Essay on political science

Law, Security

Global Cultures & Security, U. S. Military perspective

Abstract

The global security in the 21st century is very different from, the threats that occurred about 20-50 years ago. There have emerged various issues that have posed threats to the global view. These aspects have shown that the effects encountered by one nation have similarly affected another nation. Globalization in some instances has emerged as the biggest threat to global security while other instances have depicted terrorism as the biggest threat. These issues are all related in that they all affect the security of nations across the world. However, these are not the only threats to national security as other issues such cyber-attacks similarly affect the security of nations. The 21st century has faced many global security threats where technology has emerged as the leading cause of these threats. There have been many advanced modes of technology based threats that are complex, offer multidimensional problems against the degree to which the United States technical superiority in stealth is likely to suffice. These technological based threats range from biological weapons, nukes, cyber-attacks, climate change and transnational crimes. As mentioned earlier, globalization and terrorism are also categorized as threats to global security. All these aspects have different impact on the security of the world. Bio-threats have posed huge challenges on the global security as they are not easy to predict and it is practically impossible to warn other nation of bio-threats as their impact and mode of transmission have rendered serious difficulties in the prediction model. Similarly, nuclear weapons are the second phase of threats to global security as their impact is massive. Over the years, nations have indulged in

building nuclear weapons that are more sophisticated and if another war emerged these highly dangerous weapons would wipe out the entire population of the targeted states. They release radioactive particles that fill the air and destroy everything.

The other challenge that has posed a huge challenge to global security and will be the main focus of this paper is cyber wars and attacks. This mode of technology has posed massive threats in that they result in loss of life and damage to the economy with effects similar to the incident on 9/11. Nations including the United States have faced huge problems in trying to thwart or curb such attacks. This paper will discuss the global security threats in the 21st century by focusing on cyber security. It will bring out the effects of cyber-attacks and how they are brought about. This will be coupled with the actions and strategies that should be taken in order to protect people from cyber-attacks. The paper will also discuss the re-set of focus to Asia and the possible reactions and responses that will be given by China.

Technology has brought about immense advancement in the way things are done all across the world. Over the years cyber threats have evolved into sophisticated attacks that offer huge threats to large enterprises, stolen credit card numbers and personal identities, empty bank accounts and probe the depths of enterprises and government networks before draining databases that contain sensitive documents to the national security or trade secrets. Initially, viruses were the most common way of getting computers infected through a malicious executable file that was attached to an email message. This attack become vague as emails would be blocked and it became easy to identify computers that had been infected with such viruses

(Bullock, 2013).

Over the years, this sophisticated malware has been advanced and it lurks silently on infected systems and hacks on to data that is collected by the personnel behind it for their own personal benefits. This has posed a huge challenge as it has become next to impossible to identify systems that have been infected. Cyber threats are now generated by criminals with intentions of stealing money, extremists who want to pass a message or make a point and nation-states engaged in espionage (Bullock, 2013). Such instances can be evidenced through the recent attack on Pakistan where Osama Bin Laden was killed, many cyber attackers have been doing all they can to access the files and information from the Navy Seal. The internet has formed a platform for cyber attackers as they rely on the latest forms of technology to plan and execute their attacks. Scams on social media are another category of cyber attackers as they steal money from innocent people and mislead them on various activities. Many people across the world have complained of being conned or threatened by unidentified people (Hathaway, 2012).

The most harmful activities that have been accredited to cyber space are cybercrime, cyber-attacks, cyber espionage, cyber terrorism and cyber warfare. They all have different ways in which they can be accomplished although at times they overlap. Cyber-crime targets computers and involves theft and damage of property as well fraudulent and espionage related activities. Cyber-attacks are mostly prevalent in the network and they are harmful for destroying and disrupting computer equipment reliability, changing the processing logic and corrupting data (Bullock, 2013).

Cyber espionage on the other hand involves use of computer systems or

information technology to illegally obtain confidential information from the government, private sector other entities. The main objectives behind cyber-attacks include loss of integrity that aims at improperly modifying information, loss of availability which renders mission critical information unavailable to authorized users and loss of confidentiality where information is disclosed to unauthorized users. Cyber terrorism involves unlawful attacks and threats against computers, network and information (Jackson, 2013). These forms of cybercrimes have led to governments taking precaution that are very expensive as technological innovations keep emerging every now and then. In this case, they have not fully managed to curb the issues of cyber-crimes and attacks. For instance, in 2007 Younes Tsouli among others was arrested after pleading guilty to inciting other people to commit an act of terrorism outside the United Kingdom. The result of the cyber terrorism act would result to the murder and they also admitted conspiring with others to defraud banks, credit card companies as well as charge card companies. This act of terrorism involved the use of websites; online forums produced and distributed online literature and videos in support of violent jihad. These convicts were closely related to the Al Qaeda group in Iraq (Andreasson, 2012).

The contents of the graphic videos they posted included instances of beheadings and a series of steps on how to make a suicide bomb vest. These instances brought a clear image of how global security is at threat. Another instance that depicts the dangers posed by cyber crimes is when Wiki leaks published and commented on leaked documents alleging government and corporate misconduct. This was an instance of cyber espionage as the

incident involved the unlawful hacking of government confidential files and publication that would draw negative attention into the United States.

Terrorists and cyber criminals are forming organization groups to conduct cyber-crimes. These attempts have given them specialized skill sets and professionalized business practices that increase the complexity of cyber-crime. This is achieved through providing individuals with all the technical abilities and the necessary tools and resources to conduct cyber-crime.

Cyber espionage affects the global security as hackers tap on to governmental information systems and acquire information that is crucial and confidential (Hathaway, 2012). They use this information to threaten the parties involved or even sell it to other parties who may use it to cause war. This breaches the security of nations as they acquire information of the confidential motives each has and hence war emerges.

The instance on Wiki leaks brought much tension to the United States as it involved confidential information about the navy’s operations and the hackers involved had released it to the public view. If this information landed in the wrong hands, disastrous events would have occurred. Most of the things we see on TV and movies have come to reality as the actions of espionage are being used by rivaling nations and organizations to acquire confidential information to each other. This has led to drastic actions that offer threats to the global security (Cavelty, 2007).

Security across the globe does not necessarily mean warfare; it can also be on the economic aspects that may affect the trade and other aspects such as food production. Cyber-crimes offer threats to the economic aspect as they destroy the market trends when hackers and cyber-criminal steal from the

organizations.

Cyber-crimes in the United States can be controlled in order to protect the people. This would involve certain measures such as: protecting their malware by using passwords that are not shared with anyone. This should involve avoided the use of common words, phrases or personal information. The systems should also be updated regularly. The operating system, browser, antivirus and other critical software should be up to date where securing updates and patches are available for free from major companies (Bullock, 2013).

of the authenticity of requests from companies or individuals by contacting them directly should be maintained as a requirement. Computer users should never provide any personal information through emails and people should independently contact the company directly to verify online requests. Much attention should be given to website URLs as malicious websites at times use variation in common spelling or a different domain to deceive unsuspecting computer users (Jackson, 2013).

Similarly, cyber security regulations that require American Businesses to secure data and computer networks should be enacted. Disclosure ion the cyber threats should be brought to the light in order for people to be aware and take precautions. The government should do more public reporting and related companies should be candid with shareholders and customers about the problems. Companies that operate critical U. S infrastructure should meet some basic standards to protect their customers, and the way of life government agencies and private industries especially the communications companies that run web infrastructures should share more information about

the threats by creating more awareness to the people (Bullock, 2013). Prosecutors should have the resources to pursue international cyber criminals as they are involved in the damage of intelligence and diplomatic and foreign law activities. Americans should be trained in the aspects of cyber security in order to keep them aware of the dangers involved. The firewall should be built in the crucial parts of the government and organizations in order to offer hindrance to the hackers who try to access the information. This should be accompanied by a system that tracks down cyber criminals using their IP addresses in order to identify where they are located (Andreasson, 2012).

The re-set of focus to Asia is a genuine initiative as countries such as China offer greatest cyber threats to the United States. Hackers from China try to penetrate United States networks and compromise national security and economic competitiveness. According to IT scholars, conducted cyber spies and hackers sponsored by the government are hired to steal American military and technological secrets in order to cause mischief in government and financial services. These actions have brought about much controversy between China and the United States.

China has in many instances attempted to acquire useful information from America to an extent where they have sent spies posing as employees to steal information or plant viruses and products imported from China are infected with malware. The re-set focus on China should be taken with much precaution as any move that would jeopardize the security of America would lead to war between the two states. This should be handled with precautions where the manufacturing and production of communication and information

technology equipment should be limited to the United States. All these aspects have been brought about by economic globalization where nations are willing to do anything in order to be ahead of the other. It has given China an opportunity to tamper with and steal technology during the manufacture of American goods that include military technology components (Cavelty, 2007).

The re-set of focus to Asia has brought about close watch in the organizations and government bodies for any form of spies. It is not a means of trying to contain China as the United States aims at protecting their confidential information. This would require limited importation of goods from China in order to protect the interests of the United States in a manner that does not jeopardize IS-Sino relations or alienate the international community. The United States should strategize and beat the Chinese at their own game by strengthening their digital security. They should come up with new and better ways of conducting espionage on the Chinese firms. These should include strategies such as submarines that would not be detected in water, tapping their communication channels and hacking into their systems using more sophisticated technology that is unpredictable to them (Bullock, 2013).

This would be a tricky game but hey as the saying goes, tit for tat is a fair game. Therefore, the United States should concentrate on using better and more advanced strategies to sneak up on China. This would to a competition between the two nations as they would improvise new ways that would be aimed at dominating on the other. It would lead to another cold war that involves dominance of the market and technology. Chinas reaction would be

that they would concentrate on building firewalls on their systems to limit the United States agencies from gaining access. Another causative reaction would be fighting back the United States which would lead to war.

References

Andreasson, K. J. (2012). Cybersecurity: Public sector threats and responses. Boca Raton, FL: CRC Press.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2013). Homeland security: The essentials. Waltham, MA: Butterworth-Heinemann.

Cavelty, Myriam Dunn. (2007). Cyber-Terror--Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. Journal of Information Technology & Politics , 4 (1), 19-36.

Hathaway, Oona A.; Crootof, Rebecca; Levitz, Philip; Nix, Haley; Nowlan, Aileen; Perdue, William; Spiegel, Julia. (2012). The Law of Cyber-Attack. California Law Review, 100 (4), 817-885.

Jackson, R. J. (2013). Global politics in the 21st century. Cambridge: Cambridge University Press.