UNSC

MITMUNC III, 2011

Committee Welcome Letter

Dear Delegates,

I am Albert Wang, your head chair, and it is my pleasure to welcome you to the third annual Massachusetts Institute of Technology Model United Nations Conference 2011. I look forward to our committee in February, and cannot wait to hear the discussion that is produced. I believe that bioterrorism and cybersecurity are interesting topics to discuss as they are relatively new fields that have not been overly debated such as a topic on the Middle East.

If you've never been on a United Nations Security Council committee in the past, you should know the procedure is slightly different. You still need a majority vote on procedural matters, but binding resolutions need all five permanent members (that is, the United States, the United Kingdom, France, China, and Russia) on board. If any of these five countries disagree, your resolutions will not get passed. Any resolutions that do get passed will alter events and change the political climate - perhaps detrimentally - so thinking on your feet is very important. The overall expected quality of the discussion will be higher as well.

Some information about me, my co-chair, and crisis staff:

I am a junior majoring in electrical engineering and computer science with a concentration in international relations. I was the crisis director for the UNSC committee two years ago and Secretary-General of MITMUNC last year. This year, I am also the Charge d'Affaires and webmaster for MITMUNC.

Bahar Shah, the co-chair for the UNSC, is a 2013 (a sophomore) currently majoring in 18C- Math with Computer Science and minoring in 21L-Literature, although that may change. Bahar was crisis director for MITMUNC last year and she is currently also the PR Director for AIRMUN.

Emad Taliep, a member of the class of 2014, is a newcomer to MITMUNC who is considering majors in Brain and Cognitive Science as wåell as Philosophy and/or Linguistics. He looks forward to making your committee sessions interesting as one of the crisis staff members for this conference.

Suan Tuang, also a member of the class of 2014, will be joining Emad on the crisis staff. Although his choice of major is currently unknown, his interests lie within the biomedical science and its applications. With him on the crisis staff, the committee will truly be a memorable experience.

Please be reminded that position papers are due at noon on January 30. We expect a one page position paper from each delegate and they are a requirement to win awards. More information about position papers, as well as background guides, are available on the mitmunc.org website.

See you in February,

Albert Wang

This year, our discussion topics are:
Cyber Warfare
Bioterrorism

Cyber Warfare

What's the problem? What needs to be fixed?

The rising prominence of the Internet over the past few decades has also given rise to a novel, insidious method of waging war. The ubiquity of Internet access and the cheap cost of computers and other technologies makes cyberwarfare an obvious alternative to an attack with more conventional weapons. Such a minimal investment of resources can yield astronomic rewards; after all, a nation's most sensitive information - even its very infrastructure - is only as secure as its strongest cyber security protocols.

For the purposes of debate, we can divide Internet attacks into two categories. The more common category of cyber attacks is what we will call "cyber crime". Cyber crime is an Internet attack that originates from individuals or nongovernmental organizations and are usually directed at other individuals or nongovernmental organizations usually for the purpose of making money. On the other hand, the less common category is "cyber warfare". Cyber warfare is conducted by governments or governmental agents against others as a political, economic, or military instrument in order to advance their policies and beliefs. Cyber warfare can also be carried out by non-governmental organizations whose main aim in committing cyber attacks is to gain political rather than monetary benefits. Obviously, there is an overlap between the cyber crime and cyber warfare so the UNSC will need to also debate about what forms of cyber attacks it should focus on and which it should refer to other policing bodies such as Interpol.

Presently, almost all nations have had cases of cybercrime originating from their countries. In particular, developing nations such as Russia, India, and China play host to much of the cybercrime happening around the world. For example, China's internet routers have been implicated in diverting large amounts of internet traffic from the United States. The relative ease that a hacker has in compromising security systems is a function of the fast evolution of technology - and the clumsy, largely unreactive response of the international community. In the face of such elusive, vaguely-defined, and efficient threats, the world would stand to gain from further progress made in the realm of cyber security.

Technical Overview

Please note that the UNSC is a political committee, not an expertise committee. Therefore, debate should be focused on the political rather than the technical details of cyberwarfare. The chairs, crisis staff, and/or home government will answer any questions relating to technical background during the conference. However, in order to have all delegates on the same page in terms of technical expertise, here is an overview of the technology behind cyberwarfare.

The Internet is a network of computers that communicates in a standardized way so that almost any computer in the world can send information to any other computer in the world. For example, to access a website, a computer would send a request to a server (a specialized computer) and the server would send back the code for the website. Between the two computers, there are Internet Service Providers (ISPs). ISPs have machines called routers that move Internet traffic between themselves so that information gets to the correct computers. These routers can range from small ones that handle a few computers to very large network backbones that switch hundreds of gigabytes of data from millions of computers every second.

Cyber attacks can occur in many ways. The most common method is the creation of computer programs, commonly known as viruses or worms, that spread by infecting computers through a bug in its code. A well crafted computer virus can then let the virus's writer take control of the computer as well as using the computer to infect other computers without the owner noticing.

Through computer viruses, hackers can create botnets which are groups of computers that are under the control of a specific person or organization. These botnets can then be directed to send spam mail or attack other computers. Large botnets can be used to launch a

Distributed Denial of Service (DDoS) attack. In a DDoS attack, a malicious actor directs the computers in his botnet to send huge amounts of information to a specific computer, such as a website's server, thereby overloading the computer and making it not work for other users. Given the fact that botnets rely on their large size and not necessarily the craftiness of their human controllers, botnets are easy to detect but are hard to fight directly. Usually, they are defeated by removing the botnet's central control computers from the Internet, metaphorically "cutting the head off the snake".

Past Problems and Effects

While cybercrime occurs every day, we will give three examples of cyberwarfare in this background guide. Our first example, the first generally recognized instance of state-sponsored cyberwarfare, started in 2003. These attacks, codenamed "Titan Rain" by the US government were directed at the US and its allies. These attacks have exhibited great ingenuity on the part of the hackers, which have been traced to the Chinese government. Though not as publicized as some later cyber attacks, Titan Rain's perceived purpose is to hack into military, industrial, and research computers, retrieve any files of military, economic, or political value, then erase all log files of the attack. Though the full extent of Titan Rain still has not been determined, it is known that Titan Rain has successfully gained access to computers owned by the Pentagon, US Department of Energy, and NASA. Additionally, many corporations or universities that do research applicable to military technologies, including Lockheed Martin and MIT, were also attacked. In 2005, Shawn Carpenter, using legally questionable tactics, traced the Titan Rain hacking back to computer systems in China. Given the scope and complexity of the attacks, the attacks were probably run by the Chinese government or their proxies.

In 2007 and 2008, there were two large instances of cyber attacks originating in Russia and attacking Estonian and Georgian networks. In 2007, many of Estonia's computers, including governmental and telecommunications servers were attacked by a massive DDoS attack. Since DDoS attacks originate from other compromised computers, tracing the hacking back to Russia was difficult and the result is still contested by the Russian government. The 2008 attack on Georgian networks was also similar in that attackers used botnets to DDoS Georgian governmental and telecommunications networks. However, the cyberattack on Georgia was a forerunner to the 2008 South Ossetia war between Georgia and Russia. The cyber attack on Georgian networks was probably aimed at giving Russia an advantage over Georgia's military, compromising its chain of command. These two attacks have led military planners to start considering cyber warfare as a major example of unconventional warfare, rather than cyber crime due to its effects on Georgian and Estonian military and governmental networks.

In 2010, the Stuxnet worm infected many industrial targets that used Siemens control systems. The originator of the Stuxnet worm is still unknown, but it is suspected that Israel created the worm to target Iran's nuclear program. The complexity of the worm, which included reprogramming certain industrial machines to malfunction, again shows that the originators of the code had to have considerable technical experience. Through the reprogramming of certain machines important to the development of Iran's nuclear technology, Iran's nuclear development has been damaged.

Past Solutions And Effects

Many countries bemoan the inadequate state of cyber security measures, yet sharply contrasting ideas prevent much of the necessary progress against solving cyber crime. One of the most contentious debates concerns the nature of cyberdefense. The United States has consistently suggested policies advocating for increased cooperation between different law enforcement agencies. This was the inspiration for a Convention on Cybercrime from the Council of Europe back in 2001 [4], which produced a treaty accomplishing this very goal while also suggesting legislation to be adopted at the national level.

The European Cybercrime Treaty, the agreement formed by the convention, is a considerable milestone, and it has fostered a degree of collaboration on the global scale. On the whole, however, it has a lot of room for improvement. Most alarmingly, a good number of signatories were slow in ratifying the treaty's ordinances, and 17 out of 47 countries that have signed the treaty have yet to complete ratification. [5]

Notably absent from the list of signatories is Russia, which continues to propose a treaty that would both place a halt on developing additional cyberweapons and act as a non-aggression pact. This idea resurfaced at an annual conference on cyber security [6], along with other concerns, raised by Russia, that current gaps in

international law would make any offensive approach to cyber terrorism troublesome.

Though these complaints have not yet inspired much action, they are not completely without merit. International laws do not yet have ordinances to explicitly moderate cyber warfare. In the war with Iraq, the Bush administration severely hindered military and government telecommunications in the area, though the collateral damage spread to neighboring areas. However, they stopped short of freezing Iraq's finances [7], for fear of causing far greater repercussions, even though the United States possessed the capacity to do so.

And this year, a cyber attack was implicated in the disruption of a nuclear facility in Iran [8]. Clearly, without solid restrictions, any service, piece of infrastructure, or provider is at risk and could be crippled considerably by cyber attacks.

Some experts, in lieu of this offensive approach, advise preventative measures - allegedly, firewalls are worth more than cyber sharpshooters [9], the argument goes. Still others raise the suggestion of exposing hackers before they can do serious, irreversible damage [10], a tactic that would necessarily compromise the anonymity hackers now enjoy, and one which may consequently infringe upon privacy in favor of security.

Country Blocs

Western Bloc

The Western bloc is at most risk of cyberwarfare attacks because of its high level of technological dependence. It is also the best equipped to handle and make cyber attacks. Due to the West's deep rooted political beliefs in free speech and privacy, the West would be loath to accept some of the possible solutions to cyber attacks, such as the creation of computer monitoring software.

East European Bloc

Eastern Europe, like the Western bloc, is also at high risk of cyberwarfare. It also has had to two major wars, those against Georgia in 2008 and Estonia in 2007. In some ways, the countries of eastern Europe are more at risk of cyber attacks as a result of governments not having sufficient cyber security personnel.

Asian Bloc

While most parts of western Asia are technologically less developed, many east Asian countries are as dependent on their electronic infrastructures as Western nations. While many east Asian countries (e.g. Japan, South Korea) also have liberal political governments that promote free speech, others (e.g. China) have more conservative governments that have implemented measures to control the flow of information on the Internet, the most prominent of which are national firewalls. While the firewalls are arguably deplorable as a political tool, they can also possibly be used for national cyber defense. Additionally, because of the technical sophistication of these countries, many east Asian countries have defensive as well as offensive cyber warfare abilities.

African Bloc

The African bloc, as the least technologically developed, has the lowest direct stake in cyber security. However, many African nations are developing at a fast rate and are starting to integrate electronic systems into their governments. Additionally, as many are close allies or reliant on more developed nations, they would be indirectly affected by any cyber wars. Therefore, African countries would be heavily against the development of any offensive cyber warfare capabilities.

Middle Eastern Bloc

The Middle Eastern bloc has also been affected by cyber warfare. As stated above about Iran, many Middle Eastern nations have certain economic or government infrastructures that are reliant on the Internet. Also, as many nations in the Middle East are fearful of the West's influence, they may seek to develop their own defensive cyber capabilities. They may also seek to develop offensive capabilities as well, as a deterrence measure against Western incursions.

What the UNSC Should Do

The first thing the UNSC should do is define cyber warfare. As the UNSC's jurisdiction is about international security and not criminal activities, the UNSC should focus on cyber warfare and not cyber crime. Therefore, the UNSC should define for itself the limit of cyber warfare.

A possible contention point between eastern and western powers is the limit of defensive and offensive cyber warfare capabilities with regards to human rights such as free speech. As an extreme example, whereas a country such as North Korea, which is almost entirely cut off from the World Wide Web, may have little to fear

from cyber warfare, this does not mean that most countries (and none of the UNSC members) would advocate cutting off their entire country from the Internet as a form of cyber defense. On the other hand, a country that carries free speech to the extent that it doesn't have passwords on its secret military or diplomatic networks will have its secrets stolen. Therefore, the UNSC must find a balancing point between closed and open networks that is favorable to all countries.

Another consideration is the political ramifications of cross-border attacks. If an attack is traced from Country A to Country B, is Country B required to aid Country A in apprehending the attacker? If the attacker is found to be in Country B, is Country B required to extradite the attacker to Country A for prosecution? If the attacker is found to be in Country C, is Country B liable for being negligent in its cyber security and being the launching point for the attack on Country A?

Although the chair does not recommend that this committee decide to establish a subcommittee to evaluate cyber warfare (i.e. to establish a subcommittee to do what this committee is supposed to do), the chair would look favorably upon the establishing of some kind of technical oversight or coordination organization.

References

[1]http://gizmodo.com/5692217/chinas-secret-internet-hijacking-uncovered
[2]http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249
[3]http://sciencecareers.sciencemag.org/career_magazine/previous_issues/articles/2010_12_03/caredit.a1000115
[4]http://conventions.coe.int/Treaty/Commun/QueVoulezV
[5]http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
[6]http://www.nytimes.com/2010/04/16/science/16cyber.html?scp=19&sq=&st=nyt
[7]http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?ref=cyberwar
[8]http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?ref=computer_security
[9]http://news.cnet.com/8301-27080_3-20024210-245.html
[10]http://www.technologyreview.com/computing/25060/page1/

Bioterrorism

What's the problem? What needs to be fixed?

Guns, swords, missiles and bombs are not the only types of weapons existing in the world; the threat of bioterrorism always weighs on the minds of policymakers and of international agencies. The Center for Disease Control and Prevention in the United States considers bioterrorism to be "the deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants." Bioterrorism is distinct from chemical warfare as live threats are used in bioterrorism as opposed to chemical agents. Additionally, depending on the resilience of the infectious agent, sustained, wide-scale contamination is possible with bioterrorism. As these weapons are, in all other aspects, naturally-occurring organisms that have been modified to cause harm, containing the threat they pose is a great challenge; these bioweapons spread just as microorganisms would.

With damage control being understandably difficult, the best protection involves securing and protecting any areas that could be co-opted as potential reservoirs for lethal bioweapons. Even in theory, however, this is a daunting challenge. Much of the western world is connected and sustained by public transportation and infrastructure and many areas in developing nations are very densely populated; thus, any disease would spread like wildfire.

Three levels of pathogens have been recognized by the CDC [4] as potential agents of bioterrorism, with each level corresponding to its ability to cause harm. Category A agents are the most dangerous kind, with their great notoriety and high rates of communicability and mortality making them popular bioweapons. Anthrax, Smallpox, and Ebola are some contagions that fit under this category. Category B agents still pose a considerable threat to large populations, but when compared to category A agents, this threat is moderate. Staphylococcal infections, Cholera, E. Coli and Salmonella are good examples of these types of agents. Category C agents are emerging threats whose potential for mass production, quick dissemination, and/or severe health consequences warrant some extra attention.

Naturally, the threat of bioterrorism marks a point of convergence for the interests of national security and public health, but the current level of cooperation,

particularly across national borders, remains insufficient to tackle the threats associated with bioterror.

Past Action and Effects

Bioterrorism prevention starts with limiting the resources available to insurgents. To that end, the Biological Weapons Convention, an agreement whose primary objectives include limiting and discouraging the creation and proliferation of biological weapons, was signed in 1972, and it has since grown to encompass 163 countries as signatories [5]. Its level of multilateral support is impressive, but critics have claimed that it uses broad strokes to deal with issues that require more care.

Chiefly, opponents argue that the convention has yet to establish good measures verifying that a member state is in accordance with the convention. Admittedly, the task is difficult, as any pharmaceutical company or research university possesses the means to manufacture both legitimate drugs and malicious, harmful substances usable for bioterrorism. [6]

In addition, critics take issue with how the convention is considered binding on private and public parties [14]. This aspect of the agreement, according to the US ambassadors present at the Fifth Review Conference for the convention in 2001, has the potential to interfere with legitimate industries. Disagreements over this issue led to a good degree of tension between the delegates at this conference; this tension was tabled along with the remainder of the conference, which resumed a year later [15]. In recent years, the conversation has expanded [16] to other groups who would be influenced by the Biological Weapons Convention's terms.

Throughout the 20th century, bioterrorism has typically emerged from fringe groups that are unaffiliated with larger entities. In 1984, followers of the Bhagwan Shree Rajneesh, in an effort to influence the election results in their town in Oregon, contaminated salad bars all across The Dalles, Oregon, with samples of salmonella. More than 700 residents were diagnosed with severe food poisoning as a result of the incident, but there were no deaths. The Rajneeshee bioterror attack marks the first documented case of United States bioterrorism. As it occurred in the 20th century, this event represents the relative novelty of contemporary bioterrorism. [17]

In a separate incident in 1995, Aum Shinrikyo, a Japanese religious group, was found to be in the process of weaponising anthrax. While they are most known for the 1995 sarin gas attack on the Tokyo subway, later investigations found they had hired scientists to make more deadly anthrax spores. Luckily, they were stopped before they could weaponize what turned out to be a harmless strain of anthrax intended for vaccinations, but if they were successful, they could have used the spores to kill many more people.

A high-profile case of bioterrorism involving anthrax nearly paralyzed the United States in 2001. Two U.S. senators and several news media organizations were targeted by Bruce Edwards Ivins, a vaccinologist and biodefense researcher whose anthrax attack claimed the lives of five civilians. The anthrax was enclosed in envelopes and sent directly to the intended recipients. After the ensuing panic, the United States Postal Service began irradiating all messages sent to government officials as a preventative measure. The attack renewed some of the discussion on matters of bioterrorism. [7]

This response, however, seems to indicate a generally reactive approach to bioterrorism, at least in the United States. A US Congressional commission published a report in January 2010 [8] warning that in spite of the anthrax attack on American soil, the US is still poorly prepared for another attack of that caliber. The report indicates that rapid-response capabilities are not yet implemented to respond to such threats, and that the proper management of oversight over select security and intelligence agencies has not yet taken place.

The attack, however, did help to raise global awareness of bioterrorism. In particular, the European Union assembled a Health Security Committee in October 2001 that created BICHAT [9], a program that aimed to increase the level of coordination of all European Union member states on issues of bioterrorism. Some of BICHAT's objectives included setting up an "alert and information exchange mechanism," monitoring the European Union for infectious agents; forming an index of all vaccinations and medicines available to the EU, allowing for resources to be quickly mobilized in health emergencies, and drafting rules and guidelines that nations should refer to in the case of a bioterrorist attack.

The effectiveness of these types of protocols, which have seen implementation in EU member states and certain other countries, remains to be tested by an actual bioterrorist attack; since the anthrax scare in 2001, no high-profile cases of confirmed bioterrorism have emerged. However, the worldwide panic that accompanied the H1N1 epidemic suggests a lack of

preparedness and an inability to roll out a proper response. Had H1N1 been intrinsically fatal, it may have been a greater liability. Thus, something needs to be done to ensure that the international community is equipped to handle a bioterror attack.

Country Blocs

Western Bloc

Judging from the increased participation of private parties in discussions of biological arms limitation, it appears as if the objections raised by US diplomats in 2001, though they may or may not be addressed to their satisfaction, are at least receiving the broad discussion that is merited. In light of how the issue was first handled, however, should the issue resurface, it is unlikely that European nations and the United States will see eye to eye - at least, not without a good deal of compromise.

Their relatively high population densities means that western nations, in spite of current shortcomings in procedures to deal with bioterrorist threats, stand to lose many lives in the event of a successful attack. Yet countries like the United States also police areas that would be susceptible to attack due to the added weakness of developing infrastructure. Diplomatic cables between the US and India [10] reveal worries of bioterror attacks from jihadi groups in India. In 2006, Indian intelligence revealed that these concerns were, at the time, “no longer an academic exercise.” [11]

The potential involvement of extremist Islamic groups in international bioterrorist activity could provide western nations with a strong, moral impetus to crack down on bioterrorism.

Asian Bloc

Countries in Asia would be particularly susceptible to bioterrorism, due to their extremely high population densities. However, they are becoming increasingly informed on the threats they face, as Asian countries have been conducting more research and development in the biomedical field in recent years. This rise in research has prompted countries such as Japan to work on overseeing where harmful agents are being shipped. Singapore has been noted by the Asia-Pacific Center for Biosecurity as possessing strong detection systems and good intelligence work amongst other nations in the region.

African Bloc

Africa has a high number of signatories to the Biological Weapons Convention who have yet to ratify its terms, as well as parties that have not even signed the convention. For many of these countries, however, either satisfactory progress toward ratification has been made, or other priorities have prevented these countries from considering the threat of biological weapons.

Egypt is distinct from other African countries as being the only signatory country from whom no further progress on assenting to the convention is expected. In addition, statements from US officials state that Egypt, believed to have developed the capacity to produce bioweapons by 1972, has not shown that such capabilities have been discontinued. Egyptian officials deny these claims.

Even so, several African nations possess the ability to produce bioweapons, and concerns have been raised about the integrity of these facilities from neighboring insurgents. In particular, Kenya and other nations in Eastern Africa have received assistance from the Nunn-Lugar program [12], a United States initiative, to shore up their defenses.

Middle Eastern Bloc

Most countries in the Middle East are parties to the convention. Notably absent from the list of signatories is Israel, who participated in an EU Joint Action regional seminar for the Middle East in April of 2008, but has yet to take substantive action on the Biological Weapons Convention’s terms. They are believed to have developed the capacity to produce both chemical and biological weapons, but their ambiguous response to speculation means that nobody currently knows if they still possess these capabilities.

However, Israel is not the only country suspected of retaining these capabilities. Even back in 1996, several other countries, some of which were signatories to the convention, possessed the capacity and knowledge to create bioweapons. [13]

References

[1]http://www.interpol.int/Public/Bioterrorism/news/Default.asp
[2]http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=11745
[3]https://onug.ch/80256EDD006B8954/(httpAssets)/27B1A436740E1F2FC1257507003DD1AA/$file/Preliminary+Report+on+universalization+-+distributed+19+Nov+08.pdf

[4]http://www.bt.cdc.gov/agent/agentlist-category.asp
[5]http://www.unog.ch/80256EE600585943/(httpPages)/7BE6CBBEA0477B52C12571860035FD5C?OpenDocument
[6]http://www.newsweek.com/2001/10/28/tracking-anthrax.html
[7]http://www.homelandsecurity.org/newjournal/articles/niemeyer.html
[8]http://www.washingtonpost.com/wp-dyn/content/article/2010/01/26/AR2010012601265.html
[9]http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/c11576_en.htm
[10]http://www.guardian.co.uk/world/us-embassy-cables-documents/67227
[11]http://www.guardian.co.uk/world/us-embassy-cables-documents/65230
[12]http://gsn.nti.org/gsn/nw_20101123_8958.php
[13]http://books.google.com/books?id=REcEBtmvn-kC&printsec=frontcover&source=gbs_atb#v=onepage&q&f=false
[14] http://www.cato.org/pubs/fpbriefs/fpb-061es.html
[15] http://www.nti.org/e_research/e3_7a.html
[16] http://www.thebulletin.org/web-edition/op-eds/opening-the-biological-weapons-convention-to-new-voices
[17] http://www.efilmgroup.com/News/Bioterrorism-in-Oregon.html