Comprehensive Survey of Cyber-Terrorism

George Jarvis, george.jarvis@wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download

Abstract

This paper is a survey of the current Cyber-Terrorism landscape. It will cover how the definition of Cyber-Terrorism varies and how Cyber-Terrorism differs from Cyber-Warfare. In addition, this paper will cover what has been currently happening, what some believe will happen, and what new attack vectors lay on the horizon. This paper is intended for cyber security researchers looking to get a crash course on the current state of affairs and what one needs to anticipate in the coming years.

Keywords:

Cyberterrorism, cyber, terrorism, cyber-terrorism, cyber-warfare, cyberwarfare.

Table of Contents

1. Introduction

This paper discusses the emerging concern and threat of cyber-terrorism. This concern is shared amongst corporations, governments, militaries, and other organizations. Modern society is currently thrust in a situation whereby it is forced to address the gray areas of what constitutes actionable offenses as well as categorize what have historically been trivial situations. Technology has been the great enabler but in contrast it can be equally disabling. Any abrupt change to our networks has enormous financial and national security consequences as society becomes ever more network-centric and more dependent on performing day-to-day things such as banking, transportation, energy, water, etc. online. *"The growing complexity and interconnectedness of these infrastructure systems, and their reliance on computers, not only make them more vulnerable to attack but also increase the potential scope of an attack's effects."* [Knop08]

Before reading further, it is important that the reader understands that there is nothing personal towards any particular culture or any particular ethnicity. This is not brought up for the sake of political correctness, but as a reminder that the mere mention of a country or organization is about that country's government or organization's political platforms and not about the cultures or ideals of any group of people. This is often forgotten when dealing with topics such as cyber-terrorism because people have a tendency towards a deep sense of pride in one's country or culture but forget that government or organizations are usually outside of that scope.

2 Defining Cyber-Terrorism

How does one define "cyber-terrorism"? This is not an easy question to answer. One cannot tackle the topic of cyber-terrorism with any degree of intellectual honesty without addressing the chaos associated with how one defines "cyber-terrorism".

To be blunt, there is no universally accepted definition for the word cyber-terrorism. Depending on which definition is embraced determines what agenda is set forth. *"even when people agree on the rough definitions, they sometimes disagree about whether or not the definitions fit particular incidents"* [Dogrul11]. There is obviously a reason why there are so many differing nuances in trying to define cyber-terrorism in that a cookie cutter definition cannot fully cover all the scenarios under the umbrella of cyber-terrorism (much like there is difficulty in universally defining terrorism)

It is important to note these variations of the meaning of cyber-terrorism since this field has a broad influence on government and private interests.

This section will try to detail the varying perspectives of how cyber-terrorism is defined. In order to familiarize the reader with cyber-terrorism it is imperative to discuss the splitting of hairs and/or shades of gray when defining cyber-terrorism. Some readers may feel this section is overkill but in reality, it is necessary to underscore the lack of uniformity in defining this word. It is simply not black and white. The size of this section is proportional to the level of chaos in defining what some would believe is a simple word and it is necessary to illustrate the magnitude of what some would consider a simple problem.

To kick things off, it would be prudent to start with the most obvious source of definitions; the dictionary.

2.1 Dictionary

One approach to defining cyber-terrorism is to take a purely dictionary-based approach in order to come to some sort of general understanding. The dictionary has generally been the most straightforward and efficient way to determine the meaning of a word. However it should become quite clear that within the context of this paper, the dictionary is grossly inadequate.

The Merriam-Webster online dictionary defines terrorism with words involving terror, organization, and coercion. The word terror itself means a very deep state of fear or *"violent or destructive acts (as bombing) committed by groups in order to intimidate a population or government into granting their demands".* [Merriam-Webster11]

Taking a step back, it should become clear to the reader that there are gaping holes in the definition of terrorism such that concatenating this word with cyber should be equally inconclusive. To be honest, societies are still trying to flesh out what exactly cyber-terrorism is. Therefore, if societies cannot agree, what reason is there for the dictionary to somehow clarify things? Another way to see if there can be some closure to defining this word would be to see how this word is understood by the academic mind.

2.2 Cyber-Terrorism in the Eyes of Academia

If the dictionary has proven to be unreliable in this matter, surely the buck stops with academia. After all, this topic is being closely studied by academics around the world so one would think there should be some closure after academia has weighed in on this matter.

Professor Dorothy Denning of the Naval Postgraduate School probably has one of the most well known and popular definitions of the word cyber-terrorism. At its root core her definition states that cyber-terrorism requires the following [Denning06]:

1. Participants are non-state actors
2. Attacks are computer-based with a big payload (highly damaging) on IT-based infrastructures
3. Victims are either governments or societies
4. Attackers' goals are either political or social
5. Destruction / disruption is done against digital property rather than persons or physical property
6. Cyber-terrorism IS terrorism but limited within the scope of cyberspace.

What is unclear with Professor Denning's definition is how state-sponsored terrorist organizations fit. Professor Denning made it a clear point that the attackers are non-state actors. Therefore one must conclude that state-sponsored terrorist organizations do not fall under Professor Denning's definition.

In probably an overly-simplistic approach, international security lecturer Maura Conway describes cyber-terrorism as the union of two fears [Conway11]:

1. Fear of technology
2. Fear of terrorism

As the reader can see, academia's definition is either very rigid or overly simplistic. It is for these reasons that academia also fails to come to some concrete definition on what seemed to be a black and white word. The question the reader should now ask is whether or not the academic world agrees with the real world / government (those who work on a daily basis to confront the cyber threat)?

2.3 Cyber-Terrorism in the Eyes of the FBI

In his speech at the March 2010 RSA Cyber Security Conference in San Francisco, Director Robert Mueller discusses cyber-terrorism in some detail with these points [Mueller10]:

1. In 10 years' time al Qaeda's online presence is equivalent to their physical presence
2. Extremists use cyberspace for more than recruitment or radicalization
3. Cyberspace is being used to incite terrorism / terrorist acts
4. Thousands of extremist websites target an undisclosed number of captive audience members in promoting violence.
5. Viewers to these extremist websites can learn to build backpack bombs and bio-weapons through posted videos.
6. Social networking has been useful in linking terrorist plotters and plans

Director Mueller's speech clearly indicates the FBI sees cyber-terrorism essentially under the umbrella of "classical" terrorist groups. In fact, the specific portion of Director Mueller's speech concerning cyber-terrorism is monopolized by the usage of the Iranian Cyber Army, Al Qaeda, extremists, and Osama Bin Laden. Ignoring that some of these examples may be state-sponsored, all of these examples seem to be consistent with peoples' general understanding of a terrorist or terrorist group.

However Director Mueller seems to backpedal by expanding his definition of cyber-terrorism by including nation-states as attackers in his final paragraph concerning cyber-terrorism [Mueller10]. Director Mueller specifically cites distributed denial of service attacks that occurred in Estonia in 2007 and the Republic of Georgia in 2008. The results of these attacks left banks, utility companies, grocery stores, and parts of those countries' governments shut down. It is after the inclusion of nation-states that Director Mueller's definition of cyber-terrorism takes a sharp detour from Professor Denning's definition. Under Director Mueller's definition, a state-sponsored terrorist organization as well as nation-states would also fall under his umbrella of cyber-terrorism.

Given how the definition of cyber-terrorism seems to be growing into what some may consider cyber-warfare, it would be wise to go over how cyber-terrorism differs from cyber-warfare.

2.4 Distinction between Cyber-Terrorism and Cyber-Warfare

Cyber-terrorism and cyber-warfare; is there a difference? Both seem to employ the same tactics and have similar goals, but there is a difference.

One of the most confusing things in the whole cyber debate is how cyber-terrorism differs from cyber-warfare. Professor Denning seems to cover this rather succinctly in that [Denning06]:

1. Cyber-terrorism is done by non-state participants
2. Cyber-warfare is done within the context of a declared war
3. Cyber-warfare is performed by a government's military

By these criterion, cyber-terrorists have no formal connection with their national government. However, cyber-warfare only involves a country's military. How do organizations such as the FBI, DHS, or CIA fit within Professor Denning's definitions of cyber-terrorism and cyber-warfare? What of the NSA who has very close ties with the U.S. military?

Throw in that the FBI's seemingly myopic definition of cyber-terrorism seems to have been expanded with the mere mentioning of nation-states, and one can see how the lines are getting blurred between what is cyber-terrorism and cyber-warfare in addition to simply defining cyber-terrorism. The question now is are these ambiguities rare or are they part of a systemic problem in how society copes with defining words? Are these definitional problems a symptom of society?

2.5 Pace of Technology Forces Society to be Introspective

Society at times seems to be in flux. Technology compounds this societal flux in ways people a decade ago could not imagine. The difficulty in giving a pinpoint definition for cyber-terrorism is perhaps rooted in this societal flux.

In an out-of-the box way to illustrate how technology influences legal issues in the United States, below are some completely unrelated technological cases on how the threshold for defining something has been changed or lowered due to the unintended consequences technology affords society.

1. Six Pennsylvania high school students were charged with felonies for manufacturing trafficking, and

possessing child pornography. The incident started when it was discovered three 14 to 15 year old girls sent nude or semi-nude photos of themselves via their cell phones to three 16 to 17 year old boys [Brunker09]. Eight other students from another Pennsylvania high school a year later faced similar charges for the same / similar acts [Miller10].

2. A paraplegic California man was sentenced to 72 months in prison for his "psychological warfare" and "sustained effort to terrorize victims." when he successfully hacked into a number of women's computers and extorted them for sexual content [Anderson11].
3. A California man was arrested for sending more than 21,000 harassing and threatening tweets to a Google executive. The man faces 7 years in prison [Wilson11-3].
4. A U.S. attorney general has stated that software and hardware piracy fund terrorism [Anderson08].
5. A woman was arrested and charged with a felony for recording 4 minutes of her sister's surprise birthday party at a showing of "New Moon" in a movie theater [Doctorow09].
6. The FBI allegedly believes hacking groups like Anonymous and LulzSec are a threat to national security [Fogarty11].
7. A company sues an ex-employee for keeping his personal Twitter account and followers. The ex-employee's Twitter account was partially composed of the name of his former employer. The account was not the company's official Twitter account [Masnick11].

Technology has the capacity of making gray out of what was once black and white. As the pressure of dealing with cyber-terrorism grows with a maturing threat, so too will society's definition of cyber-terrorism. It seems that defining cyber-terrorism will continue to be in a state of flux until society or the international community can come up with a grand unified definition of cyber-terrorism.

Until then, the definition of cyber-terrorism is relegated to one's own subjectivity rather than an ideal universal definition in which all policies and procedures can clearly be based off of. When such a definition comes to fruition, society may find itself in a predicament where the threshold for being labeled a terrorist could be quite low.

In this section, I have covered and illustrated how a simple dictionary approach, an academic approach, and a government approach all seem to point in the general direction of defining cyber-terrorism but all three sources cannot agree due to varying nuances of their definitions or how they choose to expand upon them. Although the reader may question the level of effort put forth in defining this word, it was absolutely necessary in order to lay the framework of what the current state of affairs is with cyber-terrorism in general. If the reader can accept some form of cyber-terrorism to be generally agreed upon, the next section will try to investigate the historical and present threat of cyber-terrorism.

3 Is Cyber-Terrorism a Realistic Possibility?

Much of the news today is fairly depressing. The global economy is still in a slump. The Middle East is still at unrest. Terrorism still persists as if unabated. Mysteriously absent in the nightly newscasts are cyber-terrorist attacks. Has the whole topic of cyber-terrorism been much ado about nothing, or is the threat clear and present?

The following sections will go over the historical context, the pragmatic likelihood of a cyber-terrorist attack, and what cyber-terrorist scenarios are anticipated to be in the future. Let's kick things off with whether or not an actual cyber-terrorist attack has ever happened.

3.1 Has a Cyber-Terrorist Attack Ever Happened?

In spite of the varying nuances and degrees for the definition of cyber-terrorism, the general consensus is that cyber-terrorism has not yet happened; at least not in the high impact scenarios that cyber-terrorism is foretold to create. According to the Global Terrorism Database, there has only been one cyber-related attack since 1970 [GTB11]. However, Robert Knake of the Council on Foreign Relations points out that in the last 10 years there have been over 63,000 terrorist attacks none of which were cyber-related [Knake10]

Professor Denning does point out that cyberspace is under constant attack by non-state agents, but none of the acts committed by these agents are considered acts of cyber-terrorism. Denning states that these acts fall short for two reasons [Denning06]:

1. The most destructive and feared attacks are conducted for non-political and non-social reasons. Historically denial-of-service attacks have been used to: Extort money from victims, put competitors out of business, or satisfy egos and curiosity of young hackers.
2. Attacks linked to political and social goals have historically not been intimidating: Web defacement or behavior is more in line with a protestor and not a terrorist (aka hacktivism)

Denning's point on hacktivism should be noted. If hacktivism is nothing more than a protest for the sake of some principle matter then one needs to wonder why the FBI has allegedly asserted hacking groups such as Anonymous are a threat to national security. This evolution of potential charges / consequences is demonstrative of an earlier point about how technology has forced society to redefine the threshold of a crime or in this case what is a potential terrorist since it seems that any actions hacking groups take could be interpreted as a form of terrorism in the eyes of law enforcement. Did Anonymous actually do a DDOS attack against Sony in support of hacker George Hotz as a form of hacktivism? Or did Anonymous look for a reason to launch a cyber-attack against Sony due to irreconcilable differences?

Director Mueller of the FBI does concede that terrorists have yet to use the Internet for any kind of "full-scale cyber attack". However, he asserts that *"the Internet is not only used to plan and execute attacks; it is a target in and of itself."* [Mueller10] The key takeaway here is the FBI is making a similar argument as that of people who make home-made bombs. The resources are certainly available to the general public if one knows what they are doing and know where to look. However the question is how likely is such a scenario to happen? And how determined is the terrorist?

3.2 Is a Cyber-Terrorist Attack Likely to Happen?

Much of whether or not the cyber-terrorism threat is actually real all depends on who you choose to ask. Maura Conway will tell you that the likelihood of an actual cyber-terrorist attack is slim to none for the following reasons [Conway11]:

1. *The argument of technological complexity - Violent jihadis' IT knowledge is not superior*
2. *The argument regarding 9/11 and the Image Factor - Real-world attacks are difficult enough*
3. *The argument regarding 9/11 and the Accident Issue - Hiring hackers would compromise operational security*

Robert Knake has a similar sentiment in that a terrorist groups' intent does not mean capability [Knake10]. The FBI's cyber division has a different take in that if terrorist groups are allowed to develop cyber capabilities that they intend to wield destructive and deadly intent. [Gorman09]

It's worth noting that cyber attacks come in two flavors [Dogrul11]:

1. Targets data to sabotage services - Theft or Corruption
2. Targets control systems - Disable or Manipulates Physical Infrastructure

It should be noted that Conway's definition is in the same context of the FBI's initial definition of cyber-terrorism in that the participants are conventional terrorist groups. Conway's conclusions differs in that she does point out that of all the jihadis with a higher education, approximately less than 2% have any kind of computing background. And of those, she questions how many would possess a mastery of the big picture in implementing an actual cyber-attack.

Using Director Mueller's expanded definition, the likelihood of such attacks happening is dramatically increased when accounting for certain nations / nation-states. In this context, one would have to ask if it is worth waiting to put out a fire or are we better off in preventing a fire? The caveat being that once the fire happens, the level of destruction can be so rapid that there is nothing to salvage.

In hindsight, it seems plausible that the FBI desires to expand their sphere of influence by expanding their definition of what a cyber-terrorist is due to the devastating impact a crippled Internet would have on the United States alone. In other words, hacktivism and the actions of some nation-states will fall under the umbrella of cyber-terrorism in the eyes of agencies like the FBI.

If one asks Conway or Knake, they would argue an actual cyber-terrorist attack is very unlikely even in the presence of a very determined terrorist (or hacktivist for that matter). If one asks the FBI, they will assert that it is possible and if so, then the dangers of the consequences require some preparation in the event of such an attack. The question in the eyes of the FBI is not what is likely to happen. The question is what is the worst possible thing that could happen? If such actions do occur, then what infrastructures are the most anticipated to be attacked?

3.3 Current Cyber-Terrorism Scenarios

If a cyber-terrorism attack occurred under what conditions would it happen? What would be targeted?

Former Director of National Intelligence, Retired Admiral Mike McConnell, states *"if I were an attacker and wanted to do strategic damage to the United States I would either take the cold of winter or the heat of summer. I probably would sack electric power on the U.S. East coast; maybe the West coast and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker."* [Kroft09]

In other words, a cyber-terrorist would likely want to target high population areas where the demands of the targeted infrastructure would have the biggest impact or highest demand. Generally speaking, ideal targets are ones that service the most populous cities or have their highest loads during certain times of the year (heat of summer / cold of winter).

Infrastructures that are prime targets for cyber-terrorism are [Lee11]:

- Power
- Gas
- Transportation
- Water
- Financial
- Communications
- Offshore oil rig
- Medical

Imagine your life without any power or gas. Living conditions would be unbearable more so in the heat of summer or cold of winter. People, especially the elderly, would be at risk of perishing due to exposure to temperature extremes. Food could potentially become rotten. Cooking food would not be possible for the most part. Hot showers and clean clothes would be non-existent.

Although this scenario sounds theoretical, Idaho National Labs demonstrated back in 2007 that a 27 ton power generator can be created to rip itself apart and blow up via the Internet if the right set of commands were sent in a project called Aurora. The consequence of this is type of attack is not fully realized until one considers that the power generators are [Kroft09]:

- Highly expensive
- No longer made domestically
- Require a lead time of 3 to 4 months when ordering new ones

Understanding what destroying a generator at a power plant now encompasses, the potential for cascading effects now starts to be fully realized.

What if a cyber-terrorist could meddle with the transportation infrastructure? Trains, planes and automobiles could all be impacted with head-on collisions in all three situations. In 2009, two Washington D.C. metro trains collided due to an automated system failure not detecting a train already on the tracks [Lee11]. This disaster was actually caused by human error. What would the impact be if someone really wanted to have similar collisions?

In the early 2000s, a hacker in Maroochy Shire, Queensland Australia was arrested and jailed after it was discovered he was responsible for having the automated waste management control system dump raw sewage into local parks and waters out of revenge for not getting a job with the city. The consequence was not only foul stench but hundreds of thousands of marine life dying. What if a similar such attack was done onto potable drinking water?

What if a cyber-terrorist decided to attack the financial system in which money is backed instead of someone's particular bank account? What would a frenzy of people all rushing to withdraw their money from their accounts at the same time do to the banking system? Sound far-fetched? The United States averted a potential situation such as that by forcing banks to take what was called TARP money in order to confuse concerned Americans about which banks were failing by potentially averting such a financial crisis in 2008. The efficacy of the TARP funds has been called into question, but the goal of the TARP money was for this reason. *"Banking is based on confidence. What happens when you destroy confidence?"* [Kroft09]

It's already been asserted that hackers have already caused U.S. weather and terrain satellite disruptions four times in recent years [Mills11]. If the Internet, cable / satellite / cellular service providers were hacked and compromised, how would this affect people's day-to-day lives? How would people communicate? How would they conduct business? How would news be disseminated?

Offshore oil rigs are also not immune. Sandia National Laboratories has already demonstrated that by setting things to manual controls that automatic safeguards can be willfully circumvented [Lee11].

In terms of the medical community, there are two main ways in which medical service providers are vulnerable. In one situation, some people receive life and death medication by mail. Any interference in the way medication is allowed to be delivered can have a profound effect on whether someone can live or die. A similar concern arises when one realizes some equipment such as insulin pumps have also been found to be "hackable" [Robertson11].

The other situation in which medical service providers are vulnerable is in the way medical equipment has evolved. Prior to the Windows 95 / Windows 2000 days, most hospital equipment were highly specialized and designed with proprietary operating systems. When medical equipment companies looked for ways to improve their efficiencies and reduce costs, many resorted to using MS Windows operating systems in some or many of their equipment. The problem is two-fold. First is how common Windows viruses are introduced and spread. The second is when Microsoft decides to discontinue support for a particular OS. Hospitals cannot simply install the next version of MS Windows for those medical equipment. The equipment is much too complicated.

Going forward should a country's agenda be set so as to prevent cyber-fires or to simply put them out? The entire section has covered whether or not a cyber-terrorist attack has ever happened. It then went on to discuss the rational likelihood of a cyber attack along with the ideal targets of such an attack. In a nutshell, there has been no documented evidence of a cyber-terrorist attack and the likelihood of a cyber-terrorist attack from highly motivated terrorists is still very unlikely. However if one expands on the FBI's definition of what would qualify as cyber-terrorism, then the game has changed considerably when accounting for the actions of hacktivists and nation-states. What does the current landscape hold? One can only wonder.

4 The Cyber Landscape

Most people go on about their day without a care in the world about the privacy of their data or who could access their systems. It isn't until someone's bank account or private information has been stolen that people start to wonder. If individuals are at risk, what about one's country? The following sections go into topics that some people are acutely aware of but never bother to think about the bigger picture. What is happening or potentially happening before our very eyes is a sobering thought.

4.1 Spy Games

"Any successful penetration has the potential for leaving behind a capability." [Kroft09]

By now "made in China" has been ubiquitous with virtually anything consumers buy these days; especially technological things. Due to the exchange rate of the Chinese Yuan to other international forms of money, China has experienced an explosion of corporate investment within their country that has probably never been seen before in any other country. For this reason, most of the technologies used in today's world have some form of Chinese-manufactured goods in it.

Since the 1990s, any corporation wanting to do business in China has been required to provide the Chinese government with some snippet of their intellectual property or otherwise miss their opportunity to be a part of the next big business revolution [Lee11].

China has also been accused by numerous governments and corporations of hacking into their computer systems and successfully stealing intellectual property through cyber-attacks. Assuming the allegations are true, it does not take much to see where some organizations or governments become suspicious of whether or not China may be doing more than simply manufacturing circuits for the corporations that outsource to the Chinese.

Before delving into what some are suspecting the Chinese of doing, one must address the justification of how an entire country or some of its companies can be associated with the notion of participating in or fostering any kind of terrorism. In January of 2002, former President George W. Bush re-labeled a group of countries that the Clinton administration formerly called "rogue states" [BBC02] as the "Axis of Evil" (sponsors of terrorism) in his state of the union address [Bush02]:

1. **Iran**
2. Iraq
3. **North Korea**

In May of 2002, UN Ambassador John Bolton gave a speech titled "Beyond the Axis of Evil" which included [Bolton02]:

1. **Cuba**
2. Libya
3. **Syria**

In January of 2005, Secretary of State Condoleezza Rice gave a speech titled "Outposts of Tyranny" which included [Rice05]:

1. Belarus
2. **Zimbabwe**
3. Myanmar

Of the three aforementioned lists, China is a strong ally of more than half of those countries (highlighted in boldface). This in of itself does not prove anything since coming to any sort of conclusion would be a logical fallacy. The only thing that can be established is a correlation at best, but for some readers a correlation is all that is needed to raise some suspicion. There are probably a number of other reports which could embellish on this suspicion, but that is beyond the scope of this paper.

If the reader can at least accept China's role in potentially nurturing international terrorism by whom they strongly associate themselves with as being somewhat realistic, then the remainder of this section will be justified in its coverage under the umbrella of cyber-terrorism since even the most narrowest definitions of cyber-terrorism limits itself to terrorist organizations (or those who help to empower them). Throw in China's role in manufacturing IT technologies for the rest of the world, and it should be somewhat clear where some of the cyber concerns lie.

A growing number of government, military, and law enforcement agencies are acutely aware of the potential possibility of integrated chips or circuits to be modified from their original design during manufacturing in order to feature a backdoor, kill switch, or degraded performance. The scope of China's influence on consumer electronics is so large, that the United States military has been most concerned given the liberal use of commerical off-the-shelf (COTS) amongst defense contractors and original equipment manufacturers (OEM) such as Dell. Imagine the electronics to a missile guidance system being compromised. In reality, this has already happened but has fortunately been detected [Lee11].

Due to the actual and perceived concerns of backdoors and kill switches, the Harris Corporation is one of a number of defense contractors tasked with trying to actually identify such devices within post-fabricated electronics bound for some government agency. According to the Harris Corporation, about 10% of the devices they inspect have such malicious capabilities. [Lee11] Not to be outdone, the Defense Advanced Research Projects Agency (DARPA) has created a program called "Trust in Integrated Circuits" which is also trying to come up with an effective and efficient way of determining backdoors and kill switches in post-fabricated integrated circuits (IC) and circuits [Adee08].

A subset of Darpa's Trust in Integrated Circuits is a program called TRUST (short for "Trusted Integrated Circuits"). The focus of TRUST is to determine which techniques and testing methodologies can be trusted in order to quantify and qualitatively determine what weapon systems are free of malicious ICs or circuits based on a metric of probability of detection versus probability of false alarms [McCants11].

China is no stranger to accusatory remarks over theft of intellectual property or cyber attacks. China is also in the unique position of providing the IT technology used by the very countries they are allegedly attacking. Due to China's potential motivation and ability to insert malicious capabilities that the rest of the world consumes, the military and other government agencies are looking for ways to detect such things after post-fabrication. But are countries like the United States any different?

4.2 Corporate Collusion

Much attention has been focused on China over the years and their alleged activities concerning cyber-attacks at the very least. The question is whether or not countries like the United States are any different. For Machiavellian reasons, the United States has gotten the cooperation of an unknown number of corporations to aid in their efforts of fighting crime and terrorism in the name of national security. Below are a few known examples:

1. For some less security savvy readers, one of the reasons why cell phones are not allowed in classified government areas is due to the fact that cell phones can be turned on remotely by the cell phone companies to act as listening devices. Members of the mob found out the hard way when the FBI was able to "bug" conversations simply by using the mob members' own cell phones [McCullagh06].
2. In the 1990s, the FBI used a program called Carnivore which was installed at a particular ISP in order to packet sniff e-mails of certain individuals (or potentially all clients of the ISP). [Konrad00] Carnivore was later replaced by another program called Omnivore which was ultimately replaced by something called the DragonWare Suite [Tyson11].
3. More recently it was discovered through an AT"&"T whistleblower that AT"&"T provided the NSA with unlimited access to shunt all customer internet traffic and phone calls into a secret room for data mining purposes at its San Francisco switching center [Singel06].

The above is what is known. The question the reader should be asking is what else could the U.S. government be doing in the name of fighting cyber-terrorism with the aid of corporations? Conspiracies are abound.

4.3 Conspiracy Theories

This is the part of the paper where imaginations may run wild, but I ask that the reader suspend their disbelief and humor the possibilities for this section. As much as it has been said that China could be a significant participant in cyber-terrorism, the Chinese maintain that countries like the United States do exactly the same thing against China; some of which could be considered cyber-terrorism.

Case in point would be the alleged U.S. involvement of producing the Stuxnet virus which specifically targeted an Iranian nuclear facility. To be fair, an individual would have to be somewhat naïve to think that countries like the United States do not at least reciprocate those they accuse of wrong doing. However there is one caveat to the Chinese counter-point. Countries like the United States have the most to lose in terms of intellectual property and infrastructure. China at this point in time does not have any such intellectual property that other want. However the Chinese would have the most to gain by allegedly conducting cyber-attacks or cyber-terrorism [Lee11].

As an aside, some readers may be familiar with Intel's attempt at personally identifying CPUs remotely by reading the CPUs serial number over the Internet back during the Pentium III days. This "feature" was not very well received by civil liberty proponents. Needless to say, Intel eventually abandoned their serial number identification scheme due to the features poor public reaction; or did they?

In the previous section, it was established that corporations have colluded at least with U.S. government agencies. It was also pointed out U.S. military concerns of backdoors and kill switches originating most likely from China in another section. Is it far-fetched to think that if Intel or other companies are fully capable of being able to read a CPU's serial number remotely by incorporating enhanced "features" that these same companies could still continue to incorporate additional undocumented "features" at the request of U.S. government agencies in the name of national security?

The very thing the public is being conditioned to fear about the "other side" could potentially be loaded with backdoors and kill switches for domestic uses. Does this sound far-fetched? China has already started fabricating its own line of CPUs [Latif11]. It is doubtful these CPUs are entirely about national pride. China is likely concerned that the very chips that they are allegedly putting backdoors and kill switches in may also have backdoors and kill switches in place by the U.S. If true, there is now a battlefield over the very chips being fabricated and over who actually controls them. Given the smoke and mirrors some government agencies thrive in, it would not be surprising that all sides utilize "agent provocateurs" in order to launch allegations as well as drum up domestic concern in order to gain some upper hand in the court of public opinion.

As the reader can see, where there is a will there is a way. One country has the means to insert new features into circuits and chips they are fabricating while the other country has the cooperation of corporations with the potential possibility of inserting the very same things the Chinese are accused of doing. But how much further down the rabbit hole must one go to say enough is enough? That depends on how well you can think out of the box.

4.4 Thinking Out of the Box

To thwart cyber-terrorism, the international community needs to be at least one step ahead of the terrorists. This means covering attacks that are on the cutting edge of imagination, technology, or ingenuity. One can never underestimate the ingenuity of some. Motivations may range from simple curiosity to intellectual enrichment while others are looking for cost-effective or pragmatic ways to backdoor into a system. The following are just some potential attack vectors that are being exposed or discussed today:

- Using a stealth virtual machine to run in parallel with an insecure virtual machine [Gallagher11].
- Keylogging a PC using an iPhone's accelerometer [Foresman11].
- Cracking passwords within 12 seconds using a $48 GPU [Wilson11-1].
- Hacking car computers with mobile phones to remotely unlock and start a car, disable a car remotely, track a driver's location, activities, routines, steal personal data from bluetooth system, disrupt navigation systems, and isable emergency assistance[Wilson11-2]:

How does one secure their systems from the above attacks? One can only wonder. Although the above attacks seem small in scale to downright trivial, the reader needs to realize that terrorists work to achieve their goals in very small steps. It is not unreasonable to think the above attack vectors would be used by cyber-terrorists for some diabolical master plan.

It is hoped that this last section was not too much of a roller coaster ride for the reader and was at least a little entertaining. The attempt was to loosely establish some connection with China and countries known for some element of terrorism. It was then necessary to point out China's capability to insert malicious features into the very chips and circuits the rest of the world consumes. Things were then turned around a bit to see if there was evidence of countries like the United States having a similar capability or motivation to do similar acts by means of corporate cooperation. Lastly, new attack vectors were mentioned to show just how clever security experts will need to be in order to thwart would be cyber-terrorists.

5 Summary

In closing, the world of cyber-terrorism is a chaotic one. One could ask ten different security experts what their definition is concerning cyber-terrorism and one would likely get nine different answers. That is downright scary. If security experts cannot universally agree on how to define the problem, then there's little chance that a proper solution has been put in place. Society is almost doomed to be continually victimized as the experts try to put out fires that weren't exactly part of their job description. As humans continue to find ways to innovate and create technologies that did not exist a number of years ago, the redefining of common words will likely result due to unintended consequences that technology brings. Case in point is the FBI's posture of singling out hacking groups as a threat to national security. One can see the writing on the walls even though the FBI has all but called hackers a group of cyber-terrorists.

Although there is no disagreement that an actual cyber-terrorist attack has ever occurred (Stuxnet being one exception depending on your perspective), there is a lot of disagreement over what needs to be done in preparing for an attack. Some will argue that since there are too many hurdles to overcome in order to reach the objective that any amount of money spent in preparing for a coming cyber-terrorist attack is money wasted. Others will argue that the tools are already out in the wild and the potential for damage is clearly there. Does a country spend money to prevent a potential fire or does it wait and see to put them out as they happen? The FBI's mentioning of nation-states participating in terrorist acts certainly crosses the line of what some may consider cyber-warfare.

And somewhere in all of this China likely has a hand in how things unfold. China is a strong ally of many countries deemed by many to be terrorist states. China makes a lot of the IT technologies the rest of the world uses and also happens to be the most accused of cyber attacks. Will the FBI eventually expand their definition of cyber-terrorism to include China as well?

If such attacks are actually accomplished then the payoffs for a cyber-terrorist group would be huge. Think 9/11. It is for reasons like 9/11 that governments like the United States will employ tactics to try and mitigate any potential foreign threat in cyberspace. Are countries like the United States equally as bad as what China is allegedly doing? That is up to the reader to decide.

Going forward, the international community must commit to creating a clear and concise definition of cyber-terrorism. Once done, the experts can focus in on new and emerging attack vectors that could be employed by a group of cyber-terrorists. Until that day happens, much of the cyber security agencies will continue to operate within their own fiefdoms pursuing their own agendas based on varying but similar definitions of what a cyber-terrorist is.

6 References

[Dogrul11] Dogrul, Murat; "Developing an international cooperation on cyber defense and deterrence against Cyber terrorism", 2011 3rd International Conference on Cyber Conflict, ICCC 2011 - Proceedings, 2011, ISBN: 9789949904020

[Denning06] Denning, Dorothy; "A View of Cyberterrorism Five Years Later", Naval Post Graduate School, 2006

[Mueller10] Mueller, Robert; "Tackling the Cyber Threat", 4 Mar 2010, FBI, http://www.fbi.gov/news/speeches/tackling-the-cyber-threat

[Conway11] M. Conway; "Privacy and Security Against Cyberterrorism", Communications of the ACM vol.54, no.2 pgs 26-28, 2011, ISSN: N/A

[Knake10] Knake, Robert; "Cyberterrorism Hype v. Fact", Council on Foreign Relations, 16 Feb 2010, http://www.cfr.org/terrorism-and-technology/cyberterrorism-hype-v-fact/p21434

[Kroft09] Kroft, Steve "60 Minutes - Sabotaging the System", CBS, 8 Nov 2009

[Lee11] Lee, Melissa, "CNBC Originals - Code Wars", Season 2, Episode 11, CNBC, 26 May 2011

[Gorman09] Gorman, Siobhan, "FBI Suspects Terrorists Are Exploring Cyber Attacks", The Wall Street Journal, 19 Nov 2009, http://online.wsj.com/article/SB125850773065753011.html

[GTD11] Global Terrorism Database, Search String "Cyber", Nov 2011, http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200703120002

[Knop08] Knop, K., "Institutionalization of a Web-Focused, Multinational Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System - A Discussion Paper", Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey (Ed.) IOS Press, 2008, pgs 8 to 23.

[Adee08] Adee, Sally, "The Hunt for the Kill Switch", IEEE Spectrum, May 2008, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0

[McCants11] McCants, Carl, "Trusted Integrated Circuits (TRUST)", DARPA, http://www.darpa.mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_%28TRUST%29.aspx

[Foresman11] Foresman, Chris, "Researchers can keylog your PC using your iPhone's accelerometer", ArsTechnica.com, Oct 2011, http://arstechnica.com/apple/news/2011/10/researchers-can-keylog-your-pc-using-your-iphones-accelerometer.ars

[Gallagher11] Gallagher, Sean, "Researchers create stealth virtual machine that can run alongside insecure VMs", ArsTechnica.com, Oct 2011, http://arstechnica.com/business/news/2011/10/researchers-create-stealth-virtual-machine-that-can-run-alongside-insecure-vms.ars

[Wilson11-1] Wilson, Dean, "Passwords can be cracked in 12 seconds with £30 GPUs", The Inquirer, 5 Oct 2011, http://www.theinquirer.net/inquirer/news/2114746/passwords-cracked-gbp30-gpus

[Wilson11-2] Wilson, Dean, "McAfee warns of security holes in car computer systems", The Inquirer, 7 Sep 2011, http://www.theinquirer.net/inquirer/news/2107383/mcafee-warns-security-holes-car-systems

[Mills11] Mills, Elinor, "Hackers reportedly behind U.S. government satellite disruptions", CNET, 27 Oct 2011, http://news.cnet.com/8301-27080_3-20126293-245/hackers-reportedly-behind-u.s-government-satellite-disruptions/

[Singel06] Singel, Ryan, "Whistle-Blower Outs NSA Spy Room", Wired, 7 Apr 2006, http://www.wired.com/science/discoveries/news/2006/04/70619

[Latif11] Latif, Lawrence, "China Builds Petaflop Supercomputer without Intel, AMD, or NVIDIA", Inquirer, 31 Oct 2011

[McCullagh06] McCullagh, Declan, "FBI taps cell phone mic as eavesdropping tool", CNET, 1 Dec 2006, http://news.cnet.com/2100-1029-6140191.html

[Konrad00] Konrad, Rachel, "New documents shed more light on FBI's "Carnivore"", CNET, 16 Nov 2000, http://news.cnet.com/2100-1023-248762.html

[Tyson11] Tyson, Jeff, "How Carnivore Worked", HowStuffWorks.com, 2011, http://www.howstuffworks.com/carnivore.htm

[Bush02] Bush, George "Bush State of the Union address", CNN, 29 Jan 2002, http://edition.cnn.com/2002/ALLPOLITICS/01/29/bush.speech.txt/

[BBC02] British Broadcasting Corporation, "Analysis: 'Axis of evil' capabilities", BBC, 13 Feb 2002, http://news.bbc.co.uk/2/hi/1809227.stm

[Bolton02] British Broadcasting Corporation, "US expands 'axis of evil'", BBC, 6 May 2002, http://news.bbc.co.uk/2/hi/1971852.stm

[Rice05] British Broadcasting Corporation, "Rice names 'outposts of tyranny'", BBC, 19 Jan 2005, http://news.bbc.co.uk/2/hi/americas/4186241.stm

[Fogarty11] Fogarty, Kevin, "'Leaked' FBI document calls Anonymous a national security threat", IT World, 12 Sep 2011, http://www.itworld.com/security/202439/leaked-fbi-document-calls-anonymous-national-security-threat

[Robertson11] Robertson, Jordan, "Insulin Pumps,Mmonitors Vulnerable to Hacking", Associated Press, 4 Aug 2011, http://www.foxnews.com/scitech/2011/08/04/insulin-pumps-vulnerable-to-hacking/

[Anderson08] Anderson, Nate, "US Attorney General: Piracy funds terror", ArsTechnica.com, Mar 2008, http://arstechnica.com/tech-policy/news/2008/03/us-attorney-general-piracy-funds-terror.ars

[Doctorow09] Doctorow, Cory, "Woman jailed, charged with felony camcordering after recording 4 mins of sister's birthday party in a movie theater", BoingBoing, 4 Dec 2009, http://boingboing.net/2009/12/04/woman-jailed-charged.html

[Masnick11] Masnick, Mike, "Company Sues Ex-Employee Because He Kept His Personal Twitter Account & Followers", TechDirt, 11 Nov 2011, http://www.techdirt.com/articles/20111111/04161816721/company-sues-ex-employee-because-he-kept-his-personal-twitter-account-followers.shtml

[Wilson11-3] Wilson, Dean, "Man faces up to seven years in prison for threatening Google executive on Twitter", The Inquirer, 7 Sep 2011, http://www.theinquirer.net/inquirer/news/2107350/seven-prison-threatening-google-executive-twitter

[Brunker09] Brunker, Mike, "'Sexting' surprise: Teens face child porn charges", MSNBC, 15 Jan 2009, http://www.msnbc.msn.com/id/28679588/ns/technology_and_science-tech_and_gadgets/t/sexting-surprise-teens-face-child-porn-charges

[Miller10] Miller, Michelle, "'Sexting' Leads to Child Porn Charges for Teens", CBS, 7 Jul 2010, http://www.cbsnews.com/stories/2010/06/05/eveningnews/main6552438.shtml

[Anderson11] Anderson, Nate, "How an omniscient Internet "sextortionist" ruined the lives of teen girls", ArsTechnica.com, Sept 2011, http://arstechnica.com/tech-policy/news/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives.ars

[Merriam-Webster11] Merriam-Webster Online Dictionary, http://www.merriam-webster.com/

7 List of Acronyms:

CIA	Central Intelligence Agency
COTS	Commercial Off The Shelf
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
NSA	National Security Agency
OEM	Original Equipment Manufacturer
RSA	Rivest, Shamir and Adleman
TARP	Troubled Asset Relief Program
TRUST	Trusted Integrated Circuits

Last Modified: 28 Nov 2011
This and other papers on latest advances in network security are available on line at
http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page