A Background Guide for the

Disarmament and International Security Committee

Dalton Model United Nations III

Saturday, April 25, 2015

Table of Contents

Dalton Model United Nations

A LETTER FROM THE CHAIR

Dear Delegates,

Welcome to DMUN III and the Disarmament and International Security Committee (DISEC)!! My name is Calder McHugh, and I am thrilled to be chairing DISEC, the largest, debatably most important, and certainly most fun committee at DMUN III! I am a senior at Dalton, and have been involved in Model UN for all four years of high school: I served as an Under Secretary-General during my Junior year and am now a member of the Senior Executive Board and our Director of Delegate Management and Recruitment. I have attended around 20 conferences of varying length over the last four years, and DMUN will mark my last, so I hope to make it one of the most memorable!

Outside of Model UN, I am the Editor-in-Chief of Dalton's official student newspaper, *The Daltonian* and the Senior Class President. Finally, and maybe most importantly, I am the Dance-General of Dtown Prettyboy Swag, Dalton Model UN's official dance troupe.

This year, DISEC will choose to debate on one of two issues: Protection of Civilians in Modern Warfare and Technology Developments in the Context of International Security. While owning long-winded titles, both of these topics are shifting every day and are increasingly important in our current political climate. Civilians are at risk from drone strikes or chemical weapon attacks, while access to and use of new technology has changed the landscape of international relations. This committee can center around anything from chemical weapon usage in Syria to the morality of Wikileaks; this background guide will give delegates a jumping off point for research, but it is up to all of you to make this committee stimulating.

Although DISEC does not technically have the power to force nations to take up any resolutions passed, this committee will still discuss both the humanitarian and political sides of whichever issue is chosen. I am looking for substantive debate, which means that you shouldn't be afraid to disagree with other delegates - in fact, I encourage you to do so. Know your policy well and stick to it.

Now, let me quickly introduce my moderator. Molly Shapiro is a sophomore on Dalton's MUN team and the enforcer of the committee. If your speaking time has expired, who knows what she's liable to do. She can crack the whip at times, so make an effort not to get on her bad side.

If you have any questions or concerns before the conference, feel free to contact me.

Calder McHugh

Chair, Disarmament and International Security Committee (DISEC)

calder_mchugh@dalton.org

Topic A: Protection of Civilians in Modern Warfare

The Scope of the Problem

Civilian casualties are almost inevitable during times of war, especially with recent developments in technological warfare. A 2003 European Union Security Strategy reveals that "since 1990, almost 4 million people have died in wars, 90% of them civilians."[1] Though this fact has been disputed -- researcher Adam Roberts called it "based on shaky foundations," -- the amount of civilian deaths that result from war is indisputably daunting and far too high.[2] As military operations are more and more often carried out in public areas and cities, civilians have become increasingly vulnerable and affected. This increase is partly attributable to the fact that internal conflicts have become more prominent in the wake of World War II. When internal contention arises, civilians often become targets of terrorist organizations and non-state actors that are militarily weaker than the governments that they are fighting. In an attempt to offset their lack of military strength, the weaker party may turn to aggression of civilians who are easy targets because they are typically unarmed and untrained. This is known as "asymmetric" warfare.[3]

Dr. Jakob Kellenberger, President of the International Committee of the Red Cross, said, "What is required in most cases -- to improve the situation of persons affected by armed conflict -- is greater compliance with the existing legal framework, not the adoption of new rules."[4] Such a task is increasingly difficult to accomplish, however, when terrorist organizations are largely responsible

---

[1] Brussels, 12 December 2003. A SECURE EUROPE IN A BETTER WORLD (n.d.): n. pag. Web.

[2] "Lives and Statistics: Are 90% of War Victims Civilians?" last modified July 2010, https://weblearn.ox.ac.uk/access/content/user/1044/Survival_Jun-Jul_2010_-_AR_on_lives___statistics_-_non-printable.pdf.

[3] "Protection of Civilians under international humanitarian law: trends and challenges," last modified August 2011, https://weblearn.ox.ac.uk/access/content/user/1044/Survival_Jun-Jul_2010_-_AR_on_lives___statistics_-_non-printable.pdf.

[4] "Strengthening Legal Protection for Victims of Armed Conflicts." Strengthening Legal Protection for Victims of Armed Conflicts. N.p., n.d. Web. 18 Feb. 2015.

for the harm of civilians. In 2014, the U.N. credited the Taliban with 75% of the civilian deaths thus far in the mounting conflict in Afghanistan between the government and rebel groups.[5] As Kellenberger stated, the frameworks are irrelevant if not obeyed by all participants of war. When ignored by one party, other groups will follow suit, and the established legal boundaries will be broken altogether.

In Bazaar e Panjwaii, a village in Afghanistan, children and an Afghan soldier cross paths[6]

Legal frameworks on the issue include The Fourth Geneva Convention, which incorporates the International Humanitarian Law, basic internationally accepted principles pertaining to warfare.[7] Implemented in 1949, the Convention details regulations and mandates, such as the differentiation between civilians and persons involved in the conflict and other matters regarding the protection of civilians in war.[8]

In Article 36 of Additional Protocol I, countries are called upon to analyze the threat or legality of any new potential weapons in the context of the established international law. This is especially relevant today.[9] Such a Convention, regardless of how comprehensive and intricate it may be, continually must be reevaluated in the context of technological developments and changing military

---

[5] The Wall Street Journal. Dow Jones & Company, n.d. Web. 18 Feb. 2015.

[6] "Afghanistan civilian deaths up 31% this year, says United Nations," last modified August 10, 2010, http://www.theguardian.com/world/2010/aug/10/afghanistan-civilian-deaths-up-un.

[7] Respect for International Humanitarian Law. Geneva: Inter-Parliamentary Union, 1999. Web.

[8] "Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva," last modified August 12, 1949, https://www.icrc.org/ihl/INTRO/380.

[9] Waszink, Camilla. "Protection of Civilians under International Humanitarian Law: Trends and Challenges1." Norwegian Peacebuilding Resource Center. N.p., n.d. Web.

tactics. The military use of drones, for example, has caused the death of nearly 700 civilians but only 17 terrorist targets, Pakistani sources told the *New York Times*.[10] As military capabilities increase, the risk of civilian casualties is heightened due to the potential of drone missions that are aimed at terrorists in urban areas or other densely-packed regions. As the delegates of DISEC at DMUN 2015 seek to strengthen the protection of civilians in armed conflicts, the aforementioned challenges (internal conflict, compliance of terrorist organizations, introduction of new military technology, etc...) that come with such a task must also be taken into account.

History of the Issue

High numbers of civilian casualties is not a new phenomenon. In World War I, which lasted from 1914 to 1918, nearly 7 million civilians died.[11]

Even more startling, however, were the number of civilian casualties that resulted from World War II. Beginning in 1939 and ending in 1945, World War II was the accumulation of tensions rising on an international scale. With poor economies, over fifty nations fought in the war that ended with a total of 45 million civilian casualties.[12] The Battle of Stalingrad, which lasted from 1942 and drew to a close in 1943 with 40,000 civilians dead, not only saw the death of countless civilians, but also heavily affected non-combatants otherwise.[13] The Soviet Union, in its defense of the city of Stalingrad, surrounded German forces until Germany had to surrender due to a lack of resources and unbearably low temperatures. The Soviet army prohibited the departure of any civilians from the city, which impacted civilian lives for nearly a year. Civilians had to endure bombings and warring in densely-populated areas.[14]

---

10 Kilcullen, David, and Andrew Mcdonald Exum. "Death From Above, Outrage Down Below." The New York Times. The New York Times, 16 May 2009. Web. 18 Feb. 2015.

11 "Casualties | WW1 Facts." WW1 Facts. N.p., n.d. Web. 13 Feb. 2015.

12 "By The Numbers: Worldwide Deaths." The National WWII Museum. N.p., n.d. Web.

13 "Battle of Stalingrad." History.com. A&E Television Networks, n.d. Web. 11 Feb. 2015.

14 "World War II: The Battle of Stalingrad." The Battle of Stalingrad. N.p., n.d. Web. 11 Feb. 2015.

In the same vein, the United States bombing of Japan at the end of World War II resulted in the deaths of a total of nearly 200,000 people and the surrender of Japan in the most devastating war in history.[15] The United States dropped two atomic bombs in 1945, the first in Hiroshima on August 6th, and the second in Nagasaki, on August 9th. In Hiroshima, 80,000 people were instantly killed, and in Nagasaki, the bomb ended the lives of 40,000. Tens of thousands of additional civilians died in the aftermath of the event due to the remnants of the radioactive material.[16]

The Current Situation

Events

Though the mistreatment of civilians in warfare has an extensive history, the topic's relevance today has not ceased. The current situations in Afghanistan and Syria exemplify the grim reality that civilians in conflict regions face. In Afghanistan's war, in which there have been a total of over 21,000 civilian deaths, 1,564 civilians died in the course of six months in 2009, a large increase from the numbers of the previous year.[17] Though insurgents are responsible for nearly 75% of these deaths, authorities primarily ignore such actions, failing to properly punish those who committed blatant humanitarian crimes.[18] The war in Afghanistan, which began in 2001 as a result of 9/11, had seen a decrease in civilian casualties in early 2013, but this progress was reversed when American soldiers began to depart from Afghanistan, leaving all military responsibilities with Afghan soldiers. With an aim of maximizing such a transition, the insurgent forces began heavy attacks on the Afghan military, some of which took place in urban areas such as Kabul, the capital of Afghanistan.

---

15 "Fact File: Hiroshima and Nagasaki." BBC News. BBC, n.d. Web. 13 Feb. 2015.

16 "Bombing of Hiroshima and Nagasaki." History.com. A&E Television Networks, n.d. Web. 11 Feb. 2015.

17 "Afghan Civilians | Costs of War." Afghan Civilians | Costs of War. N.p., n.d. Web. 18 Feb. 2015.

18 STANCATI, MARGHERITA. "Civilian Casualties on Rise in Afghanistan." The Wall Street Journal. Dow Jones & Company, n.d. Web. 18 Feb. 2015.

Roadside bombs were a large contributor to the high civilian death toll, making up a third of civilian deaths in the beginning of 2013.[19] Even in the notoriously safest parts of Afghanistan cities, though, there is no safety for the high numbers of civilians, with gun battles occurring on streets that are typically packed with Afghans going to or coming from work.[20]

In Syria, the situation is similar. The war in Syria began in 2011 and now has an estimated death toll of 191,000 -- a number that does not account for the over 50,000 deaths of undocumented persons.[21] It is estimated that almost a third of the dead are civilians.[22] These numbers are even more frightening beyond their staggering nature because some of the civilians were killed

intentionally by the Syrian government. A chemical weapons attack purposefully killed 1,500 civilians, at least 426 of whom were children. In response to such an alarming event, the United States threatened military intervention, but neglected to enter Syria after Bashar al-Assad agreed to destroy all toxins.[23]

A Photograph of Activists in Syria as they examine the bodies of those thought to be killed by the chemical weapons attack[24]

[19] Ahmed, Azam. "As Afghan Pullout Nears, Civilian Casualties Rise." The New York Times. The New York Times, 31 July 2013. Web. 18 Feb. 2015.

[20] Ahmed, Azam, and Matthew Rosenberg. "Ground Battles in Afghanistan Contribute to Surge in Civilian Casualties, U.N. Says." The New York Times. The New York Times, 09 July 2014. Web. 18 Feb. 2015.

[21] Cumming-bruce, Nick. "Death Toll in Syria Estimated at 191,000." The New York Times. The New York Times, 22 Aug. 2014. Web. 18 Feb. 2015.

[22] Gordts, Eline. "Death Toll In Syria Surpasses 130,000, Monitoring Group Says." The Huffington Post. TheHuffingtonPost.com, n.d. Web. 18 Feb. 2015.

[23] "More than 1,400 Killed in Syrian Chemical Weapons Attack, U.S. Says." Washington Post. The Washington Post, n.d. Web. 18 Feb. 2015.

[24] "Syria Crisis: Obama to Meet with National Security Team." Msnbc.com. NBC News Digital, 25 Sept. 2013. Web. 18 Feb. 2015.

The fixation on Syria, however, has unfortunately decreased as new conflicts arise in other nations. Navi Pillay, the former United Nations High Commissioner for Refugees, addressed this issue in a speech to the Security Council. "Given the onset of so many other armed conflicts in this period of global destabilization, the fighting in Syria and its dreadful impact on millions of civilians has dropped off the international radar," Pillay stated. She then accused the Security Council of complacency in regards to the conflict: "There has not always been a firm and principled decision by members to put an end to crises. I firmly believe that greater responsiveness by this Council would have saved hundreds of thousands of lives," Pillay said.[25] Delegates on DISEC should keep the conflict in Syria as a primary concern as they seek to address the humanitarian crisis plaguing our world today.

The Military Use of Drones

Unmanned Aerial Vehicles (UAVs), more commonly known as drones, can be used militarily, for killing terrorist targets, or peacefully, for surveillance and delivery of resources to areas that are dangerous for humans on the ground. The aircrafts are known for their stealth, ability to fly low, and precision, though civilians are too often harmed by drone strikes in cities or other highly populated areas.

A UAV on a United States Air force operation, flying above Southern Afghanistan[26]

Because UAVs do not put pilots or militia at risk, they are seen as largely positive, but opposition to the aircrafts typically stem from the danger posed to innocent civilians.[27] A 2009 Human Rights Watch Report stated that "Drones...are only as good at sparing civilians as the care taken

---

[25] Cumming-bruce, Nick. "Death Toll in Syria Estimated at 191,000." The New York Times. The New York Times, 22 Aug. 2014. Web. 18 Feb. 2015.

[26] "Global Journalist." Drone Warfare -. N.p., n.d. Web. 18 Feb. 2015.

[27] "Drones: What Are They and How Do They Work?" BBC News. N.p., n.d. Web. 18 Feb. 2015.

by the people who operate them."[28] In Pakistan, sources revealed that an average of fifty civilians are killed for every one target.[29] These devastating numbers, coupled with the disruption that drones have caused with their constant hovering above marketplaces and towns and the ever present threat that they pose, reveal the countless negative effects that drones have had on civilian lives.[30]

Proposed Solutions

When looking to combat humanitarian crisis worldwide, solutions must be elastic, durable, and detailed. As more and more cases of civilian suffering arise in different countries, solutions must be applicable to a wide range of scenarios, while also remaining specific and grounded in past experiences.

One possible solution is the reworking and amendment of the existing frameworks so that the laws are not as imposed as they are a collaborative agreement. Another could be the stricter enforcement of laws pertaining to warring in urban areas. Lastly, perhaps local officials could attempt to keep civilians in cities informed with the current threats posed to the region so that they are not unprepared should an emergency evacuation of an area become necessary or recommended.

Questions to Consider

- How can a nation ensure that its militia is distinguishing civilians from soldiers?
- What can be done to ensure that the International Humanitarian Law is respected, observed, and maintained?
- Should stricter drone regulations be imposed in order to minimize the civilian casualties that result from UAV strikes?
- Should countries reevaluate the current legal frameworks entirely?

---

[28] "I. Overview." Precisely Wrong. N.p., n.d. Web. 18 Feb. 2015.

[29] "Protection of Civilians under international humanitarian law: trends and challenges," last modified August 2011, https://weblearn.ox.ac.uk/access/content/user/1044/Survival_Jun-Jul_2010_-_AR_on_lives___statistics_-_non-printable.pdf.

[30] Walsh, Declan, and Ihsanullah Tipu Mehsud. "Civilian Deaths in Drone Strikes Cited in Report." The New York Times. The New York Times, 21 Oct. 2013. Web. 18 Feb. 2015.

- How can the international community address the recent increase in "asymmetric" warfare?
- What are recommended courses of action for a nation that is targeting a terrorist in a densely-populated region?

Topic B: Technology Developments in the Context of International Security

The Scope of the Problem

While technology continues to advance and create new milestones, threats increase, and the safety of international security faces risks. Although there are many benefits from new technology, the increased dangers that come as a result can lead to the publicizing of nation's private information. This information could jeopardize the nation's security, as well as induce repercussions that could affect security at an international level.[31]

As the borders of technology expand and reach a larger realm than they ever have before, the space that is then left open for harmful attacks widens. As these limits grow hackers and terrorist organizations can commit cyber attacks on a larger scale. This cyber warfare can range from national security breaches, to

---

[31] "Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment | Meetings Coverage and Press Releases." UN News Center. October 28, 2014. http://www.un.org/press/en/2014/gadis3512.doc.htm. Accessed November 20, 2014.

interfering with and impairing vital communication and commands.[32] These breaches on nations' security would result in sensitive, or secret information falling into the wrong hands, and the consequences could be detrimental. The exposed information could put the safety of a country at risk, or produce unruliness and tension among countries. An estimated 148,000 computers are jeopardized globally on a daily basis, which involves viruses and the obtaining of information.[33]

Interfering with military communication poses many risks for both the safety of these personnel, and the accomplishing of the task at hand. If the commands get altered or blocked, the danger that arises can put the outcome at peril.[34] In addition to military interference, cyber warfare can affect national systems, such as electric power grids. Attacks on this would cause mayhem

throughout the country, and generate fear within the people. Giving these hackers and terrorists the potential power

A team of people relying on monitors to give them access to security footage[35]

of inflicting such chaos is something that must be prevented, in order to maintain international security.

Since surveillance can be easily compromised from hacking, this form of cyber attack can fuel further attacks that are not only placed under the umbrella cyber warfare. The

---

32 "Developments in the Field of Information and Telecommunications in the Context of International Security." http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf. Accessed December 13, 2014.

33 "Finding Solutions. Together." Dealing with Cyber Crime – Challenges and Solutions. http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/dealing-with-cyber-crime-2013-challenges-and-solutions. Accessed December 12, 2014.

34 Snow, Gordon. FBI. April 12, 2011. http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism. Accessed December 7, 2014.

35 "Too Many Security Cameras – or Too Much Hype?" *Too Many Security Cameras – or Too Much Hype?* N.p., n.d. Web. 08 Feb. 2015. http://www.ianvisits.co.uk/blog/2008/06/27/too-many-security-cameras-or-too-much-hype/.

frequency in which criminal organizations are disrupting online activity has drastically increased, since the growth of technology allows for more advanced attacks and opportunities to arise.[36]

Financial systems are often at risk of cyber attacks, because the outcome of one of these attacks would contribute to the interference of a core system. As well, these attacks may lead to the access of large quantities of money and knowledge. Cyber related crime has grown to a trillion dollar a year business, which is why ways to prevent further attacks, and the protection of important information must be found and implemented, if we want the development of new technology to be a positive addition to our society today.[37]

History of the Issue

In spite of the fact that cyber attacks generally exist virtually, the effect they have can be international. As new technologies continued to arise in the 20th century, the risk they posed on international security grew. The information that could be obtained from cyber attacks became more classified, allowing for terrorists and hackers to truly infiltrate national security. They found new ways in turning the growth in technology into a doorway for committing cyber attacks.

One of the first cyber attacks, The Morris worm, occurred in 1988. It spread a virus through computers within the United States, causing problems related to the cyber infrastructure.[38] Although this attack did unintentional harm, it showed the prospective uses of technology, and began a new era of cyber attacks. Once people discovered the cracks in new technology, they realized the damage a cyber attack could have, which led to the commencement of cyber warfare.

---

[36] "Cybersecurity: A Global Issue Demanding a Global Approach | UN DESA | United Nations Department of Economic and Social Affairs." UN News Center. December 12, 2011. http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html. Accessed December 13, 2014.

[37] "The History of Cyber Warfare." The History of Cyber Warfare. http://online.lewisu.edu/the-history-of-cyber-warfare.asp. Accessed December 13, 2014.

[38] "The History of Cyber Attacks - a Timeline." NATO Review. http://www.nato.int/docu/Review/2013/Cyber/timeline/EN/index.htm. Accessed December 13, 2014.

In the past these attacks have included identity theft, viruses, and stealing sensitive data, with not only one culprit behind them.[39] Cyber attacks happen for a surplus of reasons, though they have generally been intended as sabotage, with the perpetrator ranging from terrorist organizations, the mafia, to even nations conspiring against other nations.

In January 2009 a massive cyber attack was aimed at Israel, in an attempt to hinder their internet infrastructure. This attack was committed by an estimated 5,000,000 computers, generally intended to target government websites. An attack that was not directed at one specific target was found in October 2012, although it was believed to be in operation since 2007. The goal of this virus, which was due to problems within Microsoft and Excel programs, was to obtain information from governments, militaries, energy companies, and major infrastructures. The goal was was successfully achieved, acts as a significant

worldwide cyber attack. These two examples show how the development of technology and increased reliance can put national and international security at risk, and result in dangerous situations.

The Current Situation

Now, in the 21st century, technology is an imperative part of our society, that has been integrated into everyday life. Since veering away from technology or not constantly developing new technologies is not an option due to its vital role, solutions to prevent future cyber attacks are essential. Terrorist organizations are still using cyber warfare by finding the cracks in technology, to obtain information and spread viruses. The damage that they are able to do is unfathomable, which is why steps towards prevention must be taken.

Since nations are increasingly trusting technology to store their top secret information, if someone is able to hack into that the nation will not

---

[39] "United Nations Official Document." UN News Center. http://www.un.org/ga/search/view_doc.asp?symbol=A/45/568. Accessed December 10, 2014.

only be at risk, but international security could be at risk.[40] As new technology develops, hackers continue to find ways to crack it, so being one step ahead is often implausible. Protecting information and access from falling into the wrong hands is at the utmost importance in order to maintain a basic level of security, but steps need to be taken because cyber attacks are still occurring. Today, countries understand the risks that they are faced with, so they are continuously attempting to enhance their cyber security and prevent future attacks.[41]

Case Study: Edward Snowden

An example of a cyber attack blowing up to an international scale, is the story of Edward Snowden acquiring and releasing the National Security Agency's private information. Snowden managed to hack into the NSA computers and collected highly classified documents and information, undetected. He went on to leak the documents he found to the public, damaging, as well as embarrassing NSA.[42] The documents he leaked revealed secret programs, rules that had been broken, and unauthorized surveillance and spying. The consequences NSA faced once the documents had been leaked were enormous, because the secrets that were revealed ruined their image, and publicized classified information.[43] This oversight went unknown for so long, clearly showing it was unexpected and caught the NSA extremely off guard. This example shows how even one of the most protected systems is at risk of being hacked.

Relevant UN Action

---

[40] "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience." Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience. Accessed December 5, 2014.

[41] Drew, Christopher, and Scott Shane. "Résumé Shows Snowden Honed Hacking Skills." The New York Times. July 4, 2013. http://www.nytimes.com/2013/07/05/us/resume-shows-snowden-honed-hacking-skills.html?pagewanted=all&_r=0. Accessed November 23, 2014.

[42] Elliott, Kennedy, and Terri Rupar, Published: Dec. 23, 2013. "Six Months of Revelations on NSA." Washington Post. December 23, 2013. http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/. Accessed December 3, 2014.

[43] https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf. Accessed November 8, 2014.

Seeing as these are relatively recent problems, the United Nations has tried to do whatever is in their reach to prevent technology developments from damaging international security. The UN has already created laws defining cyber attacks, warfare, and terrorism, in an attempt to reprimand perpetrators who have committed crimes that fit their description. The first attempt to internationally address cyber attacks was the Convention on Cybercrime.[44] This convention which is commonly referred to as The Budapest Convention was a treaty written in 2001, by the Council of Europe on cybercrime. This was a beginning attempt at combating cybercrime, by declaring what offenses falls under it, so they can easily be deemed a violation internationally, in order to prevent an international crime from being defined nationally.[45]

Although the UN rejected a treaty proposed by Russia on cybercrime in 2010 due to disagreement between countries, the UN is still seeking out a treaty that is both universally agreed on, as well as effective in solving the problems of cybercrime. The UN has created an intergovernmental expert group to understand and assess the problem of cybercrime. This was requested in its resolution 65/230, and in resolution 67/189 the group's work and contribution is acknowledged.[46]

Proposed Solutions

In order for a solution to effectively solve the problem of cybercrime many steps must be taken. Finding safer ways to do business on the internet, or protecting business that is done on the internet is essential to prevent hackers from infiltrating these systems. Since a cybercrime can occur in more than one location, deciding whether or not jurisdiction laws should be changed due to the unconventional demeanor of this problem is something that should be taken into consideration. Also, due to technology being such a critical part of nation's infrastructure, ensuring that no attacks or attempts to damage

---

[44] "Council of Europe - ETS No. 185 - Convention on Cybercrime." Council of Europe - ETS No. 185 - Convention on Cybercrime. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Accessed November 20, 2014.

[45] http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/solutions/Create_an_international_treaty_to… Accessed November 23, 2014.

[46] "Comprehensive Study on Cybercrime." February 1, 2013. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed December 13, 2014.

or interfere with a nation's key structures can be committed, is pertinent to hindering future attacks. Understanding how to react to these attacks in a timely manner is something that must be done to counter the degree of their effect. As well, you should begin to think about future actions that could lead to the decrease of cybercrime, such as implementing new laws, or editing existing ones. Ways to prepare for cyber attacks, such as training more people on how to react quickly is one way of dealing with the situation at hand. Also, think about the benefits, and plausibility of creating a program that can look through systems for any viruses or unknown users to potentially eradicate the risk of undetected hackers.