CHRIST JUNIOR COLLEGE

MODEL UNITED NATIONS 2016

THE UNITED NATIONS SECURITY COUNCIL

THE POSSIBLE THREAT OF A CYBER WAR WITH SPECIFIC REFERENCE TO CYBER ESPIONAGE

Letter from the President

Dear Delegates,

Welcome to the Security Council. My name is NylaSaldanha and I will be serving on the executive board as the President of the Security Council along with my Vice-president, Aayush Shah.
It gives me immense pleasure to return to CJCMUN for my third consecutive year in the Security Council.
As delegates in this committee, you are expected to put forward 'step-by-step solutions' as opposed to 'goals'. Be fierce and firm in your arguments while maintaining a keen sense of diplomacy in committee. I hope to see highly progressive debate and hope that every one of you has something to take back from our three days of committee, be it growth as an individual, an improvement in your debating skills or a trophy.
Please feel free to go beyond the background guide and address issues you think we've missed out when you are in committee. Also note that this guide has been formulated to serve as the basis of your research and not stand as your research alone.
First timers are welcome to approach Aayush or me with any questions regarding procedure, how to go about research, etc prior to the MUN.
I look forward to seeing you in committee and wish you all the very best.
Happy researching!

Nyla Ann Saldanha
President, The United Nations Security Council
CJCMUN 2016

Letter from the Vice-President

Dear esteemed delegates,

Welcome to one of the most powerful committees of The United Nations and my personal favorite The Security Council.

This year it will not only be the debate but also diplomacy which will help us find a common goal. I believe that there exists no such problem that cannot be solved keeping in mind the principle of diplomacy. It gives me great pleasure welcoming you all to this year's chapter of Christ Junior College Model United Nations.

Please feel free to approach us for any queries whatsoever. I hope this session would be very helpful, and not only provide a platform for collective growth but also mutual learning. Also note that this background guide is just to facilitate research. Please feel free to search beyond this guide which will not only help in the better understanding of the issue at hand but also facilitate progressive debate.

First timers, please feel free to approach us anytime prior session regarding any queries on research or procedure! Without any further ado, I wish you all the very best. Happy researching!!

Aayush Shah
Vice president, The United Nations Security Council
CJCMUN 2016

Introduction to the Security Council

Entrusted by the United Nations Charter with the maintenance of international peace and security, the Security Council is the principal organ of the United Nations. Consisting of fifteen members, the Security Council is tasked with tackling the world's most imminent security concerns. To achieve this end, the Security Council is the only body within the United Nations' framework able of imposing legally binding resolutions on any and all member states of the United Nations. In this context, the Security Council has the power to impose diplomatic and economic sanctions, deploy peacekeeping forces, and, as a last resort, deploy military forces. The enormity of the Security Council's responsibilities and mandate elucidates its ability to influence international politics.

At the United Nations' founding after the conclusion of World War II, the five permanent members (at the time, the Republic of China, or Taiwan, held the seat now occupied by the People's Republic of China; Russia's seat once belonged to the Soviet Union) were assigned seats on the Council because they were the victors of World War II. Shortly thereafter, however, relations between the United States and the Soviet Union became strained as competition and mistrust led the two into the Cold War. During this time, the Security Council accomplished very little. Many resolutions were passed, but the resolutions themselves were rather unremarkable, as anything that the United States, China and the Soviet Union actually agreed upon was, inevitably, quite straightforward. To be more accurate, all the permanent members did not have to agree, but they could not disagree so much that one of them would use their veto.

Since the end of the Cold War, however, the Security Council has had quite a few noteworthy achievements. In 1991, the Security Council voted to deploy forces against Iraq in what would be known as the Gulf War. Iraq had invaded Kuwait and the international community intervened on behalf of a state whose sovereignty had been violated. In 2001, the Council formed a counter-terrorism committee in response to the attacks of September 11 of that year. The Council has regularly imposed sanctions on other countries, and oversees all of the ongoing UN peacekeeping missions around the world, in addition to several committees and commissions, which operate under the Council's jurisdiction, in accordance with the UN Charter.

The Mandate and Functions of the Security Council

The United Nations' Security Council derives its mandate from the United Nations Charter. Tasked with the maintenance of international peace and security, the Security Council has a wide array of powers available in its toolkit. Under the United Nations Charter, the functions of the Security Council are:

- To maintain international peace and security in accordance with the principles and purposes of the United Nations; (UN Charter, Ch.5, Article 21)
- To investigate any dispute or situation which might lead to international friction; (UN Charter, Ch.6, Article 34)
- To recommend methods of adjusting such disputes or the terms of settlement; (Charter, Ch.6, Article 36)
- To formulate plans for the establishment of a system to regulate armaments; (UN Charter, Ch. 5, Article 26)
- To determine the existence of a threat to the peace or act of aggression and to recommend what action should be taken; (UN Charter, Ch. 7, Article 39)
- To call on Members to apply economic sanctions and other measures not involving the use of force to prevent or stop aggression; (UN Charter, Ch. 7, Article 41)
- To take military action against an aggressor; (UN Charter, Ch. 7, Article 42)
- To recommend the admission of new members; (UN Charter, Ch. 2, Article 4)
- To exercise the trusteeship functions of the United Nations in strategic areas; (UN Charter, Ch. 12, Article 83)
- To recommend to the General Assembly the appointment of the Secretary-General and, together with the General Assembly, to elect the Judges of the International Court of Justice. (UN Charter, Ch. 3, Article 12 and ICJ Statute, Ch. 1, Article 4)

Introduction to the Agenda

Just as World War I introduced new weapons technology and modern combat to the 20th century, the information age is revolutionizing warfare for the 21st. Cyber attack refers to the deliberate actions to alter, disrupt, deceive degrade or destroy computer networks or systems as well as the information and/or programs used in these systems or networks. Around the world, cyber technology is becoming increasingly important for weapons systems, defense infrastructures and national economies. 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.

Additionally, cyberspace is not only a new zone of strategic competition but more importantly, the subject of the next global arms-race.While the first all-out cyber-war has yet to be waged, cyber-experts and military strategists anticipate that a major interstate cyber-battle could be fought within the next few years. Currently, the international community only has a weak system of regulation and governance that covers this emergent threat. As global society becomes ever more dependent on cyberspace for both its most basic and its most critical functions, the economic and social impact from a full-scale cyber attack could cripple a modern networked state. More importantly, many political scientist and military leaders believe that a major cyber-attack on an advanced economy could result in a substantial conventional or in some cases even a nuclear response.

Moreover, cyber attacks have a number of characteristics that distinguishes them from traditional attacks through conventional or even ballistic weapons. First, cyber attacks can be carried out with high degrees of anonymity and with plausible deniability, which makes them apt for covert operations and for initiating conflict between other parties. The rules of engagement associated with conventional weapons do not carry over easily to attacks made in cyberspace. Where countries were once hesitant to attack another country for fear of retaliation, cyber attack provides for a covert method of attack and instigating conflict between other parties. The deterrence models governing theories behind why states go to war seem incompatible with cyberwar.

Second, they are more uncertain in the outcomes they produce, making it hard to determine deliberate and collateral damage. Cyber attacks involve a larger range of options and possible outcomes. A lone actor can steal information from a country's secure networks, while a coordinated state-sponsored cyber-attack could damage another country's financial system, which could result in the economic collapse of an entire region. These attacks can also be carried out by actors working in one specific location or from many locations all over the world.

Legally, the possibility of cyberwarfare is unprecedented within international treaties. Those wishing to normalize cyberwar as another component of conventional war could make the case that cyber attacks can be governed by previously existing charters, such as the Charter of the United Nations. Since a cyber attack can be considered a forceful attack as a result, states should be allowed to defend themselves against cyber attacks by conventional means. A hostile attack on a country's power grid or economic infrastructure could legally be responded to with an air or missile attack on the initiating country.

However, for cyberwarfare to work as an additional component of conventional war, accountability must be ensured. State-to-state models of deterrence work because states that are attacked are then able to locate and retaliate against aggressor states. This transparency does not transfer over into cyberspace. Without a heat signature to trace or an enemy soldier to interrogate, states are left to rely on misleading IP addresses which can be redirected several times in order to mislead state authorities.

In addition to problems of accountability, nongovernmental actors can initiate cyberwar easily and inexpensively. Extreme activists and terrorists alike can launch cyber attacks on state governments with as little as a computer, an Internet connection and a few skilled hackers. Compound this scenario with the inherent difficulty in pinpointing the origin of a cyber attack and what ensues is a cyber-battleground where everyone is attacking everyone with a misdirected sense of who the true aggressors are. An attack launched by non-state actors from within one country against the government of another can be misread as a state-to-state attack. The victim state is then in a compromised position where it must first determine whether an attack is actually the product of a state operation and secondly, whether it should merely defend itself or escalate conflict to physical space with a conventional attack.

The uncertainty surrounding cyberwar and its application by both state and non-state actors make it a difficult component of war to normalize, leaving the questions for this committee to consider: Should cyberwar be accepted as another component of conventional war? How might the international community address the problems of accountability and legality surrounding cyberwar's application? What can be done to combat non-state use of cyber weapons?

Prominent Cyber Attacks

The “Original” Logic Bomb:
In 1982 a computer control system stolen from a Canadiancompany by Soviet spies caused a Soviet gas pipeline to explode. The code for the controlsystem had been previously modified by the CIA, which had been tipped off, to include alogic bomb, i.e. a piece of code that changes the workings of a system, which changed thepump speeds to cause the explosion. An air force secretary describe d it as “the mostmonumental non-nuclear explosion and fire ever seen from space”.

Titan Rain:
The name given by the FBI to a series of coordinated attacks on Americancomputer systems since 2003 ongoing for at least three years. It was discovered that severalsensitive private and public computer networks were infiltrated by the hackers, such as thoseat Lockheed Martin and NASA. Not only was military intel and classified data stolen, but alsothousands of “zombified” machines, i.e. computers infiltrated by malicious software that canbe activated later, were left behind. Titan Rain is considered the largest state-sponsoredcyberattacks in history, said to have been organized or supported by the Chinese government.

Cyberattacks on Estonia:
A series of well-planned cyber attacks began on 27 April 2007 andswamped websites of Estonian organizations, including Estonian parliament, banks, ministriesand broadcasters, amid the country’s row with Russia about the relocation of a Soviet statue.Due to the sophistication of the attacks it was claimed that the Russian government hadassisted in orchestrating the attacks. Among others Nashi, a nominally independent pro-Kremlin youth group, has taken responsibility for the incident. Some argue that it may havebeen the second-largest instance of state-sponsored cyber attack, following Titan Rain.

Stuxnet:
In 2010 the Stuxnet worm temporarily knocks out some 1000 centrifuges at Iran’s Natanz nuclear facility, causing considerable delay to that country’s uranium enrichmentprogramme. Allegedly the highly sophisticated worm was planted manually by a flash driverinto at least one computer connected to the network. In June 2012, The New York Timesreports that the U.S. and Israel developed the worm.

Flame:
Another complex malware responsible for data loss incidents at Iran's oil ministry in2012. It was allegedly developed by the U.S. and Israeli governments to collect intelligenceabout Iran's computer networks that would facilitate future cyberattacks on computers used inthat country's nuclear fuel enrichment program. It was also planted manually into thenetwork.DDoS attacks on U.S. banks: The U.S. accuses Iran of staging a massive wave of denial-of serviceattacks against U.S. financial institutions in 2012. Defense Secretary Leon Panettawarns of cyber threats against critical infrastructure and calls for new protection standards.

Korean cyber war:
Already in 2009 and 2011 North Korea has been blamed for cyber raidsagainst South Korean organizations. On 15 March, North Korea's KCNA news agencyaccused the US and its allies of large-scale hacking attacks on its internet servers. Later inMarch around 32,000 South Korean computers at banks and broadcasters were affected by acyber attack. Even though the attack could be traced back to a Chinese IP address officialsemphasized that this did not reveal who was behind the attack, as hackers can route theirattacks through addresses in other countries to obscure their identities. North Korea issuspected to have staged the attack amid rising tensions on the Korean peninsula.

The Spectre of Cyber Terrorism

The debate on the basic definition of cyber warfare is intrinsically linked to the similar issue of cyber terrorism. Indeed, the delineation between the two has been blurred to the point where many experts acknowledge a degree of overlap. Information security specialist Eugene Kaspersky has argued that the difficulty in tracing perpetrators of cyber attacks, who utilize large-scale cyber weapons with potential destructiveness akin to conventional biological weapons, renders the two terms inextricable.

The distinction lies within how the international community approaches the two issues. The expert consensus, regardless of definitions, is that cyber attacks by both state and non-state actors must be subject to deterrence under existing international legal norms. However, as state actors alone are generally afforded seats at the negotiating table, any measures taken against the threat of cyber terrorism to international peace and security are not likely to provide such deterrence for non-state actors. Nonetheless, the issue of cyber terrorism, especially with regard to these non-state actors, should be kept in mind during the debate of international action on cyber warfare.

Case Studies

Case1:Cyber-attacks across the Taiwan Strait

The Taiwan Strait is one of world's most dangerous political and military hotspots. Taipei and Beijing are perpetually preparing for war against each other – Taiwan to maintain its democratic status and resist absorption into the People's Republic China, Beijing to unify China once and for all and to repel any moves towards legal independence by Taiwan. Both China and Taiwan use annual military exercises to simulate the war that both are trying to avoid. China has several hundred missiles aimed at Taiwan and as of 2007; Taiwan has developed offensive military capacity to attack the mainland.101 Nevertheless both sides maintain that diplomatic negotiations will come before any preemptive attack.

At the same time, cyberwarfare is deemed by both Beijing and Taipei as an acceptable way of maintaining a state of hostility without having to launch a physical military attack.In this case, cyberwar offers the prospect of a fast and relatively painless victory should a war break out and this characteristic of cyberwarfareis essential due to the nature of this conflict. Therefore, it is not surprising that both sides have invested in designing and creating new military structures, security architectures, training programs and technology that promise to take advantage of each other's dependence on computer networks.

Assessments of China's cyberwarfare capabilities vary. The first date given by Taiwan's Ministry of Defense for a possible Chinese cyber attack was 2010. However that date has since been pushed back to 2005.More recently there is evidence that China is using new communications technology to gather intelligence on foreign governments. In 2007, German security experts had discovered that the Chinese military had planted spying software in the computer networks of German government departments.Nevertheless, many argue that China has inflated their actual cyberwarfare capabilities.

If China's cyber attack potential is credible, the greatest threat to Taiwan is if China launches a cyber attack specifically targeting Taiwan's economic, social and military infrastructures, which would immediately create a crisis. This may, although not necessarily, expose Taiwan to attack by more conventional means, which China's navy or air force. China can also launch a cyberwarfare campaign that can be conducted alongside multiple concurrent or consecutive combat operations against Taiwan.Taiwan's military exercises demonstrate that Taiwan's military has planned an offensive cyber attack operation against the mainland to disrupt PRC's invasion plans, buying them enough time for foreign intervention.

The value of cyberwarfare to both the PRC and Taiwan is that a cyber attack can help each side realize their political objectives with causing the quantity of causalities associated with conventional weapons.However, this does not imply that cyberwarfare is entirely bloodless because of the collateral damage caused by a disruption to physical infrastructure. The indirect costs of a cyber attack by either side could be huge. Hospitals, electric girds, power stations, water treatment plants could all be casualties in a cyber attack.

Case 2: Stuxnet, Flame and the Iranian Nuclear Program

In 2010, the computer worm, Stuxnet, which was supposedly developed by the United States and Israel, was unleashed against Iran's nuclear facilities. In July 2010, VirusBlokAda, a Belarussian computer securitycompany, discovered the Stuxnet cyber weapon, at least several months after its creation. Security experts note that Stuxnet attacked software in specialized industrial control equipment made by Siemens by exploiting a previously unknown hole in the Windows operating system. The malware is the first such attack on critical industrial infrastructure that sits at the foundation of modern economies. It also displays an array of novel tactics — like an ability to steal design documents or even sabotage equipment in a factory — that suggest its creators are much more sophisticated than hackers whose work has been seen before.

Symantec Security Response, a security software maker that has studied Stuxnet, reported that it appeared that the malware was created to attack Iranian nuclear centrifuges. Since it was unleashed, Stuxnet has spread to plants around the world; Siemens said it had received fifteen reports from affected customers, five of which are located in Germany. Security researchers initially believed Stuxnet's primary purpose was espionage because of its ability to steal design documents for industrial control systems. But more in-depth study of the program, which is extremely large and highly complex by malware standards, has revealed that it can also make changes to those systems.

In May 2012, Kaspersky Lab, working under a request from the International Telecommunication Union, the United Nations agency that manages information and communication technologies, studied a newly discovered piece of malware that had supposedly destroyed files from oil-company computers in Iran. While pursuing the U.N.'s request, Kaspersky's automated system identified another Stuxnet variant. At first, the Kaspersky team concluded that the system had made a mistake, because the newly discovered malware showed no obvious similarities to Stuxnet. However after examining the code more deeply, the team found traces of another file, called Flame, that were evident in the early iterations of Stuxnet. Initially, Flame and Stuxnet were considered totally independent programs, however researchers now realize that Flame was actually a precursor to Stuxnet that had somehow gone undetected.

While Stuxnet was meant to destroy things, Flame's purpose was merely to spy on people. Spread over USB sticks, the cyber weapon could infect printers shared over the same network. Once Flame had compromised a machine, it could stealthily search for keywords on top-secret PDF files, then make and transmit a summary of the document—all without being detected. The Kaspersky team notes that Flame's designers went "to great lengths to avoid detection by security software."The most worrisome aspect about the Flame cyber weapon was how it got onto machines in the first place: via an update to the Windows 7 operating system. A user would think she was simply downloading a legitimate patch from Microsoft, only to install Flame instead. Experts argue that Flame spreading through Windows updates is more significant than Flame itself and that there are perhaps only 10 programmers in the world capable of engineering such behavior.

Bloc Positions

Delegates, please note, Bloc positions are being explained to you for the sole purpose of a better understanding of your foreign policy. The countries mentioned are not necessarily 'bloc heads' and will be given just as much importance as smaller countries.

1. *The French Republic*

Cyber security has been placed as a high priority to the national security agenda of France since 2008.

In 2009, the French government created the French Network and Information Security Agency (ANSSI), that bore the responsibility of addressing the challenges of cyber-attacks. At the same time, France's main policy goal in regard to cyber security is the development and further enhancement of international cooperation through bilateral relations, as well as active participation of international organisations to design more comprehensive cyber security policies.

2. *The Russian Federation*

Russia’s policy on cyber security is significantly different from the common view of the Western countries. Even in terms of language, Russia does not use the term “cyber warfare” in its analysis, but opts for the phrase “information war”. Having said that, the government signed the Russia-U.S cyber-security confidence-building agreement in 2013, which laid the ground for Cooperation on the field of information/cyber security, before Russia-U.S relations became strained with the geopolitical developments in Ukraine. In 2015, Russia signed an agreement with China on the field of international information security, providing a base for future close collaboration between the two countries.

3. *The People’s Republic of China*

China has turned into a key actor on cyber security, especially after having been pointed at as the perpetrator of numerous cyber-attacks primarily against US companies and government agencies.
The Chinese government has repeatedly denied these allegations stating that it, “opposes and forbids any cyber crimes including “hacking”” while attributing these accusations to “the dark mentality of certain people who always regard China as a threat.” In addition to that, China said that it was the victim of U.S cyber attacks, which the U.S has denied.

The official policy reaffirms the People’s Republic’s willingness to enhance communication and collaboration in the field of cyber security based on mutual respect and objectivity. In particular, in May 2015, China signed an agreement with Russia in the field of information security, which

emphasizes the commitment to close cooperation to respond to cyber-threats and attacks.
In September, a new chapter in U.S-China relations opened with the two countries signing an agreement on mutual steps towards the interception of cyber attacks.

4. *The United Kingdom of Great Britain and Northern Ireland*

The United Kingdom has been vocal about the economic and social value of a secure cyberspaceas well as the severe consequences of cyber-attacks for international peace and security. Since 2011, the government has launched a National Cyber Security Program that has been designated a total of 860 million pounds for the protection of the U.K until 2015. In accordance with that, as a member of the European Union, the country has been complying with the Union's Digital Agenda that calls for 14 actions for the advancement of cyber security, which include the establishment of a network of CERTs (Computer Emergency Response Teams).

5. *The United States of America*

The United States has taken a major role in bringing the issue of cyber security and cyber warfare to the international community in recent years. To that effect, the Office of the Coordinator for Cyber Issues (S/CCI) was established in February 2011, with an agenda that includes the full spectrum of cyber-related issues, from security, economic issues, freedom of expression and the free flow of information on the Internet.

Perhaps one of the most complex issues of the U.S policy in regards to cyber security are U.S Chinese relations. The Chinese government has been continuously been accused of a large number of cyber-attacks against U.S and foreign companies and government agencies. The current administration has taken initiative with the creation of the Cyber Threat Intelligence Integration Center (CTIIC), which "provides analysis and support to U.S. government agencies in response to cyber threats".

The most notable development in the field of Cyber Security has been the US-China agreement, which was announced at the end of September 2015. The agreement includes, among other issues, the cooperation between the two countries via information sharing in regards to cyber activities, the mutual commitment not to conduct or support cyber attacks for the purpose of "providing competitive advantages to companies or commercial sectors" along with the creation of a high-level joint dialogue mechanism for the purpose of fighting cybercrime and related issues.

6. *North Atlantic Treaty Organization*

Cyber security and cyber defense are in the center of NATO's collective defense. The Alliance first introduced a cyber-policy defense package in 2008,after the cyber-attacks in Estonia took place.
The same year, the Cooperative Cyber Defence Centre of Excellence (CCD CoE) was established.
Although not included in NATO's official command structure, this organization serves as the leading NATO-accredited research and training facility, "dealing with cyber defence education, consultation, lessons learned, research and development." In order to stay ahead of the ever changing field of cyber security, NATO has introduced two official cyber defence policies. The first, introduced in 2011, further elaborated on NATO's operational mechanisms in the event of a cyber-attack, and the new enhanced policy, introduced in 2014, establishes "cyber defence as a part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry."46
In their core, NATO policies and initiatives aim for the protection of the communications and information systems (CIS) owned and operated by the Alliance.

7. *South Asian Association for Regional Cooperation*

Since its creation in 1985, SAARC has initiated dialogue and established cooperation in areas such as agriculture, trade, science and technology among its member states. Despite efforts to make progress in the area of security, there has been no initiative so far in the field of cyber security, while many attribute the Association's failure to strengthen its ties to the bilateral conflicts among the member states.

Questions A Resolution Must Answer

1. What constitutes a cyber-attack, cyber espionage, and hacking? How should these actions be responded to? When does the use of information technology constitute an act of aggression?
2. What principles can guide an international agreement on the limitations of the use of information technology for the sake of maintaining international peace and security?
3. What role should existing bodies, such as the United Nations Security Council have in determining the responsibility for destabilizing cyber-attacks?
4. How should member states respond to the potential threat from non-state actors that acquire offensive cyber technology?
5. What is being done to guarantee that certain kinds of attacks will not repeat themselves?

FURTHER READING:

- Cybersecurity and Cyberwarfare: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

- The Quest for Cyber Peace: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf

- Cyberterrorism: How Real is the threat? http://www.usip.org/sites/default/files/sr119.pdf

- From Nuclear War to Net War: Analogizing Cyber Attacks in International Law: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil

- United Nations Security Council Resolution 678 (1990): http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/678(1990)

- United Nations Security Council Resolution 1373 (2001): http://www.un.org/en/sc/ctc/specialmeetings/2012/docs/United%20Nations%20Security%20Council%20Resolution%201373%20(2001).pdf

- InfoSec Institute summary of cyber warfare: http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/

- http://www.bbc.co.uk/news/technology-21954636

- http://www.bbc.co.uk/news/magazine-17868789