WarMUN 2021

Security Council

United Nations

Study Guide

Welcome to the United Nations Security Council

Dear Delegates,

It is our pleasure to welcome you to the WarMUN 2021 Conference, specifically our committee, the Security Council. My name is Phillip and I am delighted to be chairing alongside Soham for this conference. Without dragging on about why, it is lovely to be back to meeting new people and getting back into Model United Nations. For those who are experienced, this is likely one of the first returning conferences you will have been to, and everyone is likely to be a bit rusty. Don't worry, we'll work with it. And for those delegates who join us for their first conference – breath. There will be moments when you feel totally out of your depth, totally lost, and confused as to how anybody wearing a suit could sound so foolish. I remember my first conference – wandering around the venue holding a lanyard and a piece of paper saying something about Human Rights. If you make it to the first session in one piece and on time, you are doing much better than I ever did.

Our job as chairs is to facilitate your weekend here at WarMUN 2021. In the obvious sense, we will be chairing the session, but also, and equally as important, we are here to be of use to you as delegates and guests. If there is an issue, please raise it with us, and we will endeavour to help as best we can. The same can be said for the Secretariat team. Now, a little about both of us;

Soham is a second-year student at the University of Warwick and is currently majoring in Philosophy, Politics and Economics. He finds himself highly interested in topics like Political Economy, International Relations, Macroeconomics and Industrial Economics. Beside academics, he likes getting disappointed by watching FC Barcelona play but still hopes that they'll win the Champions League every year. He also enjoys eating fresh fruit, drinking coffee and locally brewed Ales.

I (Phillip) am a third-year student at the University of Kent studying Philosophy and Politics with Data Analytics. Outside of my studies and Model UN, I enjoy training in Karate, and as of the start of this academic year Fencing. Like Soham, I have a keen interest in watching the football, although, as an Arsenal supporter, I truly understand what disappointment feels like. I've stopped hoping now.

Anyway, that's enough about us. Now we move onto you, our wonderful delegates. Both your chairs have invested many hours on this beautiful Study Guide, and for everyone's sake, please do read it. It will help you understand where we as chairs feel debate can go, in search of the holy-grail of MUN…. multiple resolutions passed in one committee. This guide is not everything, and please do your own research as well, but hopefully this will point you in the right direction.

We are very much looking forward to meeting you all!

See you soon,

Soham & Phillip

An Introduction to the Security Council

The United Nations Security Council (UNSC) is one of the five pillars of the organization, alongside the General Assembly, The Secretary General (and the Secretariat), The Economic and Social Council (ECOSOC), The International Court of Justice (ICJ) and the Trusteeship Council (now in disuse). It consists of 5 permanent member states, popularly known as the P5 and 10 temporary member states who serve 2-year terms in the Council. The P5 member states are USA, UK, Russian Federation, China and France.

It serves as the apex body of decision making related to issues concerning peace and security, where any decision taken would have to (ideally) be followed by all member states of the UN. However, if any P5 member choses to vote against any resolution of the Council, then the resolution doesn't pass. This power is popularly known as 'veto-power' and is often used if the resolutions present interests against any of the P5 member states.

The UNSC is also the authority which enables the UN as international actor to impose sanctions or authorize the use of force in the moments of crises and does so if there is consensus in the council.

For further information about the structure, functions and jurisdictions of the Security Council, feel free to find out more on https://www.un.org/securitycouncil/.

The Role of Foreign Policy

This would probably be the toughest test for all participating delegates as knowledge about foreign policy is only developed through experience. Throughout the weekend, delegates may feel morally challenged to present a view and we acknowledge that it is completely okay to feel so. However, our aim is to understand the perspectives of various countries on major issues and then try to accommodate their views and pass a resolution.

Notwithstanding, this doesn't mean that the Council *has* to pass a resolution. Sometimes, if the domestic and foreign policy of a country (say, the US) is not in line with the resolution presented, it may very well be voted against! Nonetheless, it is the task of a delegate is to convince all member states, through tact. This is where delegates develop the skills of diplomacy and communication and are marked positively for their ability to convince other delegates.

Everything would be learnt throughout the weekend, but delegates are advised to do some research on their country's political situation, domestic policy and most importantly-foreign policy.

Topic A: Disengagement by Permanent Member States in Long-Term Military Interventions

A Brief Introduction

Military intervention itself is quite a polarizing topic. It finds itself in a mélange of ethics, desperation, disparity and controversy. Let us take the example of India's intervention in restoring peace in Sri Lanka. Sri Lanka was (and still is to an extent) a highly divided country, with the Sinhala population asserting cultural, financial and linguistic hegemony upon the Tamils living in the north of the country. A militant group known as the LTTE chose to take up arms against the Sri Lankan state to make sure that 'justice' is provided to the Tamil people. Thousands of innocent people died due to the violent clash between the two groups while compromise from either side seemed close to impossible.

India – the pioneer of freedom in South Asia (supposedly) and the world's largest democracy – promised 'peace and co-operation' between the Sri Lankan government and LTTE. However, the situation worsened. The Indian Peacekeeping Forces (IKPF) got into direct military confrontation with the LTTE, resulting in more Tamil fatalities, more insecurity and lesser co-operation. The bid to ensure peace and co-operation failed and ended up creating more problems for India. The Indian Prime Minister (and PM-elect) Rajiv Gandhi was assassinated on 21 May 1991 by an LTTE operative as revenge for the hardships caused to the Sri Lankan Tamil people. A lack of a proper disengagement strategy, ulterior political motives and a dearth of proper deliberation led to a series of mishaps, which continuing today are a major part of both countries' histories.

Why should a country disengage?

What makes a country engage in the first place?

Is military engagement even justified?

Let's try and attempt to answer the last question first. Can a country be allowed to send its troops to a foreign land to protect the local people? The short answer would be a no. No country under international law is allowed to violate any other country's territorial integrity. The long answer is, that it is complicated. The UN believes that all member states in this world are members of the international community and it constantly campaigns for the improvement of the conditions of people around the world. If a local population is seriously under threat, then it is the duty of the international community, let by the UN to ensure the population's safety.

As mentioned, the UNSC is the apex body to approve sanctions and military actions against states that may threaten local populations. We can see this partially in the Yugoslav conflict and completely in the 1991 Gulf war. Many people see this as a success of the UN in ensuring peace and safety in regions in which it wouldn't have been possible without external intervention. However, we see that once there is engagement, the withdrawal (or non-withdrawal) of militaries ends up causing even more adverse consequences – for both the local populations and states intervening with military action. The consequences are what we need to take a better look at and take decisions on in the committee.

History

Give Me Freedom or Give Me Fire?

It would be foolish to deny the fact that in the modern day, the United States of America has played an integral role in shaping the world. The US through multiple spheres of influence – be it cultural, political or economic – has asserted its dominance as a global superpower, with even lesser challenge after the fall of the USSR. The US' influence however has not all been a bed of roses. With by far the most trained, technologically advanced and funded military program in the world, the US had asserted its hard power time and again at the global stage when it has had to.

The US and the international community was tremendously successful in 1991 when a UN-approved coalition of forces prevented Iraq from invading Kuwait, saving the lives of many Kuwaiti people. However, further interventions have proven to be (allegedly) disastrous for both the US and the country which was being brought 'freedom.' The 2003 Iraq war was one of the first steps taken by the USA in their 'Global War against Terror' where they toppled the Saddam Hussein government and were militarily engaged till 2011 when Obama chose to completely withdraw. The situation in Iraq since then hasn't been close to ideal. Deeply divided, politically unstable and highly impoverished- Iraq finds itself in a position worse than it was in the early 90s. So, is it the US' fault that Iraq is in such a position? Or was the fall inevitable due to internal differences? This is something which can be discussed in the Council.

An interesting case to make here is the fact that the American public was highly opposed to the '03 invasion of Iraq and they demanded constant withdrawal of forces throughout the period of engagement. The American people don't want their children to fight more wars and come back home traumatized or in worse cases, not come back home at all! In such a scenario, disengagement doesn't remain an international or foreign policy question, but it also becomes a question of domestic policy.

Afghanistan: A Crisis of Disengagement

In 2001, a huge chunk of Afghanistan (close to 90%) was controlled by the Taliban and some parts were controlled by the Northern Alliance. Post-9/11, the US initiated its Global War Against Terror to dismantle potential security threats and kill the man who they thought was responsible for the mishap in September- Osama Bin Laden. Bin Laden was killed on May 2nd 2011 in Abbottabad, Pakistan, but the War Against Terror was far from over.

The US invaded Afghanistan in 2001 with a coalition of various forces (UN approved) and was spending billions of dollars every year to ensure stability in the area. While the presence of American forces ensured peace in certain parts of the country, Afghanistan was clearly not secure. Through constant retaliation, guerilla tactics and eventual control of certain provinces, the Taliban could never fully be eliminated from the region.

Due to growing dissatisfaction of the public and serious economic considerations, the US chose to disengage from Afghanistan in 2021. What followed was a swift Taliban takeover of the Afghani state and the establishment of the Emirate of Afghanistan. 20 years of military effort was done away with within a month, and the Afghans found themselves in a similar position relative to 2001.

Analysis

Military Intervention: Boon or Bane?

Time and again it has been mentioned in the guide that the UN Security Council has sanctioned military intervention, especially in the 21st century. Clear examples of local populations being under threat have been defended through military intervention as in the case of the '91 Iraq war. However, in some cases, for example the Indian intervention in Sri Lanka, resulted in even worse conditions for all parties. Overall, military engagement is a very subjective issue and is often successful if there is international consensus. But this is only a part of the problem.

Military Disengagement

Oftentimes, we see that military interventions are successful in preventing adverse consequences for the people vulnerable to security threats. However, disengaging is where things to take a turn for the worse. Be it vested political interests of the countries involved or retaliation from the local population- the lack of a proper plan to *stabilize* and disengage very frequently worsens the conditions of the local population. Should the international community be responsible for setting up stable governments in these countries? Can the establishment of stability be conducted without expressing vested interests?

Role of Permanent Member States

The P5 (as explained in the introduction to the committee) hold immense political, economic and military influence on the international stage. They, combined, are capable of bringing major changes on a global level. Combined action of these states can enable in the improvement of various countries and populations in the world, but it is often not in their interest to do so.

The P5 countries are not moral heroes as well. Most of the time, their military interventions are led by vested interests of their respective governments and various parties in their countries. One example is of exploiting natural resources in the country in turmoil, therefore making the very expensive intervention profitable in the long term. Withal, what the P5 members have failed in doing so far is planning disengagement strategies in countries where they are/were militarily active, worsening the situation of the country in the process.

Can active cooperation of the P5 members help in building a future where countries under voluntary external military intervention don't fall into a crisis post-disengagement?

Role of the UNSC

The UNSC remains to be one of the most prominent political bodies in making decisions regarding international peace and security. With all P5 members having a forum to discuss the issue of disengagement, the Council will try to find out what problems countries face while disengaging and whether their actions are justified. Other temporary and observer states can pitch in and give a third-person perspective about the situation of military engagement in various countries and further point out the issues.

Then, the Council can also act as a healthy symposium of various solutions to strategic disengagement, and pass a resolution to take steps towards ensuring better conditions in countries where there is a scope of future disengagement.

Bloc Positions

While we encourage delegates to do their own research, we'll try to provide some perspectives in how might the Council act if certain questions are raised. If all countries agree (they may not) on disengagement strategies being a priority, then the Council will be more solution oriented with certain disagreements on tactics and methods.

However, this may not be how the discussion pans out. There are multiple states in the committee who have been subject to external military intervention and have suffered dearly in the process of disengagement. These countries will strongly push forward for an agenda of active disengagement. On the other side, there would be countries who represent interests contrary to the countries arguing for active disengagement and might defend their own interests considering their foreign and domestic policies.

Lastly, there would be some countries that may not have a stance at all. While they may choose to take a position of their choice, it is highly recommended that delegates do their research on which countries they are allied with and which interests would favor their country's agenda.

Listed are some questions and tips to help with understanding a country's position on the issue:

Questions

a) Has your country ever been occupied by a foreign force? If so, what were the results of the process of disengagement (if the foreign force left)?
b) Do you represent a country that has militarily intervened in the recent past? If so, why did the country take such an action?
c) If your country was militarily involved and then disengaged, then why did it have to disengage? Was it forced to do so or was it voluntary?

Tips

a) Thoroughly research your allotted country's foreign policy and which blocs they belong to (e.g., NATO, EU, ASEAN etc.).
b) Understand more about which countries are closest to your country in terms of foreign relations and what benefits you reap from that relationship (e.g., India was a close ally of the USSR and often received tons of aid from them. India mostly avoided voting against USSR in the UN due to their long-term friendship and the benefits India reaped).
c) Do thorough research on the position of your country on the agenda and subsequently of other countries as well.
d) Read previously passed UN resolutions on the issue.

Solutions

While we encourage delegates to come up with their own solutions, we'll attach some questions which might guide you towards a solution.

a) Is unsanctioned military intervention justified? Should there be penalties for countries who engage in unsanctioned military intervention?
b) Is sanctioned military intervention justified?
c) What is the right to militarily disengage?
d) Who should play a role in helping with the process?
e) Which parties should overlook the process of disengagement?
f) What should be the strategies to disengage?
g) How does the time period of the intervention (short term vs long term) affect the strategies?
h) How can we fund the process?
i) Is it even possible to disengage without any consequences for the country subject to military intervention?

Delegates should not limit their discussions to these questions. Rather, they are encouraged to come with their own ideas and discuss their country's perspective if they are relevant to the Council. Please do remember that research is key and no discussion would progress without proper research.

Links to information presented in the study guide:

a) https://www.cfr.org/backgrounder/sri-lankan-conflict
b) https://peacekeeping.un.org/sites/default/files/past/unikom/background.html
c) https://digitallibrary.un.org/record/1663785?ln=en
d) https://www.securitycouncilreport.org/un-documents/afghanistan/
e) https://www.nato.int/cps/en/natohq/topics_69366.htm
f) https://www.files.ethz.ch/isn/175025/WP01-TheUNSCandIraq1.pdf

Additional Resources

a) https://core.ac.uk/download/pdf/43540278.pdf
b) https://georgetownsecuritystudiesreview.org/2014/06/10/military-disengagement-from-politics-the-case-of-pakistans-revolving-barracks-door/
c) https://www.un.org/press/en/2021/sc14564.doc.htm
d) https://peacekeeping.un.org/en/disarmament-demobilization-and-reintegration
e) https://reliefweb.int/report/syrian-arab-republic/united-nations-disengagement-observer-force-report-secretary-general-3
f) https://undof.unmissions.org/

Topic B: Addressing the increasing cyber-security threat presented by non-state actors to national infrastructures.

Introduction

Cybersecurity is a new word for an old problem. Access to information and influence over state mechanisms have been key components of international conflict, espionage, diplomacy and trade for centuries – certainly since the establishment of the United Nations. The introduction of electronic communications and networking to state institutions over the past half-century has brought with it incredible opportunities for healthy, open international cooperation. With it as well, has come a new plain for crime, espionage and sabotage, be it by state or, key for this session, non-state actors. The new "Cyberspace" has largely existed outside of the conventional border politics that the UN specialises in, particularly the UN Security Council. This session of the UNSC should be used by delegates to introduce some actionable, formalised order to an otherwise unruly sphere of geopolitics.

Large swathes of national infrastructures rely upon electronic communications and networks functioning consistently and correctly. From healthcare to energy production, state governments are increasing utilising internet and software based architectures to provide these essential services. In times of war, infrastructure is always a key target, and domestically at least, countries have begun addressing and legislating for an age where infrastructure and cyberspace are very much linked. In this light, countries have poured untold resources into offensive and defensive cyber-capabilities, with entire industrial-military complexes being predicated on cyberwarfare. Notably, all P5 countries have homegrown cybersecurity infrastructure and industries which develop and grow in response to each other. Additionally, there exist some notable examples of countries selling cyber-capabilities abroad, for example Israeli government and industry has developed some of the more widespread and effective tools for the new cyberspace. Given the nature of cyber-weaponry and tools, as broadly non-physical and often anonymous, the use of such capabilities presents a new challenge to the international community. Unlike conventional kinetic weaponry, like guns and bombs, the use of cyber-weaponry means the distance from a target often becomes irrelevant. Furthermore, the potential to avoid attribution of an attack obstructs coordinated international responses, and difficulties diagnosing the damage caused by an attack prevent reliable rebuilding of infrastructure post-attack. Simply put, setting off bombs is loud and people notice, whereas cyber-attacks can be far more confusing, quiet and deniable. These are attractive qualities to any party wishing to cause damage to a state.

Further challenges exist when considering the threat of cyber-attack from non-state actors. Be they terrorists, solo criminals, organised criminal groups, "hacktivists", or any other non-state actor who wishes to employ cyber-capabilities to cripple or damage state infrastructure. Delegates should also consider the possibility of state actors using ostensibly independent actors as proxies for their cyberspace activities. These are the topics of discussion during our session, and they are in dire need of being addressed. Rapidly advancing technologies in energy, military, transport, healthcare and bureaucratic sectors provide useful administrative tools to governments, but also opportunities for new weakness to be found by belligerent actors. Current international cooperation on responding to conventional terrorists and criminals may serve as a useful model to adapt to their cyber equivalents, however the challenges of cyber-attacks are distinct, and now might be an opportunity to decide whether cyber-weapons are simply one more tool in a terrorist's toolbox, or an entirely different concept altogether.

History and UN Action

The following section will give delegates a diverse set of examples of cyber-crimes and attacks that they may wish to call upon when discussing the need for action on this topic. This is by no means an exhaustive list, and delegates will notice that examples given here have significant state-to-state components. This fact does not necessarily render these cases irrelevant to our discussion at this session of the UNSC, as it is not unreasonable to suggest that similar attacks and strategies would, at the very least, be of interest to belligerent non-state actors. Additionally, the use of proxies by states is not uncommon in cyberspace, and it is likely that this reality will need to be recognised in any solutions from delegates. Following the brief outlines of these case studies will be a breakdown of notable UN action and literature that delegates should be aware of before taking on the issue in session.

Notable Cases

- *"Ghostwriter" hacking group – Information Control*

A pro-Russian hacking group with suspected ties to GRU (Russian military intelligence), the "Ghostwriter" group has repeatedly been blamed for cyber-attacks on European and NATO officials, with the goal of sowing mistrust in governments and NATO/EU alliances through misinformation and disinformation. Unlike other attackers, the "Ghostwriter" group makes use of psychological and social engineering to obtain otherwise secure information, which then allows further access to countries' bureaucratic and administrative nervous systems. For example, in June 2021, using "phishing" email attacks (where emails pretending to be from a legitimate source ask for private information under false pretences) "Ghostwriter" succeeded in gaining access to top Polish government officials' emails, including the President's. The group then leaked sensitive and politically compromising material, sowing distrust in Polish democracy and administrative security. Included in the emails leaked were conversations about the Polish military and responses to COVID-19.

Another attack carried out by the "Ghostwriter" group involved the fabrication of a communiqué from NATO Secretary-General Jens Stoltenberg, claiming that the defence alliance was withdrawing its forces from Lithuania due to the coronavirus. "Fake news like this piece are aimed at sowing distrust in our alliance partners and NATO unity," Lithuania's then Minister of Defence Raimundas Karoblis said at the time. Delegates will be able to appreciate the potential for damage should such disinformation be allowed to continue.

- *Bangladesh Bank hack 2016 – Financial Instability*

This example offers delegates a demonstration of the importance of human error and social factors complimenting technological aspects to cybercrime and attacks. In 2016, North Korean-backed hackers successfully infiltrated the computer systems of Bangladesh Bank, the national Bank of Bangladesh in an effort to steal $1 billion. Hackers sent fake resumés to employees within the bank, who then opened documents attached to the email, which in turn planted malware in the systems. This malware then lay dormant in Bangladesh Bank's systems for about a year. When the attack commenced hackers sent a request to the United States Federal Reserve, where Bangladesh Bank maintained an account, through the "Swift" network to empty the account in to accounts controlled by the hackers. This network is a global, intra-bank apparatus where large amounts of money is transferred amongst banks at fast speed. Because of the successful hack into Bangladesh Bank's system, the request appeared to come from legitimate employees of the national bank. The attack was further aided by careful time-planning. In short, the attack began on a Thursday evening, at the end of the Bangladeshi working week. The request was with the US Federal Reserve on Friday morning, and was processed through Friday, whilst Bangladesh was on its weekend until Sunday. When the problem was discovered in Bangladesh, the banks in the US were closed as it was the weekend there, and this large window had allowed hackers time to transfer the money to the Philippines, where a public holiday again added more time to move the money.

The theft failed largely due to a fortunate coincidence and a series of spelling mistakes made while laundering the money, which prompted the US Federal Reserve's safeguard to flag for manual review, however the attempt was remarkably close to success. Bangladesh, however, is still yet to recover $65m, and delegates might imagine the scale of the economic crisis, and thus potential national insecurity, that may have resulted if the full $1 billion dollar target had been successfully taken in a country where 1 in 5 live below the poverty line.

- *Stuxnet Attacks – Vital Systems control*

Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. It generated a flurry of media attention after it was discovered in 2010 because it was the first known virus to be capable of crippling hardware, and because it appeared to have been created by the U.S. National Security Agency and the CIA. Stuxnet reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out. Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines.

In the Iranian case, conventional espionage and cyber-weaponry combined, with the virus being introduced to the system via a USB stick. The malware would then search the systems and networks of the nuclear facility for computers responsible for controlling PLCs. After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the equipment and machinery in the nuclear facility, whilst disguising this activity to anybody monitoring the systems from within the facility. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct. Delegates are encouraged to imagine the consequences of vital infrastructure being hijacked by terrorist or other non-state actors.

- *WannaCry 2017 – Ransomware*

The 2017 WannaCry attack is the largest example of a global ransomware attack to date. Exploiting a vulnerability in an older version of the Windows operating system (a vulnerability first developed by the US NSA), malware was spread amongst the networks of organisations that had frequently neglected to update their versions of windows and security software. The WannaCry worm locked user's files behind encryption, and only offered a decryption key for varying sums of Bitcoin, the online, decentralised currency. Notably, several of the organisations affected by the attack were public bodies. These included NHS organisations in the UK, as well as several hospitals all over the world, the Russian Ministry of the Interior, several Indian State governments, and the Chinese Public Security Bureau.

The denial of access to state systems and records obviously represents a significant security risk. Whilst a decryption key was offered in the WannaCry case, and many files were recovered through the discovery of a "kill switch" several days into the attack, there is no guarantee that the same will happen in future attacks. It is not beyond reason to suggest that an actor wishing to cause a state harm could deny access to tax, criminal, hospital, immigration or any other conceivable type of file, and then not offer a recovery tool. This attack spread quickly across borders, and the speed of the attack contributed to the difficulty in a coordinated international response, thus there is space for delegates to work here to prevent similar attacks in the future.

UN Action thus far

What follows is a brief summary of the agreements and resolutions that concern cyberspace and the enforcement of international law in cyberspace. The previous section's recent examples demonstrate that UN action has not successfully stamped out state-threatening cybercrime and attack. Cyberthreats present a relatively new challenge for the UN, and existing approaches to terrorism and international crime are applied with limited success. Below are links to previous resolutions directly concerned with cyberspace. So far as providing a coherent, effective and structured international effort to respond to non-state abuses of cyberspace, there is little from the UN thus far.

- **Resolution 55/63, January 2001** - Combating the criminal misuse of information technologies
- **Resolution 56/121, January 2002 -** Combating the criminal misuse of information technologies
- **Resolution 57/239, January 2003 -** Creation of a global culture of cybersecurity
- **Resolution 58/199, January 2004 -** Creation of a global culture of cybersecurity and the protection of critical information infrastructures
- **Resolution 64/211, March 2010** - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

Analysis and Forming Positions for Debate

Cyberspace presents a security risk to state infrastructure. This is a statement that has almost universal agreement amongst policy-makers, the media and academics. The scale and immediacy of the threat is however still debated, with a not-insignificant number of academics advising against sensationalising and exaggerating the risks of a largely unknown entity. Things tend to be scarier in the dark. This section of the guide is not intended to persuade delegates either way on this point. It is merely here to expose delegates to some of the more accessible and relevant pieces of academic literature which will certainly help delegates navigate this topic during the session.

Whilst an intimate knowledge of the technologies involved is not required, a general understanding of some of the facets of cyberspace will be helpful. Useful policy is unlikely to be forthcoming if nobody in committee can think of some tangible, specific solutions that directly deal with the technologies involved. This might mean briefly devoting some time (honestly not much) to understanding what a Blockchain is, or what a Distributed Denial of Service (Ddos) attack looks like, or some other cyberspace concepts. This guide isn't a bible to our session, and delegates should put some time into preparing positions for themselves, with specific focus on their respective countries cyber-capabilities and priorities. Fortunately, much of this general technical knowledge can be gleaned from engaging with the relevant articles and papers to this issue, some of which will be linked here (however the best delegates are likely to read outside of this guide's suggestions as well).

It might, however, be useful to briefly explore a few academic positions to set delegates off. Firstly, an evocative set of scenarios presented by Weimann (2006), adapted from Collin's paper (1997), represent some of the more visceral, realistic terroristic applications of cyber-warfare and weaponry of civil infrastructure. Weimann writes;

- *"A cyberterrorist will disrupt the banks, the international financial transactions, the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a cyberterrorist attempt to gain entry to the Federal Reserve building or equivalent? Unlikely, since arrest would be immediate. Furthermore, a large truck pulling alongside the building would be noticed. However, in the case of the cyberterrorist, the perpetrator is sitting on another continent while a nation's economic systems grind to a halt. Destabilization will be achieved.*
- *A cyberterrorist will attack the next generation of air traffic control systems, and collide two large civilian aircraft. This is a realistic scenario, since the cyberterrorist will also crack the aircraft's in-cockpit sensors. Much of the same can be done to the rail lines.*
- *A cyberterrorist will remotely alter the formulas of medication at pharmaceutical manufacturers. The potential loss of life is unfathomable.*
- *The cyberterrorist may then decide to remotely change the pressure in the gas lines, causing a valve failure, and a block of a sleepy suburb detonates and burns. Likewise, the electrical grid is becoming steadily more vulnerable."*

Disagreement over the practical application of cyber-weaponry is still, despite the fear-factor the above scenarios provides, worth considering when developing positions to bring into debate. It may in some countries interests to frustrate international efforts to restrict the actions of non-state cyber-attackers, this is explored in Eilstrup-Sangiovanni's paper (2017). Along with new opportunities to cause damage, come new challenges for belligerent actors, state or otherwise. The distance of an attack provides both safety for an attacker, but also helplessness should something go wrong, for example. A good introduction to this debate in academic circles might come from reading a set of open letters (it's not too long or boring) between Lindsay and Kello (2014) and Kello's original paper (2013). Their correspondence will also fill delegates in on the Stuxnet attacks described earlier.

To come up with some useful ideas, delegates will need to be creative, well-informed, and cooperative. Cyberspace is incredibly complicated, and it is unlikely that simply re-affirming previous UN resolutions or principles contained within them will convincingly solve the issues discussed. There already exist useful examples of international cooperation on both conventional crime and terrorism, as well as cyber-action. Collective action, as displayed by the EU in confronting the Russian-backed "Ghostwriter" group, or the United Kingdom's retraction of 5G infrastructure contracts with Huawei following pressure from the United States, may provide useful models and precedents for delegates to expand upon.

Useful Questions

- How should states be held responsible if non-state actors are acting with their backing/consent?
- Is cyber-terrorism distinct from conventional terrorism? Should this be reflected by UN policy?
- What is the role of border-bound state government in a borderless internet? Where do legal jurisdictions begin and end?
- Have states invested enough in their cyber-security? Do states have a responsibility to the international community to maintain cyber-security?
- What safeguards should be implemented to defend civilian infrastructures?
- What constitutes an act of war in cyberspace?
- How should international action be coordinated?

Bibliography

- Eilstrup-Sangiovanni, M 2017, *Why the World Needs an International Cyberwar Convention*
- Weimann, G 2006, *Cyberterrorism: The Sum of All Fears?*
- Thakur, K 2016, *Impact of Cyber-Attacks on Critical Infrastructure*
- Mohurle S & Patil, M 2017, *A brief study of WannaCry Threat: Ransomware Attack 2017*
- Waxman, MC 2011, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*
- Lindsay JR & Kello, L 2014, *A Cyber Disagreement*
- Kello, L 2013, *The Meaning of the Cyber Revolution; Perils to Theory and Statecraft*
- BBC- The Lazarus heist: How North Korea almost pulled off a billion-dollar hack
- Politico - Russia's 'Ghostwriter' hacker group takes aim at German election
- Politico - Leaked email scandal engulfs Poland's political elite