Cyberterrorism in the Information Age

A Comparative Analysis of the U.S. & UK State Sponsored Strategies Against this New Credible Threat to National Security

Jason Langsner
SEST 634-21
Comparative Counterterrorism
Securities Studies Program
Edmund A. Walsh School of Foreign Service
Georgetown University
Washington, DC

Professor Jeremy Shapiro
Final Paper
Submitted: August 15, 2007

Data on the Internet circumvents boundaries, borders, and beliefs as-if the binary bits were a digital Diplomatic core. This data sent and retrieved over this quintessential public good offers great agency for those capable of accessing its rich treasure troves of information; as well as offers its users a tool – like a hammer or any other – to assist man in performing a function more efficiently. One of these functions that the Internet addresses is the creation of virtual social networks for communication, collaboration, and commerce. Thus, the Internet can best be described or simplified as an enabler that *makes the world flat* by bringing people from disparate regions from the globe together for specific purposes.[1]

Today, there is still a digital divide between "the haves" and "have nots" due to the costs related to the barriers of entry to the technology and the necessary infrastructure to access the tool to perform these specific purposes. But Nicholas Negroponte, from the One Laptop Per Child non-profit program, has been working for the last four years to bring a computer with Internet capability to two-billion children in the developing world so they have the same opportunity that the developed world has to live and participate in the Information Age, by offering them the ability to "learn how to learn" in the 21st century.[2]

Thomas L. Friedman states using a new technology, such as the Internet, "does not make you modern, smart, moral, wise, fair, or decent." [3] As an enabler it does allow the user to bridge these social networks farther and faster than

[1] Friedman, Thomas L. The World is Flat: A Brief History of The Twenty-First Century. New York: Farrar, Straus and Giroux: 2005.
[2] One Laptop per Child. 11 August 2007. <http://laptop.org/vision/mission/>.

under any other conventional means. As an inherent capability of a virtual network, it also offers users a guise of anonymity. Thus, in addition to any altruistic benefits offered to society, the Internet also enables malicious actors an ideal forum for committing or planning cybercrime under this cloak.

Beyond cybercrime, the Internet also enables sub-national political groups an opportunity to anonymously exploit a country's dependency to technology by directly attacking a nation state's digital vulnerabilities. This is Cyberterrorism. And as the cloak lays an anonymous shadow over cybercriminals, so too does it to cyberterrorists, which makes tracking terrorists much more difficult than under conventional terms. As terrorists continue to commit these malicious acts via the Internet they can also use the same tool to propagate their message farther and faster. This tool, as described earlier like a hammer, can metaphorically be used effectively by a carpenter as designed to build a home or it may have the unintended consequences to be used as a weapon to strike and paralyze. In terms of a cyberterrorist, the hammer could be used to put a country into a state of technological paralysis.

As leaders in the global war on terrorism and as technological hegemonic nation states in the private and public sectors, the United States and United Kingdom are thus being constantly threatened by terrorists and cyberterrorists and are both highly vulnerable to cyberattacks by "this hammer." Both nations' counterterrorism response strategies are similar in many fashions but differ in their main mission. Although the countries' strategies have differed in scale and scope, both have been successful in combating this new threat to-date because

[3] Friedman, pg. 374.

they view combating Cyberterrorism as a piece of their grand strategies against terrorism writ-large.

Cyberterrorism – as defined under the auspices of U.S. law – is the, "premeditated politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents." [4] It is an unconventional weapon that like the Biblical story of David versus Goliath, allows the small to topple the many or weak to topple the mighty.

Arnaud de Borchgrave, of the U.S. Centre for Strategic International Studies (CSIS), claims that no group or country "can match the U.S. in terms of conventional weapons so Cyberterrorism becomes a credible alternative." [5] Bridget Kendall, a BBC diplomatic correspondent, echoes this point by asking, "what use are traditional weapons like the Stealth bomber…against cyberterrorists" and thus cyberattacks are the, "perfect weapon for terrorists" to attack anonymously from anywhere across the *flattened world*.[6]

The United States geographic location in relation to its enemies has provided it protection in the past from conventional attacks, but in a *flattened world* this isolationist protectionism is lost. Similarly the British Isles have historically been protected by the body of water that surrounds it compared to its European brothers.

[4] Pollitt, Mark F. "CYBERTERRORISM – Fact or Fancy?" U.S. Federal Bureau of Investigation Laboratory. Computer Fraud & Security, Volume 1998, Number 2, February 1998, Available publicly at <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>.

[5] Anderson, Kevin. "Cyber-terrorists wiled weapons of mass disruption." BBC News. 22 February 2000. <http://news.bbc.co.uk/1/hi/sci/tech/specials/washington_2000/648429.stm>.

In a post-9/11 world, it has been made clear that both foreign and domestic terrorist groups are capable and driven to use unconventional means for their causes and to attack the U.S. and UK homelands domestically. A country must be prepared to have the tools available – whether legal, operational, or solely technical – to confront attacks by foreign sub-national groups and by groups of its own citizens looking for political upheaval.

In the United States on September 11, 2001, Mohamed Atta and a group of radical Islamic terrorists hijacked four commercial airplanes and used them as missiles to strike the World Trade Center and the Pentagon. United Flight 93 additionally crashed in a field in rural Pennsylvania before it was capable of reaching the U.S. Capitol or another assumed target of national significance. These highly coordinated acts of terrorism were the largest premeditated attack on U.S. soil since the December 7, 1941, Pearl Harbor bombings by the Japanese navy and air force. Just as President Franklin Delano Roosevelt said during now one of the most recognized presidential addresses in U.S. history that December 7th will be a "date that will live in infamy," so too will September 11.

The infamy of the 9/11 attacks is not just a part of United States history or solely a domestic problem. The attack resonated globally as the target was against all of Western civilization. Thus, the entire world reacted by bolstering their counterterrorism and counterattack strategies by passing new legislation, increasing funding, and showing a willingness for international collaboration against the global threat of terrorism. This reaction also included a renewed

[6] Kendall, Bridget. "Newsnight: Terrorism online transcript." BBC News. 27 May 2007. <http://news.bbc.co.uk/2/hi/events/newsnight/1050141.stm>.

focus on Cyberterrorism strategies. These strategies adopt the belief that no longer could the U.S. and the Western world live under the traditional mentality or definition of credible enemies because today's cyberterrorist could be anyone from any where; and that enemy doesn't need to be near or on the physical soil of the nation to strike. That individual can virtually strike from anywhere and everywhere in the world at the same time through tools publicly available on the Internet and connect to it via a commercial mobile telecommunication infrastructure. Although, the 9/11 attacks were orchestrated by non-U.S. citizens visiting the country legally and the Pearl Harbor bombings were an aggressive act of war by a foreign government, closing the borders does not stop the threat. It would be impossible to close the borders on the Internet because they do not exist and there are also credible threats from within the country that cannot be ignored.

In the United Kingdom, in a similar highly coordinated attack on transportation assets, on July 7, 2005, radical Islamic terrorists attacked three subway cars and a bus killing and injuring hundreds of British non-combatant citizens on their daily morning commute to work. The alleged perpetrators of the 7/7 attacks were British citizens of Pakistani descent living and assimilated in the country. This proves that even under the traditional terms of terrorism closing the borders would not have stopped the violence.

Both the U.S. 9/11 and UK 7/7 attacks are examples of conventional acts of terrorism, but it has been proven that a great deal of the preparation and coordination of the attacks were done via using computers and the Internet as a tool for information gathering, as well as for communication and collaboration. The malicious actors that attacked the U.S. and UK on these dates of infamy were greatly enabled by the Internet. Both acts prove that countries must protect their assets from threats with-in and outside of the countries borders as many terrorists have the determination and capabilities to carry out their missions. And it is also clear that cyberterrorist attacks know no borders or boundaries and as Kendall believes defensive counterattack theories and strategies from the Cold War no longer apply in today's Information Age as it is no longer rogue nation states or actors armed with nuclear weapons the world has to fear because anyone can become a cyberterrorist.[7] The computer linked to the Internet, like the swinging hammer used for illegal and malicious acts beyond its initial design, is the "newest weapon in the arsenals of asymmetric warfare." [8]

And although it takes specialized knowledge to be a credible threat to national security, there are two growing trends which instill fear in many security experts that follow cybersecurity issues that threaten the U.S., UK, and the rest of the world whom depend on the Internet to run critical assets of National Security. The first threat includes publicly available tools being made available for download on the Internet that allows anyone to become a cyberterrorist. The second fear includes terrorists without the technical expertise but with the necessary funds outsourcing their projects to cybercriminals.

Tools such as the Electronic Jihad Program, which is available on the jihadi Web site Al-jinan.org, are applications that "users can install and use to

[7] Kendall.
[8] Ibid.

target specific IP addresses" for Denial of Service (DOS) attacks against specific government or private sector institutions on the Internet via a Windows-like Graphic User Interface (GUI).[9] The tool comes preset with specific IP addresses, which allows the user to just click which target he/she would like to attack and click a second button on the GUI before the software does the backend work for them. These DOS attacks, otherwise known as Virtual Sit-ins, prevent the website from being accessed from other users.

The second threat though is more alarming and unlike the DOS attacks could become credible threats to national security and be the direct cause for violence or massive deaths. This is a growing fear that terrorists fighting an ideological war that have the necessary financial resources but who do not have the technical expertise may create a new economical market to entice cybercriminals to "undertake their missions" as outsourced projects.[10] This fear is directly from the elimination of the knowledge gap necessary for cyberterrorists to attack critical infrastructures effectively as they will no longer need the specialized education to act as David fighting Goliath, but will only need to buy David's sling-shot for him. This threat's primary motivator for the cybercriminals is money and not ideology, which further complicates "the job of the security and intelligence services vis-à-vis monitoring" because the outsourced operatives can be more cunning professionals that can hide their trails better and are

[9] Greenemeier.

[10] Trim, Peter R.J., "Public and Private Sector Cooperation in Counteracting Cyberterrorism." International Journal of Intelligence and Counterintelligence. Volume 16, Number 4. 1 October 2003. pg 595.

specialized; let alone may not be known by intelligence agencies as having a relationship with a particular terrorist group due to the anonymity of the Internet.[11]

The goals of a cyberterrorist are thus simple and finite. First they may attack data or control systems. Second whether the cyberterrorists' targets have vulnerabilities that can be affected, which lead to violence or severe harm. And additionally as the need for the outsourcing paradigm shows, whether the cyberterrorists have the capability and motivation to carry out the attacks will come into question. All factors must be factored into any model defining what type of cyberterrroist group may be a threat to a nation and how that nation should respond.[12]

Before a country can form a strategy they must define the threat in concrete terms. Cyberterrorism has no international standardized definition, which causes complications for collaboration but on September 16, 2006, at the G8 Summit in St. Petersburg, Russia, the countries that make up the G8 "agreed to exchange information on legislation on counterterrorism…and work towards harmonizing such legislation in order to tackle Cyberterrorism." [13]

Under the U.S. definition the 9/11 attack would not be construed as cyberterrorism because the use of the IT did not directly bring about the destruction and violence. Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI, during a testimony to the U.S. Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, stated:

[11] Ibid.

[12] Denning, Dorothy E. "CYBERTERRORISM." 23 May 2000. <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

> Terrorist groups are increasingly adopting the power of modern communications technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fund raising and funds transfer, information gathering, and the like. However, mere terrorist use of information technology is not regarded as cyberterrorism. The true threat of "Cyberterrorism" will be realized when all the factors that constitute a terrorist attack, coupled with the use of the Internet, are met.[14]

Nor under the U.S. definition would the Electronic Jihad Program be viewed as Cyberterrorism because it did not precipitate violence. The U.S. would view the Electronic Jihad Program as being an act of Hactivism, or the merging of hacking and activism, which although still illegal would fall under a different legal basis.[15]

On the contrary by extrapolating the UK Terrorism Act of 2000 to cyberterrorism any act by an organization to commit, participate, prepare, promote, encourage, or is otherwise concerned with cyberterterrorism would be deemed under that rubric; therefore the Electronic Jihad Program, the 7/7 attacks, and any planned or thwarted attack against the British government using a computer and the Internet could be deemed cyberterrorism.[16] For instance a British court in July 2007 convicted three Muslim men that they called "cyber-

[13] G8 parliamentary speakers agree to harmonize counterterror laws. BBC News. Transcript. St. Petersburg, Russia: 16 September 2006.

[14] Lourdeau, Keith. "Congressional Testimony Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security" U.S. Federal Bureau of Investigation. 24 February 2004. <http://www.fbi.gov/congress/congress04/lourdeau022404.htm>.

[15] Denning, Dorothy. "Activism, Hactivism, and Cyberterrorism: the Inter as a Tool for Influencing Foreign Policy." Networks and Netwars: The Future of Terror, Crime, and Militancy. Chapter 8. RAND Corporation: Washington, DC, 2001.

[16] Cuthbertson, Ian M. "The Nature of the Terrorist Threat and National Responses to Terrorism: The British Case." National Counter-Terrorism Strategies: Legal, Institutional, and Public Policy Dimensions in the US, UK, France, Turkey and Russia. Washington, DC: IOS Press, 2006.

jihadis" to ten year prison sentences for, "using the Internet to urge Muslims to wage holy war on non-Muslims." [17]

As expressed in the 9/11 attacks and what could have been critically needed during Pearl Harbor, during the 20th Century countries were faced with adapting to a new threat…that from the sky in war planes. The NSSC states:

> In the 1950s and 1960s, our Nation became vulnerable to attacks from aircraft and missiles for the first time. The federal government responded by creating a national system to: monitor our airspace with radar to detect unusual activity, analyze and warn of possible attacks, coordinate our fighter aircraft defenses during an attack, and restore our Nation after an attack through civil defense programs.[18]

The NSSC continues by expressing how the country's vulnerabilities have shifted to the Internet and how a similar response system is needed today which will, "detect potentially damaging activity in cyberspace, to analyze exploits and warn potential victims, to coordinate incident responses, and to restore essential services that have been damaged." [19]

This proposed National Cyberspace Security Response System is the first priority of five planned out in the NSSC.[20] The additional national priorities outlined in the U.S. plan to secure cyberspace include implementing a National Cyberspace Security Threat and Vulnerability Reduction Program, a National Cyberspace Security Awareness and Training Program, securing Government's

[17] Greenemeir, Larry. "Cyberwarfare: By Whatever Name, It's On the Increase." INFORMATIONWEEK. 9 July 2007. <http://www.informationweek.com/story/showArticle.jhtml?articleID=200900812>.

[18] The National Strategy to Secure Cyberspace. The White House. Washington, DC: February 2003. pg. 19.

[19] Ibid.

[20] NSSC, pg. x.

Cyberspace, and fostering National Security and International Cyberspace Security Cooperation.[21]

These five strategies under the NSSC is just part of the U.S. grand strategy against terrorism. The NSSC cites itself as, "an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*" [22]

The NSSC five national priorities, under the U.S. grand strategy of counterterrorism, can be simplified as being a duel-pronged protect and deny strategy. The NSSC states its purpose as to, "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact." [23] The report tasks the Secretary of the Department of Homeland Security as the principle figure in matters of Cybersecurity for the United States. And Secretary Michael Chertoff appointed Greg Garcia as the Assistant Secretary for Cyber Security and Communications. Many other departments and agencies are also involved with the issue, but Chertoff and Garcia are the two lead administrators of U.S. Cybersecurity policy. The United States' protection and deny strategy has been made highly public by these individuals; but the United States' third strategy of attacking cyberterrorists directly has been kept classified and although it is known that the U.S. participates in direct acts of Information Warfare against countries and sub-national groups, it is unclear to what extent they practice this strategy.

[21] Ibid.
[22] NSSC, pg. vii.

Comparatively the UK's principle counterterrorism strategy for Cyberterrorism is to downplay the problem. Kendall writes, "In Britain, thwarting Cyberterrorism is a more low-key affair" compared to the U.S. as "it's best not played out by megaphone" because instead of acknowledging the growing threat from attack, they, "play it down to reassure the public." [24] Like the U.S., Britain views cyberterrorism and cybercrime under a holistic approach that is an issue for the world, but they have taken a less concerted approach at centralizing the response. Mark Castell, project manager of the UK National Hi-Tech Crime Squad, states, "our fight against terrorism in the real world is also a multi-agency activity. Cyberspace is new, it's big, but it's not special. It's simply taking existing lessons and putting them in cyberspace, and the solution is there." [25] The National Hi-Tech Crime Squad is a specialized national police force with regional roots across England that is tasked with focusing on issues of cybercrime. Thus, they do not exclusively specialize in Cyberterrorism as they also combat Internet pedophiles, fraud, and extortion.[26] Of all the British government agencies involved with Cyberterrorism, the most applicable to the DHS Office of Cyber Security & Communications is the UK Government Communications Headquarters' (GCHQ) Communications-Electronics Security Group (CESG).[27]

[23] Ibid.

[24] Kendall.

[25] Ibid.

[26] "Cyber cops plan unveiled." BBC News. 13 November 2000. <http://news.bbc.co.uk/1/hi/uk_politics/1021352.stm>.

[27] "About CESG." Communications-Electronics Security Group Website. 12 August 2007. <http://www.cesg.gov.uk/site/about/index.cfm>.

As the Internet is a public good and not owned or operated by any institution or government, every stake-holder that uses or manages a function of the Internet must maintain its own cybersecurity. The NSSC outlines the United States strategic plan to protect its citizens, data, and critical infrastructures from cyberattacks, but the responsibility of ownership falls on the individual stakeholders. The NSSC assists private institutions through education and by trying to transform the Government's own cyber assets into best practices to lead by example. The CESG in February 2007, has also been tasked by the UK government by creating the GovCertUK (Government Computer Emergency Response Team) Program, which helps to "provide incident response to Government and Critical National Infrastructure" assets.[28]

Through the holistic approach by the U.S. and the UK, beyond the initial government response strategies, both countries have focused a great deal on their efforts on creating public and private sector partnerships. As the countries have become technological hegemonies they have become increasingly more reliant on private sector Information and Communication Technology networks to run critical national assets. For instance a concerted cyberterrorist attack against the privately ran telephone networks could lead to crippling economic repercussions for the U.S. or UK and endanger the lives of citizens who could be without access to calling for emergency responders. The U.S. Department of Defense additionally uses the Public Switch Telephone Network (PSTN) for

[28] "CESG's Incident Response Team (GovCertUK)." GovCertUK Homepage. 12 August 2007. <http://www.cesg.gov.uk/site/about/index.cfm>.

roughly 90% of its outgoing and incoming communications.[29] Therefore, this type of Cyberterrorism model directly affects national security.

Ironically, this type of fear of disruption to a nation's communication infrastructure led the U.S. government to invest in the Research & Development of the ARPANET, which was the predecessor to the Internet. Although the Internet cannot be taken down by a single attack it is highly vulnerable because it wasn't designed for the current secure uses that have evolved in the Information Age. The Internet is also highly linked and a crippling attack on one asset has a cascading effect around the world. A cyberattack triggered by a worm on hundreds of thousands of computers on January 25, 2003, slowed down Internet traffic around the world by exploiting a vulnerability in Microsoft's SQL server technology. This attack targeted at least five of the thirteen major Internet hubs and shut down Internet service in South Korea, Thailand, Japan, Malaysia, the Philippines, and India. Similarly to the 2001 "Code Red" virus, it also significantly slowed down Internet performance in the United States.[30] Borchgrave believes that, "terrorists are not just exploring weapons of mass destruction but also weapons of mass disruption." [31]

Louis Freeh, former-FBI Director (1993-2001), said in a 2000 Congressional testimony that the U.S. reliance on IT to control critical government and private sector systems is perceived to be the, "country's

[29] Kendall.
[30] "Cyber attack 'under control." BBC News. 26 January 2003.
<http://news.bbc.co.uk/2/hi/technology/2695537.stm>.
[31] Anderson.

Achilles' heal." [32] President Clinton also expressed concern on May 22, 1998, when he published the Presidential Decision Directive/NSC-63 (PDD 63) that states, "The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems." [33]

This is why the U.S. and UK have focused on creating the Public Private Partnerships (PPPs). President George W. Bush, in the introduction to the NSSC, states, "securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people." [34] In addition to the work of the GovCertUK, the British government has also formed the National Infrastructure Security Co-ordination Centre (NISCC) as an, "interdepartmental organization set up to co-ordinate and develop exiting work within Government departments and agencies and organizations in the private sector to defend the CNI (Critical National Infrastructure) against electronic attacks." [35] And the private sector has created industry specific Information Sharing and Analysis Centers (ISACs), under the direction of Clinton's PDD 63, in the fields of Information and Communications; Banking and Finance; Transportation; Emergency Services; Public Health; Electricity, Oil, and Gas; Law Enforcement; Foreign Intelligence and Affairs; and

[32] Ibid.

[33] "Critical Infrastructure Protection (PDD 63)." The White House. 22 May 1998. <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

[34] NSSC.

National Defense.[36] All of these venues of PPP collaboration assist in securing the critical assets, which are first or second tier targets for cyberterrorists.

Former Director of U.S. National Intelligence and current Deputy Secretary of State, John Negroponte, warned on May 17, 2007, that “cyber-attacks against governments and institutions were likely to increase in the future.” [37] This statement followed a series of cyber attacks in Estonia that brought down “websites and IT networks of state institutions such as the president’s office, many ministries, the parliament and the police, as well as political parties” and private entities such as the country’s two largest banks, newspapers, and other news organizations.[38] Rica Semjonova, from the Estonian Centre for Informatics, called these attacks, “a riot in the Internet.” [39]

Whether a country faces an “Electronic Pearl Harbor” as some experts have coined but skeptics doubt as possible, the threat is without argument credible. What is known is that Cyberterrorism continues to be a new and credible threat that must be addressed by a nation’s grand counterrorism strategy.[40] The UK has been historically proactive about their counterterrorism strategies because of their history combating the IRA, but the U.S. has been a very reactive society in terms of legislation and regulation. But with Cybersecurity, the U.S. has been a world leader in creating proactive steps in securing its public and private sector digital assets. By being proactive, the U.S.

[35] Trim, pg. 595.

[36] “Critical Infrastructure Protection (PDD 63).”

[37] Anderson, Robert, Daniel Dombey, Stephen Fidler, Isabel Gorst, and Maija Palmer. “US warns cyber-attacks will increase.” Financial Times. London Edition, 1. 17 May 2007. <http://www.ft.com/cms/s/324fa472-049e-11dc-80ed-000b5df10621.html>.

[38] Ibid.

[39] Ibid.

and UK have realized how debilitating a cyberattack could be on the country and have become conscious to how Cyberterrorism and Information Warfare could potentially be the future of war.

Just like how technology has improved exponentially under Moore's Law to offer cyberterrorists the computing power to act as credible threats to a nation-state's security, warfare has evolved over time. War began prior to civilization, when humans learned to hunt cooperatively. Since the dawn of written history their have been approximately 15,000 wars — roughly two and a half every year on average.[41] Within the 20th century there have been two world wars each unique to itself and each devastating in physical destruction and loss of life. Since then though, there has been a substantial decrease in violence and fatalities attributed with conventional war, but a new perceived escalating theme of violence seems to exist with regard to terrorism from non-nation state enemies.

War has changed. Anthropologist, Lawrence Keely speculates on this principal showing that each World War had a specific technological paradigm. He shows that World War I was fought with the knowledge and understanding of chemistry with the modern weaponry of the time being mustard gas and TNT. World War II was fought with physics and nuclear weapons. Keely believes that today there is an undeclared World War III, and it is not the War on Terror, but one being fought on an intangible binary battlefield. This war is fought through

[40] Anderson.

[41] Alexander, Yonah and Michael S. Swetnam. Cyberterrorism and Information Warfare: Threats and Responses. Ardsley, NY: Transitional Publishers Inc., 2001. pg 91.

the continued science of physics, but “of silicon becoming the technical basis.” [42] Consistent through the scheme of present war, the violence has diminished. Keely continues showing that his, “World War III was nearly gun-free. The actual weapons employed in this most recent conflict were computers.” [43]

As the Information Age continues to blossom, this paradigm should hold true, but it is questionable how terrorism will be judged under the historical lense in relation to the violence it has recently endured in the 20th and 21st centuries. As globalization continues and Nicholas Negroponte’s One Laptop Per Child Program diminishes the digital divide so too could the threats from terrorism. Terrorists will be less able to depend on disenfranchised youths to recruit because the Internet, as the great democratizing tool that it is, will allow these prospective terrorists to become educated. Or will terrorists have a larger audience that gain access to its propaganda online? Again, time will tell.

Their will always be vulnerabilities and malicious actors looking to exploit such security gaps for their own gains. Cyberterrorism will not be eradicated nor will terrorism. Just as the 15,000 wars show, people will always be looking to fight, but as countries forge stronger political bonds through collaboration; economies become linked through globalization; and the Internet *flattens the world* further their will be less of a threat. The United States and the United Kingdom must continue to not just fight the war on terrorism, but must be determined to achieve their grand strategies. They must also continue seeing terrorism under the holistic viewpoint that requires International collaboration.

[42] Alexander, pg 94.

Specifically they must also continue to incorporate their counterterrorism strategies towards Cyberterrorism as equally holistic and part of the grand strategy.

Through creating the PPPs the U.S., UK, and other countries around the world collaborate through these vertical groups, with inter-lapping verticals, and internationally similar vertical channels. The PPPs also have essentially by defacto-proxi militarized the brain trust of the private sector in assisting in the global war on terror. The companies that volunteer do not necessarily do it out of patriotism but they wield "the hammer" as for-profit institutions with the most to gain or the most to lose if they fail. The country's grand strategy thus benefits from this increased brain power and collaboration. As John Negroponte and Keely said, the future has been perceived to include more acts of Cyberterrorism but in addition to the U.S. and UK militaries leading the countries' grand counterterrorism strategies against this new credible threat, the terrorist enemies that threaten these nations must also combat Cisco, Google, Microsoft, Sun Microsystems, Symantec, and every man, woman, and child that can swing a hammer, click a mouse, or strike a key in the name of national defense.

[43] Ibid.

Works Cited

"About CESG." Communications-Electronics Security Group Website. 12 August 2007. <http://www.cesg.gov.uk/site/about/index.cfm>.

Alexander, Yonah and Michael S. Swetnam. Cyberterrorism and Information Warfare: Threats and Responses. Ardsley, NY: Transitional Publishers Inc, 2001. pg 91.

Anderson, Kevin. "Cyber-terrorists wiled weapons of mass disruption." BBC News. 22 February 2000. <http://news.bbc.co.uk/1/hi/sci/tech/specials/washington_2000/648429.stm>.

Anderson, Robert, Daniel Dombey, Stephen Fidler, Isabel Gorst, and Maija Palmer. "US warns cyber-attacks will increase." Financial Times. London Edition, 1. 17 May 2007. <http://www.ft.com/cms/s/324fa472-049e-11dc-80ed-000b5df10621.html>.

"CESG's Incident Response Team (GovCertUK)." GovCertUK Homepage. 12 August 2007. <http://www.cesg.gov.uk/site/about/index.cfm>.

"Critical Infrastructure Protection (PDD 63)." The White House. 22 May 1998. <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

Cuthbertson, Ian M. "The Nature of the Terrorist Threat and National Responses to Terrorism: The British Case." National Counter-Terrorism Strategies: Legal, Institutional, and Public Policy Dimensions in the US, UK, France, Turkey and Russia. Washington, DC: IOS Press, 2006.

"Cyber attack 'under control." BBC News. 26 January 2003. <http://news.bbc.co.uk/2/hi/technology/2695537.stm>.

"Cyber cops plan unveiled." BBC News. 13 November 2000. <http://news.bbc.co.uk/1/hi/uk_politics/1021352.stm>.

Denning, Dorothy. "Activism, Hactivism, and Cyberterrorism: the Inter as a Tool for Influencing Foreign Policy." Networks and Netwars: The Future of Terror, Crime, and Militancy. Chapter 8. RAND Corporation: Washington, DC, 2001.

Denning, Dorothy E. "CYBERTERRORISM." 23 May 2000. <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

Friedman, Thomas L. The World is Flat: A Brief History of The Twenty-First Century. New York: Farrar, Straus and Giroux: 2005.

G8 parliamentary speakers agree to harmonize counterterror laws. BBC News. Transcript. St. Petersburg, Russia: 16 September 2006.

Greenemeir, Larry. “Cyberwarfare: By Whatever Name, It’s On the Increase.” INFORMATIONWEEK. 9 July 2007. <http://www.informationweek.com/story/showArticle.jhtml?articleID=200900812>.

Kendall, Bridget. “Newsnight: Terrorism online transcript.” BBC News. 27 May 2007. <http://news.bbc.co.uk/2/hi/events/newsnight/1050141.stm>.

Lourdeau, Keith. “Congressional Testimony Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security” U.S. Federal Bureau of Investigation. 24 February 2004. <http://www.fbi.gov/congress/congress04/lourdeau022404.htm>.

The National Strategy to Secure Cyberspace. The White House. Washington, DC: February 2003. pg. 19.

One Laptop per Child. 11 August 2007. < http://laptop.org/vision/mission/>.

Pollitt, Mark F. “CYBERTERRORISM – Fact or Fancy?” U.S. Federal Bureau of Investigation Laboratory. Computer Fraud & Security, Volume 1998, Number 2, February 1998, Available publicly at <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>.

Trim, Peter R.J., “Public and Private Sector Cooperation in Counteracting Cyberterrorism.” International Journal of Intelligence and Counterintelligence. Volume 16, Number 4. 1 October 2003. pg 595.