PMUN 2014

Disarmament and International Security

Study Guide

Your chairs: Kapish Batura and Zoya Springwala

DISEC

To the future delegates of DISEC,

It is our pleasure to welcome you to the Disarmament and International Security Committee at PMUN 2014. As your chair and co-chair, we are looking forward to enthusiastic debate amongst your peers and you. The high level of debate, genuine camaraderie and lively atmosphere is what defines a good DISEC committee for us.

Here's some more about your chair and co-chair.

Hello delegates! My name is Kapish Batura and I am the chair of DISEC this year. I have attended 6 MUN's so far: AISA MUN, CHOEIFAT MUN, CIS MUN, AUS MUN, PMUN and, last but not the least, AWS. This year, I have the privilege to chair DISEC and heed my warning delegates; you **HAVE** to speak during committee. Since I'm supposed to give a background about myself, let me start of by saying that I'm an Otaku and proud. I also play table tennis at a state level and reading books is one of my favourite pass times. I'm an aspiring architect and hope to build a structure that's looked upon as one of the finest structures to have ever been built. Do take me seriously when I say that fooling around in my committee is not advised. May your debates be as formal as the suits and dresses you wear.

My name is Zoya Springwala and I am the co-chair for this committee. I enjoy reading, eating and sleeping amongst watching enough Doctor Who to make it socially unacceptable. Brownie points for you if you sneak in a fandom reference. I'm in IB 2 and am doing a combination of HLs and SLs that renders me unemployed in the future. I was the second best delegate of DISEC last year, and it was an explosive committee. I hope and expect that such an experience would be replicated, if not outdone this year.

The agendas that shall be covered during the span of these two days are the Iraq crisis and Cyber Warfare. Please read the study guides below and begin research on your country's stance. You must start working on your position papers and if position papers aren't submitted 72 hours prior to the MUN, you shall be barred.

Delegates you may contact your chair or co-chair for additional help:

Kapish Batura: batura.kapish@gmail.com or 9833574545

Zoya Springwala: springwalazoya@gmail.com

IRAQ CRISIS

Background.

Two and a half years ago, as the last American troops left, President Barack Obama described Iraq as "sovereign, stable and self-reliant". Today jihadists are tearing the country apart. Mosul, Iraq's second city is now part of the ISIS controlled region. On June 10th the prime minister, Nuri al-Maliki, called for a state of emergency and pleaded for outside help. The next day, in league with rebellious Iraqi Sunnis, ISIS took Tikrit, the home of Saddam Hussein, just two and a half hours' drive north of Baghdad. The Iraqi army proved has hopelessly ineffective in trying to prevent such takeovers.

ISIS aims to redraw the map of the Middle East by creating a Sunni state, starting with eastern Syria and the heart of Iraq. Its brand of militancy is spreading violence and terror across the Arab world. It is also likely that latest victories may provide ISIS with the platform to spread their jihad to the western world.

ISIS is born of regional warfare and Islamic fundamentalism. Battling against Bashar Assad in Syria, it recruited foreign fighters, some of them veterans. In the anarchy of Syria and Iraq, it has stuffed its robes with cash from kidnapping and extortion, and gained enough battlefield experience to outclass Iraq's soldiery. It is so zealous and bloodthirsty that other rebel groups in Syria have turned against it. Even al-Qaeda renounced it, partly because al-Qaeda does not approve of the idea of creating a state just now, and partly because of ISIS's savagery, including towards fellow Muslims.

Who is to blame?

European governments have handed ISIS millions of dollars to buy the freedom of kidnapped citizens. President Assad cynically helped ISIS gain an edge over the rest of the Syrian rebels by releasing extremists from his jails and selectively sparing it from attacks. He wanted the world to withhold aid for his opponents, for fear of what might come after him. It worked. But the blame also lies with President Maliki in Iraq and with President Obama. President Maliki has governed as a proto-dictator on behalf of the Shia majority. The army has rotted as he has purged independent-minded officers and put his own men in their place. Just after the last American troops left Iraq, in 2011, he ordered the arrest of the Sunni vice-president—who promptly fled. He failed to maintain links with the Sunni clans who drove al-Qaeda and ISIS's forerunner out once before, during the American occupation. He has used live fire on peaceful Sunni protesters. At the same time, life in President Maliki's Iraq is miserable. Because of ISIS, monthly death rates have climbed back to the levels of 2008; the rule of law is weaker than in the time of Saddam; corruption is rife and the lack of jobs and education means that prospects are bleak.

President Obama has helped ISIS by omission. No doubt, his predecessor's decision to go to war—which we mistakenly backed at the time—was a disaster. But in quitting Iraq,

President Obama failed to win an agreement that left some American troops behind, or that provided American aerial support. Only last month he refused president Maliki's calls for American airstrikes against the Jihadists. And in Syria, as many warned, the predictable outcome of President Obama's vow to prevent America being sucked in has been to create a terrorist threat so grave that it risks sucking America into an even worse mess.

What will happen now?

ISIS may now catalyze the disintegration of Iraq and Syria. Armed with weapons seized in Mosul and cash to pay its troops it can more easily hold its ground. In Iraq the Kurds may get their own state, which would leave a Shia-dominated rump under President Maliki at risk of communal violence. ISIS's freedom to range through parts of Syria and Iraq creates a breeding ground for global terror. Although the group's focus today is on territory, its people say that their targets include the wider region and the West. Hundreds of ISIS fighters may have European passports. Already, in eastern Syria, the group has built training camps. That is worryingly reminiscent of Osama bin Laden's set-up in Afghanistan.

Possible points for delegates to consider:

- Is there any way stability can be restored to the region/can the violence be stopped?
- Can/should Iraq and Syria win back the land under ISIS control?
- Is a new multi-state solution a viable option?
- Does the USA (or indeed the UK) bear any responsibility for recent events and does it have a responsibility to resolve the situation? And are its proposals appropriate?
- Will military action effectively improve the situation?
- Is there any other way to stop ISIS?
- Should Maliki remain in charge?
- Should Kurdistan be given independence?
- What should be done about the human rights abuses committed by ISIS?
- How can Islamic extremism be prevented in a long-term view?

International bodies

- **Arab League** – On 12 June, Arab League Secretary-General, Nabil al-Arabi condemned what he described as the "criminal activities" committed by ISIS group in Mosul. He emphasized on the necessity of "national consensus in Iraq at this critical time, which threatens Iraq's security and political stability.

- **United Nations** – On 10 June, the United Nation's Secretary-General, Ban Ki-moon, asked all political leaders in Iraq to show national unity against the ISIS invasion, expressed grave concern about the "serious deterioration", and condemned the recent terrorist attacks that have left scores dead and wounded in Iraq's northern and eastern provinces. He recalled that all UN Member States have an obligation to

implement and enforce the targeted financial sanctions, arms embargo and travel ban imposed on ISIS under the sanctions regime pursuant to Security Council Resolution 1267 (1999) and Security Council Resolution 1989 (2011). It also evacuated its 60 staff members from Baghdad to neighboring Jordan. After ISIS released graphic photographs of its fighters shooting scores of young men, the United Nations said on 16 June, cold blooded "executions" said to have been carried out by militants in northern Iraq almost certainly amount to war crimes.

The international bodies statements are present for the nations who have not been listed below since the nation(s) don't address the crisis directly. The delegates of these nations can refer to the statements made by the international bodies and also study up on their foreign policies to formulate their position papers.

U.N.

-  **India** – On 16 June, Indian External Affairs Ministry condemned the takeover of Iraqi cities like Mosul and Tikrit by terrorists and reiterated its support to the government and the people of Iraq in their fight against international terrorism. It also set up a 24-hour helpline at Indian embassy in Baghdad for assistance of Indian nationals stranded in these cities. It has been reported that 46 Indian nurses were abducted from the Iraqi town of Mosul who were later freed and flown back to India.

-  **Iran** – On 12 June, the Iranian president, Hasan Rouhani, stated: "For our part, as the government of the Islamic Republic of Iran, we will combat violence, extremism and terrorism in the region and the world." On 11 June, the Foreign Minister of Iran, Mohammad Javad Zarif, had condemned the "murder of Iraqi citizens" as he offered Iraq's government support against terrorism. However, Iranian officials have not explained how Iran will help Iraq's government. Iran dispatched Revolutionary Guard forces to help Iraq's government recapture Tikrit. Iran sent three battalions of the special operations Quds Force and has sent a total of 2000 men between 12–14 June. According to Washington Post, any support from Iran will be subtler, confined to military planning and strategy rather than manpower.

-  **Russian Federation** - Russian President Vladimir Putin has expressed "full support" to the Iraqi government. Eight days later, Deputy Foreign Minister Sergei Ryabkov announced that "Russia will not stand idle toward attempts by terrorist groups to spread terrorism in regional states" and urged Europe and the United States to take action against ISIS. On 29 June, Russia delivered Sukhoi Su-25 ground attack aircraft to the Iraqi Air Force, days after a request by the Iraqi government. Unconfirmed reports suggest that six Sukhoi Su-30 multirole aircraft are to be delivered as well. Photos have appears on Iraqi social media depicting Russian-made rocket artillery TOS-1 arriving in Baghdad.

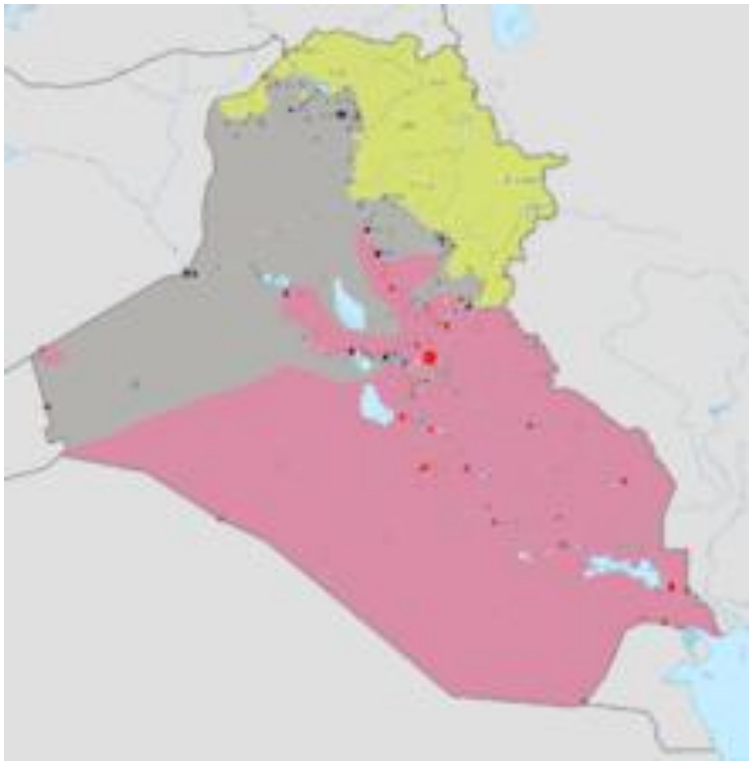
- **Syria** – On 11 June, Syrian Ministry of Foreign Affairs and Expatriates condemned recent terrorist acts of militants from the Islamic State in Iraq and the Levant on the territory of Iraq. It also expressed support and solidarity to the Iraqi government in its fight against the armed terrorist groups in Iraq. On 15 June, the Syrian Air Force was carrying out airstrikes on ISIS bases in coordination with Iraq. Airstrikes were carried out against ISIS bases in Raqqa and Al-Hasakah inside Syria, and headquarters in Shaddadi, a town close to the border with Iraq.

- **Saudi Arabia** – The Saudi Arabia government said that the tensions there were due to sectarian policies, which threatened its stability and sovereignty, according to the official Saudi Press Agency. It warned against foreign intervention and urged Iraqis to form a national unity government.

- **Turkey** – ISIS captured Ankara's consul general in Mosul and detained 49 Turkish citizens including the Consul-General, Öztürk Yılmaz. It also took hostage 31 Turkish truck drivers. Some reports suggest that the hostages have been moved to the residence of the ISIS-sponsored Mosul governor, in possible preparation for their release. Turkey has called an emergency NATO meeting.

- **United Kingdom** – On 17 June, Prime Minister David Cameron said the UK would be reopening the British Embassy in Iran in an effort to rebuild the nations' diplomatic relationship to help combat the recent event in Iraq. On 18 June, PM Cameron said that he believed ISIS was planning a terror attack on the UK.

- **United States** – On 12 June, U.S. President Barack Obama said he was exploring all options to save Iraq's security forces from collapse, and U.S. companies evacuated hundreds from a major air base. "Our national security team is looking at all the options... I don't rule out anything," he declared. U.S. Senator Lindsey Graham warned an ISIS takeover in both Iraq and Syria would create a "hell on earth" and called for the urgent deployment of U.S. air power to "change the battlefield equation.



Map to IRAQ

Legend

Gray - Insurgent-controlled territory
Red - Iraqi-controlled territory
Yellow - Kurdish territory

The delegates can refer the following links to help formulate their position papers.

http://www.bbc.co.uk/news/world-middle-east-24179084

http://www.ft.com/cms/s/2/69e70954-f639-11e3-a038-00144feabdc0.html#axzz35Ue3PPtU

http://www.washingtonpost.com/news/morning-mix/wp/2014/06/13/isis-beheadings-and-the-success-of-horrifying-violence/

http://www.usatoday.com/story/news/world/2014/06/23/kerry-iraq-militants/11253211/

http://www.bbc.co.uk/news/world-middle-east-27921931

http://www.bbc.co.uk/news/world-middle-east-27983222

http://www.bbc.co.uk/news/uk-27848460

CYBER WARFARE

This study guide will attempt to acquaint you with the key terms regarding Cyber Warfare as well as introduce the delegates to the relative idea and set the scope. This guide will give you a short history regarding cyber war-crime and establish the current situation at hand.

As technology rapidly advances in the 21st century, it is getting more and more important to maintain our privacy and protect our private information and preventing it from falling into the wrong hands. Economic development and security enhancement is dependent on development in telecommunications and information technology.

Around the world, cyber technology is becoming increasingly important for weapons systems, defense infrastructures and national economies.[9] As such, military leaders consider cyberspace the next frontier of combat – beyond land, sea, air or space. In the past, military victories were won through physical conflict of weapons or soldiers. Now technology permits hackers acting with or without state support to wage a new kind of warfare that involves computer sabotage.

Terminology:

Cyber space:
Cyberspace is the global electronic medium of computer networks, including all forms of networked and digital activities, in which online communication takes place. It is the global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems.

Cyber espionage:
Is the practice of obtaining classified information from groups, governments, organizations, individuals or competitors for military, political or economical advantage using illegal hacking and exploitation on the internet, software, networks or computers. Secret information can be intercepted and modified, making Cyber Espionage possible from anywhere in the world.

Cyber attacks:
Refer to the deliberate use of hacking to alter, disrupt or destroy computer networks or systems. It also attempts to obliterate the information and programs used in these networks. Cyber warfare involves obtaining and/or modifying classified information stored electronically. They are attacks which target computers, satellites or other vulnerable components of a system which could lead to the disruption of equipment. The disruption could be military, or civilian in nature. Power, water, fuel, communications and transportation infrastructure all may be vulnerable to disruption.

Cyber crime:
Any criminal activity that takes place in, through, or directly with cyberspace and involves a computer and a network is a cyber crime. Computers may have been used in the commission of a crime, or they may be the targets. Such crimes may threaten a nation's security and financial health. Some issues such as cracking, copyright infringement, child pornography, and child grooming, espionage both in the private sector and from governmental portals became high-profile.

History:

Stuxnet:

In mid July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is believed to have been created by the US and Israeli agencies to attack Iran's nuclear facilities. Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial control systems. 5While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," notes The New York Times.

Timeline:

April 2007 - As a country with heavy reliance on the Internet, the government of Estonia is one of the largest internet service providers and many citizens have wide access to wireless connections. Due to the relocation of a Soviet statue, the cyber attack was launched from numerous zombie computers around the world, and one of the IP addresses was traced back to Russia. This resulted in Estonia being the first country in the world to be targeted and defended itself from a cyber attack. The targets of these attacks were ministries, banks and media.

September 2007 - During Israel's attack against the Syrian nuclear program, it is likely that cyber warfare was used by the air force for the detection of radar.

August 2008 - Immediately before the South Ossetia War, Russia attacked the Georgian and Azerbaijani Internet sites. During the war in Russia, any Russian citizen could aid in the attack by logging on to a Russian website. Cell phone service and online banking was damaged in Georgia in result of this attack.

July 2009 - Coordinated denial-of-service attacks against government, media and financial web sites in the US and South Korea.

November 2010 - As a revenge for the Mumbai terrorist attacks, the Indian Cyber Army attacked all the websites belonging to the Pakistani Army.

December 2010 - The Pakistani Cyber Army attacked the website of India's lead investigating agency, the Central Bureau of Investigation.

August 2011 - 72 organizations, including but not limited to: the UN, the Olympic Committee, ASEAN, and 14 other countries were under a cyber attack, likely from the Chinese government. This attack was launched by sending an e-mail, which downloaded a malicious program into the computer when opened. This further allowed the perpetrator to gain access to the victim's computer's network. Discovered by McAfee, a US computer security company, this cyber attack is known as the largest to date.

May 2012 - Flame, a computer virus developed by the US and Israel was discovered. This malware was aimed at Iran for their nuclear weapon program.

Current Situation:

What can be qualified as an 'act of war' under currently existing international lawThe problem lies that there exists no agreed international consensus as to what act in Cyberspace can be considered as an 'act of war'. Due to the inherent nature of the Internet and vast character of Cyberspace, it is extremely challenging to determine the origin of a cyber-attack. All devices connected to the Internet, are at risk from either being hacked into or from being used as a device to trigger a larger attack. Unlike nuclear or chemical warfare, cyber-attacks that can be potentially disastrous can be initiated relatively inexpensively, and items required for such an attack are fairly easily available. This makes Cyberspace a perfect playground for both sovereign countries and independent actors to carry out attacks on cyber infrastructure and to gain information from foreign powers. Countries across the globe are recognizing Cyberspace as the new battleground.

Russia and several other Nations recently have been pushing for the UN to create a Code of Conduct to be followed by all Nations in Cyberspace. Cyberspace is a hybrid of the other four dimensions- land, air, sea and space- it can be used to conduct attacks with unprecedented consequences in any of the other dimensions. The huge potential of Cyberspace and Cyber warfare is yet to be seen. Another problem is the ambiguity of the application of existing international war treaties in Cyberspace and whether, due to its vast and different nature, it requires a new international treaty to govern its application. The first step in combating cyber warfare is convincing the world that it is, in fact, a real and urgent threat.

Delegates shall then discuss the countermeasures in order to be able to regulate cyber activity taking into account the stated focus points. This can be a start for new laws of Global constraint of digital mobility for everyone. Delegates shall then discuss the countermeasures in order to be able to regulate cyber activity taking into account the stated focus points. This can be a start for new laws of Global constraint of digital mobility for everyone. Therefore, they should determine how violation of the law is going to be approached not only in terms of most powerful parties but also against little agitators.
In sum, until the U.N. issues an effective international treaty to combat cybercrime, states, businesses and individuals have to protect themselves from cyber-attacks. This is nearly impossible as cyberspace is too large, too sophisticated and too interconnected to be dealt with alone without cooperation. Therefore, it is time for governments to sit together and formulate a single solution to this top concerning problem at the international level.

Regulation:

State Actors:
As cyber warfare often involves state-actors at the highest level, these activities could be considered acts of aggression or war without being outlawed by the domestic law of the country launching the attacks. Hence this poses several problems in legislation and policy-making both on a domestic and international level.

Non-State Actors:
Non-state actors who have the capacity to engage in acts of cyber warfare also pose a grave and veritable threat to national and international security. Terrorist organisations could have the capacity to target mass civilian structures as well as classified government systems to pose significant damage and destruction.

Countries:

United States of America:
The United States began to address cyberspace in the context of national security as early as 1996. The U.S. cyber war assets continue expanding now a day in response to on growing cyber-attacks done by other governments working through national means including the so-called "patriotic hackers." In May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM) in order to defend American military networks (especially from threats coming from China and Russia) and attacks other countries' systems.
Last year, McAfee, the U.S. security firm, released material of a cyber-espionage operation that had penetrated 72 governmental and organizations within the U.S. and elsewhere in order to copy military secrets and industrial designs. This report was called "Operation Shady Rat" and offered real evidence pointing to China as the main responsible. On the other hand, in January 2012, Mike McConnell, the former director of national intelligence at the National Security Agency, stated that the U.S. has already launched attacks on the computer networks of other countries not mentioned in his speech.

China:
Relations between the United States and China are harmed by their disagreements over information technology. U.S. government departments have identified China's People's Liberation Army (PLA) as the source of cyber attacks against the US government and key private companies. The Shanghai Cooperation Organization (members include primarily China and Russia) defines cyber war to include dissemination of information "harmful to the spiritual, moral and cultural spheres of other states". In September 2011, these countries proposed to the UN Secretary General a document called "International code of conduct for information security". The approach was not endorsed by most western countries as it entailed too many hints on political censorship of the internet.

Russia:
Russia has been accused of attacks done in 2007 that left Estonian's without internet for a period of two weeks as well as for disputes taken place during the conflict between the Russian military and Chechen fighters. The panorama today, is not only about international threats and attacks, weeks before Russia's presidential elections, a cyber-war raged between rival political factions. On February 8 and 9, for example, Anonymous hijacked the website of Putin's United Russia party. Just before that, the websites of several opposition parties had been attacked.

India:
Within the Indian boundaries, a group called the Indian Cyber Army has risen. They define themselves as "the largest group of ethical hackers and cyber security experts involved into social service". In recent months Indian and Bangladeshi hackers have been attacking websites between each side. The dispute apparently started from a physical conflict along the border, with Bangladesh claiming Indian guards had shot innocent civilians, and has been hash especially for local banks. Also, this year, India has been accused of hacking a U.S commission's e-mail communications, which deal with the economic and security relations between U.S and China. It is said that an Indian spy managed to post on the Internet a document stating a length of ways to target the U.S –

China supported by transcripts of the emails exchanged between members of the commission.

Israel – Palestine:
Despite recent successful hacking attempts coming from pro-Palestinian hacker groups and done on Israeli websites, Israel has been ranked as one of the most protected countries in terms of cyber defense. Israel created in 2011 the National Internet Defense Taskforce in charge of creating tools to defend vital infrastructure networks against cybernetic attacks done by foreign countries and terrorist groups.

Pakistan:
The main issue, in which Pakistan is involved, regarding cyber-attacks, has been going on since 1998 and is linked directly with India. The intensity of the war increased last year after a reported attack by Pakistani hackers on the Central Bureau of Investigation (CBI), India's top civilian investigation agency, Indian hackers attacked 40 Pakistani websites. However, Pakistan's government is not taking any specific measures to protect state websites from the approaching threat of hackers.

Questions to be answered:

- If cyber warfare is normalized as another wartime component, how will it's application and usage be governed?
- Do previously existing charters apply to this or will new treaties have to be formed?
- Should a cyber warfare attack be considered a traditional act of war?
- How can countries defend themselves from cyber warfare attacks?
- Should there be regulations and conventions that govern cyber warfare similar to how conventions govern conventional warfare?
- Should the government have control of all Internet and telecommunications assets in case of a national emergency?
- What type of cyber warfare has your country been alleged of conducting or has your country experienced as a victim?

Further Reading:

- http://www.pwc.com/en_US/us/it-risk-security/assets/e-espionage.pdf
- www.cfr.org/technology-and...cyber.../p15577
- http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500795
- http://www.un.org/Docs/journal/asp/ws.asp?m=s/res/1701(2006)
- http://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html
- http://online.lewisu.edu/the-history-of-cyber-warfare.asp
- http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf
- http://www.un.org/disarmament/topics/informationsecurity/

- http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacy
- andtransborderflowsofpersonaldata.htm
- http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- http://www.hrcr.org/docs/American_Convention/oashr.html
- http://usun.state.gov/briefing/statements/216133.htm