Topic 1: Cyber Warfare

Background:

Cyber Warfare is defined as the use of computers and information technology to cause severe disruptions among governments and corporations. Now that technology is exponentially progressing, hackers are finding newer and more creative ways to break into a system. The Pentagon System that contained sensitive information was accessed illegally 250,000 times, however only 150 of those break-ins were detected. This poses a huge threat to not only countries because hackers can disrupt energy grids and government websites, but to large corporations as well. Many countries are in a cyber warfare with one another because they feel the need to disrupt the government, or society. There are three main types of cyber warfare: between large corporations, among governments, and between governments and corporations.

Cyber attacks among corporations can happen quite frequently. Hackers in 2015 breached Anthem Incorporated, a healthcare provider, and exposed over 70 Million personal records. The hackers exposed birthdays, mailing addresses, email addresses, and even social security numbers. This is a huge threat to the people using the health plans because their identities have the potential to be compromised since their social security numbers were exposed. The CEO’s personal information was exposed as well. Another high profile attack was on an adultery website called Ashley Madison exposing over 37 million users information. The group that hacked into the website, called Impact Team, wanted the site to be taken down, however a month later when the site did not listen, all information was exposed. Names, corporate emails, and
physical addresses were exposed, leaving many people in trouble with their identities including politicians.

Cyber attacks occurring in governments is getting to be more popular as more people are getting access to networks and have more cohesively developed software to hack into the system. A cyber attack that happens in state governments is a huge threat to security because it has the potential to disrupt the daily flow of life. For example, in December 2015 Ukraine’s region of Ivano-Frankivsk had a huge power outage that resulted for several hours. Though many of Ukrainian officials point the finger to Russia, the hacker that affected 80,000 customers is still unknown. This raised the red flag for many countries, as many electrical grids are extremely susceptible to hackers. Malware, a type of intrusive software, was able to compromise controls of the electrical grid. As Malware development progresses, the world should expect to see more deliberate attacks conducted by private hackers, or countries. Many hackers are looking to perpetrate attacks on a country’s critical infrastructure, which has a direct threat to society. For example, Cyber attackers were able to hack into a Turkish pipeline, causing the most secure pipeline in the world to explode into 150-foot flames. This ultimately affected networks around the area, and caused physical damage as well. Not only cyber terrorists can expose identities of people, however they can do much more physical damage to a society as well.

Cyber warfare between state governments and corporations occur as well. In 2014, North Korea attacked Sony Pictures by exposing personal information in response to the satirical movie “The Interview”. Studio executives and movie stars’ personal lives were exposed due to the satirical movie produced by Sony. The United States imposed sanctions upon North Korea in response to the cyber attack.
Many cyber attacks can be detrimental to an individual by exposing personal information, or can greatly harm a society through power and electrical grid blackouts. In 2014, 47% of American adults had their personal information stolen by hackers through a data breach from a corporation or large company. Many attacks are done through a “denial of service” chain, which makes attacks become nearly untraceable.

**UN Involvement:**

Considering that there is a lack of agreement among countries regarding cyber-warfare and cyber-terrorism policies, the UN is continually attempting to get countries to agree on multiple frameworks in order to stop disruption. The United Nations established the Counter-Terrorism Implementation Task Force in 2005 to stop all types of terrorism, including cyber attacks. In A/RES/60/288 of Section II, paragraph 18, the resolution states that it wants “to step up all efforts to improve security and protection of particularly vulnerable targets, such as infrastructure and public places… while recognizing that States may require assistance to this effect.” Though this resolution mainly focuses on the Global Counter-Terrorism Strategy, it does have many phrases and statements that focus on cyber terrorism as well.

In 2003, the General Assembly passed Resolution 57/239 that created a global culture of cybersecurity. The resolution recognizes that more information systems are getting exposed to a greater number of threats. This resolution initiates cooperation among member states to work together to create a framework for a global cybersecurity. Through this cybersecurity, there are nine parts: Awareness, Responsibility, Response, Ethics, Democracy, Risk assessment, Security design, Security management, and Reassessment.
One year later, the General Assembly passed Resolution 58/199, which strives to protect Critical Information Infrastructures. Most hackers are looking to disrupt a nation’s way of life, if they are attempting to breach into a state government; the United Nations created this resolution for that specific reason. This resolution is a platform for countries to discuss how their own cybersecurity strategies worked in the past, and how they can improve upon it as well. The resolution additionally calls for countries to share their cybersecurity strategies to their fellow member states in order to ensure a more balanced international community regarding cyber warfare.

The African Center for Cyber Law and Cybercrime Prevention is an organization that studies the internet’s development and dynamics. Additionally, it assesses the lack of laws and places sanctions upon countries that perpetrate cyber attacks. Founded in 2009, the organization is a research center to explore cyberspace and work with other NGO’s and governmental bodies. The International Multilateral Partnership Against Cyber Threats (IMPACT) is another platform that is against cyberterrorism. It was established in 2008 through the World Cyber Security Summit, and stands to protect and aid governments in dealing with cyber attacks on morale, or critical infrastructure.

Questions to Consider:

1. Have there been any cyber attacks in your country in the last decade?
2. What is your country’s stance on cyber warfare and cyber terrorism and how are they dealing with it? Are there any systems that are put into place to combat this issues?
3. What resolutions or agreements have your country taken part of?
4. What kind of solutions can you bring to the table that complement the majority of member states’ policies?

5. How should cyber attacks be prevented?

6. What is an acceptable response to an act of cyber warfare?

7. How can the perpetrators of cyber attacks be identified, as there is often no way to tell whether attacks are government-sponsored or independent?

Works Cited:


<http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of%20Attacks.xhtml>.
Topic 2: Peacekeeping Reform

Background:

UN Peacekeeping began in 1948 to mediate ceasefires where political unrest was occurring and to facilitate peace when there is civilian discontent with the government. The first peacekeeping mission was the UN Truce Supervision Organization (UNTSO) in 1948, and was in the Middle Eastern countries of Israel, Jordan, Lebanon, Egypt, and Syria. The purpose of the mission was to monitor and enforce the Arab-Israeli ceasefire.

Peacekeepers are important because they are a neutral force that helps create peace without threatening either group. They play a critical role in maintaining peace and aiding civilians during times of conflict. However, sexual exploitation and abuse are emerging as a major issue in conflicts in countries such as the DR Congo. For example, in 2011, 18 reports of sexual harassment and abuse in minors came to international news, drawing attention to the social injustices that are occurring and the inhumane treatment of citizens in countries where peacekeeping intervention is occurring. In addition, a study conducted by the UN known as The Impact of Armed Conflict on Children, found that 6 out of 12 cases of UN peacekeeping missions experienced a dramatic rise in child sexual trafficking as soon as peacekeepers entered the region. In Haiti, in June 2014, 200 women reported being abused sexually by a peacekeeper, and a third of these women were minors, under the age of 18. Girls in impoverished nations are vulnerable to peacekeepers who offer them as little as $4 worth of food or cash. These girls are then also susceptible to contracting STI’s which they have little to no access to medical care for
the treatment of such. The Central African Republic alone totaled $814 million in charges regarding peacekeeper abuse following conflicts in this region in 1997.

A recent statement made by the head of UN peacekeeping operations noted that “UN peacekeeping missions lacked the specific equipment, intelligence, logistics, capabilities and specialized military preparation” that is so often vital to overpowering the terrorist groups from gaining control of an area. The underfunding of UN Peacekeeping missions make the peacekeepers unable to protect civilians and furthers the conflicts in these regions of civil upset. As of 2012, the UN had a budget of $7.26 billion for peacekeeping missions, 2.5 times more than the budget from 10 years prior. While this seems like adequate funding, it still has left peacekeepers at a disadvantage to terrorist and rebel groups in the countries that they are deployed to.

Another issue surrounding peacekeeping is that regarding the changing nature of conflict. There is much debate over whether peacekeepers should have the right to shoot first in the case of present danger, although this defies the current regulation that peacekeepers have weapons of self-defense after initial attack, given their purpose of security and neutrality, not offensive attack. The debate surrounding UN peacekeeping offensive missions was brought to international attention following the conflicts surrounding the M23 rebel movement in the DR Congo, as peacekeeping intervention came to peak involvement in 2012, when civilian safety was at risk, and Peacekeeping as an offensive force has since been under consideration. In areas of varying conflict, it is important to assess each situation on a case-by-case basis so as to provide countries with the most effective peacekeeping mission possible. The change in legislation to a “case by
case” determination of offensive use in peacekeeping missions is outlined in the 2008 Capstone doctrine.

The most notorious failure on the part of the UN peacekeepers, was the Rwanda conflict of 1999, in which delayed UN action and the dismissal of genocidal evidence led to the deaths of more than 1 million people.

UN Involvement:

The Brahimi Report, an analysis of past peacekeeping operations and the causes of their successes and failures was written in March of 2000. The goal of this report as stated by Ban Ki-Moon was to narrow the issues down to a select few so that the Security Council could work to improve peacekeeping operations. Because of the Brahimi Report, three key factors of peacekeeping operations were analyzed; participation of member states, institutional change, and financial support. These key factors lead to the implementation of the “Capstone Doctrine”, the 2005 World Summit and A/RES/60/1, Peace operations 2010, and A/59/565. The Brahimi report lead to a more “effective and efficient peacekeeping sector” as according to Lakhdar Brahimi, the Chair of the Panel in the Security Council.

The Capstone Doctrine, published January of 2008, stresses the importance of international cooperation and spreading the values of peace and social justice internationally as well. The Peace Operations 2010 was a plan to adapt the peacekeeping process for the technological and social changes that are to occur over the next decade. A/59/565 addressed the security aspects of peacekeeping such as the issue of monitoring organized crime within countries and across borders. The resolution also focused on reforming the protocol of UN facilitated ceasefires and the means to ensuring long-lasting stability. Because of the Capstone
Doctrine, the UN was able to control the Cholera outbreak in 2010 as a part of the MINUSTAH mission in Haiti.

Also, UNITAR works with the UN Nonviolent Peaceforce to aid the 1.5 billion people that are living in areas of political and social violence. UNITAR works to use innovative training such as natural resource management and adaptation within foreign countries, since they recognize the effects that an unstable government has on its citizens and the chances for political violence to erupt from such a situation. Through UNITAR, 120,000 peacekeepers from different countries have received training since September 2012 along with reinforcement training that reminds them of laws and stipulations they have to abide to while completing their mission.

The UN also created the Department of Field Support which began in 2007 and provides direct support to peacekeeping missions in the field and in areas of political missions. The Department of Field Support provides peacekeepers with advice and training regarding finance, communication through technology, human resources, and overall support that ensures the peace and security of peacekeeping missions.

Questions to Consider:

1. What are the major social, humanitarian, and financial issues within UN peacekeeping that must be reformed?
2. How can the UN protect citizens without infringing upon a country’s sovereignty?
3. What are the specifics surrounding the right to protect oneself in the case of a peacekeeper being attacked and how should the nature of this change if it should at all?
4. How can the rights of women be protected in countries with peacekeepers to prevent further sexual harassment?

Works Cited:

Story Kevin Sieff. "The Growing U.N. Scandal over Sex Abuse and 'peacekeeper Babies'"


