SECONDARY SCHOOLS' UNITED NATIONS SYMPOSIUM 2015

Disarmament and International Security Committee 2015

Chair:
Ida Mahmoudi

Vice Chairs:
Miles Khanna
Katherine Fleshner
Valeria Vendries

NOVEMBER 12-15, 2015 | MONTRÉAL, QUÉBEC

Hello and welcome wonderful delegates!

Besides the gorgeous Mont Royal and Old Port, delicious poutine and smoked meat, and my favourite university in the world (McGill, just in case there was any confusion), McGill Model United Nations is one of the most hectic, most rigorous, and most enlightening things offered in Montréal. My name is Ida Mahmoudi and I am honoured to serve as your chair for DISEC. Coming from an intensely political and Persian family, politics has followed me around from a very young age. I've participated as a delegate in several conferences, and served as Vice Chair and Chair in previous SSUNS (our fall conference) and McMUN events. Currently, I am pursuing a major in Political Science, followed by a double minor in World Islamic and Middle Eastern Studies and Communication Studies. I'm from Toronto, Ontario and like long runs up and down the soccer field. I'm also obsessed with pandas, cry while watching videos of them, and making it my life's mission to travel to Chengdu to hold one for two minutes. On the side, I serve as the incumbent Vice President Communications of the McGill Political Science Student Association, Vice President Sponsorship for McGill Women in Leadership, and teach piano as a Heart of City Piano Program volunteer. But enough about me.

Supporting me are three wonderful Vice Chairs: Katherine Fleshner, Miles Khanna, and Valeria Vendries. They're the nicest people you will ever meet, so I hope you are looking forward to an amazing few days.

Katherine is originally from Toronto and entering her fourth year here at McGill, majoring in Pharmacology. When she isn't doing MUN, she loves cooking, exercising and travelling! This will be her 3rd SSUNS conference but first on DISEC and she's very excited to work with all of you!

Miles, when not actively participating in Model UN conferences, can be seen studying Political Science at McGill. He was born in Vancouver, British Columbia where he participated in Model UN for 6 years mostly serving as a Chair or Director for numerous conferences. He is looking forward to being the Vice-Chair of DISEC and truly believes that the committee will be an enriching experience for delegates of all skill levels. In his free time, he enjoys competitive bike riding and watching movies most notably Whiplash, Grand Budapest Hotel and any film by David Fincher.

Valeria is originally from Colombia where she started doing MUN and competitive dancing as hobbies, came to Canada four years ago and is about to complete her degree in Anatomy and Cell Biology at McGill University. This will be her first and last SSUNS!

We will be covering three important, interesting, and intricate topics during this conference. First, the General Assembly will examine the potential threats to territorial sovereignty and security as a result of Cyber Terrorism. Next, DISEC aims to produce effective legislation on the production, stockpiling, and use of biological and chemical weaponry. In other words, in keeping with the theme of terrorism, the ramifications and rectifications of Bioterrorism will be explored. Finally, member states will discuss the Militarization and Weaponization of Space. These topics are mutually reinforcing and important in alleviating the several international tensions we have been witnessing. I urge delegates to search the Web (the Economist is great) for current events regarding these topics. Apart from all that, I hope you have one of the best times of your lives, and that this committee will be an amazing place to foster some amazing friendships and connections.

Just as a heads up, if there is anything you need during the conference, give us a call or shoot us an email. We are more than happy to help you out and we're excited to get to know all of you as the days go by. We're here as facilitators, true, but also as resources and hopefully friends by the end of the weekend!

I'm excited to meet you all personally. If you have any questions, feel free to email me at ida.mahmoudi@mail.mcgill.ca. See you soon!

Ida Mahmoudi

Chair

Topic 1: Maintenance of a Peaceful Space

Section 1: Background Information

The exploration of outer space has dramatically changed the world over the last century. Investment into space technology has led to novel advances in telecommunication abilities, weather forecasting and global positioning systems[1]. There is no doubt that these have improved society immeasurably. However, space technologies have the potential to be abused if placed into the wrong hands.

Since the commencement of space exploration in the 20th century, the idea of utilizing space for military purposes has existed. While the vast majority of countries have consistently come together to put measures into place to prevent the weaponization of space, a few countries, namely the United States, have been showing unwavering resistance. The role of the United Nations is to put measures in place that prevent space weaponization and ensure that current and future space technologies are used for only self-defensive military purposes as they pose a serious threat to worldwide safety.

Section 2: Origins of Space Exploration and The Outer Space Treaty

The idea of a militarized space originated during the Cold War of the 1950s. The United States and the Soviet Union engaged in a heavy arms race, both sides vying to showcase their military capabilities. One of the most famous and highly publicized areas of competition was ‘The Space Race’, where both countries competed for dominance of spaceflight technologies. The underlying premise of this race was that the winner would become the ultimate world superpower[2]. While many believed that the Space Race emerged out of mankind’s curiosity to explore worlds outside Earth, in reality, it originated from the ongoing competition to develop and display powerful nuclear weapons and missile technology[3]. The Space Race concluded in 1969 with the American moon landing and eventual collapse of the Soviet Union.

Long before the conclusion of The Space Race, however, it became apparent that space exploration and satellite capabilities could be easily abused and required both cooperation and regulation. During the United Nations General Assembly of 1959, the Committee on the Peaceful Uses of Outer Space (COPUOS) was established and mandated to recommend ways to foster cooperation between countries over the peaceful uses of space[4]. In 1966, the United Nations drafted a proposal called The Outer Space Treaty, which sought to bring countries together in agreement about the use of space for exclusively peaceful endeavors. This treaty outlines that countries must work together to ensure that space is utilized for the benefit and interests of all nations and mankind. It

[1] “Benefits Stemming From Space Exploration”, *NASA*, September 2013. https://www.nasa.gov/sites/default/files/files/Benefits-Stemming-from-Space-Exploration-2013-TAGGED.pdf

[2] "The Space Race." *History.com*. A&E Television Networks, n.d. Web. 03 June 2015. <http://www.history.com/topics/space-race>.

[3] "The Space Race." *History.com*. A&E Television Networks, n.d. Web. 03 June 2015. <http://www.history.com/topics/space-race>.

[4] "United Nations Office for Outer Space Affairs." *United Nations Committee on the Peaceful Uses of Outer Space*. United Nations, n.d. Web. 03 June 2015. <http://www.unoosa.org/oosa/COPUOS/copuos.html>.

also explicitly states that nations may not place any nuclear weapons or other weapons of mass destruction into space, in orbit or onto celestial bodies such as planets or moons[5]. This resolution, which was signed and adopted in 1967, acted as the basic framework for space law.

Section 3: Further Efforts Towards a Peaceful Space

Despite the implementation of the Outer Space Treaty, the United Nations has repeatedly voiced ongoing concerns over the future of space as a peaceful entity. In the early 2000s, it became clear that the Outer Space Treaty was not sufficient and that COPUOS was becoming increasingly ineffective as several countries continued to develop space military programs[6]. The most problematic area of the Outer Space Treaty appears to be the sole ban on weapons of mass destruction, but not other weapons. In recent years, several other draft resolutions with the same goals have been passed including 'Prevention of an Outer Space Arms Race' and the 'No First Placement of Weapons in Outer Space'. These resolutions reaffirm the need for a peaceful space and they call on countries with powerful space capabilities to pave the way towards it[7].

In 2008, China and Russia proposed the 'Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects' (PPWT). Its aim was to define the term 'weapons' more clearly in order to limit what could be brought into space as a way to prevent weaponization. This resolution was problematic, as it defined a weapon as:

> "…any device placed in outer space, based on any physical principle, which has been specially produced or converted to destroy, damage or disrupt the normal functioning of objects in outer space, on the Earth or in the Earth's atmosphere, or to eliminate a population or components of the biosphere which are important to human existence or inflict damage on them."[8]

Since this definition is so broad, as David C. DeFrieze points out, it both encompasses too much and not enough. It allows anything that could potentially be used to cause harm, if the person wielding it intends to do so, to be classified as a weapon. By this definition, a hammer would have to be outlawed, because a person intending to cause harm could do so with a hammer. Another flaw is that it does not specifically prohibit harming or killing, only the materials with which one could facilitate these acts. It is likely that an

[5] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." *United Nations Office for Outer Space Affairs*. United Nations, n.d. Web. 03 June 2015. <http://www.unoosa.org/oosa/SpaceLaw/outerspt.html>.

[6] Anup Shah. "Militarization and Weaponization of Outer Space." *Global Issues*. N.p., 13 May 2001. Web. 03 June 2015. <http://www.globalissues.org/article/69/militarization-and-weaponization-of-outer-space#USSeeksMilitarizationofSpace>.

[7] "General Assembly Adopts 63 Drafts on First Committee's Recommendation with Nuclear Disarmament at Core of Several Recorded Votes | Meetings Coverage and Press Releases." *UN News Center*. UN, 2 Dec. 2014. Web. 03 June 2015. <http://www.un.org/press/en/2014/ga11593.doc.htm>.

[8] "Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT)." *CFR.org*. Council on Foreign Relations, 5 Dec. 2011. Web. 2 June 2015. <http://www.cfr.org/space/treaty-prevention-placement-weapons-outer-space-threat-use-force-against-outer-space-objects-ppwt/p26678>.

individual that wants to do harm will surely find a way to accomplish it, meaning that moving forward will require the prohibition of causing harm to and from space[9].

Section 4: Ongoing Threat of a Militarized Space

Despite these measures, there has not been unanimous support for the maintenance of a weapon-free space. The United States of America, specifically beginning under the Bush Administration, has already quietly invested billions of dollars into space military technology[10]. America has also consistently been the only opponent of every United Nations resolution for a peaceful space, except for the 1967 Outer Space Treaty. Their argument is that currently employed technologies actually help maintain peace and that America needs military dominance in space to further eliminate vulnerability[11]. Technologies used by militaries for self-defense programs often include very precise global positioning and surveillance programs that serve two primary purposes. The first purpose is to allow countries to anticipate incoming attacks and retaliate both faster and more precisely than with technology on Earth. As a result of this first purpose, space military defense systems can serve to intimidate or discourage aggressors from initiating attacks[12].

While many individuals support this program under the guise of increased anti-terrorism efforts and defense systems, it is hard to discount a possible underlying motive of furthering their own national interests and becoming a stronger military power. Similarly, many attribute China and Russia's strong opposition of space weaponry to fear of American military dominance. This is where the militarization and weaponization of space becomes a slippery slope. In fact, in response to America's development of a space weapons program, other countries such as Japan, China and India have begun development of their own space military programs, including missiles and other anti-satellite technology[13]. The European Union has also been working on satellite technologies to rival American ones.[14]

Section 5: Why Must Space Be Kept Peaceful?

Throughout the last century, as space technology improved, the world became more reliant on it. Space technologies have profoundly impacted the way the world operates

[9] David C DeFrieze. "Defining and Regulating the Weaponization of Space." International Relations And Security Network, 18 Aug. 2014. Web. 03 June 2015. <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182863>.

[10] Tim Weiner. "Air Force Seeks Bush's Approval for Space Weapons Program." The New York Times, 18 May 2005. Web. 3 June 2015. http://www.nytimes.com/2005/05/18/business/air-force-seeks-bushs-approval-for-space-weapons-programs.html.

[11] Anup Shah. "Militarization and Weaponization of Outer Space." *Global Issues*. N.p., 13 May 2001. Web. 03 June 2015. <http://www.globalissues.org/article/69/militarization-and-weaponization-of-outer-space#USSeeksMilitarizationofSpace>.

[12] David C DeFrieze. "Defining and Regulating the Weaponization of Space." International Relations And Security Network, 18 Aug. 2014. Web. 03 June 2015. <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182863>.

[13] Anup Shah. "Militarization and Weaponization of Outer Space." *Global Issues*. N.p., 13 May 2001. Web. 03 June 2015. <http://www.globalissues.org/article/69/militarization-and-weaponization-of-outer-space#USSeeksMilitarizationofSpace>.

[14] Ambrose Evans-Pritchard. "EU Agrees Satellite System to Rival US." *The Telegraph*. Telegraph Media Group, 6 Apr. 2001. Web. 03 June 2015. <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1315476/EU-agrees-satellite-system-to-rival-US.html>.

through satellite technologies, whether through communication, global positioning or weather forecasting. These technologies have also enabled better surveillance and prediction of natural disasters, saving a countless number of human lives. There is no doubt that if space were to become an arena for combat, these vital technologies would be at risk, which would compromise both the global economy and human safety. Considering how many satellites are shared among nations [15] and space-based technologies that are used worldwide, there is no doubt that a combat in space between two countries would affect the rest of the world. What's more, with the ongoing development of more plentiful and powerful space weapons, the threat of mutual assured destruction grows greater as well.

Space debris is another issue that would be aggravated with the use of space for military purposes. Every time an attack would destroy or break off part of a space weapon or satellite, it would create a lot of space debris. Since these objects are orbiting the Earth, they are travelling at great speeds. Anything they collide with, such as satellites or space stations, will create a powerful and devastating impact. Currently, the US Air Force tracks 13,000 objects that orbit the Earth, 94% of which is space debris. There are also an estimated 100,000 additional bits of space debris that are about the size of a softball or smaller[16]. There is already an ample amount of space debris that governments are constantly monitoring, and space combat would only increase this burden.

Section 6: Conclusion

Currently, space is used for benevolent purposes. Communications and global positioning technologies as well as self-defense systems both improve and protect mankind. However, despite agreements in the past, the future of space as a peaceful domain remains unclear. Most countries agree that weaponization of space would lead to an arms race that would promote tension among big countries with space capabilities and would threaten the safety of the global population. Thus, the future of space as a peaceful entity will rely on the cooperation and commitment of countries that currently possess space capabilities as well as pressure from countries that do not currently possess these capabilities. Countries must also work together to set better and more specific framework for the military acts of weaponization and attack. The fate of military defense systems will also rely on such cooperation and likely will need to be strictly regulated. If this cooperation can be achieved, a peaceful future for space is possible.

Questions to Consider:

1. How can we incentivize countries to stop development of space military programs?

[15] Victoria Samson. "Space Weapons Cause Problems." *Project On Government Oversight*. N.p., 15 July 2005. Web. 03 June 2015. <http://www.pogo.org/ourwork/straus-military-reform-project/conflict/2005/space-weapons-cause-problems.html>.

[16] Victoria Samson. "Space Weapons Cause Problems." *Project On Government Oversight*. N.p., 15 July 2005. Web. 03 June 2015. <http://www.pogo.org/ourwork/straus-military-reform-project/conflict/2005/space-weapons-cause-problems.html>.

2. What steps can be taken to foster cooperation over a military and weapon-free space?
3. How can we regulate the use of military defense systems to ensure that they are used solely for defense purposes?

Works Cited:

DeFrieze, David C. "Defining and Regulating the Weaponization of Space." International Relations And Security Network, 18 Aug. 2014. Web. 03 June 2015. <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182863>.

Evans-Pritchard, Ambrose. "EU Agrees Satellite System to Rival US." *The Telegraph*. Telegraph Media Group, 6 Apr. 2001. Web. 03 June 2015. <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1315476/EU-agrees-satellite-system-to-rival-US.html>.

"General Assembly Adopts 63 Drafts on First Committee's Recommendation with Nuclear Disarmament at Core of Several Recorded Votes | Meetings Coverage and Press Releases." *UN News Center*. UN, 2 Dec. 2014. Web. 03 June 2015. <http://www.un.org/press/en/2014/ga11593.doc.htm>.

Samson, Victoria. "Space Weapons Cause Problems." *Project On Government Oversight*. N.p., 15 July 2005. Web. 03 June 2015. <http://www.pogo.org/our-work/straus-military-reform-project/conflict/2005/space-weapons-cause-problems.html>.

Shah, Anup. "Militarization and Weaponization of Outer Space." *Global Issues*. N.p., 13 May 2001. Web. 03 June 2015. <http://www.globalissues.org/article/69/militarization-and-weaponization-of-outer-space#USSeeksMilitarizationofSpace>.

"The Space Race." *History.com*. A&E Television Networks, n.d. Web. 03 June 2015. <http://www.history.com/topics/space-race>.

"Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT)." *CFR.org*. Council on Foreign Relations, 5 Dec. 2011. Web. 2 June 2015. <http://www.cfr.org/space/treaty-prevention-placement-weapons-outer-space-threat-use-force-against-outer-space-objects-ppwt/p26678>.

"Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." *United Nations Office for Outer Space Affairs*. United Nations, n.d. Web. 03 June 2015. <http://www.unoosa.org/oosa/SpaceLaw/outerspt.html>.

"United Nations Office for Outer Space Affairs." *United Nations Committee on the Peaceful Uses of Outer Space*. United Nations, n.d. Web. 03 June 2015. <http://www.unoosa.org/oosa/COPUOS/copuos.html>.

United States. NASA. International Space Exploration Coordination Group. Benefits Stemming From Space Exploration. NASA, Sept. 2013. Web. 26 May 2015. <https://www.nasa.gov/sites/default/files/files/Benefits-Stemming-from-Space-Exploration-2013-TAGGED.pdf>.

Weiner, Tim. "Air Force Seeks Bush's Approval for Space Weapons Program." The New York Times, 18 May 2005. Web. 3 June 2015. <http%3A%2F%2Fwww.nytimes.com%2F2005%2F05%2F18%2Fbusiness%2Fair-force-seeks-bushs-approval-for-space-weapons-programs.html>.

Topic 2: Cyberterrorism

Section 1 : Background Information

The Federal Bureau of Investigation has defined cyberterrorism as a *"politically motivated attack against computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."*. [17] Cyberterrorism is a form of terrorism that involves computer networks and the public Internet in order to cause destruction for a personal objective. Cyberterrorism is an effective way to instigate fear or intimidate a society towards an ideological goal. However, cyberterrorist attacks are also more than capable of causing physical violence and even extreme financial harm. This leaves banking industries, power plants, and air traffic control centres all as viable targets.[18]

Cyberterrorism is, unfortunately, unpredictable. Eugene Kaspersky who serves as the co-founder of the Global IT Security Firm explains that *"It's not easy to predict what will happen, but the worst terrorist attacks are not expected."* This implies that cyberterrorism is truly erratic, making it one of the most lethal forms of terrorism in this day and age.[19] The Disarmament and International Security Committee truly places an emphasis on topics dealing with international issues and threats that impact security, which is why the committee feels that it is necessary to resolve this reoccurring conflict.

The History of Cyberterrorism

Cyberterrorism was a term created by Barry Collin, who worked for the Institute for Security and Intelligence. This form of terrorism has been traced back all the way to the **1980's.** It began with a PC virus known as "The Brain", which was first made in Pakistan. Two brothers, Basit Farooq Alvi and Amjad Farooq Alvi, had programmed the virus in order to infect the boot sector of media. The Brain is only a minor case of cyberterrorism in comparison to the other examples.[20]

In **1994,** a Russian hacker known as Vladimir Levin and his brilliant followers broke into Citibank's computer systems and managed to steal millions of dollars. He was sentenced to merely three years in prison.[21]

[17] Rouse, M. (n.d.). What is cyberterrorism? Retrieved June 25, 2015.

[18] Rouse, M. (n.d.). What is cyberterrorism? - Definition from WhatIs.com. Retrieved June 2, 2015, from http://searchsecurity.techtarget.com/definition/cyberterrorism

[19] Ellyatt, H. (2015, January 27). Beware: A national cyberterrorism attack may loom. Retrieved June 2, 2015, from http://www.cnbc.com/id/102367777

[20] Keefe, M. (2009, April 27). A short history of hacks, worms and cyberterror. Retrieved June 2, 2015, from http://www.computerworld.com/article/2523672/government-it/a-short-history-of-hacks--worms-and-cyberterror.html

[21] 19, A. (1995, August 19). Hacking Theft of $10 Million From Citibank Revealed. Retrieved June 2, 2015, from http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system

In **1996,** a group of hackers broke into the websites of the United States Department of Justice, the Central Intelligence Agency, and the United States Air force. Allegedly, the hackers attempted to breach the defense department files more than 250,000 times in one year. However, less than 65% of the attempts were actually effective. [22]

Closer to the **21st century,** there had seemed to be a persistent fear over the '*millennium bug'*. Essentially, the millennium bug was used to provoke fear of what could have been a detrimental cyberattack. It's true purpose was to threaten corporations, finance companies, and a handful of government agencies. Interestingly enough, the millennium bug was created as an accident from a simple programming error.[23]

https://cdn.psychologytoday.com/sites/default/files/field_blog_entry_images/CyberTerrorism.jpg

Section 2: When is it considered Cyberterrorism?

Many have felt that the term cyberterrorism is inappropriate and often misused. In many situations, an actual cyberattack only causes irritations, as opposed to actual terror. However, there is also another side that argues that any form of a computer attack deserves to be deemed as cyberterrorism regardless of how mild or severe the attack is. That being said, there have been two views established when defining the term 'cyberterrorism.' The first one is **"Effects-based". Effects-based** is used to describe a computer attack that causes fear similar to other 'traditional' forms of terrorism. The next view is **"Intent based"** which involves a much more politically motivated attack, used to spread fear to the government or simply advocate for a political objective. [24]

[22] Anthes, G. (1996, August 1). Attack highlights Web security risks. Retrieved June 25, 2015.

[23] Morgan, K., & Oppenheimer, L. (n.d.). WiseGeek. Retrieved June 2, 2015, from http://www.wisegeek.com/what-is-the-millennium-bug.htm

[24] Rollins, J., & Wilson, C. (2007, January 22). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. Retrieved June 2, 2015, from https://www.fas.org/sgp/crs/terror/RL33123.pdf

Why is cyberterrorism becoming more and more of an 'attractive' option for terrorists? Traditionally speaking, cyberterrorism is far cheaper than other terrorist methods. Fundamentally, the terrorist only needs a computer and an online connection as opposed to guns and explosives. Another advantage of cyberterrorism is the anonymity factor. Terrorists can rely on code names, proxy servers, and anonymous accounts making it problematic for security agencies to be able to track down their real identity.

The number of potential targets is endless. As mentioned before, the most common targets for cyberterrorists are government computers, public utilities, and airline companies. With the growing number of targets come an inevitable amount of loopholes for the terrorists to find. The United States Institute of Peace (USIP) has conducted a study showcasing how vulnerable critical infrastructures are to any general cyberterrorist. These infrastructures need to rely on computer systems that are highly complicated in nature, which can make it difficult for a terrorist to find any weaknesses. [25]

Another key advantage to cyberterrorism is that the method can be pursued remotely. Simply put, cyberterrorism requires far less physical training, mental investment, and conventional travel, which make it extremely inevitable for a terrorist group to recruit countless followers.

One aspect that cyberterrorists admire is any form of media coverage. Cyberterrorism is capable of affecting more people as opposed to traditional terrorist methods, as shown by the "I love you" virus. (A computer worm that infected millions of computers.) [26]

Section 3: Classifying the Cyberterrorists

Michael Vatis who had served as the former head of the FBI's cyberterrorism unit has classified cyberterrorists into four general categories. The first category merely identifies as them as **'terrorists.'** Only a handful of acclaimed terrorist groups have actually relied on cyberattacks as an actual method of destruction. Recently, more and more terrorist groups have become invested into the practice and it seems inevitable that the popularity of cyberterrorism will only increase.

The second group is identified as **'nation states.'** Simply put, countries such as North Korea, Iran, Sudan, and Libya have recently developed information warfare capabilities that are more than capable of harming their enemies. Furthermore, China has recently become extremely invested in cyber warfare activities.[27]

[25] Weimann, G. (2004, December 1). Cyberterrorism How Real Is the Threat? Retrieved June 2, 2015, from http://www.usip.org/sites/default/files/sr119.pdf

[26] Seltzer, L. (n.d.). 'I Love You' Virus Turns Ten: What Have We Learned? Retrieved June 2, 2015, from http://www.pcmag.com/article2/0,2817,2363172,00.asp

[27] Powers, S. (n.d.). The Threat of Cyberterrorism to Critical Infrastructure. Retrieved June 2, 2015, from http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/

The third group is identified as **"Terrorist Sympathizers."** This group has been proven to have a higher chance of actually carrying through with the attack. In a hypothetical situation, if a campaign created by the US government is perceived as 'insulting' to the beliefs of a terrorist group then the same terrorist group will feel provoked to launch cyberattacks against the United States for creating the campaign.

The fourth and final group identifies the cyberterrorists as **"Thrill Seekers"** or simply put **"cyberjoyriders".** This group is certainly the least threatening, but still potentially detrimental. These hackers essentially want to gain 'popularity' through an array of high profile attacks. The *2000 DoS attack* is a prime example of why this group still needs to be perceived as a perilous threat.[28]

It is important to note that the first three categories are entirely related to terrorism while there really is only a minor chance that the last category will engage in a serious act of cyberterrorism.

Section 4: Proposed Solutions:

What solutions can the government and society undertake to prevent these acts of cyberterrorism? A few years ago, the United Nations had developed universal 'instruments' in order to combat terrorism through a global plan. Yet the primary issue was that it had never accounted for Internet terrorism in its plan. Shortly after, a paper written by Barry Collin outlined a series of potential resolutions that can be used to combat cyberterrorism.

- ***"We must accept that while the theories of terrorism stand true, the way in which we approach counter-terrorism, in this case, counter-Cyberterrorism, must change.***
- ***We must cooperate and share intelligence in ways we have never have before.***
- ***We must enlist the assistance of those individuals who understand the weapons we are facing and have experienced fighting these wars.***
- ***We must learn the new rules, the new technologies, and the new players."***[29]

In 2001, the Council of Europe proposed the Convention on Cybercrime. It serves as the only international treaty that focuses on law violations over the Internet or any other networks. It requires any states to update their laws against hacking and other cyber

[28] Weimann, G. (n.d.). Cyberterrorism: The Sum of All Fears? Retrieved June 2, 2015, from http://www.princeton.edu/~ppns/Docs/State Security/Cyberterrorism - sum of all fears.pdf

[29] Collin, B. (n.d.). The Future of CyberTerrorism:. Retrieved June 2, 2015, from http://www.egov.ufsc.br/portal/sites/default/files/anexos/29436-29454-1-PB.html

activities deemed illegal. Currently, only 8 out of 42 European countries have signed this process.[30]

Currently, the European Union has proposed the Critical Information Infrastructure Research Coordination Office, which strives to determine exactly how its member states can protect their infrastructures from any level of cyberattack. This project serves to identify any research groups and programs concentrated on IT security and critical infrastructures.[31] Because the Disarmament and International Security Committee places an emphasis on resolving issues that can be detrimental towards international security, it is imperative that the committee can look for long-term solutions to this conflict.

Case Study (The Estonian Cyber war of 2007):

One of the most distressing acts of cyberterrorism was the cyberattack on Estonia in 2007. Starting in April 2007, a group of hackers had released a series of cyberattacks that severely damaged hundreds of government and corporation sites in Estonia. The authorities tracked the attacks all the way to Russia; reports suggested the Kremlin might have been accountable. Later, this accusation was inevitably denied by Moscow.[32]

This online incident was the result of Estonia’s choice to move a Soviet World War 2 memorial from downtown Tallinn. This instigated protesters who were outraged with Estonia’s decision. Throughout the process it was reported that more than 100,000 computers were required in order to coordinate the attacks against the government banks and agencies. [33]

Despite the persisting anger, a group of Russian activists that identify as a pro-Kremlin youth group said they were responsible. The group known as Nashi is based in Transnistria. They relied on a series of techniques such as ping flogs and botents in order to attack every government website. It was these extremely complex methods that prompted the Estonian government to blame the Russian government. Understandably, the bronze statue of Tallinn was important to the people. It had served as a soviet-era war symbol. [34]

[30] Council of Europe - ETS No. 185 - Convention on Cybercrime. (n.d.). Retrieved June 2, 2015, from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[31] Moteff, J. (2015, May 12). Critical Infrastructures: Background, Policy, and Implementation. Retrieved June 2, 2015, from https://www.fas.org/sgp/crs/homesec/RL30153.pdf

[32] Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. Retrieved June 2, 2015, from http://www.theguardian.com/world/2007/may/17/topstories3.russia

[33] Rehman, S. (2013, January 14). Estonia's Lessons in Cyberwarfare. Retrieved June 2, 2015, from http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

[34] Nashi exposed. (2012, February 9). Retrieved June 2, 2015, from http://www.economist.com/blogs/easternapproaches/2012/02/hackers-and-kremlin

The consequences were dire. The North Atlantic Treaty organization had immediately improved its cyber-war capabilities and established an entire cyber defence research centre in Tallinn nearly a year later. Furthermore, they had contacted the European Union in order to make cyberattacks a severe criminal offense. In 2009, the FBI had stated they would base an entire computer crime expert in Estonia in order to combat any international threats that go against their computer systems. [35]

Section 5: Conclusion

It is clear that cyberterrorism is one of the most dangerous acts of terrorism that affects us today. Cyberterrorism has become such a popular form of terrorism mainly because of the convenience and anonymity. Despite past proposed solutions, cyberterrorism still persists as an internationally threatening issue. While the actual definition of cyberterrorism has been debated, many countries are still at risk despite having protection from NATO or the EU.

Questions to Consider

What are the key elements of cyberterrorism and what kinds of methods can be used to prevent cyberattacks?

What exactly is the appeal of cyberattacks to terrorists and how has this changed in the past 20 years?

What have previous cases of cyberterrorism taught us and if so can we learn from these cases?

What has the government done to combat cyberterrorism? Are they relying on effective strategies?

What should the repercussions be to cyberterrorists? Are they to share the same penalty as other terrorists?

Helpful links

http://list25.com/25-biggest-cyber-attacks-in-history/5/

http://penguinrandomhouse.ca/hazlitt/blog/timeline-cyberwar-and-cybercrime

http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/

http://iconof.com/blog/cybercrime-cyberterrorism-inducing-anxiety-fear-on-individuals/

[35] A look at Estonia’s cyber attack in 2007. (2009, July 8). Retrieved June 2, 2015, from http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.VWwrz1xViko

http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Sources

Rouse, M. (n.d.). What is cyberterrorism? - Definition from WhatIs.com. Retrieved June 2, 2015, from http://searchsecurity.techtarget.com/definition/cyberterrorism

Ellyatt, H. (2015, January 27). Beware: A national cyberterrorism attack may loom. Retrieved June 2, 2015, from http://www.cnbc.com/id/102367777

Keefe, M. (2009, April 27). A short history of hacks, worms and cyberterror. Retrieved June 2, 2015, from http://www.computerworld.com/article/2523672/government-it/a-short-history-of-hacks--worms-and-cyberterror.html

19, A. (1995, August 19). Hacking Theft of $10 Million From Citibank Revealed. Retrieved June 2, 2015, from http://articles.latimes.com/1995-08-19/business/fi-36656_1_citibank-system

Rollins, J., & Wilson, C. (2007, January 22). Terrorist Capabilities for Cyberattack: Overview and Policy Issues. Retrieved June 2, 2015, from https://www.fas.org/sgp/crs/terror/RL33123.pdf

Weimann, G. (2004, December 1). Cyberterrorism How Real Is the Threat? Retrieved June 2, 2015, from http://www.usip.org/sites/default/files/sr119.pdf

Seltzer, L. (n.d.). 'I Love You' Virus Turns Ten: What Have We Learned? Retrieved June 2, 2015, from http://www.pcmag.com/article2/0,2817,2363172,00.asp

Powers, S. (n.d.). The Threat of Cyberterrorism to Critical Infrastructure. Retrieved June 2, 2015, from http://www.e-ir.info/2013/09/02/the-threat-of-cyberterrorism-to-critical-infrastructure/

Weimann, G. (n.d.). Cyberterrorism: The Sum of All Fears? Retrieved June 2, 2015, from http://www.princeton.edu/~ppns/Docs/State Security/Cyberterrorism - sum of all fears.pdf

Collin, B. (n.d.). The Future of CyberTerrorism:. Retrieved June 2, 2015, from http://www.egov.ufsc.br/portal/sites/default/files/anexos/29436-29454-1-PB.html

Council of Europe - ETS No. 185 - Convention on Cybercrime. (n.d.). Retrieved June 2, 2015, from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Moteff, J. (2015, May 12). Critical Infrastructures: Background, Policy, and Implementation. Retrieved June 2, 2015, from https://www.fas.org/sgp/crs/homesec/RL30153.pdf

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. Retrieved June 2, 2015, from http://www.theguardian.com/world/2007/may/17/topstories3.russia

Rehman, S. (2013, January 14). Estonia's Lessons in Cyberwarfare. Retrieved June 2, 2015, from http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

Nashi exposed. (2012, February 9). Retrieved June 2, 2015, from http://www.economist.com/blogs/easternapproaches/2012/02/hackers-and-kremlin

A look at Estonia's cyber attack in 2007. (2009, July 8). Retrieved June 2, 2015, from http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.VWwrz1xViko

Topic 3: Bioterrorism

Section 1: Background Information

Bioterrorism is described as any attack caused by the release of pathological agents such as viruses, bacteria, and modified toxins; with the purpose of threatening the mass population or a specific population[1]. Both biological and chemical weapons fall into the category of weapons of mass destruction WMD, according to the original definition given by the UN and the international community[2]. With increasing research and technological advances in the development of such, there is a concern that they might be used for terrorist purposes, posing a threat to the worlds international peace, security, economy and health[3].

Chemical and biological weapons pose a real threat. They have been used in the past and have been historically responsible for affecting many civilians ever since the First World War, when political tensions increased and countries became interested in more effective weapons to threaten their enemies[2]. Many countries still hold an active biological weapon program, some of which are still not signatories of The Biological and Toxic Weapon Convention or the Chemical Weapon Convention. This hinders the inspection, supervision of production, and regulation of these weapons[4].

Such infectious agents may be relatively easy and inexpensive to obtain.[4] They can be produced in any research or basic facility from a large variety of pathogens that can be obtained from crops, animals, or human diseases. In addition, they have multiple means of delivery; they can be spread via air dissemination, via contact with contaminated water or food, or from person to person[1, 3, 4]. (**Figure 1**)

One of the main issues concerning this type of warfare is that biological and chemical agents may be silently released making it difficult to detect if an attack has been made until someone already presents symptoms of infection or illness[1]. Despite the fact that there are many agencies and research centers that focus on prevention, currently, there are no effective means of detection. Therefore, one of the main questions is how to develop better monitoring systems and increase public preparedness.[36]

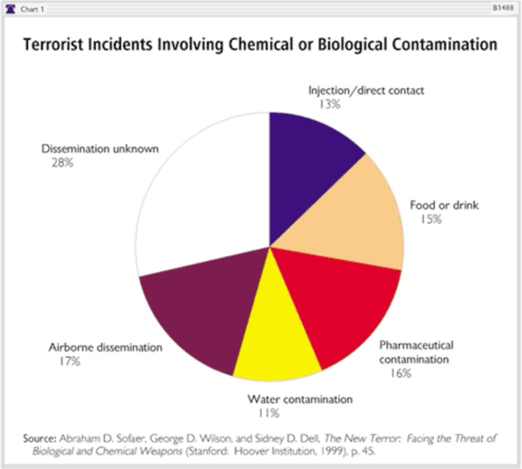
[36] "Bioterrorism Overview." Centers of Disease Control and Prevention. 1 Feb. 2007. Web. 6 May 2015.

[2] Carus, W. Seth. "Defining Weapons of Mass Destruction". (n.d) Jan. 2012. Web. 12 Apr. 2015

[3]"Biological Threats." Ready. Web. 1 May 2015.

[4] Spencer, Jack, and Michael Scardaville. "Understanding the Bioterrorist Threat." The Heritage Foundation Backgrounder (2001). Web. May 2015

Figure 1: Means of delivery



Source: Abraham D. Sofaer, George D. Wilson, and Sidney D. Dell, *The New Terror: Facing the Threat of Biological and Chemical Weapons* (Stanford: Hoover Institution, 1999), p. 45.

Retrieved from: Spencer, Jack, and Michael Scardaville. "Understanding the Bioterrorist Threat." The Heritage Foundation Backgrounder (2001)[4].

Section 2: Agents Commonly Used for Biological Warfare

The factors listed in **Table 1** are key determinants for the likelihood of an agent being used over another for a bioterrorist attack.

Table 1: Summary of Common agents to be used in Bioterrorism

Name	Category	Characteristics
Antrax	Bacterium	• Found in nature and easy to culture in the lab • Low amounts are effective • Disseminates easily • High lethality. Vaccine available to treat anthrax from skin contact, but ineffective to treat inhaled anthrax. • Easy to weaponized
Smallpox	Virus	• Difficult to obtain • Moderate lethality and little vaccine available
Ricin	Toxin	• Easy to obtain and process • High lethality • Requires high amounts
Sarin	Chemical Gas	• Nerve agent • Artificially synthetized (not naturally occurring) • High toxicity, rapid

		action
Chlorine	Chemical Gas	• Commonly manufactured, found in household products, modified into the form of a poisonous gas.

Anthrax (*Bacillus antracis*)

Anthrax has historically been used as a weapon in terrorist attacks and continues to be a potential threat. Anthrax spores are easily found in nature and spread easily. Thus, only small amounts are required to affect many people. It can be easily delivered, released into the air, or placed in food or water. Furthermore, it has long lasting effects since the spores can stay active for extended periods of time in the environment.[1]

Additional information:

- Anthrax was used by the Germans during World War I to silently infect horses and livestock to be delivered to the USA and other enemy countries.[1,4,5]
- Another well documented case of an anthrax attack was during the 1930's when Japan performed Bio-warfare research in northeastern China. Many people died as a result of the human testings and the anthrax released from aircrafts above 11 cities[6].
- In the Soviet Union in 1979, the largest case of inhaled anthrax in humans was documented from an accidental outbreak from a military microbiology research facility. Different versions exist as to what triggered the accident; the Soviet Union claimed it was due to defective air filters in the facility. Other investigations on the case claimed that the activities being carried out by the facility were not in agreement with the Biological Weapon Convention [4,7]

Case Study: Amerithrax, the case of anthrax mailings US

In 2001, letters containing powdered Anthrax were intentionally mailed around the USA and targeted to specific individuals, including senators and media agencies. As a result, twenty-two people were infected with anthrax, five of which died. In addition to the targeted people, the spores also affected the postal workers and others who came in contact with these letters. Though tragic, this episode gave the world a fuller understanding of the vulnerability and risk of exposure of biological and chemical weapons. Furthermore, it displayed how easily anthrax can be spread and go undetected. The FBI investigated the case and concluded the investigation seven years later. The origin of the anthrax strain was determined to be a research laboratory in the state of Maryland, and they found a pathologist named Bruce Irvin to be responsible for the production and delivery[8]. This case illustrates the balance between the use of bioresearch for peaceful and productive applications and the misuse for bioterrorist or hostile purposes if they fall in the wrong hands. [37]

[5] Riedel, Stefan. "Biological Warfare and Bioterrorism: A Historical Review."*Proceedings (Baylor University. Medical Center)* 17.4 (2004): 400–406. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1200679/.

Ricin

Pellets with lethal Ricin can be used as a method to silently assassinate people. One well documented example occurred in 1978 in Bulgaria, where the secret police used the tip of an umbrella to infect a dissident to the Bulgarian communist regime, Georgi Markov[9,10].

Smallpox

Smallpox is also considered to be a possible biological weapon, as the disease is highly infectious and associated with a high mortality rate. There are also few available vaccines and no effective treatment.[4,11]

Section 3: Bioweapons Programs

The United States bioweapons program started in 1942 with the intention to prepare against possible attacks from Germany. Anthrax bombs and other Biowarfare were developed and tested, as well as potential vaccines to protect their soldiers. This program was further expanded during the Korean War. In the 1970's, after the Convention on the Prohibition of the Development, Production, and Stockpiling of Biological and Toxin Weapons and on their Destruction, the United States, possessing a large stock of these weapons decided to take a different approach and switch from an offensive bioweapon programme to a prevention and preparedness oriented program[1]. China's Biowarfare program started in the 1950's, and it is currently classified as a proliferation concern along with other countries such as North Korea, Libya and Syria, who are thought to be in possession of toxic materials and the necessary infrastructure to subsequently produce weapons[4].

Section 4: Treaties and efforts concerning the use Biological and Chemical weapons

Ever since the 1960's, there have been many efforts towards the implementation of measures that prevent the use of biological weapons. Despite the existence of multiple treaties, it is nearly impossible to ensure compliance to anti-proliferation obligations.

The Geneva Protocol for the prevention of wartime usage of asphyxiation, poisoning and other bacteriological methods of warfare was created after the First World War as the first attempt to limit the use of biowarfare. However, this treaty was ineffective at limiting the research or production of this weapons.[12]

[6] KRISTOF, NICHOLAS. "Unmasking Horror -- A Special Report.; Japan Confronting Gruesome War Atrocity." The New York Times 17 Mar. 1995. Web. .

[7] Meselson, M. "The Sverdlovsk Anthrax Outbreak of 1979." Science (1994): 1202-8. Web. .

[8] "Amerithrax or Anthrax Investigation." The FBI Bureau of Investigation. Web. .

[9] "When Ricin Was Used to Kill." BBC News 13 Apr. 2005. Web. .

[10] "Ricin and the Umbrella Murder." CNN. 23 Oct. 2003. Web. .

[11] Inglesby, TV. "Consensus Statement: Smallpox as a Biological Weapon: Medical and Public Health Management." Journal of the American Medical Association 281.22 (1999): 2127-137. Centers of Disease Control and Prevention. Web. .

The Convention on the Prohibition of the Development, Production, and Stockpiling of Biological and Toxic Weapons and on Their Destruction: This treaty was ratified in 1972 to address the issue of production and stockpiling of these agents. This treaty also addressed the issue of production, requiring state parties to destroy their biowarfare arsenal[12].

The Chemical Weapons Convention (CWC) and the Biological Weapons Convention: This was created with the purpose of prohibiting development, production, stockpiling, transfer or use of chemical and biological weapons[13]. However, there is a concern that it lacks measures to ensure strict compliance to the conventions. Deadlines to destroy the remaining weapons have not effectively been met, and methods of verification are absent. Nations are currently working to create amendments that enforce and encourage compliance towards the treaty and the Organization for the Prohibition of Chemical Weapons (OPCW)[12,14].

The new START treaty: This exists between the United States and the Russian Federation in an effort to limit the use of strategic offensive arms. This treaty has shown great promise as progress has already been made using reliable verification and inspection methods[15,12].

The Non Proliferation Treaty (NPT): This is a keystone treaty to prevent the proliferation of WMD and to pursue international peace and security. Nations are still working towards strengthening it and call upon all states to sign it[15, 38]

Section 5: The Threat Nowadays

For the international community, the most concerning possibility surrounding the existence of biological warfare is the potential acquisition by non- state actors and terrorist groups. The lack of effective treaties and regulation make this issue even more prominent. Deliberate use of such weapons of mass destruction would pose major concerns for human health and the environment. Therefore, it is at the upmost importance for nations to enhance protection measures and to ultimately eliminate all biological and

[12] "First Committee, in Draft Resolution, Seeks Cooperation of Syrian Authorities, Organisation for the Prohibition of Chemical Weapons, on Outstanding Issues." United Nations Meetings Coverage and Press Releases. 3 Nov. 2014. Web. .

[13]"Chemical Weapons Convention." ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS. Web. .

[14]"Recent Battlefield Use of Chemical Weapons, Absence of Verification Mechanism for Biological Weapons Ban Trigger Strong Rebuke in First Committee." United Nations Meetings Coverage and Press Releases. 24 Oct. 2013. Web. .

[15]"Recent Use of Chemical Weapons 'Stark and Horrific Reminder' of Duty to Eliminate Them, Speaker Tells First Committee as It Continues Full-scope Debate." United Nations Meetings Coverage and Press Releases. 8 Oct. 2013. Web..

[16]"New START." U.S Department of State. Web. .

[17] Borger Julian. "Syrian Chemical Attack used Sarin and was worst in 25 years says UN": The Guardian. Sept. 2013. Web. 12 Apr.2015

[18]"Syria's Chemical Weapons Stockpile": BBC news. Jan 14.2015. Web. 12 Apr.2015.

chemical weapons to keep them from falling in the wrong hands and being used for hostile purposes[16,17].

Case Study: The Gouta Chemical Attack

On August 21st 2013, a release of Sarin chemical Gas from rockets affected 3,000 civilians in Damasco-Syria. The United Nations classified this "the worst chemical weapons attack in 25 years"[17,18]. This attack was a wake-up call to the international community as a reminder that these weapons are a real threat even in modern days.

The attack is thought to be conducted by the Syrian regime against the opposition. In April and May, previous chlorine gas attacks against small villages in Syria were also reported by the OPCW. During First Committee meetings, several delegations have condemned the use of chemical weapons in Syria, and many called it an unacceptable "crime against its own people". The international community expressed its deep concern that if the Syrian regime had already used chemical weapons against its own people, nothing would prevent it from doing it again. For a long time, Syria had been denying the existence of a chemical weapons program, but the reports from the OPCW and the recent Sarin and chlorine attacks have shown otherwise.

Syria acceded to join the Chemical Weapons Convention, and to work in conjunction with the OPCW and the United Nations. Steps are being taken towards destroying existing weapons in the Syrian territory, eliminating Syria's chemical weapons programme, and implementing inspection mechanisms in the declared sites of the region. The international community is determined to have the Syrian government follow up, cooperate, and comply with the obligations under the CWC. The Syrian Government has declared all its intentions to cooperate to the abolishment of such weapons, but still defends the regime as innocent[12,13,14].

http://media.worldbulletin.net/news/2014/02/28/kimyasal-suriye.jpg

Case study: ISIS and Chemical Weapons

Recently, attention has been dragged to the militant group Islamic State ISIS, and their intention to build a chemical weapons arsenal by recruiting trained professionals. There is already evidence of the use of chlorine chemical gas against Iraqi soldiers. Additionally, the terrorist group recently took control over an abandoned chemical weapon facility that belonged to Saddam Hussein in Iraq with the intention of utilizing the old stockpiles to develop new weapons[19,20].

Bio- preparedness/Biodefense and Response

Public awareness of biological and chemical weapons and response training in case of an attack is essential to prevent and mitigate the effects of bioterrorism. The establishment of research facilities and detection systems are also important steps to prevent, respond, and find treatment options after an attack. For example, the Centre of Disease Control and Prevention (CDC) in the United States conduct research in specialized laboratories and develop monitoring systems that both detect releases of toxic substances and accelerate the process of diagnosis by doctors[1].

Section 6: Conclusion

Both past and recent episodes involving biological and chemical weapons have demonstrated their potential for destruction. Furthermore, there is a huge risk associated with weapons falling into the wrong hands that pose a threat to the international peace and security.

The international community is committed to preventing such attacks from occurring again, and these efforts involve the destruction of existing weapons, effective prohibition of their development accompanied with the appropriate verification mechanisms, and to ensure the peaceful uses of life sciences. The existence of diplomatic attempts, such as the various aforementioned treaties, is very important towards the achievement of this goal. However, questions of sovereignty, the malintention of some nations, and the various gaps in the content of such treaties have made it difficult to achieve unanimity.

The question of bio-preparedness and public awareness also must be addressed. Security efforts, proper infrastructure, preventive research, and the appropriate controls of the transport and use of such agents are important factors that the international community should focus on.

Questions to consider

1. Which countries should be or not be allowed to develop/maintain a biowarfare program? Under which conditions and regulations?
2. Is there a way to make sure a country that claims its program is for defense purposes is actually for defense and not for offense? Should there even be a need for defense programmes if the ultimate goal is the eradication biological and chemical weapons?

3. How easy is it for outlaw groups to have access to toxic agents and weaponized them?
4. How can the UN, the OPCW and other organizations make sure nations are complying the regulations and obligations under the treaties?
5. Are nations prepared to respond to a bioterrorist attack?
6. Are the CWC and the BWC as well and other existing treaties effective? Should new ones be made or should these be modified?
7. What kind of research and monitoring systems should allow for the early identification that an attack has been made?
8. What kind of measures for prevention and response should be implemented/improved?

Sources

"Bioterrorism Overview." Centers of Disease Control and Prevention. 1 Feb. 2007. Web. 6 May 2015.

Carus, W. Seth. "Defining Weapons of Mass Destruction". (n.d) Jan. 2012. Web. 12 Apr. 2015

"Biological Threats." Ready. Web. 1 May 2015.

Spencer, Jack, and Michael Scardaville. "Understanding the Bioterrorist Threat." The Heritage Foundation Backgrounder (2001). Web. May 2015.

Riedel, Stefan. "Biological Warfare and Bioterrorism: A Historical Review."*Proceedings (Baylor University. Medical Center)* 17.4 (2004): 400–406. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1200679/.

KRISTOF, NICHOLAS. "Unmasking Horror -- A Special Report.; Japan Confronting Gruesome War Atrocity." The New York Times 17 Mar. 1995. Web. .

Meselson, M. "The Sverdlovsk Anthrax Outbreak of 1979." Science (1994): 1202-8. Web. .

"First Committee, in Draft Resolution, Seeks Cooperation of Syrian Authorities, Organisation for the Prohibition of Chemical Weapons, on Outstanding Issues." United Nations Meetings Coverage and Press Releases. 3 Nov. 2014. Web. .

"Recent Battlefield Use of Chemical Weapons, Absence of Verification Mechanism for Biological Weapons Ban Trigger Strong Rebuke in First Committee." United Nations Meetings Coverage and Press Releases. 24 Oct. 2013. Web. .

"Chemical Weapons Convention." ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS. Web. .

"Recent Use of Chemical Weapons 'Stark and Horrific Reminder' of Duty to Eliminate Them, Speaker Tells First Committee as It Continues Full-scope Debate." United Nations Meetings Coverage and Press Releases. 8 Oct. 2013. Web..

"New START." U.S Department of State. Web. .

Borger Julian. “Syrian Chemical Attack used Sarin and was worst in 25 years says UN”: The Guardian. Sept. 2013. Web. 12 Apr.2015

“Syria’s Chemical Weapons Stockpile”: BBC news. Jan 14.2015. Web. 12 Apr.2015.

"Amerithrax or Anthrax Investigation." The FBI Bureau of Investigation. Web. .

"When Ricin Was Used to Kill." BBC News 13 Apr. 2005. Web. .

"Ricin and the Umbrella Murder." CNN. 23 Oct. 2003. Web. .

Inglesby, TV. "Consensus Statement: Smallpox as a Biological Weapon: Medical and Public Health Management." Journal of the American Medical Association 281.22 (1999): 2127-137. Centers of Disease Control and Prevention. Web. .

"Iraq Says 'terrorists' Seize Ex-chemical Weapons Site." CBC NEWS. 8 July 2014. Web.

Barnes, Julian. "Sunni Extremists in Iraq Occupy Hussein's Chemical Weapons Facility." The Wall Street Journal. 19 June 2014. Web.