
UNSC
Middle School Specialized Committee

Background Guide

Virginia Invitational

VIMNC

Model United Nations Conference

11th Session

March 1st-2nd, 2024

VIMUNC XI

MEI TORREY

SECRETARY-GENERAL

PEYTON WALCOTT

DIRECTOR-GENERAL

RYAN DADOO

CHIEF OF STAFF

SOPHIA BONGIOVI

UNDERSECRETARY-GENERAL OF GENERAL ASSEMBLIES AND SPECIALIZED AGENCIES

MATT TAM

UNDERSECRETARY-GENERAL OF CRISIS

Esteemed delegates and sponsors of VIMUNC XI,

Welcome to the eleventh annual Virginia Invitational Model United Nations Conference. As the MUN year winds down, we hope to provide the best experience yet, with paramount service and attention to detail that creates the greatest conference. From broad UN organizations to regional bodies, from corporations to criminal organizations, VIMUNC has committees that truly serve every interest. With experienced chairs, czars, and staff, we will ensure that every delegate truly has a positive experience, and we hope that you can enjoy your experience with us.

VIMUNC's 21 committees and over 850 delegates make this year's conference one of the largest editions ever, and we look forward to expanding our outreach across the DMV region to continue to provide a wonderful experience for all delegates. With a large MUN team that has years of experience, we hope that every single minute of the committee is filled with substantive debate that will create learning experiences that last for years to come.

So much hard work has been put into every single crisis update, background guide, and dossier, and we sincerely hope that the work and care placed in each aspect of this conference is displayed in its quality. If at any time you feel something about the conference is unsatisfactory, please don't hesitate to talk to your chairs, a staffer, or a member of the Secretariat.

Thank you so much for your commitment to VIMUNC XI, and best of luck in your committee, future conferences, and ambitions.

Sincerely,
Mei Torrey
Secretary-General, VIMUNC XI

UNSC

TOPIC A: *Cybersecurity and Its Potential Threats*

TOPIC B: *Cyberattacks and Hacking*

Overview of the Body

The UNSC (United Nations Security Council) was originally formed as a replacement to the League of Nations during World War II. The UNSC is one of six in the UN and is in charge of ensuring international security and safety, admission of new UN members, and approving any changes to the UN Charter. The UNSC has 15 members, each member has one vote, and all members are obligated to comply with council decisions. The security council takes the lead on all threats of aggression or attempts to break the peace, usually solving disputes with peaceful recommendations and terms of settlement. In dire cases, the committee can resort to imposing sanctions or the use of force to restore the peace. The council was first made in 1947 January 17 at Court House, Westminster, London and now takes permanent place at the United Nations headquarters in New York City and travels to many other countries today. When made the UNSC had five permanent members (The United States, Russian Federation (in succession of the USSR), The United Kingdom, China, and France) as well as 10 non-permanent members elected for two-year terms by the General Assembly

.

To quote the UN, “the Security Council has primary responsibility for the maintenance of international peace and security.” This includes identifying potential threats to peace or aggressive acts and calling on involved parties to find peaceful settlements. In escalatory cases, the Security Council may “resort to imposing sanctions or even authorize the use of force to maintain or restore” peace and security. It has the power to impose sanctions and other diplomatic actions of UN

member states against other states. The use of force to maintain safety and security for member states and others involved are within the jurisdiction of the UNSC. However, this jurisdiction is limited and requires the consent of many other parties.

Topic A: Cybersecurity and Its Potential Threats

Background Information: Cybersecurity encompasses more than just installing your preferred anti-virus software. It requires training and understanding of the methods that are used to attack organizations or individuals. This includes hiring professionals to install, manage, and monitor the infrastructure and tools used to defend their respective networks. Networks are as strong as their weakest link, and if users do not have basic fundamental awareness of cybersecurity, it leaves those networks vulnerable to compromise. Cybercriminals use ICTs to deliver spam to individuals personal email inboxes in the hopes an unsuspecting victim would click on a link that could download malware or send them to a site pretending to be legitimate with the intent for the victim to enter their credentials and other information. The same risks apply to corporations and governments. Any unsuspecting individual can fall victim to these sorts of phishing attacks, where the results could lead to catastrophic consequences. Misuse of ICTs does not stop there. Cybersecurity and Its Potential Threats Malware has been developed so that it can wipe out entire digital data repositories, spy on and track its victims4, hold entire institutions at ransom5, and effectively destroy physical infrastructure. These are some of the most notable examples of cyberattacks allegedly perpetrated by state-actors and criminal groups. It is important to differentiate between cybercrime and cyberwarfare and their potential motives, but to also note that criminal groups and state-actors' interests may align. In many cases, governments would seek to avoid direct involvement, and would sponsor groups to do its bidding. The issues that arise due to cyberattacks, is that eventually, if not immediately, regular citizens will fall victim to the downstream effects. In the case of JBS USA, service was restored within 72 hours. With the size of JBSs operation, any longer could mean that meat products would not get to supermarkets or grocers. JBS capitulated and paid the ransom to unlock its

system, but this does not necessarily bode a good outcome. The issue with this action is that victims never know if they will actually get back full control of their system. Good practice would be to have backups ready to restore your data, or even better, secondary sites that can go online in the event of disaster. These consequences can be worse for more upstream infrastructure, like energy. If a major energy provider were to fall victim to a cyberattack that reduced or completely shut off service to a region, country, or countries, hundreds of thousands to millions of people would be affected. With no electricity to power life-sustaining medical devices, chill their food, or control the climate of their homes especially during summer and winter months, people could suffer adversely or even perish. As technology continues to progress, the UNSC must take appropriate measures to combat cybercrime effectively, in order to protect the security and safety of millions of civilians worldwide.

The Role of Social Media in Cybercrime:

Fundamental disagreements between major powers still hinder progress in the advancement of peace and security in cyberspace. Although broad consensus was reached in the UN's Cybersecurity Open Ended Working Group (OEWG) on its language and recommendations, it fell short of addressing root causes of global cyber instability. 6 These current issues are known problems like inadequate protections for civil society in cyberspace and the infrastructure they rely on for their daily lives. Social media is also a vector for cyberattacks. With an estimated 4.59 billion people using some form of social media in 2022, and that number expected to grow close to 6 billion in 2027, it would be the fastest growing and possibly largest attack surface.7 Through the use of social engineering over social media, threat actors can fool users into giving up account names and passwords or other Personal Identifiable Information (PII). These attacks do not only leave society at risk from cybercriminals who wish to gain financially or for simple thrill-seeking, but from state and state sponsored threat actors. Social media can also be used to spread misinformation and sow discontent. Western liberal democracies in Europe and the United States tend to favor a more open and permissive internet, which leaves their societies susceptible to misinformation. Throughout the COVID-19 Pandemic, medical misinformation ran rampant over social media, and companies struggled to keep up with and police the proliferation of this phenomena. The usage of social media to spread discontent and misinformation is no new phenomena. Facebook was used as a vector to spread hate speech which led to

ethnic violence against the Rohingya Muslim minority in Burma (Myanmar) by the Burmese military from 2016 to 2017. The United Nations has accused the Burmese military of committing genocide against the minority population, where hundreds of thousands were displaced, and tens of thousands were

Questions to Consider

1. How will we prevent future cyber-terrorism?
2. Where will the funding for your plan come from?
3. What specific solutions can stop hackers from continuing their crimes?
4. What policies can the UN establish to improve cyber-security globally?

Topic B: Cyberattacks and Hacking

Background information: The growth of the Internet has allowed nations, organizations, and people to connect in ways previously unimagined. This new interconnectivity has allowed for collaboration, partnerships, and growth to reach unprecedented levels and has permitted the world to become a much smaller place. However, along with the benefits of the Internet, there are many new dangers created by this technology. The very nature of the Internet allows for individuals to hack information systems to steal information, cripple the delivery of services, and commit fraud. These cybercrimes are difficult to fight against, so it takes an international effort to combat them. This issue has come to the forefront in recent months after it came to light that organized hackers based in China were responsible for a series of hacks against American government offices and businesses. In 2015, the United States Office of Personnel Management was hacked which resulted in over 20 million government employees' sensitive information being leaked, including some confidential information about intelligence community officials. While government officials and experts have told press that the evidence demonstrates that the Chinese government was responsible for this breach , the US government has not made an official statement on Chinese government involvement, and Chinese state media has denied any government involvement in the hacks, stating it was carried out by criminals within China . In recent years, numerous hacks against businesses around the world have also been identified, perpetrated by groups ranging from underground hacking collectives like Anonymous, to cyber-wings of military organizations such as the Syrian Electronic Army or ISIL. The objective of these hacks has been to steal or government secrets, cripple infrastructure, or co-opt communications systems, which angers corporations and governments wishing to protect their interests, their information, and their security. Sometimes cyberattacks can have more tangible effects. In 2009, the US and Israel allegedly launched the Stuxnet virus against Iranian nuclear enrichment facilities and destroyed roughly a fifth of all Iranian centrifuges by making them spin out of control. In 2007, Estonia was targeted by Russian sympathizers for wanting to remove a Soviet statue from the capital, Tallinn. Several prominent government websites were hacked, and essential government services were disrupted. In December 2013. the credit and debit card information was stolen from over 40 million shoppers at Target stores over the holiday season. After
it was announced, people avoided shopping at Target and the company lost 46% of its profits and had to pay over $10 million in damages to affected shoppers. Some analysts warn this is only the beginning. As the internet and internet-linked technology become more widespread, the potential danger of cybercrimes

increases. If nothing is done to combat this scourge, almost nothing can be considered safe. Smartphones could provide hackers with a wealth of financial and other private information from its users. Stock markets could be manipulated to wipe out entire economies overnight. Power plants and water treatment facilities could be switched off, leaving people without basic necessities. Clearly this is an issue which needs to be addressed and the only way to address it is through international dialogue and cooperation.

Questions to Consider

1. What incentives can we provide member nations in order for them to enact policies to prevent cyberattacks?
2. What is the current scale of cyberattacks?
3. What has worked in the past to prevent cyberattacks?

Dossier

1. Albania
2. Algeria
3. Belgium
4. Brazil
5. China
6. Dominican Republic
7. Ecuador
8. Estonia
9. France
10. Gabon
11. Germany
12. Ghana
13. Guyana
14. India
15. Indonesia
16. Ireland
17. Japan
18. Kenya
19. Malta
20. Mexico
21. Mozambique

22. Niger
23. Norway
24. Republic of Korea
25. Russia
26. Saint Vincent and the Grenadines
27. Sierra Leone
28. Slovenia
29. South Africa
30. Switzerland
31. Tunisia
32. United Arab Emirates
33. United Kingdom
34. United States
35. Vietnam

Bibliography

Arindrajit Basu, Irene Poetranto, and Justin Lau, "The UN Struggles to Make Progress on Securing, Cyberspace," Carnegie Endowment for International Peace, May 19, 2021, https://carnegieendowment.org/2021/05/19/unstruggles-to-make-progress-on-securing-cyberspacepub-84491

Christopher Bing et al., "Ukraine Computers Hit by Data-Wiping Software as Russia Launched Invasion," Reuters (Thomson Reuters, February 24, 2022), https://www.reuters.com/world/europe/ukrainiangovernment-foreign-ministry-parliament-websitesdown-2022-02-23/

"Chinese government has arrested hackers over OPM breach" Washington Post http://wapo.st/1PwmNiO

S. Dixon, "Number of Worldwide Social Network Users 2027," Statista, September 16, 2022, https://www.statista.com/statistics/278414/number -of-worldwide-social-network-users/

"United Nations Security Council |." United Nations, United Nations, www.un.org/securitycouncil/. Accessed 15 Feb. 2024.