”\textsuperscript{426} Also included are “agent[s] of a foreign power,” which, under the statute so-called lone-wolf provision, includes “any person other than a United States person, who . . . engages in international terrorism or activities in preparation thereof.”\textsuperscript{427} FISA’s definition of international terrorism contains the following phrase: “activities that involve violent acts or acts dangerous to human life,”\textsuperscript{428} which makes this definition ambiguous as to whether it applies to cyber-terrorism. The definition could exclude a non-violent cyber-terrorist attack, such as the destruction of financial or national security data.

FISA’s increased importance over the last decade is evident from the rising number of FISA warrants granted.\textsuperscript{429} In 1998, the courts

\textsuperscript{419} § 2056(f)(2).

\textsuperscript{420} See Keating, supra note 100.

\textsuperscript{421} See § 1189.

\textsuperscript{422} Ben Flanagan, Former CIA Chief speaks out on Iran Stuxnet attack, The National (Dec. 15, 2011), http://www.thenational.ae/thematicconversation/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack (referring to statements by General Michael Hayden, former head of the National Security Agency, in which he stated that “the precision with which Stuxnet targeted Iran mean that “responsible nations” could not be excluded”).


\textsuperscript{424} § 1801(b)(1)(C); Elizabeth Bazan, Cong. Research Serv., RS22611, Intelligence Reform and Terrorism Prevention Act of 2004: ‘Lone Wolf’ Amendment to the Foreign Intelligence Surveillance Act (2004).

\textsuperscript{425} § 1802(a)(1).

\textsuperscript{426} § 1801(a)(4).

\textsuperscript{427} § 1801(b)(1)(C).

\textsuperscript{428} § 1801(c)(1).

granted 800 FISA warrants.\textsuperscript{430} By 2008, that number was over 2000.\textsuperscript{431} The ability to conduct electronic surveillance on those suspected of terrorism is invaluable to both prevent terrorist activities and lead law enforcement officials to those who support terrorists. FISA would be particularly useful against organizations that operate primarily in the electronic realm, and therefore should be expanded to cover cyber-terrorism.

Congress should amend FISA to include as a foreign power groups "engaged in international terrorism, cyber-terrorism, or activities in preparation thereof." The lone-wolf provision should similarly be amended to include cyber-terrorism. Adding cyber-terrorism to FISA’s definition of international terrorism would be an important step in making FISA an effective tool to prevent cyber-terrorism.

\section*{C. Conspiracy}

Using 18 U.S.C. § 956, "conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign country,"\textsuperscript{432} against cyber-terrorism is problematic because it is unclear if the phrase "to damage or destroy specific property" or "other public utility" would include damage to data contained in information systems. This statute could be amended to more clearly cover cyber-terrorism in two different ways, one broad and one narrow. The broad solution would be to include "information systems related both to foreign governments and operation of the included infrastructure components" in the list of included targets. This inclusion, however, would include minor CNA, such as denial of service attacks. This would undermine the intent of this particular statute. The narrow solution would be to add a clause to § 956 that amends it to read:

\begin{quote}
To damage or destroy specific property through any physical means or act of cyber-terrorism, situated within a foreign country and belonging to a foreign government or to any political subdivision thereof with which the United States is at peace, or any railroad, canal, bridge, airport, airfield, economic data system, or other public utility, utility control system, public conveyance, or public structure, or any religious, educational, or cultural property so situated.
\end{quote}


\textsuperscript{432} See supra Section V(C)(4), for a discussion of conspiracy statutes.

\section*{D. Weapons of Mass Destruction}

As seen with the Stuxnet virus, the effects of cyber-weapons may equal those of weapons of mass destruction ("WMD"). Although WMD are often thought of as chemical, biological, radiological, and nuclear weapons ("CBRN"), the definition under 18 U.S.C. § 2332A of a WMD\textsuperscript{433} is much broader. Along with the CBRN type weapons, the statute includes a wide variety of destructive devices as defined under 18 U.S.C. § 921, including bombs and grenades.\textsuperscript{434} Thus, WMD is not as narrow a category as the public believes. However, CNA is not included in § 2332A, or in the WMD definition under the FISA,\textsuperscript{435} unless these statutes encompass a CNA that causes the release of chemical, biological, or radiological substance.

Despite the lack of statutory inclusion, there are indications that cyber-weapons could be another form of WMD. As recently as January 2009, former Director of National Intelligence, Mike McConnell, equated cyber-weapons with WMD when he expressed concern about terrorists’ use of technology to degrade the nation’s infrastructure.\textsuperscript{436} Director McConnell noted that terrorists aim to damage infrastructure and “when the level of sophistication reaches a point that there could be strategic damage to the United States, and that time is not too far off.”\textsuperscript{437}

Congress could easily remedy this exclusion by adding cyber-weapons designed to cause cyber-terrorism to the statutes that include WMD in the U.S. Code. Again, however, the added definition should exclude all but the most serious CNA from its scope. Incorporating these types of weapons into the definition of WMD criminalizes the use of any cyber-weapon by or against a national of the United States. This amendment would also bring an extraterritorial statute into the legal arsenal of law enforcement and help address the jurisdictional dilemma posed by CNA. Incorporating this


\textsuperscript{434} § 2332A(c)(2)(A).

\textsuperscript{435} § 1801(p).

\textsuperscript{436} Interview by Charlie Rose with Mike McConnell, Director of National Intelligence, on The Charlie Rose Show – PBS (Jan. 8, 2009) (including cyber-weapons with chemical, nuclear, and biological weapons as the four things with the highest ability to degrade the infrastructure).

\textsuperscript{437} Id.
granted 800 FISA warrants. By 2008, that number was over 2000. The ability to conduct electronic surveillance on those suspected of terrorism is invaluable to both prevent terrorist activities and lead law enforcement officials to those who support terrorists. FISA would be particularly useful against organizations that operate primarily in the electronic realm, and therefore should be expanded to cover cyber-terrorism.

Congress should amend FISA to include as a foreign power groups "engaged in international terrorism, cyber-terrorism, or activities in preparation thereof." The lone-wolf provision should similarly be amended to include cyber-terrorism. Adding cyber-terrorism to FISA's definition of international terrorism would be an important step in making FISA an effective tool to prevent cyber-terrorism.

C. Conspiracy

Using 18 U.S.C. § 956, "conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign country," against cyber-terrorism is problematic because it is unclear if the phrase "to damage or destroy specific property" or "other public utility" would include damage to data contained in information systems. This statute could be amended to more clearly cover cyber-terrorism in two different ways, one broad and one narrow. The broad solution would be to include "information systems related both to foreign governments and operation of the included infrastructure components" in the litany of included targets. This inclusion, however, would include minor CNA, such as denial of service attacks. This would undermine the intent of this particular statute. The narrow solution would be to add a clause to § 956 that amends it to read:

To damage or destroy specific property through any physical means or act of cyber-terrorism, situated within a foreign country and belonging to a foreign government or to any political subdivision thereof with which the United States is at peace, or any railroad, canal, bridge, airport, airfield, economic data system, or other public utility, utility control system, public conveyance, or public structure, or any religious, educational, or cultural property so situated.


432. See supra Section V(C)(4), for a discussion of conspiracy statutes.


434. § 2332A(c)(2)(A).


436. Interview by Charlie Rose with Mike McConnell, Director of National Intelligence, on The Charlie Rose Show - PBS (Jan. 8, 2009) (including cyber-weapons with chemical, nuclear, and biological weapons as the four things with the highest ability to degrade the infrastructure).
definition into the FISA would bring those who develop or proliferate in cyber-terrorism weapons under the jurisdiction of the FISA.

**CONCLUSION**

From hacktivists who wish to make a political point by temporarily altering websites,⁴⁴⁸ to foreign governments and corporations wishing to steal valuable intellectual property,⁴⁴⁹ to common criminals wishing to steal credit card information for financial gain,⁴⁴⁰ the motivations behind CNA are almost as broad as the various uses of the Internet. Given the broad range of CNA, the tendency has been to seek legal responses that cover these crimes as a whole. Just as non-Internet related activities such as espionage, theft of intellectual property, financial crimes, and terrorism have each developed unique legal regimes to deal with the particularities of each crime, so have different types of cyber-crimes. However, a notable exception is cyber-terrorism, which has yet to be defined in the U.S. Code.

Despite certain sections of the CFAA being listed as predicate offenses in the federal crime of terrorism, the resulting applicability is narrow and does little to address the prevention of cyber-terrorism. As terrorist organizations become more sophisticated in the field of information technology, it will only be a matter of time before they attempt to use information systems to conduct terrorist activities. These attacks could be broad-based denial of service attacks such as the attacks on Estonia,⁴⁴¹ or they could be narrow malware attacks on SCADA systems, such as the Stuxnet virus in Iran.⁴⁴²

As of yet, there has not been a cyber-terrorist event in the United States, but this should not stop Congress from enacting legislation to help prevent cyber-terrorism. The first step in any such legislation must be a careful definition of cyber-terrorism. This Article proposes a definition that is broad enough to cover the potentially unique effects of a weapon of cyber-terrorism, while narrow enough to exclude CNAs that are relatively minor in nature; a definition that is either too broad or too narrow risks being either irrelevant or useless.

Once a proper definition is agreed upon, it can be incorporated into existing counter-terrorism legislation. Material-support statutes, the FISA, conspiracy, and WMD statutes all hold the potential to prevent cyber-terrorism, but must first incorporate cyber-terrorism into their definitions and coverage. A formal legal definition will also allow government agencies to operate from a common standard in developing tactics, techniques, and procedures for countering cyber-terrorism.

These steps will obviously not provide all the tools needed to stop cyber-terrorists. Increased cyber-security aimed at government and critical infrastructure information systems and greater information sharing are important requirements in stopping cyber-terrorists. Potential laws aimed at requiring widespread use of data encryption also hold potential for stopping would-be cyber-terrorists. But just as the fight against terrorism has left no stone unturned in finding ways to defeat terrorists, so should the fight against cyber-terrorists. The fact that there has not yet been a “cyber 9/11” should not deter government taking the extremely important steps of defining the problem and using the definition to amend existing counter-terrorism statutes.

---

⁴⁴⁸ See, e.g., Wood, supra note 12 (discussing Anonymous’ takedown of several U.S. Government websites, including the FBI and DoJ, following the arrest of several executives associated with megaupload.com, a file-sharing site).


⁴⁴⁰ See, e.g., Matt Richtel, Credit Card Theft is Thriving Online as Global Market, N.Y. TIMES (May 13, 2002), http://www.nytimes.com/2002/05/13/business/credit-card-thefts-is-thriving-online-as-global-market.html?scp=2&sq=credit+card+theft&st=nyt (noting that tens of thousands of credit card numbers are offered for sale every week on the Internet).

⁴⁴¹ See supra Section III(E).

⁴⁴² See supra Section III(D).
definition into the FISA would bring those who develop or proliferate in cyber-terrorism weapons under the jurisdiction of the FISA.

CONCLUSION

From hacktivists who wish to make a political point by temporarily altering websites, to foreign governments and corporations wishing to steal valuable intellectual property, to common criminals wishing to steal credit card information for financial gain, the motivations behind CNA are almost as broad as the various uses of the Internet. Given the broad range of CNA, the tendency has been to seek legal responses that cover these crimes as a whole. Just as non-Internet related activities such as espionage, theft of intellectual property, financial crimes, and terrorism have each developed unique legal regimes to deal with the particularities of each crime, so have different types of cyber-crimes. However, a notable exception is cyber-terrorism, which has yet to be defined in the U.S. Code.

Despite certain sections of the CFAA being listed as predicate offenses in the federal crime of terrorism, the resulting applicability is narrow and does little to address the prevention of cyber-terrorism. As terrorist organizations become more sophisticated in the field of information technology, it will only be a matter of time before they attempt to use information systems to conduct terrorist activities. These attacks could be broad-based denial of service attacks such as the attacks on Estonia, or they could be narrow malware attacks on SCADA systems, such as the Stuxnet virus in Iran.

As of yet, there has not been a cyber-terrorist event in the United States, but this should not stop Congress from enacting legislation to help prevent cyber-terrorism. The first step in any such legislation must be a careful definition of cyber-terrorism. This Article proposes a definition that is broad enough to cover the potentially unique effects of a weapon of cyber-terrorism, while narrow enough to exclude CNAs that are relatively minor in nature; a definition that is either too broad or too narrow risks being either irrelevant or useless.

Once a proper definition is agreed upon, it can be incorporated into existing counter-terrorism legislation. Material-support statutes, the FISA, conspiracy, and WMD statutes all hold the potential to prevent cyber-terrorism, but must first incorporate cyber-terrorism into their definitions and coverage. A formal legal definition will also allow government agencies to operate from a common standard in developing tactics, techniques, and procedures for countering cyber-terrorism.

These steps will obviously not provide all the tools needed to stop cyber-terrorism. Increased cyber-security aimed at stopping and preventing cyber-terrorism is an important requirement in stopping cyber-terrorism. Potential laws aimed at requiring widespread use of data encryption also hold potential for stopping would-be cyber-terrorists. But just as the fight against terrorism has left no stone unturned in finding ways to defeat terrorists, so should the fight against cyber-terrorism. The fact that there has not yet been a "cyber 9/11" should not deter government taking the extremely important steps of defining the problem and using the definition to amend existing counter-terrorism statutes.

438. See, e.g., Wood, supra note 12 (discussing Anonymous’ takedown of several U.S. Government websites, including the FBI and DoJ, following the arrest of several executives associated with megaupload.com, a file-sharing site).


440. See, e.g., Matt Richtel, Credit Card Theft is Thriving Online As Global Market, N.Y. TIMES (May 13, 2002), http://www.nytimes.com/2002/05/13/business/credit-card-thefts-is-thriving-online-as-global-market.html?scp=2&sq=credit+card+theft&st=nyt (noting that tens of thousands of credit card numbers are offered for sale every week on the Internet).

441. See supra Section III(E).

442. See supra Section III(D).