DISEC

Topic A: Defining Cyberterrorism and Permissible Responses

Topic B: Drug Cartel in Mexico

Township of Langley Model UN 2012

DISEC

Table of Contents

Welcome from Dias

History of DISEC

The United Nations General Assembly, including six main committees, is composed of 30 committees. Disarmament and International Security Council (DISEC), the first committee of the General Assembly, is concerned with disarmament and related international security questions. DISEC has been working "*to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources*" (Article 26 of United Nations Charter). DISEC has been dealing with a variety of issues including illegal weapon trade and non-proliferation of biological weapons. Although DISEC is *unauthorized* to impose sanctions, pass binding resolutions, or to command armed intervention, DISEC has been reporting to the United Nations Security Council and the UN Secretariat, suggesting the solutions of the issues and assisting the production of conventions and treaties; for instance, Non-Proliferation Treaty (1968) and the Chemical Weapons Convention (1992) are significant documents that show DISEC's critical role in the General Assembly.

All member states and observers of the United Nations are members of the committee of the General Assembly; all members have an equal vote, and majority must vote for the documents in order to be passed.

Topic A: Defining Cyberterrorism and Permissible Responses

Introduction

"Terrorism" is defined as "the use of violent action in order to achieve political aims or to force a government to act" (Oxford). Although the definition of "terrorism" is well studied, it is rather difficult to define cyber terrorism; the concept of cyber terrorism is not only abstract, but is also inconstant as the tactics and technology used in cyber terrorism develop and change over time.

According to Denning's Testimony, Cyber terrorism "is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. [Furthermore], to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not" (Denning, 2000).

There are varieties of different forms of cyber terrorism: (a) privacy violation, (b) data theft, (c) destruction of e-governance base, (d) distributed denial of services attack, and (e) network damage and disruptions.

The cracker community is generally known to be based in the Middle East, the United States, Asia, Europe, and in the nations of the former Soviet Union. Nevertheless, as the attack is anonymous, it is difficult to identify the hacker or the attacker.

As it is described above, it is significant to have the "scale" of the cyber terrorism. It not only assists to have a clear definition of cyber warfare, but also helps to determine appropriate responses against it.

History

Intensifying the anxiety and uncertainty about the millennium bug, public interest in cyber terrorism began in the late 1980s. Millenium bug, however, was learned to be irrelevant to a terrorist attack or plot against the world. The potential threats of cyber terrorism in the United States increased after the United State's declaration of War on Terror that was resulted by the terrorist attacks on September 11, 2001. The media discussed about the possibility of a large attack on computer networks and significant infrastructures, which may cause economical depression and disruption to national affair. Furthermore, after a Chinese fighter collided with an American surveillance plane in April of 2001, Chinese hacker groups cyber- attacked American targets, causing millions of dollars in damage. Moreover, there were cyber attacks during the 2008 South Ossetia War; on 5 August 2008, three days before Georgia launched its invasion of South Ossetia, the websites for OSInform News Agency and OSRadio were hacked, involving denials of service. In July 2009, United States and South Korea were attacked by unidentified hackers; institutions such as the department of Transportation, State and Treasury, the White House, and the New York Stock Exchange were targeted. Recently, "India was [condemned] for hacking a U.S. commission's e-mail communications, which contained sensitive information regarding to the economic and security relations of the United States and China". Despite the efforts to prevent cyber terrorism, cyber terrorism is constantly occurring, causing economical, social, and physical damages. Further, it is unsure how accurate claims of cyber warfare are; not only the attackers are anonymous but it can also create conflicts in international relationship and public unrest.

Impacts

Germany, as a response to increasing cyber attacks, established a Cyber Defense Center (CDC) in June 2011; however, CDC became a target of a group of hackers a few weeks later and information from a criminal-tracking program was stolen. Despite the efforts to prevent cyber terrorism, attacks against the Internet are increasing at an annual rate above 60%. According to the computer professionals, it is important for the government and people to understand the concept of cyber terrorism and its effects to prevent potential cyber attacks. Several effective measures against cyber terrorism include "firewalls, antivirus software and complex password systems". "Censoring sensitive information to select personnel, establishing added security barriers to prevent the theft of IT equipment, using more advanced systems to prevent unauthorized reading of visual, acoustic, or analog signals" are also effective measures to prevent cyber terrorism. Government organizations, financial organizations and other significant information units are enhancing their network safety by taking appropriate measures.

DISEC's Job?

It is significant to determine the definition of cyber terrorism to prevent confusion; determining the "scale" of the cyber terrorism may be helpful for the government and United Nations to make a permissible response to prevent further cyber terrorism. DISEC is also to suggest effective responses and measures that prevent serious cyber attacks.

Questions to Think About

1. Which countries are currently involved in cyberterrorism? What is my country's position on the issue?
2. How should cyberterrorism be classified?
3. When should a cyber attack be considered a threat to a nation?
4. What measures should be taken to prevent cyberterrorism?

Topic B: Drug Cartel in Mexico

Introduction

The Mexican drug war has been an ongoing conflict amongst drug cartel rivalries combating for conquering regions and the Mexican government forces to halt their spread. Drug Trafficking organizations have existed since the 1990s as illegal drug routes that allowed flows of marijuana, cocaine, heroin, etc. into Mexico from bordering nations of South America and the Caribbean regions. The official date the war broke was on December 11, 2006 when the Mexican government decided to initiate Operation Michoacan and involve military enforcements.

Presidencies of Mexico have experienced the drug chaos over the past few years but none effectively handled the issue of undiscovered drug routes. The impact of this drug war varies significantly. Fore mostly, drug itself is considered as an addictive as well as lethal when abused. This has direct link to the problem that the drug war in Mexico is ultimately leading to an increase of drug usages and drug transportation world-wide.

Following the smuggling of drugs worldwide, such as to nations of Europe, Guatemala, West Africa, Canada, and primarily United States, the drug smuggling can't be kept inside Mexico to be fought solely on Mexican soil by the Meixcan government but has to be stressed on other nations that the drug smugglings are being spread to.

Other types of issues easily ignite from drug cartels in fight with the Mexican government and those issues are heavily dependent on the usages of firearms. The possessions of firearms naturally lead to heavy casualties both on the sides of the government and the citizens (including drug smugglers), further affecting death tolls of Mexico, global image and reputation, and fall in tourism revenues. As illegal drug cartels in Mexico are devastating Mexico and putting Mexico closer to the title of 'land of doom,' DISEC's responsibility to keep the nation of Mexico under seize of firearms, illegal drug smugglings and drug abusers is urgent.

The most affected country by the Mexican chaos has to be the United States, since the Mexican-American border is at a fragile state of being passed through with drugs any time anywhere. Thus, to stop the spread of the profits the drug smugglers get in Mexico from North America, the United States has the full obligation to enact newer funding or bill plans to strengthen the border.

As the United States continues to work on reinforcement of the border, DISEC's job is to call upon spread the alert state of Mexico worldwide and come together to send UN troops as peacekeepers to keep civilians safe, seize all live drug routes, retrieve a plan from the past that Mexico has failed with attempting to locate all possible drug smuggling sites and renew it, and effectively join forces with the Mexican government for further guidance.

Other solutions are possible whereas countries that supply drugs to Mexico investigate their own lands for drug smuggling and cut off routes that are all leading to Mexico from abroad that contains any type of drug-related plantations or corporations.

Impacts

"*Drug trafficking is a [profitable] activity for the Mexican cartels, generating estimated annual revenues of US$35 billion to US$45 billion for Mexico, with a profit margin of approximately 80%. For this reason, many cartels are [combating] for the profits involved in producing and distributing drugs. Currently, seven powerful drug-trafficking organizations occupy different regions of Mexico…*" (Drug Trafficking, Violence and Mexico's Economic Future).

During this process, violence related to Mexican drug trade has been increased. For instance, "[according to the news], …in July 2010, drug criminals used a car bomb for the first time in the history of Mexico's drug war and killed four people in Ciudad Juárez. In August, the bodies of 72 migrants were found in northern Mexico. They had been shot after refusing to work for a drug gang. [In addition], a prosecutor and police officer investigating the crime [became missing]" (Drug Trafficking, Violence and Mexico's Economic Future).

Impacts

The previous administrations, until Calderón was elected in 2006, did not respond to the drug trade aggressively, whereas Calderón launched a total power, claiming that Mexican drug cartels are serious threats to the country's security.

"*Calderón deployed national troops to destroy crops, collect intelligence, interrogate suspects, and confiscate contraband. He has also initiated a variety of public security and judicial reforms. [Furthermore], Plataforma Mexico, which aims to create real-time interconnectivity within Mexico's police force by developing a national crime database to facilitate tracking drug criminals, is known as a recent effort that is related to information management*"(Drug Trafficking, Violence and Mexico's Economic Future).

Operation Michoacan

"*[Initiated on December 11, 2006, to eliminate drug plantations and to combat drug trafficking], Operation Michoacán is a joint operation by Federal, Police, and The Mexican Military, under the supervision of The Secretary of Public Safety, Attorney General of Mexico (PGR), Secretary of the Interior, Mexican Navy, and Mexican Army. In some occasions, state and municipal police have participated despite not being part of it. The joint operation has distinguished itself as one of the operations against drug trafficking, which has employed the largest number of military and police elements, as well as most state forces.*"

In May, 2007, Soldiers engaged drug traffickers, killing 4 cartel gunmen. Still ongoing, the casualties and losses during Operation Michoacán are great in number; 50 soldiers, 100 police officers were killed while 500 cartels are killed.

References

Topic A

Collin, Barry C. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge." 31 August 2012 <http://afgen.com/terrorism1.html>.

Gordon, Sarah. "Cyberterrorism?" 2003. 31 August 2012 <https://www.symantec.com/avcenter/reference/cyberterrorism.pdf>.

Cyber Crime Revealed. Cyber terrorism history and timeline. 16 August 2010. 31 August 2012 <http://www.cyberwarzone.com/cyberwarfare/forums/cyber-terrorism-history-and-timeline>.

Cyber Crime Revealed. Cyberattacks during the 2008 South Ossetia War. 17 May 2010. 31 August 2012 <http://www.cyberwarzone.com/content/cyberattacks-during-2008-south-ossetia-war>.

Malone, Michael S. Cyber-Terrorism and How We Should Respond. 10 July 2009. 31 August 2012 <http://abcnews.go.com/Business/Technology/story?id=8045546&page=1>.

Wikipedia. Cyberterrorism. 27 August 2012. 31 August 2012 <http://en.wikipedia.org/wiki/Cyberterrorism>.

Canadian Future Model United Nations. NATO Backgrounders. 2012.

Coleman, Kevin. "Computer Crime Reserach Center." 2009. Cyber Terrorism. 31 August 2012 <http://www.crime-research.org/library/Cyberterrorism.html>.

Acharya, Subhojyoti. "Articlesbase." 12 February 2008. Cyber Terrorism- the Dark Side of the Web World. 31 August 2012 <http://www.articlesbase.com/law-articles/cyber-terrorism-the-dark-side-of-the-web-world-331261.html>.

Topic B

"Analysis: Mexico's Drug Wars Continue." *BBC News*. BBC, 03 Dec. 2002. Web. 02 Sept. 2012. <http://news.bbc.co.uk/2/hi/americas/1867842.stm>.

"INSI News." *INSI: International News Safety Institute*. N.p., n.d. Web. 02 Sept. 2012. <http://www.newssafety.org/index.php?option=com_content>.

"High U.S. Cocaine Cost Shows Drug War Working: Mexico." *Reuters*. Reueters, 03 Dec. 2002. Web. 02 Sept. 2012. <http://www.reuters.com/article/2007/09/14/us-mexico-drugs-idUSN1422771920070914>.

"US Plans to Combat Mexico Drugs." *BBC News*. BBC, 13 Mar. 2009. Web. 02 Sept. 2012. <http://news.bbc.co.uk/2/hi/americas/7941043.stm>.

Borderland Beat Reporter Buggs. (2010 йил 14-July). *Operation Michoacan*. Retrieved 2012 йил 9-September from Borderland Beat: http://www.borderlandbeat.com/2010/07/operation-michoacan.html

Duff, D., & Rygler, J. (2011 йил 26-January). *Drug Trafficking, Violence and Mexico's Economic Future.* Retrieved 2012 йил 9-September from The Knowledge Behind the News: http://knowledge.wharton.upenn.edu/article.cfm?articleid=2695