



VAMUN

XXXIX

United Nation's Security Council

Chair: Rahul Dhansinghani

Honorable Delegates,

It is my distinct pleasure to welcome you to the United Nations Security Council (UNSC) at the 39th Session of the Virginia Model United Nations Conference. These upcoming three days will be filled with heated yet fruitful debates, so prepare yourselves to be challenged as delegates. At VAMUN, you will have the opportunity to meet students from all over the country with different backgrounds while debating about important and prominent topics; most importantly, you will have an all-around amazing experience whether that is within the committee or outside.

I will be serving as your chair. My name is Rahul Dhansinghani and I am currently a second-year at the University of Virginia. I grew up in the Caribbean and moved to the United States, more specifically Richmond, Virginia, in 2011. At U.V.A, I study Systems & Information Engineering and Economics. On grounds, I am involved with the International Relations Organization, Indian Student Association as well Engineering Student Council.

At this session of the UNSC, we will be discussing two topics of significance within a region and globally: China's Uighur Internment Camps & Cybersecurity. Given the ambiguity regarding the China situation and the lack of effort regarding a uniform framework for cybersecurity, UNSC has the responsibility to use the power it has within the United Nations to enforce realistic and effective solutions to these issues.

Given the framework of our committee, the P5 countries will indeed have veto power; however, I encourage delegates who represent the other members of the UNSC not to be discouraged and understand that they do too have jurisdiction in the committee as well.

I look forward to seeing what all of you have to offer during debate and the creativity each one of you has when it comes to constructing solutions. More importantly, I am eager to see the different personalities each one of you have to bring to our small, yet important committee. I encourage each one of you to be well read – going beyond the background guide – on our topics as they can be confusing and hope everyone gives their very best at VAMUN this year. I look forward to meeting all of you and I know everyone will have an unforgettable experience at VAMUN 2019. In the time during preparation for VAMUN and this committee, please do not hesitate to contact me should you have any questions or concerns regarding the background guide, committee, or something else that is on your mental.

Best wishes,

Rahul Dhansinghani

Chair of the United Nations Security Council | VAMUN 2019

rad7ps@virginia.edu

Introduction to the Committee:

The United Nations Security Council (UNSC) is the organ of the United Nations (UN), in charge of maintaining international peace and security. This committee is also in charge of accepting new members into the UN, as well as voting on changes to the Charter of the UN. Due to the nature and importance of its job, the UNSC is the only UN body whose resolutions are binding to member states. In its purview also lie several UN enforcement mechanisms and peacemaking apparatuses, such as the deployment of peacekeepers and peacekeeping operations, the introduction of economic sanctions and the approval of permissions for military action. It is comprised of 15 members, 5 permanent members (P5) and 10 non-permanent members with 2-year terms. The P5: are the United States, United Kingdom, France, the People's Republic of China, and the Russian Federation. The UN Charter grants each country the right to veto resolutions under Article 27 (3) "Decisions of the Security Council on all other matters shall be made by an affirmative vote of nine members including the concurring votes of the permanent members." This means that a "nay" vote by a P5 member would result in the vetoing of a resolution; therefore, if a P5 nation may use an abstention as a soft "nay", in order to not instantly veto the resolution, nor count in favor of it.

China's Uighur's 'Internment Camps'

Background and Origin

Enclosed within a 2-kilometer exterior wall and punctuated by 16 guard towers, the massive secure compound has materialized three years later after the beginning of an aerial investigation of the land. Initially, satellites detected a patch of empty, untouched grey sand over the rolling deserts and oasis cities of China's vast far west, but in reality, the land was covered with internment camps. Xinjiang was where the first reports of the system of internment camps for Muslims began to emerge last year.

As of October 2018, the images captured by investigators not only suspect a big internment camp but rather an enormous one – one of the few that have been built across Xinjiang in the past few years.

"Re-education school" is the term that floats around Xinjiang to paint over the reality of what the internment camps are truly there for. With a denial attitude of locking up Muslims without a trial, China has used a euphemism for the camps as being educational purposes rather than the reality behind the curtain. The Chinese responded to the international criticism with a full-on propaganda drive showing glossy reports of clean classrooms and grateful students – who are there 'willingly', submitting themselves to the coursework. Interviews of the students sound more like confessions, where one student has even been caught proclaiming that he has "deeply understood [his] own mistakes" as he vows to a Chinese official to be a good citizen "after [he]

gets home.” It is clear that these facilities are there for one purpose that has been fallaciously represented to be by ‘re-education.’ The objective of these camps is to combat extremism, through legal theory, work skills, and Chinese language training. These facilities are exclusively built and developed in the manner of persecuting the Xinjiang’s Muslims (Uighurs) – a minority who often seclude themselves from the east and many of whom do not speak Chinese as their mother tongue. The growth and constant dodging of the reality of the internment camps that the Chinese have instituted only provide to the mystery. The international community allege that their true desire to eliminate the Uighur identity.

Uighur’s Origin in China

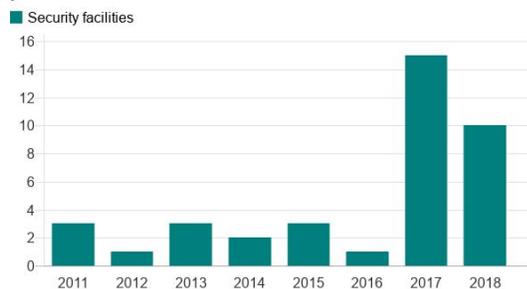
The majority of the minority population live in Xinjiang, many of whom speak a Turkic language and resemble the peoples of Central Asia at least as much as they do China’s majority population, the Han Chinese. The region, which includes southern cities of Kashgar, is often pointed out to be closer to Baghdad than Beijing – often even being succumbed by the culture of the former rather than the latter. The Uighur’s have had a history of rebellion and constant resistance with the Chinese rule and the relationship with the current established government is distant and tense. The city of Xinjiang often slipped from China’s grip given the geographical situation of the city and periods of independence with outbreaks of protest and violence; however, it has brought on huge levels of Chinese investment due to its mineral wealth having a seismic shift in economic growth and a rapid wave of settlers of the Han Chinese.

Recent tension, however, has rattled the foundations of the Chinese state with three Uighur occupants’ lives being claimed in 2013 on an attack in Tiananmen Square and 31 people slaughtered by knife-wielding Uighur attackers at a train station in Kunming – far away from Xinjiang. Over the past four years, Xinjiang has been the target of some of the most restrictive and comprehensive security measures ever deployed by a state against its own people. These include the large-scale use of technology such as facial recognition cameras, monitoring devices that read the content of mobile phones and the mass collection of biometric data. Harsh new legal penalties have been introduced to curtail Islamic identity and practice - banning, among other things, long beards and headscarves, the religious instruction of children, and even Islamic-sounding names. These actions only coincide with the tightening grip President Xi Jinping has on societies in which loyalties to family and faith must be subordinated to that of the loyalty to the Communist Party. They face severe travel restrictions, both within Xinjiang and beyond, with an edict forcing residents to surrender all passports to the police for “safe keeping”. Uighur government officials are prohibited from practicing Islam, from attending mosques or from fasting during Ramadan. Given all of this, there is the substance of a rapidly expanding network of mass confinement of a minority, aside from the distant relationship they share with the state, where the euphemism of ‘re-education’ can no longer hide the reality.

The Growth of the Camps

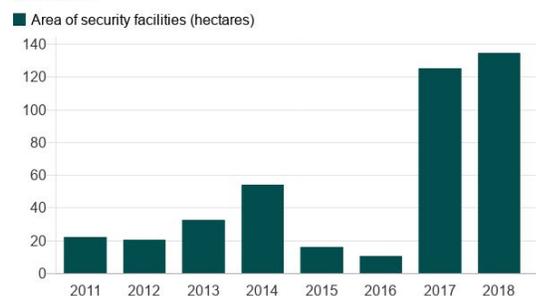
There has been mass recall of passports of Uighurs, preventing them from leaving China. There essentially is no one left outside these camps of whom the state believes should be in these camps. Analysts went through a list of 101 facilities located across Xinjiang - drawn up from the various media reports and academic research about the re-education camp system. One by one, they measured the growth of new sites and the expansion of existing ones. They identified and compared common features such as watchtowers and security fencing - the kind of things needed to monitor and control the movement of people. And they categorized the likelihood of each site actually being a security facility, placing 44 of them in the high or very high category. Then they plotted the first detection by satellite of each of those 44 facilities over time. The construction projects in 2018 have fallen in those compared to 2017; however, security facilities have increased in this coming year.

Number of new security facilities detected in Xinjiang province, 2011-2018



Source: GMV

Area of new security facilities built in Xinjiang province, 2011-2018



Given the figures above¹, the overall surface area of the facilities being built have increased every year since 2016.

Aside from the overall surface area and size of these camps, the place seems to be designed to pack as many people into as small an area as possible. With certain calculations, the estimate is of 130,000 people and minimum estimates of prisoners – around 11,000 – put it up with some of the largest prisons in the world; for a comparison, Riker's Island in New York, largest prison in the United States, has space for 10,000 people.² And the growth does not stop there, where authorities are looking at abandoned schools, public places, etc. to build more camps rather than from scratch – imprisoning more prisoners at a lower cost.

¹ "China's Hidden Camps." *BBC News*, BBC, www.bbc.co.uk/news/resources/idt-sh/China_hidden_camps.

² "China's Hidden Camps." *BBC News*, BBC, www.bbc.co.uk/news/resources/idt-sh/China_hidden_camps.



UN Response

The human rights groups called for the UN investigation into China's mass detention and to seek an international response to allegation of the abuse. The rights organizations, presenting the issue as a test of the United Nations Human Rights Council's credibility, urged it to set up an international fact-finding mission. Last year, European states and members of the group of Muslim nations had worked with in the Human Rights Council to set up an investigation of Myanmar's atrocities against Rohingya Muslims. "In our view, Xinjiang demands a similar response," UN official said.

Questions to Consider

1. What strategies can this meeting of the UNSC implement in which the abuse, and in other words 'brainwashing', can be stopped so the Uighur's have peaceful refuge in China as a minority?
2. Are the past actions by both parties justifiable in the action that the government has partaken?
3. How and to what extent should the UNSC intervene?
4. Have previous efforts in past situations as this worked? If so, how can they be altered to fit this situation should they work in this specific scenario as well?
5. How can the UNSC use its power and the backing of other organizations/committee bodies to create a resolution to stop this practice by the republic of China? With the

severity of this situation, are long-term solutions an option? What short-term/immediate actions can be taken to mitigate the situation at hand?

6. To what extent and how (if believed so) should the UNSC infringe on the sovereignty of the country?

Recommended Sources and Tips of Maneuvering for Research

- Look at all resources possible, especially personal accounts of people who have escaped or been released. There is not a lot of information regarding the details of the camp and much of the background and overarching sentiment is within the background guide; however, more information is never bad and the lack of personal accounts within this background guide can help put a better picture during research. The detailed anecdotes provide very little insight on what happens in the camps but enough for reference.
- To gain a deeper understanding on the Security Council, read the Introduction to the Committee section in this guide and branch out to witness what powers the UNSC has and when and how they have used it.
- Look at past situations in which the Security Council has acted upon, and highlight what steps they took and in which manner did they not overstep or did overstep in the sovereignty of countries.

Cybersecurity and International Cybersecurity Legislation

Key Terms

- “optionality” – regarding international law as an optional legal framework which states may or may not invoke
- “parallel tracks” – development of formal rules and informal rules shaped by practice without sense of a legal obligation, limiting state power
- Cyber domain – synonymous to cyberspace
- ICT – information and communications technology

Current Shift by the States within the UN

With more-sophisticated “cybertools” being developed to allow states to attack the systems of critical infrastructure being coupled with the ambiguity and uncertainty of the rules of states’ behavior in cyberspace, the need for common ground on international law regarding cyberspace has never been more pressing of an issue. The UN must work towards clarifying these laws to prevent future attacks and establish uniformity with acceptable uses of cyberspace. UN Secretary-General Ban Ki-moon, in the past, has appointed a group of 15 experts originating from the five permanent members of the UN Security Council alongside a handful of other

countries to study possible cooperative measures and threats regarding the use of ICT's. The report highlighted the desperate need of building confidence between states but more importantly having a set of 'norms, rules, or principles of responsible behavior of States.'

A recent study demonstrated that more than 40 states have developed military cybercapabilities – 12 of them being for offensive cyberwarfare, member states have now started to contribute in various ways in the form of cooperating in order to prevent *destabilization* of state relations in cyberspace.

Several sessions within August of 2012, January of 2013, and June of 2013 started gaining some traction as there were multiple reports of bilateral negotiation eyeing cybersecurity between the United States and with Russia and China. The summit of the Group of Eight in the June session resulted in the first-ever bilateral agreement on confidence-building measures regarding the cyber domain.

The United States and Russia established three kinds of cyber-specific crisis communication channels that were established: a channel between computer emergency response teams – known as CERTs, a 'telephone hotline' connecting the White House to the Kremlin for groundbreaking cyber-incidents, as well as the link between nuclear risk reduction centers. On the other hand, US and China agreed on another bilateral working group that stimulating discussions regarding mutual accusations of massive 'cyber-intrusions' on the sheer purpose of infiltrating military and economic intelligence of the respective States.

Highlighted in each of the meetings listed was essential categories for strengthening international cybersecurity: 'cooperation, international law, confidence-building measures, and improvements in states' capacities for building robust ICT infrastructures.' The progress achieved, especially with three major adversaries, allows for positive outcomes in expert groups as well a new-found approach of certain measures. Despite this progress, however, the international community still lacks concrete laws regarding the cyber domain.

Previous Actions

In December 2018, the U.N General Assembly adopted two resolutions – one led by the United States and the other led by Russia and China. The United States established the Group of Governmental Experts (GGE) whereas the latter two established the Open-Ended Working Group (OEWG). Both groups demonstrated significant overlap as both layout the development of rules and norms in the field of cybersecurity and the importance of international law that applies to the information and communication technology (ICT). While previous drafts of the GGE have failed (through four rounds of review), the Russians called for a new GGE which turned to be the OEWG. Usually, GGE's have a smaller membership – between 15 and 25 member states where the P5 are included – and even have time-bound mandates. By contrast, the OEWGs have a bigger membership, open to any of the 193 UN member states who can

participate in deliberations having an open-ended nature until all member states agree on common ground.

Since the failure of the UN-GGE in June 2017, the key states have developed three separate modes of action to rid of the threats possible to all states including their own. First, states have resumed the international cooperation – which led to the different-yet-similar resolutions that the U.N General Assembly adopted (see above). Second, the states have promised to exercise the voluntary international initiatives (Paris Call, the Charter of Trust, Cybersecurity Tech Accord, and Global Commission on the Stability of Cyberspace (GCSC). With cooperation from major tech corporations and private sectors there has been a sense of societal responsibility to fill the ambiguity that resides in the current policy. Major states seek to achieve this goal while preserving neutrality and credibility. The problem, however, is that many states have refrained from being involved in each other initiatives – something that needs change within the international community. Third, states have adopted a deterrence-based strategy percolating into – a vigorous cyber arms race. The approach is risky if not managed cautiously but could prove to be helpful. Unfortunately, no development for a long-term solution of ensuring security and stability in the cyber domain has been seen.

Split Personalities

Although Russia and the United States (the leaders of their respective resolutions) have positioned each other' resolution as mutually exclusive, the aura within the General Assembly has a different outlook on the two resolutions; therefore, voting in favor for both. During several meetings, many countries have argued and pushed toward a single resolution – focusing on small group of experts and much larger group of generalists that could compliment the small group of experts while raising awareness within the entire membership. The constant difference but similar resolution discussions does not allow for a stability and security from these threats and therefore, tends to be stuck in the mud when it comes to reviewing discussions.

Risks, Threats, Vulnerabilities

I. Risks

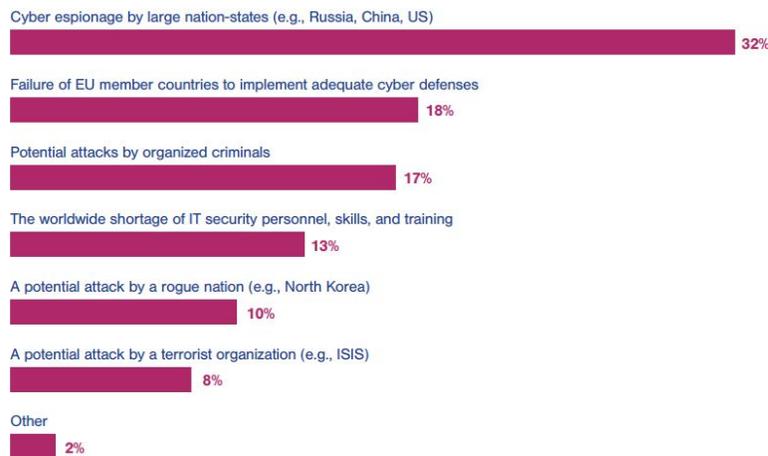
The fact that there is no common understanding on what the international rules for state behavior in cyberspace should be, is a factor that tends to be abused for legitimate and malicious reasons – proving to be a hole within recent developments. Taking a closer look, sophisticated exploitations of ICT technology can increase the risk of ‘false flag’ attacks pinning attacks on different states, groups, or individuals with different identities. Therefore, with such risks and possible developments a peaceful and open ICT environment has been called for addressing the risks and possible threats.

II. Threats

The truth about the threats is the fear of large-nation states taking advantage of a lenient framework on cybersecurity and attacking other states or groups with the possibility of no backlash. In a recent survey by the European Union 32% of the voters believed that the biggest threat to the EU cybersecurity infrastructure was large nation states. Lack of concrete framework is tearing down the trust within states and major states who seem to be controlling the discussion are the most feared in this situation.³

Greatest Cybersecurity Threat to EU Infrastructure

What is the greatest threat to the cybersecurity of EU critical infrastructure?



Data: UBM survey of 127 European IT and security professionals, September 2017

Universal Legislation

As this committee unfolds in this discussion, with the P5 being present as well as other large cyber-powers from all regions in the world, the discussion on having a recognized law that fully apply to all state behavior and provides stability and security within the legal framework is crucial.

Principles within a working developed universal legislation must address everything on the surface but cannot forget to cover areas of sovereignty and integrity as well as limiting the possibility of breaching intellectual property of companies and personal data of individuals. However, there needs to be a fine line on what specific actions need to be taken where there are diverse rules and actions that can be taken in order to protect the benefits the cyberspace provide. Legislation action is required but nevertheless so is technical attribution and as the Security Council, it is our job to focus on everything while also being able to challenge a state if needed to be.

³ <https://www.blackhat.com/docs/eu-17/Black-Hat-Attendee-Survey.pdf>

Questions to Consider

1. What is truly the root of the problem for the lack of clarity in previous resolutions being adopted? Why have no true actions been taken? Where does the Security Council play a role into that?
2. Is it better to have one universal legislation or act on many? Where is the common ground and where are the differences in previous legislations?
3. To what extent does the role of government/state have and when is it time to turn to organizations and companies? Can there be an achieved agreement between companies and state after developing an agreement of international law?
4. Till when does the dialogue shift from a broad anticipation to a narrow approach? What are the short term and long-term solutions that can be adopted?
5. Rather than developing new solutions, can the previous resolutions be adopted in a different manner that provides a universal legislation? What changes should be made as well as additions/subtractions?
6. With events of DNC, hack of Sony, Office of Personnel Management hack, and WannaCry being deemed to be executed by state or state-sponsored groups, how does the framework incorporate such events? Should there be action taken if state was involved?
7. How do we shift member states away from “optionality” and mandate the framework?

Key Tips for Committee and Maneuvering for Research

- Though the topic is heavily revolved around efforts of the P5 and major states, this does not mean other member states have little to no voice – but rather an equal impact in the committee.
- Aside from the research provided, look more into each of the resolutions and efforts made by the major states and attempt to understand whether their resolution was truly lacking proper framework or not.
- Look more into the events that aren't ‘involving’ member states to see whether the execution was a way around the current framework.
- Treat this topic as if it was in the Security Council whereas actions will be taken with the power of the UNSC and not as a General Assembly.

Works Cited

“Arms Control Today.” *The UN Takes a Big Step Forward on Cybersecurity* | *Arms Control Association*, www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity.

“China Denies Having 'Concentration Camps,' Tells US to 'Stop Interfering'.” *CNN*, Cable News Network,

www-m.cnn.com/2019/05/06/asia/china-us-xinjiang-concentration-camps-intl/index.html?r=https%3A%2F%2Fwww.google.com%2F.

“China's Hidden Camps.” *BBC News*, BBC,

www.bbc.co.uk/news/resources/idt-sh/China_hidden_camps.

“Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms.” *Council on Foreign Relations*, Council on Foreign Relations,

www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Perlez, Jane. “China Wants the World to Stay Silent on Muslim Camps. It's Succeeding.” *The New York Times*, The New York Times, 25 Sept. 2019,

www.nytimes.com/2019/09/25/world/asia/china-xinjiang-muslim-camps.html.

Stewart, Phil. “China Putting Minority Muslims in 'Concentration Camps,' U.S. Says.” *Reuters*, Thomson Reuters, 4 May 2019,

www.reuters.com/article/us-usa-china-concentrationcamps/china-putting-minority-muslims-in-concentration-camps-u-s-says-idUSKCN1S925K.

“The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.”

Council on Foreign Relations, Council on Foreign Relations,

www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.