Chair Introduction

Dear delegates,

It is an honour to welcome you to the sixth annual edition of the Lahore Grammar School Model United Nations conference, and the United Nations Security Council in particular. The Security Council is by far the most important organ of the United Nations, and the vanguard of upholding the values entrenched in the UN Charter. Although the Council has been met with significant criticism since its inception, its services in safeguarding international peace and security have been indispensable. At LGSMUN IX, the Security Council aims to find solutions to some of the most gripping issues that have plagued the global socio-political arena in recent times.

Cogent argumentation, razor sharp wit and diplomacy are just some of the skills you'll need to survive in the Security Council at LGSMUN IX. The slightest of imprudence is sure to land you in a world of hurt, so tread cautiously and think twice before any of you wants to declare war or bomb each other. My ACDs and I expect a remarkable level of debate and above all, exciting committee sessions. So come well researched, know your stance, be willing to challenge yourself and prepare for a memorable MUN experience as we set off on a four day journey to reassert key values such as equality, respect and tolerance, which the UN has stood for since the day it was created.

Anxious to see you all come November!

Huzaifa Hashim

Introduction to the Committee

The **Security Council** of the **United Nations** has primary responsibility under the UN Charter for the maintenance of international peace and security, and its resolutions are binding on all member states. During the first forty-five years of its existence, the Council was largely paralyzed by the Cold War, but since 1990 and the thawing of the global political climate, it has been very active.

The Security Council is composed of fifteen UN member States, five of which are permanent members -- United States, the United Kingdom, France, the Russian Federation, and China. The permanent members have the power to 'veto' a substantive decision of the Council by voting against it. The veto is cast much less often now than it was during the Cold War, but it is still very much in use as a threat which blocks Council action.

The other ten members of the Council are elected by the General Assembly to two-year non-renewable terms, with five new members elected each year. The ten elected members, known in Charter language as "non-permanent members," are selected according to a distribution formula from each of the world's major regions. The Security Council meets formally in both private and public sessions. The meetings normally take place in the Security Council Chamber at UN headquarters in New York and there the Council votes on resolutions and conducts other official business. The Security Council meets occasionally in private, mainly to decide on its recommendation of a candidate for the position of the UN Secretary-General. Since 1990, the Council has conducted most of its business in private

"consultations" (informal and off-the-record meetings) which are held on most weekdays during the year. Meetings are chaired by the powerful President, an office that rotates each month on an alphabetical basis among the Council's membership.

In addition to recommending the name of new secretaries-general, the Council recommends new State members of the UN, and it elects judges to the International Court of Justice, jointly with the General Assembly. In the key realm of peace and security, it performs three main functions. It assists in the peaceful settlement of disputes. It establishes and oversees UN peace-keeping forces. And it takes enforcement measures against recalcitrant States or other parties.

Acting under Chapter VI of the Charter, the Council 'shall, when it deems necessary, call upon the parties' to a dispute to settle it by peaceful means such as negotiation, mediation, conciliation, arbitration, or judicial settlement (Article 33). And it may, if all the parties to a dispute request make recommendations to the parties with a view to a peaceful settlement (Article 38). In practice, the Council often asks the Secretary-General or one of his Special Representatives to mediate or negotiate under guidelines the Council has established. Increasingly the Council members themselves have travelled to conflict areas in an effort to directly negotiate settlements or mediate conflicts.

Though the first UN peace-keeping force was established by the General Assembly, subsequent forces have been established by the Security Council, which exercises authority and command over them. The Council delegates to the Secretary-General its powers to organize and to exercise command and control over the force, but it retains close management and oversight -- too much so in the view of many Secretariat officials and military commanders. Though the Charter does not expressly provide powers to the Council for peace-keeping forces, the International Court of Justice in a 1962 case found that the Council has an implied power for this purpose.

Peacekeeping forces are usually deployed by the Council only after ceasefires have been agreed upon and so the peacekeepers are only lightly armed and should not be confused with an army fighting an opposing force. In the post-Cold War period, with greater consensus among its members, the Council has established far more peacekeeping operations than in the past. At a peak in the mid-1990s there were over 70,000 peacekeepers deployed. Some large and complex operations not only include soldiers but also civilian police, election monitors, de-mining and demobilization experts, and civilian administrative personnel.

The Security Council may also take enforcement measures which are more robust than peacekeeping. These enforcement powers are contained in Chapter VII of the Charter, which authorizes the Council to determine when a threat to, or breach of, the peace has occurred, and authorizes it among other things to impose economic and military sanctions.

The 'peace' referred to in Article 39 may involve conflicts other than those between states. At the time the Charter was established, it was envisaged that conflicts within the borders of a state could also constitute a threat to or breach of the peace, and thus that the Council could order the use of enforcement measures. The Council has broadened its definition of these cases over time, so that gross violations of human rights may now be seen as a threat to the peace, as was the case with the genocide in Rwanda.

In exercising its enforcement powers, the Security Council has imposed economic sanctions against a number of States and other parties. The great majority of these sanctions regimes have been imposed in the post-Cold War period. The Council imposed general trade sanctions on Iraq in 1990, but since then

he Council has preferred to impose more "targeted" sanctions such as arms embargoes, travel bans, restrictions on diplomatic relations, and bans on key commodities like petroleum and diamonds.

Under Article 42 of the Charter, the Security Council has the power to order the use of force to maintain or restore peace and security. However the collective use of force as a military sanction does not operate in the way originally intended. It was envisaged that States would conclude agreements with the United Nations, enabling the Council to require troop contributions to create and carry out military enforcement operations. Due to the Cold War this procedure was not implemented, and more recently there has not been the political will to return to the original intentions of the Charter.

Nonetheless the Security Council has delegated its Chapter VII powers to member States who volunteer their forces to carry out the enforcement action. These delegations of power include a delegation of a power of command and control over such forces, usually to those volunteering. Recently, the Council has delegated its enforcement powers to NATO in certain Balkan conflicts, to a force assembled by the Economic Community of West African States in Liberia and Sierra Leone, and to a multinational force led by Australia in East Timor. These are sometimes referred to as "coalitions of the willing." The best-known case is the coalition led by the United States that assembled under Resolution 678 in response to Iraq's invasion of Kuwait in 1990.

The Council has delegated its Chapter VII powers to member States for the attainment of various objectives including to counter a use of force, to carry out a naval interdiction against a state, to achieve humanitarian objectives, to protect UN declared 'safe areas,' and to ensure implementation of a peace agreement. Member states are often less than satisfied with the results of these operations, which are frequently seen as reflecting the interests of the powerful states taking part, and not sufficiently reflecting the will of the Council or the international community as a whole. But as long at the United Nations is relatively weak and short of resources, such compromises in the face of urgent crises are likely to continue.

States and non-state actors have made a wide variety of proposals concerning potential reform of the work, size, and composition of the Security Council. Concerning size and composition, the General Assembly adopted resolution 48/26 in 1993 which established an Open-ended Working Group to ‘consider all aspects of the question of increase in the membership of the Security Council’. The non-permanent membership of the Security Council has already been enlarged once in 1965 from six to its present ten. However any changes in the membership of the Security Council require an amendment of the Chartser which can only take place with the consent of ‘all the permanent members’.

The Committee at LGSMUN IX

The Security Council at LGSMUN VI aims to resolve the most pressing situations that the real world faces as the year 2016 draws to a close. The topic area, Cyber Warfare, is unique in the sense that it is perhaps the most complicated conflict that the world has seen in recent times, regardless of how clichéd the current and past efforts have been in dealing with the subject. Issues in this agenda will range from defining the parameters of cyber-warfare and recognizing the threat it poses to the world community to deciding on specifics of international law that should be in place to have a fail-safe mechanism in case of a drastic event. While this Study Guide has a comprehensive account of the issues in the Topic Area, research beyond the scope of this guide is strongly recommended for all delegates who wish to do well. Come prepared and well researched as we try to explore and re-evaluate the objectives of the United Nations and the Security Council itself.

Topic Area: Cyber Warfare

For the purposes of this Security Council simulation, the countries represented in this committee include: the USA, UK, Russia, France, and China; as well as Egypt, Senegal, Angola, South Korea, Malaysia, Ukraine, Venezuela, Uruguay, New Zealand, and Israel. A representative of each of the fifteen members must be present at all times at the UN Headquarters so that the Security Council can convene at any time as the need arises.

Voting Procedures

As per Article 27 of the UN Charter, there are usually two systems of voting in the Security Council. The first concerns procedural matters, in which decisions shall be made by an affirmative vote of nine members. The second concerns substantive matters; that is, on amendments and draft resolutions; in which decisions shall be made by an affirmative vote of nine members including the concurring votes of the permanent members. Should a P5 state exercise its veto power a resolution will not be adopted even if it has the required number of affirmative votes. Observer states may not vote on substantial matters.

Nevertheless, the Security Council in LGSMUN IX will modify the Rules of Procedure for voting so as to expedite debate. On procedural matters, decisions will be made by a simple majority. On substantive matters, decisions will be made by an affirmative vote of two-thirds of the council members (excluding abstentions), provided that no P5 state exercises its veto power.

Background

Bodiless, we swerve into Chrome's castle of ice. And we're fast, fast. It feels like we're surfing the crest of the invading programme, hanging ten above the seething glitch systems as they mutate. We're sentient patches of oil swept along down corridors of shadow.
William Gibson, "Burning Chrome", (1982)

Cyber Warfare: War of Shadow, Wall of Ice

In the short story "Burning Chrome", two IT savants Automatic Jack and Bobby Quine use a Russian software to hack the database of a local crime boss -- Chrome -- who handles the money transfers for organized crime. After a successful break-in, Jack and Bobby steal the vast amount of wealth stored in Chrome's bank accounts, only to uncover, along with other information, unexpected facts about the woman they love.

Since its introduction in 1982, the concept of cyber warfare has remained notoriously hard to define. For the initial purposes of this study guide, we use "politically motivated sabotage or espionage on information and communication systems carried out by states or non-state actors" as a working definition. The perpetrators of cyber warfare usually seek to protect their own information against misuse, damage, or destruction, while infiltrating, abusing, and damaging the data of their opponent. This is because information is power. Whereas in the past the train and the tank gave one a revolutionary upper hand in war, in the 21st Century it is information, and the Internet storing and connecting that information, that constitutes the most important factor for decision-making, aggressive campaigning, achieving domination, and for multiplying one's efforts.

Scholars have tried to categorise, organize, and understand cyber warfare. According to Igor Bernik, there are a few pertinent components of cyber warfare. It can involve psychological operations, which

affect the mental state of the opponent. For example, the Internet could be used to spread propaganda that influences the decisions and thoughts of people. It can occur electronically, in which the cyber warrior disables his opponent's access to key information. Then there is military deception, in which the cyber warrior, for example, manipulates information to deceive his opponent about his actual military capability. There is also physical cyber warfare, which Bernik defines as involving physical attacks on information systems. Finally, there are information attacks, which entail the abuse or destruction of information. Bernik's categorisations have their limitations: they do not encompass all aspects of cyber warfare, but rather present a sampling of their more pertinent effects. (One aspect of cyber warfare, for example, that Bernik does not evince explicitly is cyber warfare in support of military warfare.) These categories can also intertwine and overlap. Nevertheless, Bernik's ideas establish a laudable starting platform for delegates to understand the various effects of cyber warfare.

Real-world examples would help us anchor these theoretical postulations about cyber warfare. There have been three outstanding prongs of cyber warfare that present actual and potential threats to international peace and security: cyber-attacks, cyber espionage, and cyber operations for infrastructure attack.

The Case of Estonia: Politically-Motivated Cyber-Attacks Come of Age

Estonia and Russia's bilateral relationship has long been marred by strife and tension. The Soviet Union annexed the Baltic States in 1940, and hundreds of thousands of ethnic Russians relocated to Estonia during the Cold War. This was part of a Kremlin initiative to increase cohesion in the Eastern Bloc, and "Russify" Estonian culture. Following the end of the Cold War and the dissolution of the Soviet Union, the government in Tallinn implemented policies to minimize Russian influence in Estonia. Although Estonia joined NATO in 2004 and received the Atlantic Alliance's Article 5 mutual security guarantee, distrust of Moscow's intentions remained strong.

On the 27th of April 2007, the Estonian government relocated a Russian war memorial from the centre of its capital in Tallinn to a military cemetery. The Soviet Union had erected this memorial in 1944 to honour the fallen Soviet soldiers of the Second World War. This relocation angered the Estonian Russian-speaking population and sparked off two days of riots. At the same time, several key Estonian government, news, and bank sites were flooded with bogus requests for information that prevented them from functioning normally. These were known as Distributed Denial-of-Service (DDOS) attacks. Packet "bombs" of data hundreds of megabytes in size were sent first to one address, and then to another. Jaan Priisalu, head of IT Risk Management at Swedbank, stated, "[While] we usually [had] thousands of clients sending their queries, now there were hundreds of thousands . . . and they repeated their queries more frequently than people usually do." At their peak, more than one million computers were hijacked to create traffic equivalent to 5,000 clicks per second on some targets.

The impacts on Estonia were shocking and severe. Estonia had formerly been known as "the most wired city in Europe;" it even boasted a "paperless" "e-government". Nevertheless, this heavy reliance on the Internet proved to be a vulnerability as well as a strength. In a country where 97% of bank transactions occurred online, internet banking was disrupted first, and Estonians could not make the financial transactions needed to sustain their daily lives. As people began to panic, they turned to online news sites for information, only to discover that the DDOS attacks had disabled these as well. Without media connectivity, Estonians could not make their case abroad.

---

1 DDOS attacks are carried out when compromised personal computers organized into vast networks (botnets) are ordered by hackers to send millions of specifically composed requests simultaneously to a designated website or websites in order to

overload a server and cause it to shut down. The botnets are large sets of personal computers that have been infected with malicious software (malware) programs that allow hackers to control them remotely. The owners of these "zombie" PCs are often completely unaware that their computers are involuntarily participating in such cyber-attacks (Reuters, August 16; UPI, August 18).

Fig. 1 The "Bronze Soldier of Tallinn", the war memorial at the centre of protests in Estonia in 2007

Subsequently, government email servers and the websites of national ministries were inundated with spam, leaving the Estonian parliament unable to reassure, or instruct, their frightened population.

According to Jaak Aaviksoo, the then-Estonian Minister of Defence, "there was quite an emotional reaction . . . [when people felt that] there [was] something wrong [and yet] the government [was] not in charge." In some cases, situations were potentially life-threatening: the emergency numbers calling for ambulances or fire services were out of action for over an hour. The attacks on Estonia lasted for nearly twenty days, and brought the entire nation to a standstill.

.

Georgia: Before the Gunfire, Cyberattacks

Similar attacks occurred the next year during Georgia's war with Russia, but these appeared all the more ominous because they coincided with the advance of Russian military columns into Georgia.

Fig. 2. Map of Georgian Territory

The Russo-Georgia conflict centered on the Georgian provinces of South Ossetia and Abkhazia: These are officially part of Georgia, but have separate, "breakaway", and pro-Russian governments unrecognized by the Georgian government. On August 7, 2008, South Ossetian separatists began attacking Georgian peacekeepers. This ended a sixteen-year long ceasefire agreement since 1992, and then-Georgian President Mikhail Saakashvili sent troops into South Ossetia. Russia responded by moving its troops to the border, flying aircraft over Georgia, and beginning air strikes in South Ossetia. Interestingly enough, millions of requests for information jammed Georgian government and media websites one day prior to the Russian ground campaign. The targeted list of websites subsequently expanded to include the sites of financial institutions, educational institutions, businesses and western media such as BBC and CNN. The attacks then went beyond DDOS. At one point, the websites of the National Bank of Georgia and the Georgian Ministry of Foreign Affairs were defaced with images that likened the Georgian President to Adolf Hitler. Hackers also used the email accounts of Georgian politicians to send spam mail. In response to the cyber emergency, Estonia dispatched two information security specialists to assist Georgia, and key Georgian websites --including that of the President, the Ministry of Foreign Affairs, and the Rustavi 2 television channel -- were transferred to American servers better able to fight off sustained DDOS attacks.

The actual damage done to Georgia was minimal. Some government and commercial services were disrupted, but Georgia, unlike Estonia, was not as dependent on the Internet for its critical infrastructure.

As of 2008, there were 7 Internet users amongst every 100 Georgians. Moreover, Renesys, an Internet intelligence firm, ranked Georgia 74th out of 234 nations in terms of the number of Internet addresses, behind countries such as Nigeria, Bangladesh, Bolivia and El Salvador. The impact on Georgia was more informational and psychological. At the time of a Russian military invasion, the Georgians could not communicate their plight to the rest of the world. The Georgian media could not tell their side of the story, whereas at one point, Russian sympathizers flooded a CNN/ Gallup poll with over 300,000 respondents affirming that the Russian cause was justified. Moreover, the isolation and silencing of the Georgian people at the time of the Russian military invasion would have amplified their fear and sense of defeat. Many assume that both the cyber-attacks against Estonia and Georgia were carried out by the Kremlin.

Delegates will notice, from the two preceding sections, that the style of the study guide presents descriptions of recent cyber-attacks. These case studies may appear to be mere narrations of events but in fact contain many problems, assumptions, and implications for delegates to unpack.

Power Play in Cyber Espionage

Cyber warfare can take a more subtle form. Unlike the cyber-attacks in Estonia and Georgia which rampantly took computers offline, cyber espionage steals the data of an opposing force. Igor Bernik defines cyber espionage in this manner: Espionage seldom uses violent methods, since the aim is to obtain information secretly. The aim of the spy is, thus, to gain access to the information and pass it to the desired location without being noticed.

Many countries all over the world are committing cyber espionage, but the US, Russia, and China are arguably the most advanced and prolific cyber spies. This section, however, focuses primarily on case studies involving China. In recent years, China has directed more time, resources, and manpower towards cyber spying. Most of its cases thus far involve the stealing of financial and commercial secrets for economic gain rather than political advantage. According to US government reports, for example,

China has targeted US automotive industries, as well as the American energy, finance, and information technology sectors. Moreover, as part of Operation Aurora in 2009, China allegedly also stole the corporate intellectual property and private data of 34 major companies including Google and Adobe. Nevertheless, one of the most renowned cases of Chinese cyber espionage was launched against military and government targets. Operation Titan Rain, which began in 2003, refers to the wave of attacks on US defense networks that targeted confidential national security information. Although no data, allegedly, was stolen, many consider the attack one of the largest and most dangerous in the history of cyber espionage because each attack took a mere twenty minutes. In a single day, Operation Titan Rain could also target high-profile agencies like NASA, the US Army Information Systems Engineering Command, the Defense Information Systems Agency, the Naval Ocean Systems Center, and the US Army Space and Strategic Defense Installation.

In 2009, when hackers from an unnamed "foreign intelligence agency" made off with some 24,000 confidential files from Lockheed Martin, a big American defense contractor, China was once again implicated. The hackers could now eavesdrop on online meetings and technical discussions, and gather information about the sensors, computer systems, and "stealth" technology of the F-35 Joint Strike Fighter, a mainstay of future American air power. This thus compounded the delays of an already troubled program as American engineers tried to fix the vulnerabilities that had been exposed in the plane's design. Investigators traced the penetrations with a "high level of certainty" to known Chinese IP addresses and digital fingerprints that had been used for attacks in the past. Less than two years later, China unveiled its first stealth fighter, the J-20.

The US has called such cyber-attacks "[an] increasingly serious . . . threat to US critical industries" and has tried to bring China to order over the cases of cyber espionage. Nevertheless, the reality is that cyber espionage is becoming an increasingly integral part of modern warfare, and as long as it is possible for nation-states to commit it anonymously, they will be loath to voluntarily restrict themselves from doing so, and from gaining the upper hand over their enemy, when there is no guarantee that their enemies will do the same. For all its finger-pointing, the US is also likely guilty of illicit cyber activities itself.

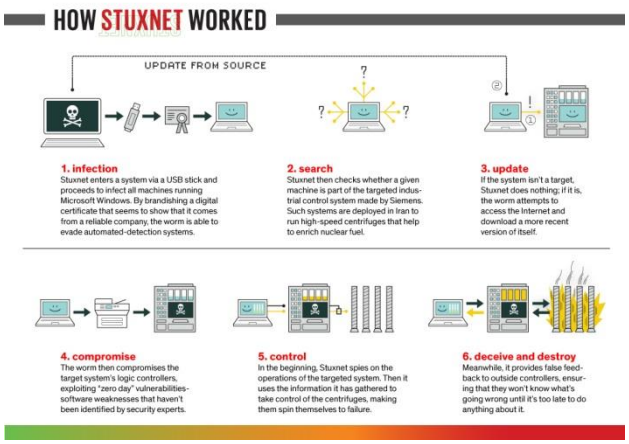

Fig.3 The inception, progression, and consequences of Stuxnet

Stuxnet: A Sabotage of Iranian Nuclear Facilities. In June 2010, a computer worm called Stuxnet infiltrated a nuclear facility in Natanz, Iran, where gas centrifuges spin like whirling dervishes to separate Uranium-238 (U-238) isotopes from Uranium-235 (U-235). Iran was allegedly collecting U-235 to build a nuclear weapon. Stuxnet infected the machine running the centrifuges and desynchronized the speeds at which the centrifuges spun, thus disrupting Iran's extraction of U-235. Stuxnet reportedly set Iran's nuclear programme back by two years.

Figure 3 above shows more clearly how the Stuxnet attack occurred. It took place in three main stages. First, it entered a system via a USB stick and through repeated replication, infected all machines running Microsoft Windows (Step 1). Next, it sought out the Microsoft Windows-based Siemens Step7 –a software which programs industrial control systems to operate centrifuges for nuclear enrichment. Stuxnet then spied on the Siemens Step7's logic controllers before seizing control of the centrifuges to make them spin themselves to death. All this was unbeknownst to the human operators at the plant. Stuxnet eventually infected the software of at least 14 industrial sites in Iran, including an uranium enrichment plant. Iran had to halt all enrichment operations at Natanz in November 2010 and decommission or replace some centrifuges.

The authors of Stuxnet have not officially been identified, but the size and sophistication of the worm -- for example, the coding to aim at precise software and hardware; the safeguard measures to prevent Stuxnet from being detected too easily; and the ability to erase itself on 24 June, 2012 from every infected device -- suggests that a national power was behind its inception. According to Roel Schouwenberg, a senior researcher for Kaspersky Lab, a leading computer security firm based in Moscow, a team of 10 people would have needed at least two or three years to create it. Thus, this makes it unlikely that Stuxnet was the brainchild of a ragtag group of black-hat hackers. The Iranian government has implicated that the US and the Israeli government were the masterminds behind the attack.
The case studies provided above crystallize the many conundrums associated with cyber warfare.

The Dilemmas of Cyber Warfare

1. Is the threat of cyber-warfare real?
Some disagree over the very existence of cyber warfare. In the view of John Michael McConnell, a former American spy chief, cyber war has already started, he says, and "[the US] is losing it." Not so, retorts Howard Schmidt, the former head of security at Microsoft: there is no cyber war. The more moderate opine that cyber warfare will be part of any future war. Then others disagree over the potential effects of cyber warfare. While McConnell believes that the effects of full-blown cyber warfare will be much like a nuclear attack, Bruce Schneier, an IT security guru, says that an apocalyptic attack on America ("movie-script stuff") will be difficult to achieve technically.

Experts may disagree over the exact nuance of the statements. But the cases of Estonia and Georgia seem to contradict Schneier's assertions, firstly by showing that modern economies can be crippled through simple technological means (e.g. a DDOS attack). Computer systems power virtually every sector of the economy, including energy, transportation, finance and banking, information and telecommunications, emergency services, defense, industrial bases, agriculture, postage, and shipping, as well as water, food, and public health systems; and more and more of these computer systems are linked up to the Internet. Could enemies then use logic bombs to, say, turn off the electricity in a country -- and from the other side of the world? The second reason why widespread damage, unlike what Schneier believes, is a possibility, is because once a key node in a network is down, other interrelated components of the network could also be negatively affected. Once electrical supplies are cut off, could oil refineries and pipelines explode, air-traffic-control systems collapse, freight and metro trains derail, or orbiting satellites spin out of control -- all within a day? This might sound like science-fiction, but can science fiction become reality? Steven Chabinsky, a senior FBI cyber-security official, believes that given enough time, motivation, and funding, all cyber barriers can be broken. If technology has made anything possible, the question is whether this is probable.

2. Cyber-attacks can render great damage, but how can we identify its perpetrators?
Many attribute the Estonian and Georgian attacks to the Russian Kremlin, but there is no concrete evidence of this. In these assaults, hackers infiltrated millions of others' personal computers from a remote distance, organized these computers into vast networks (called botnets), and then used these botnets to overload targeted websites with requests for information. In other words, the true hackers or "criminals" masked their identity and location by impersonating others, and ordinary citizens were made to advance cyber warfare unwittingly. These citizens were dispersed across countries including Egypt, the US, and Russia. Thus, this creates problems for the attribution of cyber warfare. Moreover, even though recent investigations have traced the attacks to Russian hacktivists, there is no evidence that these non-state actors were sponsored by the Russian Kremlin. To add a layer of chicanery, the Russian hacktivists were operating out of Russia. Thus, as for now, speculation of Russian state involvement only remains rife; something we note with irony in the statement of a senior NATO official, "I won't point fingers. But . . . this clearly bore the hallmarks of something concerted." Perhaps with the difficulty of attribution in cyber warfare, the alarming reality of the situation is that, in the information age, computer-savvy individuals can now threaten the sovereignty and wellbeing of nation-states from the comfort and anonymity of their own homes.

3. How can we establish a system of justice and responsibility in the cyber-world?
The challenge of attributing a cyber-attack makes it difficult to prosecute the culprits of cyber warfare, secure justice for the victim, and deter future cases of cyber-attacks. To use an analogy, traditional human spies risk arrest or execution if they are caught stealing copies of documents. But those in the cyber-world face no such risks. Consequently, as a senior American military source featured on The Economist puts it, "A spy might once have been able to take out a few books' worth of material . . . [but] now they take the whole library. And if you restock the shelves, they will steal it again." Apart from attribution, there are other legal bases of cyber warfare in disarray that hinder the act of prosecution for cyber-attacks. There is no universal definition or consensus on what cyber warfare is supposed to include, in what forms it is supposed to be carried out, and with which motives it could be identified.

4. Is cyber warfare even "warfare"?
Cyber-attacks deviate, in many ways, from the international norms of war. Firstly, the legitimate use of military weapons and tactics must discriminate between military and civilian targets, but cyber weapons often do not. This might be because networks connect most computer systems, and thus a virus aimed at a military site could spread to civilian sites. Alternatively, enemies might find it more strategic to attack civilian systems rather than military ones, firstly because the former's security is not as good, and secondly because crippling a few sites in a country's power grid, telephone system, or banking system can be more damaging to its capacity to wage war than disabling a few military command-and-control centers.

Secondly, the use of military weapons and tactics must be proportionate to the military objectives, but cyber warfare often causes unnecessary suffering or collateral damage. Because damage assessment is difficult for cyber-attacks (as most evidence of damage is hidden inside the data), this encourages massive attacks in the hopes of guaranteeing some damage. Mass destruction upon civilian computers in technologically-primitive countries could also be difficult to repair. Moreover, staging a cyber-attack sometimes involves manipulating a significant number of intermediate computers between the attacker and the victim in order to make the attacker's route difficult to trace. When attackers do considerable

exploratory trespassing, sometimes fruitlessly, to find a way to their target, they can also damage other systems along the sidelines.

5. Should victims of cyber-attacks be granted the right to self-defense and counter-attacks?
The United Nations Charter prohibits counter-attacks by nations unless attacked first, and the wording is sufficiently general to apply to cyber-attacks. However, the intended victims of cyber-attacks may be unclear, which makes it difficult to legitimize counter-attacks. Suppose an attack targets a flaw in a Microsoft operating system on a computer used by an international terrorist based in Pakistan. Is this attack directed at Pakistan, the terrorist organization, or Microsoft? Nations often think that attacks within their borders are attacks on the nation, but if the nation does not support the terrorist group, it would be unfair to interpret the nation as the target. Another concern is that counter-attacks are only allowed in international law against nation-states, and not groups within countries, however they may be defined. Yet cyber-attacks may be conducted by non-state groups (as in the Russian hackers in Estonia and Georgia) with unclear connections to the state. Moreover, given the unclear nature of the attacker, any retaliation can easily target the wrong source, possibly initiating an escalating series of tit-for-tat attacks.

Major Blocs

United States, China, and Russia

These countries have already been discussed in depth in the preceding sections. Such major countries are often both perpetrators and targets of cyber-attacks. The US may be responsible for Stuxnet. But the US also becomes the target for cyber-attacks because of its dependence on technology and its military superiority. Thus, given that a major country can either be the victim of a cyber-attack or the perpetrator of cyber-attacks to protect its own national security interests; will a major country necessarily have the incentive to regulate cyber warfare?

Countries with Smaller Economies

For this group of nations cyber weapons may prove to be a great asset. As cyber warfare is cheaper than conventional military technology and requires less manpower to sustain, it may suit countries with limited economic or social resources. North Korea, for example, may be one of the poorest countries in the world -- but it allegedly has as many as 1,800 cyber warriors that enabled its cyber-attack against Sony Pictures Entertainment in 2014. Cyber war programs also serve as a means for small nations to acquire another state's advanced technology, whether for commercial or military applications. To a small country, this would prove far more economical than developing similar technology from scratch. Finally, cyber weapons enable smaller countries to attack larger countries without as much risk of getting caught. In other words, smaller nations can now fight asymmetric warfare. Nevertheless, as small to medium-sized countries enter into discussions on cyberspace regulations, one concern remains: recent cyber-attacks suggest that fewer resources are required to wage an attack than to defend against one—which means that smaller nations may have more of a stomach for going on the cyber offensive than for stopping a similar attack.

Developing Countries

Developing countries find themselves in a bind: should they be regulating cyber warfare or opposing its regulation? The lack of regulation means that developed nations could use cyber warfare against developing countries -- from which it might be hard for nations with lower levels of technological

intelligence to recover. However, developing nations' lack of familiarity with the operations and effects of cyber space could result in the development of cyber space regulations that privilege developed nations. Could the regulation of cyber space also hinder developing nations' very abilities to catch up?

Past UN Actions on Cyber-warfare

In the General Assembly of 1998, Russia first introduced a draft resolution entitled: 'Developments in the Field of Information and Telecommunication in the Context of Security', which it developed in 2001, with a call for an international group of governmental experts who would determine the present and potential threats of the cyber realm. In 2004, the UN established its first group of governmental experts. However, the group's disagreements over the key aspects of international information security marred the production of a consensus report. The UN then appointed several groups of governmental experts over the next few years. In June 2015, the fourth and most recent group agreed upon a substantive consensus report (A/70/174) which defined the norms, rules and principles of responsible cyber behavior. The report also elucidated some of the measures for building international confidence and capacity in cyberspace. Finally, the report addressed the applications of International Law to the use of information and communications technologies and made recommendations for future work.

Between 2002 and 2004, the Economic and Financial Committee also introduced resolutions 57/239 and 58/199 directed at fostering a global culture of cyber-security while defending critical information structures. To do this, the resolutions stressed the need for developed countries to share their best practices and measures -- especially for the purpose of building the cyber defense capacity of developing nations. The Economic and Financial Committee subsequently introduced resolution 64/211 to reinforce the previous resolutions.

In addition to the UN actions listed above, delegates may wish to consult the following frameworks and examine their inherent loopholes to better determine how to regulate cyber warfare.

1. The International Law of War
2. The US National Strategy to Secure Cyberspace
3. The Cyber Security Strategy of the European Union: An Open, Safe, and Secure Cyberspace

Concluding Questions to Consider

1. What is cyber warfare?

How should we define it? How can we scope its implications and dimensions? How do we ensure that this definition remains relevant despite the continuously evolving nature of cyber warfare? A definition is fundamental to the establishment of an international legal code regulating cyber warfare.

2. How should we enforce accountability for cyber-attacks?

How can we identify the offender? What should we do in the case of Georgia where civil (non-state) actors responsible for cyber-attacks nevertheless have suspected though unproven links to the Russian state? Should the state then be blamed? Alternatively, given that the Russian activists in the Georgian case were operating out of Russia in other countries, should these countries be responsible for cyber-attacks originating from or within their region?

3. Is current international law on the use of cyberspace adequate?

Does the existing international law adequately safeguard countries against cyber-attacks or represent the interest of all state members, or should we aim to amend it? How will any international legal framework that is put in place account for the constantly evolving nature of cyber warfare?

4. How can or should a country respond to a cyber-attack?

How can the country minimize the effects of such an attack and the time taken to recover? In what circumstances does the victim nation have the right to self-defense? In the hazy world of cyber warfare

where the “perpetrators” and “victims” of cyber warfare are difficult to identify, should there even be a right to self-defense? In what circumstances can other countries come to the aid of the victim country without becoming drawn into an “act of war”?

5. What should be done to enforce cyber security on a multilateral scale?

Given the complex, fluid, and sometimes conflicting interests of each member state, how will the Security Council guarantee a safe and secure cyberspace through an agreement that is amenable to most?