SDIMUN

Model United Nations at University of California, San Diego presents
On Saturday April 4, 2014

Disarmament and International Security (DISEC)

San Diego Intercollegiate MUN

Cyber Security and Combatting Cyber Terrorism

I. Background

Cyber Security is the protection of computers, smartphones and networks intended to prevent the attainment of unauthorized access, tampering, or destruction of computer systems and information within those systems. As more nations continue to adopt platforms relying on integrated networks that oftentimes cross national boundaries, cyber warfare and terrorism has come to the top of the international agenda. Cyber warfare is defined as the politically motivated use of computers and information technology to cause severe disruption, sabotage, or espionage[1]. This could include sending viruses that harm or delete information, or the hacking of systems to obtain confidential information (private conversations, financial information) and to use this information as a weapon against one's opponent to influence decision making. While cyber security breaches oftentimes require high technical expertise to launch debilitating cyber-attacks, the ability for hackers to gain access to a system and obtain classified information can be devastating to nations or other parties affected by the attack.

Cyber warfare can be analogous to war depending on the perspective of the actors involved and oftentimes does not preclude physical fighting between two states. A common reason for any type of warfare is to wear down the government in order to achieve better negotiating leverage when an issue is being discussed by opposing parties. Cyber terrorism is more convenient because it does not cost much

[1] "Definition of Cyberterrorism in English:." *Cyberterrorism: Definition of Cyberterrorism in Oxford Dictionary (American English) (US)*. N.p., n.d. Web. 18 May 2014.

and does not cause any losses to those initiating the attacks. On the other hand, a physical attack will undoubtedly lead to the loss of lives to those attacking too. Cyber warfare puts a lot at stake without the perpetrator having to risk anything. The ability to infiltrate a government website, for instance, could reveal classified information about the interworking of a whole nation. Cyber warfare is much more passive than physical warfare and it is a method that makes it difficult to identify the source if done correctly. In addition, it is highly useful for governments to utilize because it can be blamed on independent actors as opposed to the government itself, which may shift full blame away from a government's leaders who may publically condone the use of cyber warfare.

Cyber terrorism is a particularly important issue because humanity is rapidly becoming more dependent upon computers and information systems. If cyber security and cooperation between nations does not occur, larger windows of opportunity may open as advancements in technology continue with lots of exploits for hackers to take advantage of. This is a large-scale issue that threatens national securities. A cyber threat could include threatening to attack databases and destroy them in the event that the government does not take a specific course of action in a social or political issue.[2] The loss of such information could have grave consequences that could very well include an economic collapse or the loss of vital communication. Therefore, it is essential that we not only hinder the possibility of cyber attacks, but also strengthen the technological infrastructure that can be threatened at any point.

Cyber-attacks were first seen in 1982 during the Cold War when the United States Central Intelligence Agency used a code that caused a Siberian gas pipeline in

---

[2] "The Threat of Cyberterrorism to Critical Infrastructure." *EInternational Relations*. N.p., n.d. Web. 20 May 2014.

Russia to explode.[3] The explosion was said to have been so devastating that it could be seen from space. In 1991, unknown forces were able to infiltrate the computer system of the Iraqi Republican Guard (IRG) and were able to redefine the target of Scud missiles, which are Russian missiles developed during the Cold War. Clearly, possessing the ability to do this can result in immeasurable losses to economies and governments alike.[4] Another famous incident occurred in 2004 when government-supported cells in Russia infiltrated many networks and databases including some of NASA. This, many believe, has paved the path for espionage entities to infiltrate other systems as well. Additionally, Estonia witnessed a major cyber war in 2007. It was started by the Nashi, "a pro-Kremlin group from Transnistria"[5]. Essentially, the techniques being used against the Estonian government included botnets and ping floods. These are two well-known forms of cyber warfare. Botnets entail the use of malicious warfare to infect computers while ping floods is overwhelming an individual with ping messages to make him unable to respond to the messages. These two techniques were used to infiltrate the government websites and shut them down.

There are only a few organizations that truly focus on cyber terrorism as a tool for their purposes. The Liberation Tigers of Tamil Eelam (Tamil Tigers) in Sri Lanka managed to paralyze the functioning of Sri Lankan government websites.[6] Though there were not many losses from this incident, the very fact that this occurred presents

---

[3] Balkhi, Syed. "25 Biggest Cyber Attacks In History." *List25*. N.p., n.d. 06 May 2013. Web. 21 May 2014.

[4] Tafoya, William L. "Cyber Terror." *FBI Law Enforcement Bulletin*. Federal Bureau of Investigation, Nov. 2011. Web. 17 June 2014.

[5] Balkhi, Syed. "25 Biggest Cyber Attacks In History." *List25*. N.p., n.d. 06 May 2013. Web. 21 May 2014.

[6] "The Threat of Cyberterrorism to Critical Infrastructure." *EInternational Relations*. N.p., n.d. Web. 20 May 2014.

the possibility of advancements in knowledge of that area and even graver threats in the future. A well-known organization that has used cyber attack as a threat against the United States is Al-Qaeda. They called upon cyber attacks against "US networks including critical infrastructure such as the power grid and water supplies"[7]. Denial-of-service (DoS) attacks are a well-known method of computer hacking. They are useful in the sense that they disable the user from using the device. Tools needed to launch a DoS attack can include a botnet. There are specialist programmers who write entire systems and sell them for hefty prices because they are highly undetectable. Programmers who design these systems create programs that can take remotely take control of computers or systems, called "Zombies", which may flood a targeted system and cause a malfunction, allowing further access into the system. However, typically, the tools needed depend on the scale of the attack. Some DoS attacks only require a single computer. For others targeting a multinational corporation like Chase, it could take entire server rooms to take down the services. In other instances, the server rooms are outsourced to tens if not hundreds or thousands of (knowing or unknowing) users participating in the attack.

DoS attacks have recently been used against famous American banks such as JPMorgan Chase and the Bank of America. Another was recently launched against Sony Pictures which gave the intruders access to intimate information about the corporation that was used to threaten the company to prevent the release of the film "The Interview". This was done through pressuring the networks with a high intensity of trafficking until they were not able to bear the pressure, so they immediately shut down. This could lead to the loss of revenues, being forced to pay a

---

[7] "The Threat of Cyberterrorism to Critical Infrastructure." *EInternational Relations*. N.p., n.d. Web. 20 May 2014.

ransom to the hackers, and damage the reputation of this business. It should be noted, however, that cyber attacks pose a threat to physical assets because technology is increasingly in control of our different possessions. For example, money in bank accounts is being reported through numbers which can be altered by a hacker. Therefore, one should not only consider cyber terrorism in terms of the loss or theft of information. If cyber terrorism is not controlled, its potential for harm could increase exponentially.

In response to those threats, some countries have created Computer Emergency Response Teams (CERTs) to deal with individual incidents of cyber terrorism. The United States and the United Kingdom have adopted policies to deal with any threats of that kind and have therefore set an example for other nations.[8] The term "military deterrence" describes the proactive actions that are being taken against cyber terrorism.

It is important to remember that if a single person carries out an attack on a nation from another country, bringing that person to justice may be incredibly difficult. This is because few international laws exist that can allow a government to extradite a citizen of another country and bring them to justice in their own. Governments may be unwilling to allow extradition because it sets an incredibly dangerous precedent, but then it may seem like the government is defending the actions of that citizen which also causes a diplomatic incident. These are all aspects of the issue that should be considered.

---

[8]Dogrul, Murat, Adil Aslan, and Eyyup Celik. "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism." *Page. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism* (2011): n. pag.*International Conference on Cyber Conflict*. Web. 20 May 2014.

II. United Nations Involvement

The United Nations has taken multiple steps to diminish the possibility of losses due to cyber terrorism. The United Nations helped support an alliance called the International Multilateral Partnership Against Cyber Threats (IMPACT), which aims to decrease the chances of cyber threats becoming cyber attacks.[9] IMPACT is a global platform with its headquarters in Malaysia. This organization specializes in ensuring the safety of International Telecommunication Unions (ITUs) by providing resources, knowledge, and facilities to provide the needed protection. Additionally, in October 2012, the United Nations Office on Drugs and Crime (UNODC) released a 148-page report offering guidance to the nations that face cyber terrorism in many of its forms, including the promotion of extremist ideas or the dissemination of certain propaganda to further terroristic purposes and cause disorder[10]. This report provided information on ways in which terrorists use the Internet as a tool to accomplish their goals and promoted the idea of international cooperation to fight this form of terrorism. An issue that is also addressed in this report is how to find and apprehend terrorists online while also respecting human rights. One individual's freedom of self expression must be maintained in the event that it does not promote terroristic ideas that threaten the safety of civilians.

The United Nations' Security Council has also taken an active stance on this matter. Resolution 1556 that has passed addresses terrorism in all its forms and calls upon international cooperation with the Counter-Terrorism Committee (CTC) that had

---

[9] "Committed to Connecting the World." *Drill to Tighten Global Network in Fight against Cyber Attacks*. N.p., 20 May 2014. Web. 20 June 2014.

[10] Feher, Annamaria, and Elizabeth Towell. "The Use of the Internet for Terrorist Purposes". UNODP. *Internet Search* 7.3 (1993): 195-200. Web. 18 June 2014.

been established in 2001 in resolution 1373[11]. In Resolution 1556, the idea of establishing an international fund system to compensate those who have suffered losses is presented as a possibility[12].

III. Bloc Positions

Cyber security is an issue that we usually see confronted through a collective effort by groups of nations rather than individual countries and is therefore not necessarily restricted by geographic boundaries as with other issues. Consequently, the bloc positions represent the actions of organizations within which multiple nations act. Following that, broad regional stances on this issue are explained.

NATO Members

The North Atlantic Treaty Organization (NATO) has recognized the threat that cyber warfare generally imposes and "aims to combine the cyber-deterrence abilities under centralized defense system"[13]. It continues to work on improving its abilities to detect and prevent any possible cyber attacks. Some members of NATO form an organization called the Cooperative Cyber Defense Center of Excellence

---

[11] Cordesman, Anthony H. "The Role of the United Nations in Fighting Terrorism." *To Comment: Acordesman@aol.com The Role of the United Nations in Fighting Terrorism* (n.d.): n. pag. *CSIS*. Center for Strategic and International Studies. Web. 18 June 2014.

[12] "United Nations Security Council Resolution 1566." *U.S. Department of State*. U.S. Department of State, 08 Oct. 2004. Web. 20 June 2014.

[13] Dogrul, Murat, Adil Aslan, and Eyyup Celik. "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism." *Page. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism* (2011): n. pag.*International Conference on Cyber Conflict*. Web. 20 May 2014.

(NATO CCD COE) published the Tallinn Manual, which provides information on how to implement a nation's laws on cyber terrorism[14].

Commonwealth Nations

The Commonwealth Nations have adopted the Commonwealth Model Law on Computer and Computer Related Crime via the recommendations of the Council of Europe Convention on Cybercrime. This law aims to harmonize the existing differences in legislation between the different Commonwealth nations in order to facilitate cooperation and standardize actions against cybercrime.

International Telecommunication Union

This is a United Nations agency that has created the Toolkit for Cybercrime Legislation in 2010 which aims to push forth the concept of harmonizing national cybercrime legislation[15]. This law mainly revolves around the use of the Internet and was written based on an analysis of the Council of European Convention on Cybercrime, but also the cyber security policies of developed nations.

Permanent Security Council Members

These nations exceedingly depend on information systems and cyber terrorism therefore poses an even greater threat to them than most other nations, which is not to undermine the impact this could have on every nation. Barack Obama, the US President, and Vladimir Putin, the Russian President, met to establish plans for

---

[14] Pototsky, Dan. "US, Russia, China Meet to Tackle Cyberterrorism | Russia Beyond The Headlines." *Russia Beyond the Headlines*. N.p., 07 June 2013. Web. 20 June 2014.

[15] "Cybersecurity Gateway." *ITU*. N.p., n.d. Web. 18 June 2014.

collaboration on this issue[16] At another meeting, Xi Jinping, the General Secretary of China, joined Obama to discuss similar plans[17]. As for France, around 2010, files called G20 on the subject of economic affairs had their information redirected to Chinese sources[18] and are therefore working to establish better cyber security to avoid such incidents from recurring. The United Kingdom has already adopted policies on this matter.

There are multiple perspectives from which one can view this issue. For instance, one could claim that the United States is a cyber-terrorist for its utilization of the National Security Agency's capabilities to obtain information about top-level officials in other countries and tracking the movements of their citizens. From the inside, the US government may not view it as such, but the rest of the world may consider it so. China is similar in that it uses hackers to steal valuable patent information from other countries to improve its own economy. Yet both of these countries stand against cyber terrorism in some form. It is therefore important to identify any hypocrisy one discovers.

---

[16] Corrin, Amber. "Obama, Putin Join Hands against Cyber Threats, Nuclear Risk Reduction Center – FCW." N.p., 19 June 2013. Web. 20 June 2014.

[17] Pototsky, Dan. "US, Russia, China Meet to Tackle Cyberterrorism | Russia Beyond The Headlines." *Russia Beyond the Headlines*. N.p., 07 June 2013. Web. 20 June 2014.

[18] "Cyber Attack on France Targeted Paris G20 Files." *BBC News*. BBC, 07 March 2011. Web. 18 June 2014.

Regional Positions

Asian Bloc

Many nations in the Asian bloc continue to advance their technology, especially countries like Japan. Therefore, it is in their best interest to ensure there is no cyber terrorism that harms their products. Japan is already working with the US to protect energy systems. These nations could work on finding ways to develop technology only available to governments that can detect any cyber threats.

Western Bloc

The Western Bloc is extremely dependent on information systems with their thriving economies. Therefore, cyber terrorism is a major threat to them. However, one must also acknowledge the fact that their possession of technology can allow those with the wrong motives to become cyber terrorists.

African/Middle Eastern Bloc

These blocs are not as highly dependent on technology as the other regions. However, there are some scattered and probably independent cyber terrorists here. For instance, a cyber attack was launched by an unknown group, in which 20,000 Israelis' credit card information of was posted online[19]. Also, some claim that Iran is behind some cyber attacks that have occurred on US banks' websites.

Latin American Bloc

[19] Kain, Erik. "Cyber Attacks Take Down Two Israeli Websites - Is Cyber Warfare The Next Front In The Middle East Conflict?" Forbes Magazine, 16 Jan. 2012. Web. 27 June 2014.

In Latin America, anonymous groups have attacked countries like Chile and Venezuela, through the Internet. This bloc should focus on the aspect of identifying cyber terrorism, developing their cyber security, and acting against any threats they face without delay due to the damage one problem can cause in a minimal amount of time.

Important Note

Generally, most, if not all, nations wish to combat cyber terrorism due to its debilitating effects on not only government functionality, but also civilians' safety. However, it is essential that each delegate discuss incidents of cyber terrorism in their country, the actions their country has taken to combat cyber terrorism, and their country's current situation in regards to cyber terrorism. Each unique perspective is indispensable to the formulation of a comprehensive set of policies to confront cyber-based acts of terror.

More importantly, it is necessary that delegates address any double standards in the policies of a nation that seems to uphold respectable ideals against cyber terrorism yet uses it for its purposes without being transparent. In a book called "Cyberterrorism: The Use of the Internet for Terrorist Purposes", the line between a government acting to fight cyber terrorism and another that merely infringes upon their citizens' rights to acquire information for their own purposes is defined. The distinction is described in the following words:

"[Societies] should also abstain from ineffective control methods of symbolic nature, especially if these methods infringe information rights, contribute to the development of uncontrollable surveillance systems, and create high costs for the Internet industry. Thus, it is essential to investigate the possibilities, the dangers, and

the limits of international efforts to prevent illegal content on the Internet and in other electronic information systems." [20](76)

On the base level, every country would like to see legislation that begins to stop cyber terrorism as a defensive measure. However, a good amount of countries are comfortable utilizing cyber warfare as an offensive capability. The difference between what constitutes cyber terrorism and cyber warfare is the group using it and the motive for which it is used.

IV. Questions to Consider

1. What definition should be adopted for the term "cyber terrorism"?
2. What effective measures can be taken to combat cyber terrorism?
3. How do we implement such proposed measures?
4. How can we promote international collaboration with regards to this problem?
5. In retrospect, what policies have proven to be successful and how can they be extended to a wider scale?
6. Why would some countries be opposed to cyber terrorism laws?
7. How can we ensure all nations' transparency regarding cyber security?

[20] "Cyberterrorism - The Use of the Internet for Terrorist Purposes." *Google Books*. Council of Europe, n.d. Web. 27 June 2014.

V. Suggested Sites

1. United Nations Security Council Resolution 1556:
   http://www.state.gov/j/ct/rls/other/un/66959.htm
2. A brief critique and a different perspective on the usefulness of the released UN report:
   http://www.computerworld.com/s/article/9232844/UN_More_international_cooperation_needed_to_fight_cyberterrorism
3. Extensive overview of cyber terrorism and how it impacts the physical world:
   http://www.sans.org/reading-room/whitepapers/country/sensitive-unclassified-information-threat-physical-security-1221
4. UN Role in Fighting Terrorism (General):
   http://csis.org/files/media/csis/pubs/roleofun.pdf
5. US Institute of Peace (USIP) Report on Cyber terrorism:
   http://www.usip.org/sites/default/files/sr119.pdf
6. UNODC Report on Cyber terrorism, its impacts, and specific countries' actions:
   http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

VI. Bibliography

Balkhi, Syed. "25 Biggest Cyber Attacks In History." *List25*. N.p., n.d. 06 May 2013. Web. 21 May 2014.

"Committed to Connecting the World." *Drill to Tighten Global Network in Fight against Cyber Attacks*. N.p., 20 May 2014. Web. 20 June 2014.

Cordesman, Anthony H. "The Role of the United Nations in Fighting Terrorism." *To Comment: Acordesman@aol.com The Role of the United Nations in Fighting Terrorism* (n.d.): n. pag. *CSIS*. Center for Strategic and International Studies. Web. 18 June 2014.

Corrin, Amber. “Obama, Putin Join Hands against Cyber Threats, Nuclear Risk Reduction Center – FCW.” N.p., 19 June 2013. Web. 20 June 2014.

“Cyber Attack on France Targeted Paris G20 Files.” *BBC News*. BBC, 07 March 2011. Web. 18 June 2014.

“Cybersecurity Gateway.” *ITU*. N.p., n.d. Web. 18 June 2014.

"Cyberterrorism - The Use of the Internet for Terrorist Purposes." *Google Books*. Council of Europe, n.d. Web. 27 June 2014.

"Definition of Cyberterrorism in English:." *Cyberterrorism: Definition of Cyberterrorism in Oxford Dictionary (American English) (US)*. N.p., n.d. Web. 18 May 2014.

Dogrul, Murat, Adil Aslan, and Eyyup Celik. "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism." *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism* (2011): n. pag.*International Conference on Cyber Conflict*. Web. 20 May 2014.

Feher, Annamaria, and Elizabeth Towell. “The Use of the Internet for Terrorist Purposes”. UNODP. *Internet Search* 7.3 (1993): 195-200. Web. 18 June 2014.

Kain, Erik. "Cyber Attacks Take Down Two Israeli Websites - Is Cyber Warfare The Next Front In The Middle East Conflict?" Forbes Magazine, 16 Jan. 2012. Web. 27 June 2014.

Pototsky, Dan. "US, Russia, China Meet to Tackle Cyberterrorism | Russia Beyond The Headlines." *Russia Beyond the Headlines*. N.p., 07 June 2013. Web. 20 June 2014.

Tafoya, William L. "Cyber Terror." *FBI Law Enforcement Bulletin*. Federal Bureau of Investigation, Nov. 2011. Web. 17 June 2014.

"The Threat of Cyberterrorism to Critical Infrastructure." *EInternational Relations*. N.p., n.d. Web. 20 May 2014.

"United Nations Security Council Resolution 1566." *U.S. Department of State*. U.S. Department of State, 08 Oct. 2004. Web. 17 June 2014.