States rather than criminals pose a greater threat to global cyber security: a critical analysis

Fahad Ullah Khan*

Introduction

Attacks by States as well as criminals pose significant threats to internet security during the 21st century. In fact it is difficult to divide threats posed to internet security into two such groups, as the nexus between organized crime and the state is becoming increasingly blurred.[1] Governments in both developed and developing nations, defence industries, and corporations in the finance and telecommunications sectors are increasingly being hit by various cyber attacks from either criminals or countries looking for monetary or military benefit.[2] With so many attacks through highly sophisticated means, organizations have difficulty in pin pointing which new threats and susceptibilities present the greatest risk, and also struggling with questions of how to deal with them, and using what resources.[3]

Internet security is greatly threatened by attacks from cybercrime, cyber warfare, and cyber terrorism.[4] Of increasing concern is how these attacks may pose a threat to a nation state's critical infrastructure, and how such a threat may be managed or contained in the event of such an attack. This does not mean, however, that threats by cybercriminals should be regarded as a lesser threat in any manner as there is significant difficulty in defining the difference between criminal organizations and state sponsored attacks.[5] As the world becomes increasingly computerized and connected through information communication technologies (ICTs), so does our cyber security threat increase both on an individual and national level. In this paper, I wish to explore how internet security is threatened equally by both states and criminals, even though at times the focus or objective of the attack, and its consequences, are very different.

Definitions and distinctions

Before embarking on responding to the question of whether criminals or states pose a greater threat to internet security, it is wise to first define what internet security is. One way to describe this is that,

* The writer is Research Fellow, the Institute of Strategic Studies Islamabad (ISSI).

> When a computer connects to a network and begins communicating with other computers, it is essentially taking a risk. Internet security involves the protection of a computer's Internet account and files from intrusion of an unknown user. Basic Internet security measures involve protection by well selected passwords, change of file permissions and back up of computer's data.[6]

However, could internet security also take into account the human element of security? For example, the feeling of security when browsing the internet or chatting in chat rooms without having to worry that one will become the victim of cyber-stalking, or falsely implicated for downloading child pornography.[7] Indeed, both technical and human elements must be considered when trying to evaluate the threat towards internet security.

Threats to internet security can come from a multitude of separate but interlinked sectors, including cybercrime, espionage by the military and foreign intelligence services, economic espionage and lastly cyber-warfare.[8] Each poses its own unique threat, yet all can be devastating in their own manner. By looking at the meaning of these concepts we may possess a greater understanding of how such acts may represent a serious threat to internet security.

Cybercrime

Threats to internet security by criminals are often referred to as cybercrime. McQuade has defined cybercrime as being the "use of computers or other electronic devices via information systems to facilitate illegal behaviours."[9] However, while this may help shed light on the meaning of cybercrime, the truth is that no universal definition of the term exists,[10] and in fact it remains a fluid concept as it may even encompass traditional crimes being committed in a high tech manner.[11]

Dividing cybercrime into two types, Type 1 and Type 2, eases our understanding further.[12] Type 1 cybercrime may be characterized as being "singular or discrete … facilitated by the introduction of crimeware programs such as root kits or Trojan horses… [and] can but may not necessarily be facilitated by vulnerabilities."[13] Examples of crimes under this category may include phishing, identity theft, ecommerce fraud and hacking in which data or services are manipulated.[14] Type 2 cybercrime on the other hand, is performed by software such as instant messaging programs, or transfer of files through FTP which does not fall under the typical crimeware classification.[15] Such cybercrimes are not limited but

may include cyberstalking, cyber harassment, preying on children through online activities, cyber terrorism, and corporate espionage.[16] While both cyberstalking and hacking into another computer may be defined as cybercrime, one is more people-oriented, utilizing social engineering techniques, while the other is more technological in nature.[17]

Cyberwarfare

Cyberwarfare on the other hand, like its partner cybercrime, has no clearly agreed definition.[18] Clarke has defined cyberwarfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[19] Perhaps a clear example of a recent cyberwafare attack was the Stuxnet worm in which supposedly the United States and Israel, in possible collaboration with Germany and Great Britain, were able to successfully target the Siemens systems at Iranian nuclear plants causing damage and failure to centrifuges, despite the appearance of normal operations during the attack.[20]

Cyber espionage

Cyber espionage involves obtaining secret or classified information without permission from individuals, companies or governments for economic, political or military advantage using illicit means through the internet, networks and/or computers, and can involve cracking or malicious software such as Trojan horses and spyware.[21] The Chinese People Liberation Army (PLA) is perhaps the most famous for its cyber espionage campaigns such as Titan Rain and Aurora,[22] and Byzantine Hades,[23] where China was accused of cyber spying and stealing sensitive information from both the private and government sector including the Pentagon.[24] The PLA has been accused of using Trojans to infiltrate and attack computers as part of its "pressure point warfare", which is to attack nodes within the cyber area or physical infrastructure in order to put the enemy in a crippling position.[25]

Cyber terrorism

Cyber terrorism has been defined as "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage."[26] The Federal Emergency Management Agency (FEMA) has defined cyber terrorism as "unlawful attacks and threats of

attacks 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."[27] Numerous groups, such as the terrorist organization al-Qaeda have been suspected of cyber terrorist threats, hacking into computers and gaining backdoor entry into systems.[28] While no actual confirmed cyber terrorist attack has ever taken place, some commentators have argued that the Code Red DoS attack, in which 300,000 computers at the White House were infected with the Nimda virus that required almost $3 billion to clean up, was conducted by terrorist groups to test U.S. critical information infrastructures (CII's) defences.[29]

Numerous groups, such as the terrorist organization al-Qaeda have been suspected of cyber terrorist threats, hacking into computers and gaining backdoor entry into systems.

However, should these threats be categorized in a separate manner? Does one pose a greater threat to internet security than the other? Is it more important for us to focus on cybercrime as a threat than cyberwarfare, or economic espionage or even cyber terrorism? Do we design our cyber defence capabilities according to simply a name? All these questions are relevant because in this day and age the thin boundary lines between cybercrime, cyberwarfare, cyber espionage or cyberterrorism or any other lexicon we can create are becoming increasingly blurred.[30] This does not mean that all cyber attackers share the same motivation or purpose. Some will be financially motivated, others may have political agendas, and some may simply be testing their new skill sets, and so forth.[31]

However, the defences employed against internet attacks are important to reflect the borderless nature of the cyberworld where cybercriminals or hackers may work in tandem with their nation states to carry out attacks on foreign governments and civilians.[32] This was the speculation in the Estonian case that we will discuss later, in which it was suspected that the Russian government had collaborated with groups of hackers to carry out a large scale cyber attack on the government and economic sectors of the country.[33] Trying to label an attack as cybercrime or cyberwarfare, cyber this and that, creates various problems because it is extremely difficult to determine accurately the person, motivation and purpose behind the attack.[34]

Internet security and critical infrastructure

For many years there has been discussion of a digital Pearl Harbor in which a nation state's critical infrastructure (CI) is damaged or shut down through the internet.[35] What exactly is critical infrastructure? According to the President's Commission on Critical Infrastructure (PCCIP), CIs are "combinations of systems and facilities which are so vital that their incapacitation or destruction would have a debilitating impact on a [nation's] defence or economic security."[36] The infrastructure is crucial because it provides goods and services that are important to the economy and defence of the country.[37]

What is the relevance of CI to this paper? The importance lies in the fact that when assessing attacks against states, particularly in cases of cyberwarfare in modern nation states, cyber attacks against CIs is a cause of concern.[38] This is since any disruption or attack against infrastructures that provide oil, power, gas and water may prove devastating to a nation under attack.[39] This can occur on a global, national, societal economical and individual level.[40] Cyber attacks by States against military installations of foreign countries, government and private organizations such as the banking industry also pose a real threat both to the society and the government as illustrated in two cases below.

National security and cyber threat incidents

Syria

While there is some controversy as to how serious the threat really is,[41] there is no doubt that real and serious threats to governments exist worldwide. This can be illustrated by numerous incidents during recent years. For example, in 2007, the Israelis bombed the site of a suspected Syrian nuclear installation.[42] The supposedly state of the art Syrian radar was unable to notify the Syrian military of the air raid.[43] Speculations were that the microprocessors of the radar had hidden backdoors in which a programmed code could be sent, hence damaging their function and provisionally blocking the radar.[44]

Estonia

An interesting event illustrating the shocking power of an attack on a country's internet security can be illustrated by a case in 2007 when Estonia was hit by a series of major cyber-attacks directed against its government and critical infrastructure.[45] Estonia is one of the most wired

nations in the world[46] with an extremely high tech government, economy and banking system.[47] Attacks were the result of botnets, which are "networks of compromised computers," that launched massive Distributed Denial of Service Attacks (DDoS), swamping email accounts with spam.[48] Normally DDoS, which are "preprogramed floods of internet traffic designed to crash or jam networks" are not considered a major threat.[49] However the attack in Estonia was massive, with numerous forms of botnets each with thousands and thousands of infected machines on the attack.[50] Jaak Aaviksoo the Minister of Defence at the time stated that,

> The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia.. All major commercial banks, telcos, media outlets, and name servers — the phone books of the Internet — felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.[51]

Clearly, the incident above illustrates the danger a cyber attack may pose towards internet security for the State. Unknown vulnerabilities combined with malicious state actors and continually advancing threats by adversaries and criminals pose significant threats to a critical infrastructure of a State.[52]

Types of attacks

It is worth mentioning briefly the kinds of attacks that can be initiated through cyber warfare or cybercrime. For instance, spear phishing has been used by China in numerous attacks against the United States.[53] This involves social engineering in which hackers design official looking emails and send them to particular individuals with the hope that the target then will click on the attachment or link and be taken to a malware site.[54] This type of attack has led to serious losses of intellectual property[55] as well as important and confidential government information.[56]

DNS hijacking, another type of attack, involves the redirection or hijacking of the DNS address to fake DNS servers for the objective of placing malware onto ones computer, usually for criminal purposes.[57] Hijacked DNS addresses interpret the genuine IP address or DNS name into IP address of malicious site[58] and websites can be turned into malicious websites without the knowledge of the user.[59]

Computer worms can also create major issues by taking advantage of holes and defects within softwares to spread from one computer to the

next. Worms spread by looking for and placing damaging codes onto other systems.[60] They can very quickly replicate, spreading and taxing system memory and toppling corporate networks.[61] Perhaps one of the most destructive worms recently that caused severe problems for the Iranian government was the Stuxnet worm that destroyed almost one-fifth of the Iranian nuclear centrifuges and delayed the Iranian nuclear weapon program by almost another couple of years.[62] While it is believed that the U.S. and Israel were behind the designing of the worm, the possibility that it could be used to hurt any industrial nation should also be considered.[63] The Department of Homeland Security believes that this worm was the first developed of its type, written to specifically hit "mission critical control systems" utilizing certain blend of software and hardware.[64]

Cybercrime - a greater threat?

There is no doubt that state-sponsored cyber attacks can cause chaos particularly if combined with a physical attack as witnessed in the Syrian case above. However, some commentators have argued that we must first deal with cybercrime as that poses a far more immediate threat than cyber warfare where a state's CIs may suffer an immeasurable blow.[65] For instance Christopher Painter, the White House's Senior Director for cyber security, has stated that transnational organized cybercrime involving credit card theft and cyber espionage is of greater importance currently than cyber war attacks towards critical infrastructure such as electricity grids.[66] Painter has argued that while CI needs to be made safer, the best defence is first to start fighting cybercrime.[67] He is not the first one to suggest that cyber threat may not be as serious as envisioned.[68] Lewis has argued that CIs are designed to be strong and can absorb damage without affecting operations, and are used to doing this after natural disasters or very bad weather conditions and that really the threat to CI is exaggerated.[69]

According to recent statistics, cybercrime in just the UK is costing the country 27 billion pounds a year, which are mostly hitting businesses, although the government has also reported a loss of 2.2 billion pounds and individuals up to 3.1 billion pounds

Taking all this into account, what information do we have on the threat of cybercrime to internet security? According to recent statistics, cybercrime in just the UK is costing the country 27 billion pounds a year, which are mostly hitting businesses, although the government has also reported a loss of 2.2 billion pounds and individuals up to 3.1 billion

pounds.[70] Indeed, "industrial espionage, intellectual property theft and extortion have been the most costly crimes."[71] Just online theft itself is costing one trillion U.S. dollars a year.[72] Cybercrime is no longer simply being committed by a lone teenager sitting behind a computer desk but by thoroughly organized criminal groups which may consist of numerous experts, including IT experts, legal personnel and those who are responsible for harvesting data.[73]

In addition, cybercrime is not limited to attacks within the physical world but is now also occurring in virtual worlds,[74] which are presenting a completely new scenario and opportunity for criminals to exploit.[75] Virtual worlds are no longer a place for a few individuals to gather, but represent a billion dollar industry that is only loosely regulated.[76] With everyday real crimes such as money laundering, theft, child pornography, suspected terrorist activities can now occur in a virtual environment.[77] Interestingly enough, in almost 20% of massively multiplayer online role-playing games (MMORPG), players have reported that the virtual world is their main place of residence and that the physical world is solely a place to grab food and sleep.[78] If this percentage continues to grow, threats to internet security may no longer simply occur in the real physical world but increasingly occur in the virtual world where victims, and a loosely regulated environment exist.[79]

Legal obstacles and enforcement of internet security

Whether cyber attacks are directed by organized criminal groups, governments, terrorists, individuals or a combination of all, finding and apprehending parties to such heinous crimes is difficult, regardless of the attacker.[80] Neither cybercrime nor state sponsored cyber attacks can be dealt with by traditional methods of law.[81] This is due to a number of reasons. Firstly, there are no physical limitations; perpetrators and victims are not necessarily tied to the same geographical location, and perpetrators can target their victims whether they are in Nigeria or Rio.[82] Secondly, anonymity, fraud and deception are far easier to achieve online than in the physical world.[83] Thirdly, traditional methods of gathering evidence are not necessarily effective with cyber criminals as they can perform their activities without being physically present and can do so through automatic agents.[84]

In regard to state sponsored cyber attacks the difficulty in prosecuting and apprehending suspected cyber criminals becomes even more difficult; as suspected in the Estonia case where Russia did not cooperate in the "investigation, apprehension, and extradition" of those involved in

subversive attacks against Estonia.[85] Given the secretive nature of the internet, it is not difficult for States to instigate civilians within their country to carry out cyber attacks and then pretend they had nothing to do with it.[86] In addition, the unclear status and ambiguity surrounding State responsibility for cyber attacks makes it very difficult to bring States to task for actions they may have sponsored during a cyber attack on another country.[87]

Since 1998, there have been only sixty two successful prosecutions against cybercrime,[1] and according to some estimates, a "new piece of malware is created every 2.2 seconds."

However cybercrime itself is also a recurrent and deadly threat to internet security, and continues to grow with insufficient prosecution despite flashy news reports occasionally when a cyber heist is successfully busted.[88] Since 1998, there have been only sixty two successful prosecutions against cybercrime,[89] and according to some estimates, a "new piece of malware is created every 2.2 seconds."[90] Organized criminals are said to have more money to spend on research and development than even governments or the IT security industry.[91] If this is true then there has to be even more done to combat cybercrime on a global level.

Perhaps the leading international instrument against global cybercrime is the Council of Europe's Convention on Cybercrime, which was passed in 2001.[92] Although it is open to signature and ratification of non-members, only one non-member, the United States, has ever ratified it.[93] While the Convention appears to be quite comprehensive, due to the ever changing nature of cybercrime there are certain areas of cybercrime that are not sufficiently dealt with, including "attacks on critical infrastructure and cyber terrorism", denial of service attacks and massive spamming .... phishing ... pharming of passwords and identity theft."[94]

Internet security cannot be protected sufficiently in the long term if we cannot prosecute those who perpetrate crimes against it. However, there are a host of problems that exist with enforcing cybercrime law on a global scale. Nevertheless, solutions need to be developed in order to resolve this situation if we are develop any comprehensive legal system to tackle cybercrime or cyberwarfare worldwide. Firstly, if the Convention or any treaty that prosecutes crimes against internet security is to operate on a global scale, it has to be accepted by every country in the world. Otherwise cybercriminals can easily operate from havens with little fear of

prosecution.[95] However, this will not happen until the agreement is acceptable to governments worldwide, and takes into account the needs of every member and not just European states.[96]

Only recently, an international cybercrime treaty was rejected by the UN due disagreement among nations on sovereignty and human right issues.[97] If one takes a look at Article 47 of the Convention on Cybercrime, it states that parties to the Convention may "denounce this Convention" at any time.[98] This makes it very easy for a country to simply withdraw from a major international agreement if there is any issue of concern.[99] How is one to formulate any sort of binding global treaty to fight cybercrime or cyber warfare if members can simply withdraw from any agreement at any time? Weismann has argued that,

> International law does not fit neatly in into the characterization of one body of unified rules displacing national decision making, particularly where choices involving the processes of accession, compliance and withdrawal remain relatively unpredictable.[100]

A global legal instrument on fighting cybercrime or cyber warfare that is acceptable to all governments may be difficult to achieve. Perhaps encouraging voluntary public-private partnerships would be more feasible, as it is clear that solely government efforts to combat cyber attacks are not enough, whether technically or legally, to prosecute cybercriminals.[101] This is partly due to the fact that many of the ICTs are managed by private actors, with the internet being a global network without any hierarchal structure.[102]

States only have a limit as to the resources they can expend, and in reality their criminal justice systems very much depend on the information technology industry to efficiently investigate and prosecute cybercrimes.[103] This can be witnessed in the Mikado Operation of 2006 in which a child pornography website that had been identified by a German TV station led a public prosecutor to ask 22 German credit card firms to supply details of client credit card transactions that would assist in the investigation – a request to which the credit card firms voluntary complied with.[104] As a result, many suspects were identified and search and seizure orders were brought against them.[105]

Some authors have even suggested that one agency should be appointed to manage and prosecute cybercrime around the world.[106] This agency could be embedded with investigation, prosecution and sanctioning powers.[107] However, it is unlikely that nation states would be

willing to give up complete control over cybercrime related matters to an external agency.[108] Could we then take a more middle approach where powers of prosecution and sanctioning would remain in the hands of the state whilst the procedure of investigation would be managed by a global policing agency designated solely for such tasks?[109] A global agency could coordinate efforts among nation states in identifying dangerous trends before they occur to individual governments or investigators.[110]

Further solutions to enhanced cyber security

It is clear that cyber attacks, whatever name they fall under, represent a clear and present danger to internet security internationally and this includes governments, corporations and common individuals. More than 80% of information infrastructure is owned by the private sector in democratic countries.[111] In addition, at least in the U.S., close to 40% of critical infrastructure companies have no collaboration with the federal government on cyber security issues.[112] This differs in China where only roughly 5% of Chinese executives reported that they did not work with their government on internet security.[113]

A close partnership between the private and the public sector is also crucial in order to ensure that private interests are maintained including privacy concerns that have been voiced over government initiatives to further secure cyberspace.

To counter increasing threats, it is imperative cooperation between the private and public sectors is enhanced.[114] The recent paper "Improving our Nation's Cyber security through the Public-Private Partnership" has also stated that public-private partnerships are beneficial in defending internet security.[115] However, in order for this to happen, it is imperative that sufficient incentives exist as well.[116] A close partnership between the private and the public sector is also crucial in order to ensure that private interests are maintained including privacy concerns that have been voiced over government initiatives to further secure cyberspace.[117] Also, rather than focusing so much on state sponsored cyber attacks and their danger to critical infrastructure, we should also take into account that 90% of attacks being conducted by organized gangs, most of which are motivated by financial gain.[118]

Criminal groups can also be used as "cyber proxies" in carrying out attacks against civilian CI for political reasons as well as economic purposes.[119] Therefore, focusing resources on finding and prosecuting cybercriminals is also imperative if we are to help prevent attacks on CIs. While not dismissing cyber threats by state actors, fighting cybercrime has a dual purpose as cyber criminals may act as "cyber proxies" for nation States or for pure criminal purposes.[120] Companies must invest in stronger anti-fraud systems and learn to secure their systems better to avoid cyber espionage from occurring.[121]

Another issue to take into consideration is that both companies and individuals need to be more open when disclosing cyber attacks conducted against them, as reports of what we find in the news may simply represent the peak of the pyramid.[122] Individuals represent a critical aspect of cyber security. People who are not careful about taking measures to protect their computers can risk their machines being taken over as a botnet.[123] These botnets pose significant security threats whether used for attacks against a State's CIs, corporations or individuals.[124] This can be countered partially through awareness and educational programs[125] that could be much more helpful in bolstering cyber defences than simply technical measures themselves. In order for this to be effective, there has to be a culture of internet security, just as we have a culture of traffic security where we obey when to stop or pass the green light. This can only be done if awareness is developed within the community to respect cyber security.[126]

Conclusion

It is clear that whatever form of cyber attack is initiated, clear and well thought out solutions must be devised to counter this problem globally, regionally and nationally. The strength of internet security lies in its ability to adapt to new and evolving threats. This is where governments and the private sector must focus their work in developing continuous solutions to ward off perpetual and newly designed threats. The question whether attacks by States or criminals represent a greater threat to internet security can be answered by stating that both pose a significant threat and are often intertwined as it has been seen that they may be complicit in carrying out attacks.

We can no longer draw thin red lines as to whether attacks by states or criminals constitute a greater threat as the methods and techniques utilized to plug holes in internet security are the same even if the purpose may be different. In addition, technical measures to maintain internet security cannot be done solely to protect users; legal initiatives must also

complement this endeavour. However, as we have seen above, without clearly defined and updated rules on how to punish those who perpetrate crimes be it states, groups or individuals, it is very difficult to stop those who are willing to breach internet security in the long term. Governments and organizations must learn to cooperate more effectively and move beyond self serving interests if the internet is going to be secure for everyone in future. Nevertheless, this represents a utopian concept which many may share in theory but differ in practice.

One must also realize that the gap in conventional military superiority between developed and undeveloped nations remains quite wide and that asymmetric warfare techniques such as cyberwarfare and the attack on critical infrastructure as well cyber espionage operations remain a far more economical and powerful choice to use than trying to match the military superiority of countries such as the United States.

One must also realize that the gap in conventional military superiority between developed and undeveloped nations remains quite wide and that asymmetric warfare techniques such as cyberwarfare and the attack on critical infrastructure as well cyber espionage operations remain a far more economical and powerful choice to use than trying to match the military superiority of countries such as the United States.[127] The same applies in different facets to cybercrime. If the criminal today can multiply his profits without even having to step out his front door, operate and carry out his activities in havens where cyber laws are lax or non-existent, exploit loopholes in any existing legal conventions or agreements and realize that digital evidence to prosecute will be hard to gather, then the internet becomes the perfect vehicle to carry out attacks. Therefore, to protect internet security we must recognize these harsh realities and start from there.

Ironically, perhaps the threats to internet security simply represent the peak of the pyramid, and the accumulation and evolution of years of humanity unwilling to work beyond self interest and for the greater good of civilization. We can go on for centuries as to whether this or that represents a greater threat and what solutions one should present. Nevertheless, while it is important to acknowledge current threats to internet security, perhaps greater attention needs to be focused on how to

develop trust and cooperation rather than simply devising solutions that may not make it in the long term.

Notes & References

[1] Quentin Reed, 'Squeezing a Balloon : Challenging the nexus between organized crime and corruption', *U4 Anti Corruption Resource Center*, 2009, Vol. 7, p. 12 http://www.cmi.no/publications/file/3399-squeezing-a-balloon.pdf

[2] 'The Top Cyber Security Risks, *SANS*, 2009, http://www.sans.org/top-cyber-security-risks/

[3] Ibid.

[4] Paul C Dwyer, 'Cybercrime in the UK', *ICTTF*, 2011 http://www.icttf.org/blogs/2/29/cybercrime-in-the-uk?PHPSESSID=bd8e352e1d37962dd9bb167820556d11

[5] Shane Sims, 'Inside the Cyber Threat Landscape', *CIO Update*, March 25, 2011, http://www.cioupdate.com/trends/article.php/3929201/Inside-the-Cyber-Threat-Landscape.htm

[6] 'Ultimate Internet Security', *Itunes*, http://itunes.apple.com/us/app/ultimate-internet-security/id360063332?mt=8#

[7] 'Child Pornography and The Trojan Horse Defence', ESCRIPT https://www.escript.law.ed.ac.uk/ node.asp?id=7862

[8] Scott Charney, 'Rethinking the Cyber Threat, A Framework and Path Forward', *Microsoft*, 2009, http://www.microsoft.com/downloads/en/details.aspx?FamilyID=062754CC-BE0E-4BAB-A181-077447F66877

[9] Sam C. McQuade., III ,2006, 'Understanding and Managing Cybercrime', Allyn & Bacon, p.2

[10] Joachim Vogel, 2007, 'Towards a Global Convention against Cybercrime', http://www.penal.org/IMG/Guadalajara-Vogel.pdf

[11] Susan W. Brenner, 2001, 'Is There Such a Thing as Virtual Crime', California Criminal Law Review, Vol. 4 No. 1

[12] Sarah Gordon & Richard Ford, 2006, ' On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol 2, p.13-14

[13] Ibid.

[14] Ibid.

[15] Ibid. p. 15

[16] Ibid. p. 14-15

[17] Ibid.

[18] Mike Lennon., 'Defining and Debating Cyberwarfare', *Security Week*, April 16, 2010, http://www.securityweek.com/content/defining-and-debating-cyber-warfare

[19] Richard A. Clarke & Robert Knake, 2010, 'Cyber War The Next Threat to National Security and What to Do About It', Ecco

[20] Jonathon Masters, *Confronting the Cyber Threat*, , *CFR*, May 23, 2011, http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577

[21] Angel T. Redoble, Cyber Weapons Proliferation and Deterrence, *ISCSP*, http://iscsp.org/wp-content/uploads/2010/08/cyber-weapons-proliferation-and-deterrence.pdf

[22] Richard Norton Taylor, 'How Chinese Attackers Targeted Whitehall' *The Guardian*, September 5, 2007, http://www.guardian.co.uk/technology/2007/ sep/04/ news.internet

[23] 'China Ahead of US in Cyber Espionage Report', *CBR*, April 15, 2011 http://security.cbronline.com/news/chinese-ahead-of-us-in-cyber-espionage-report-150411

[24] Collin A. Spears, 'Trading With the Enemy: Sino American Cyber Espionage', *FPB*, April 18, 2011, http://chinatrade.foreignpolicyblogs.com/2011/04/18/trading-with-the-enemy-sino-american-cyber-espionage/

[25] Tom Kington 'A Dangerous Web : Defending Against Cyber Attacks is a Growing Concern', *C4ISR*, March 6, 2008,http://www.c4isrjournal.com/story.php?F=3240550

[26] Clay Wilson, 'CRS Report for Congress,' Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, *FAS*, January 29, 2008 http://www.fas.org/sgp/crs/terror/RL32114.pdf

[27] Ibid.

[28] Ehsan, Ahrari, 'Al Qaeda and Cyber Terrorism', *Asia Times Online*, August 18, 2004, http://www.atimes.com/atimes/Front_Page/FH18Aa01.html

[29] Sam C. McQuade., III ,2006, *Opcit* p.104

[30] Dave DeWalt, 'No Line Between Cyber Crime and Cyberwar', The Hill, December 2, 2009 http://thehill.com/opinion/op-ed/70319-no-line-between-cyber-crime-and-cyber-war

[31] Andrew Donoghue, Infosec 2010: Experts Overlook Motivation for Cyber Attacks', *E week Europe*, April 27, 2010, http://www.eweekeurope.co.uk/news/experts-admit-motivation-for-cyber-attacks-overlooked-6696

[32] Ibid.

[33] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

[34] Clay Wilson, *Opcit*

[35] 'Cyberwarfare: Marching off to Cyberwar', *The Economist*, December 4, 2008 http://webcache.googleusercontent.com/search?q=cache:ekAvGFUp7YMJ:www.economist.com/node/12673385+definition+of+cyberwarfare&cd=7&hl=en&ct=clnk&source=www.google.com

[36] Sam C. McQuade., III ,2006, *Opcit.* p. 53

[37] Rosslin John Robles & Min-Kyu Choi, (2009), 'Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems', *International Journal of Grid and Distributed Computing*, Vol. 2 No. 2, p.29

[38] Gabriel Perna, 'Report: Smart Grid Not Smart When It Comes to Cyber Attacks', *International Business Times*, April 20, 2011, http://www.ibtimes.com/articles/136601/20110420/cyber-crime-critical-infrastructure-energy-smart-grid.htm

[39] Ibid.

[40] Heli Tiirmaa-Klaar, 'Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels', *CERI CNRS*,2011, http://www.ceri-sciencespo.com/archive/2011/mars/dossier/ art_htk.pdf

[41] James A. Lewis, 'Cybersecurity and Critical Infrastructure Protection', *CSIS*, 2006 http://csis.org/files/media/csis/pubs/0601_cscip_preliminary.pdf

[42] 'Shock Waves from Syria: Did Israel Bomb a Secret Nuclear Facility Equipped by North Korea', *The Washington Post*, September 20, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/19/AR2007091901965.html

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

[44] Ibid.

[45] Henry S. Kenyon (2009), 'Cyber Attacks Reveal Lessons', *USACAC*, December 10, 2009 http://usacac.army.mil/cac2/call/docs/10-12/ch_7.asp

[46] Joshua Davis, 'Hackers Take Down The Wired Country in Europe', *Wired Magazine*, Issue 15.09, http://www.wired.com/politics/security/magazine/15-09/ff_estonia

[47] Larry Greenemeier (2007), 'Estonian Attacks Raise Concern Over Cyber Nuclear Winter', *Information Week*, May 24, 2007, http://www.informationweek.com/ news/internet/ showArticle.jhtml?articleID=199701774

[48] Ibid.

[49] Richard A. Clarke & Robert Knake, 'Cyber War The Next Threat to National Security and What to Do About It', Ecco

[50] Ibid.

[51] Joshua Davis., *Opcit.*

[52] Phillip Reitinger, 'Examining the Cyber Threat to Critical Infrastructure and the American Economy, *Emergency Management*, March 18, 2011 http://www.emergencymanagement.org.uk/mar2011/DHS180311/tabid/5148/ Default.aspx

[53] Dan Dieterle, 'Chinese Hackers Spear Phishing for US Military Secrets', *INFOSEC*, April 24, 2011, https://www.infosecisland.com/blogview/13308-Chinese-Hackers-Spear-Phishing-for-US-Military-Secrets.html

[54] Ibid.

[55] Kelly Jackson Higgins, *Spear-Phishing Attacks Out of China Targeted Source Code, Intellectual Property, Information Week*, January 13, 2010, http://www.informationweek.com/news/security/ attacks/222301157

[56] Peter Bright, 'Hackers Spear-Phish, infiltrate French Ministry of Finances', *ARS Technica*, http://arstechnica.com/security/news/2011/03/hackers-spear-phish-infiltrate-french-ministry-of-finances.ars

[57] 'DNS Hijacking : What it is and How does it work?', *Spam Laws*, http://www.spamlaws.com/dns-hijacking.html

[58] Ibid.

[59] Ibid.

[60] 'Computer Worms', http://articles.winferno.com/antivirus/computer-worms/

[61] Ibid.

[62] William J. Broad, Johan Markoff, & David E. Sanger, 'Israeli Test on Worm Called Crucial In Iran Nuclear Delay', *New York Times*, Jan 15, 2011, http://www.nytimes.com/2011/01/16/world/ middleeast/16stuxnet.html

[63] Ibid.

[64] Phillip Reitinger, *Opcit.*

[65] 'To avoid cyberwar and protect infrastructure first-fight cybercrime first' *HSNW*, April 14, 2010, http://homelandsecuritynewswire.com/avoid-cyberwar-and-protect-infrastructure-fight-cybercrime-first

[66] Ibid.

[67] Ibid.

[68] James. A. Lewis, Cybersecurity and Critical Infrastructure Protection, *CSIS*, January 2006, http://csis.org/files/media/csis/pubs/0601_cscip_preliminary.pdf

[69] Ibid.

[70] 'Cyber Crime and Cyber Warfare Pose Growing Threat', http://www.clubdoconline.com/news/press-release/cyber-crime-and-cyber-warfare-pose-growing-threat/

[71] Ibid.

[72] Tim Weber, 'Cybercrime Threat Rising Sharply' *BBC*, January 31, 2009 http://news.bbc.co.uk/2/hi/business/davos/7862549.stm

[73] Ibid.
[74] Marc Godman, 'Virtual World Crime, Council of Europe Octopus Interface Conference', *COE*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/if_2009_presentations/2079if09pres_goodman_virtualcrime.pdf
[75] Ibid.
[76] *The Growth of Cybercrime and Cybercrime Prevention in Virtual Worlds (2010)*, http://www.pixelsandpolicy.com/pixels_and_policy/2010/03/cybercrime-review.html
[77] Marc Godman, *Opcit*
[78] Ibid.
[79] Ibid.
[80] 'Madison Policy Forum Report : Cyber Security Conference', Vol. 1 Issue 1, February 2010, http://www.madisonpolicyforum.org/publications/gfx/MPF%20Cyber%20Security%20Report.pdf
[81] Warren B. Chik, 'Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore', presented at the VI Computer Law World Conference, 6-8 September 2006, www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc
[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Scott J. Shackelford, 'State Responsibility for Cyber Attacks : Competing Standards for a Growing Problem', Proceedings of the NATO CCD COE Conference on Cyber Conflict held in Tallinn, Estonia July 15-18, 2010. Available at SSRN: http://ssrn.com/abstract=1535351
[86] Ibid.
[87] Ibid.
[88] 'Cybercrime Busted*', The Windsor Star*, http://www.windsorstar.com/news/Cyber+crime+busted/ 4612564/story.html
[89] 'Madison Policy Forum Report : Cyber Security Conference', *Opcit*
[90] Ibid.
[91] Ibid.
[92] Brian Harley, 'A Global Convention on Cybercrime' *The Colombia Science & Technology Law Review*, March 23, 2010, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/
[93] Ibid.
[94] Ibid.
[95] Susan W. Brenner, 2001, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law', Murdock University Electronic Journal of Law, Vol. 8 No. 2, http://www.austlii.edu.au/au/journals/MurUEJL/2001/8.html
[96] Brian Harley, *Opcit.*
[97] Ibid.
[98] 'Article 47, Convention on Cybercrime', http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm
[99] Miriam F. Weismann, 2010, *Regulating unlawful behavior in the global business environment: The functional integration of sovereignty and multilateralism*, Journal of World Business, Vol. 45(3), p.314
[100] Ibid.

[101] Joachim Vogel, *Opcit. p.4*
[102] Ibid.
[103] Ibid.
[104] Ibid. p. 5
[105] Ibid.
[106] Ibid. p. 218
[107] Ibid.
[108] Ibid. p. 219
[109] Ibid.
[110] Ibid.
[111] 'Critical Infrastructure Protection Topics', http://www.thenihs.org/cip-topics
[112] J. Nicholas Hoover, 'Cyber Threats to Critical Infrastructure Spike, *Information Week*, April 19, 2011, http://www.informationweek.com/news/government/security/229401858
[113] Ibid.
[114] Heli Tiirmaa-Klaar, 2009, 'Cyber Security Threats and Responses at Global, Nation State, Industry and Individual Levels'. Report Issue 26, Australian Strategic Policy Institute, http://www.aspi.org.au/publications/publication_details.aspx?ContentID=233
[115] Laura Spadnuta, 'Public Private Partnerships Pay Off in Cybersecurity', *Security Management,* March 18, 2011, http://www.securitymanagement.com/news/public-private-partnerships-pay-cybersecurity-008329
[116] 'Improving our Nation's Cybersecurity through the Public-Private Partnership : A White Paper' *BSA,* March 8, 2011, http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/cybersecurity_white_ paper_publicprivatepartnership.ashx
[117] Grant Gross, 'Obama's Cybersecurity Initiative Wins Praise', *PC WORLD,* May 30, 2009, http://www.pcworld.com/article/165773/obamas_cybersecurity_initiative_wins_praise.html
[118] John Kennedy, 'Organized Criminals Behind 90% of Internet Security Threats*',* *Silicon Republic*, May 7, 2010, http://www.siliconrepublic.com/strategy/item/16845-organised-criminals-behind
[119] Heli Tiirmaa-Klaar. *Opcit.*
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Ibid.
[126] Ibid.
[127] Jason Fritz, 2008, 'How China Will Use Cyber Warfare to Leapfrog In Military Competiveness', Culture Mandala, Vol. 8 No. p.28.