Committee: UN Security Council

Topic: Cyberattacks in Warfare

Theme of AUSMUN 2024

The theme for this year's AUSMUN is "Forging Tomorrow with Yesterday's Lessons". Dating back to 500 BC, great minds such as Confucius have spread this ideal: "Study the past, if you would divine the future". During a typical Model United Nations conference, delegates are expected to learn from their country's past and, in many cases, actively rewrite it. Historical knowledge when used effectively can lead to informed decisions; by reflecting on what has and has not worked in the past, collectively we are able to gain perspective on current and future policy. We encourage delegates to keep this ideal in mind while wrestling with the nuances and complications inherent in the ideas of modern day problems.

AUSMUN is committed to actively serving its community and combating pressing issues. As we continue to expand in numbers, we further seek to expand our positive impact on the world around us. We are proud to announce that we have partnered with Dress for Success, a non-profit organization that enables women to become economically independent by offering professional clothing, a network of support, and the resources necessary for both personal and professional growth. By participating in AUSMUN 2024, in addition to debating "model" policy, you are actively bettering society and changing the world.

The 2024 AUSMUN board is honored to host all delegates for our largest conference yet. We cannot wait to see what delegates bring forward to each committee in their efforts to embody values of collaboration and this year's theme. Looking twenty twenty-forward to seeing you!

Rationale

With the growing digitalization of the past decade, cyber warfare has become an increasingly prevalent issue. Starting in 2010, cyber warfare has threatened the infrastructure of countries and posed a threat to civilian populations. When used as a method of war, cyberattacks have the potential to harm numerous people (Gillis). With widespread power outages, data breaches, and financial losses, finding a solution to rebound and protect from cyber warfare attacks is critical for the safety of citizens of the world. Earth's heavy reliance on technology in all sectors of life has created a vulnerability to these attacks. Individuals, governments, and entire electrical grids are at risk of falling to cyberattacks from enemy countries. In only the past year, the risk of attack has increased from 12% to 23% (A Guide to). This statistic will continue to rise if not addressed immediately, and because information is so valuable in wartime, state-sponsored cyberattacks are growing in popularity. These breaches of data allow countries to gain access to military plans, infrastructure, and most harmfully, citizens' personal data. This threatens national security and can easily sway conflicts in favor of one side. Additionally, cyberattacks in warfare harm global economic stability. With an extremely interconnected and globalized economy, harm to one nation is felt worldwide. Cyber attacks in warfare have the potential to halt economies via the shutdown of specific industries. Lastly, the protection of citizens' freedoms is compromised

by a lack of cybersecurity. It is the duty of a nation to protect its citizens from attacks like these, which call for an immediate solution. This matter of national and personal security is a pressing issue that must be addressed to prevent harm to countries and our world as a whole. It is up to the delegates to create regulations around cyberwarfare and build up their cybersecurity systems to protect themselves from this growing issue.

Background of the Issue

Cyberwarfare is the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attack of information systems for strategic or military purposes. Cyber in the use of warfare is relatively new, having existed in the 20th century, but taking shape in the 21st century due to the reliance on more digital technologies. Cyber warfare has been used by various actors for decades, but it gained significant attention in the early 21st century with several high-profile incidents. For example, the Stuxnet malware attack in 2010, believed to be a joint effort by the United States and Israel, targeted Iran's nuclear program and demonstrated the potential of cyber weapons to disrupt physical infrastructure.

Cybersecurity has evolved from its origins in the early days of computing to a complex and ever-changing field in the modern era. In the 1960s and 1970s, cybersecurity focused on physical access and basic encryption, with early computer viruses like "Creeper" appearing on ARPANET. The 1980s saw the rise of personal computing, which brought new threats like computer viruses and the emergence of a hacking culture. As the internet grew in the 1990s, cybersecurity became more crucial, with large-scale attacks like the "Morris Worm" and the rise

of commercial antivirus software and firewalls. The 2000s ushered in an era of significant data breaches, exemplified by the TJX Companies breach in 2007, leading to government involvement in cybersecurity. Advanced Persistent Threats (APTs) like Stuxnet emerged, often linked to nation-states. The 2010s brought cloud computing and mobile security challenges, along with an increase in ransomware attacks such as WannaCry. Government regulations like the EU's General Data Protection Regulation (GDPR) aimed to enhance data protection. The 2020s witnessed the impact of COVID-19 on cybersecurity due to remote work, advanced cyber threats like the SolarWinds attack, and a growing arms race involving artificial intelligence and machine learning. This journey highlights the constant need for innovation and vigilance in the face of evolving cyber threats

Cyber Warfare has evolved over the years, marked by key events and developments that have significantly shaped its history. The Morris Worm in 1988, the first widely recognized computer worm, exposed vulnerabilities in networked systems, sparking an increased focus on cybersecurity. Stuxnet, a sophisticated malware targeting Iran's nuclear facilities in 2010, demonstrated cyberwarfare's potential to cause physical damage, while also highlighting nation-states' active participation in cyber operations with the alleged U.S. and Israeli involvement in Operation Olympic Games. The 2014 Sony Pictures hack by North Korea showed cyberwarfare's impact on private corporations and political motives. Additionally, Russia's interference in the 2016 U.S. elections through cyberattacks and disinformation campaigns revealed the influence of cyberwarfare on political processes and the role of social media in spreading misinformation. Significant developments in cyber warfare include the Tallinn Manual, establishing legal frameworks for cyber operations, and the formation of

military entities like U.S. Cyber Command, signifying the integration of cyber capabilities into military strategies. Despite progress in creating international agreements such as the Budapest Convention and the Paris Call for Trust and Security in Cyberspace, challenges persist due to rapid technological advancements, state-sponsored cyber activities, and the need for improved global cooperation and intelligence sharing.

Contemporary Evidence

The structure of warfare has seen many evolutions and transformations, especially since the modern invention of cyber warfare. Cyber warfare possesses the capability to impact both individuals and groups in many ways, including “Identity theft, financial loss, and even physical harm resulting from disruption to vital infrastructure and services” (Cyber Warfare). A recent notable cyberattack in warfare is Russia’s ‘NotPetya’ Cyber Attack in 2017, attacking Ukraine. Since then, several other countries have raised similar concerns surrounding Russia’s role in cyberattacks worldwide. Some problems that the world as a whole needs to address include setting regulations and restrictions against appropriate times for cyber warfare and keeping ethical considerations in mind. Another conflicting issue with this topic is the exploitation of organizations and countries, and how stealing information and money can become a solvable issue.

Across the world, many countries are currently combating the issue of cyber warfare. The United Kingdom, which is taking advice and following along behind the United States, is,

“strengthening its Network and Information Systems (NIS)” in order to “enhance cyber resistance” (Know the Risk). Other countries, including Germany, Japan, and Australia have been creating similar systems and policies for further prevention, such as the BSI in Germany and the ACSC in Australia. Other organizations, such as NIST and WIF are “issuing advisories” in order to fight cyber attacks on warfare as well (Know the Risk). Many countries are also investing in cybersecurity, and global spending on this is rising continuously. As of 2023, the global spending has more than doubled since the year 2017.

Directive

Delegates are encouraged to approach the issue of cyber warfare already familiar with prevalent instances of cyberattacks and understanding the nuances of the vast topic. Throughout the debate, delegates should prioritize exploring diplomatic solutions and collaborative strategies for addressing cyber threats. Delegates must engage in respectful and constructive dialogue, and all perspectives should be considered in debate. Emphasize the importance of working together as a unified committee to tackle this complex issue effectively. Delegates should consider the following questions:

1. What role should international organizations play in regulating and maintaining cyber threats?
2. How can international cooperation be strengthened to respond to and maintain the impact of cyber-attacks effectively?

3. How can the United Nations play a role in developing norms and regulations for responsible state behavior in cyberspace?
4. What strategies can be employed to address the growing threat of cybercrime and cyberterrorism?
5. How can the international community ensure that cybersecurity measures are balanced with the protection of individual privacy and human rights?
6. What tactics should be established to hold state and non-state nations accountable for cyber-oriented actions?
7. What role should emerging technologies, such as artificial intelligence and quantum computing, play in shaping the future of cyber warfare?
8. What is an act of cyber warfare, and how should it be defined in international law?

Resources for Delegates

Cyberwar

Cyber Attacks as War Crimes

Cyber Operations Tracker

Cyber Warfare

Future Warfare and Critical Technologies

History of Cyber Warfare and the Top 5 Most Notorious Attacks

Significant Cyber Incidents

The Global Cyber Threat

What is Cyber Warfare

Why State-Sponsored Cyber Attacks are a Global Threat

Delegations

---

1. **Afghanistan-** As a country plagued by seemingly endless war, cyber warfare is a new issue Afghanistan has experienced. The Taliban, a militant Islamic fundamentalist group, controls much of Afghanistan and poses a serious threat if they gain access to cyber warfare devices. While having already been attacked by the Taliban, Afghanistan works to strengthen the prevention, investigation, and persecution of cyber criminals.

   Does the Taliban Pose a Cyber-Threat

   Afghanistan, The Taliban, and National Security

2. **Australia-** Australia views Cybersecurity as an important part of foreign policy, values international peace and stability, and recognizes that resilient technology is critical. Australia has put many procedures in place in order to address this situation, such as the 2023-2030 Australian Cyber Security Strategy, which is meant to shield the cyber environment. Australia is encouraging others to join them in fighting against cyberattacks, hoping to get their neighboring countries on

board. An example of this would be the technology they implemented to prevent cyberattacks prior to their occurrence.

Cyber Affairs and Critical Technology

Offensive Cyber

3. **Canada-** As Canada has experienced the pressing matter of cyberattacks, the demand for security workers has profusely increased. The Canada Centre for Cyber Security serves as a beneficial resource for Canada, providing aid after any cyber incidents. Canada is known to be highly targeted and prone to cyber attacks.

   National Cyber Threats In Canada

   Significant Cyber Incidents Canada

4. **Chile-** In recent times, Chile has become a victim to many different cyberattacks. This has, in turn, caused Chile to become weaker in their cybersecurity, opening doors for more cyberattacks. The government of Chile has come to recognize this and implemented the Law and the National Cybersecurity Policy. In 2023, Chile was threatened by a hacker gang named Black Basta. They took many precautionary measures and have put efforts into updating their cybersecurity since.

   Cybersecurity Considerations in Chile

   Chilean government warns of Black Basta ransomware attacks after customs incident

5. **China-** China is at a great risk of cyber attacks given their vast technological advancements. Groups worldwide, such as Volt Typhoon, have threatened widespread attacks and received very little response. Along with criminal activity, fraud is a very common form of cyber crime in China.

   In the Evolving Cyberwar, China Aims to Take Down our Critical Infrastructure

   What to Know About China's Cyber Threats

6. **Cuba-** Because of Cuba's less advanced technologies compared to other countries and their internet blocks, the country is prone to receiving cyber attacks. The Cuba Ransomware Group has gained millions of dollars through their attacks on Cuba. Though Cuba recently launched their first planned strategy against cyberattacks, it was widely unsuccessful due to the lack of access to the internet across the country.

   #Stopransomware: Cuba Ransomware

   Cuba on Cyber Security

7. **Czech Republic-** The Czech Republic has been very adamant about preventing attacks. The Czech Republic has been attacked various times, with the attack on the Czech National Bank being one of the worst. Because of this, the government put in place the Act on Cyber Security, act No. 181, for the protection of infrastructure and information.

Cyber Security Strategy of the Czech Republic

Czech Republic - Country Commercial Guide

8. **Egypt-** Currently, Egypt is ranked ninth in the world on the Global Security Index (GSI). Unfortunately, many organizations are threatened by this. Egypt's cybercrime rate has drastically increased in recent years.

   Egypt on Global Security Index

   Manipulating uncertainty: cybersecurity politics in Egypt

9. **France-** France has been developing their cybersecurity systems since 2015 to prepare against attacks. These efforts are aimed at guaranteeing national sovereignty, responding to cyber crimes, informing the public, and mobilizing the international community. France does not actively use cyber warfare to attack other countries but is extremely dedicated to defending their country and its citizens. Additionally, France has taken the lead in proposing a Cyber Defense Pledge within NATO to ensure the safety of the global community.

   France and Cyber Security

   The French Government Says it's Being Attacked by Unusual Intense Cyberattacks

10. **Germany-** The BSI's report on cybersecurity in Germany from June 2022 to June 2023 revealed a heightened threat level, characterized by a record-breaking

increase in malware variants and a surge in ransomware attacks. The Cyber and Information Domain Service (CIR) will focus on combating disinformation, electronic warfare, and other hybrid threats. This service is just one response to increasing Russian aggression, including recent cyberattacks on German political parties.

Germany to launch cyber military branch to combat Russian threats

German government reports risk of cyber threats higher than ever

11. **India-** In 2015-16, around 58-59% of cyberattacks targeting India originated from Pakistani threat actors or operators based in the Middle East. However, today only 6.4% of threats stem from Pakistani actors or their affiliates, with a significant increase to 79% of threats originating from China.

    Indian organizations at very high risk of cyber attacks

    State-sponsored Cyberattacks Against India up 278% in Three Years

12. **Iran-** Iran is known for its aggressive cyber warfare tactics, often linked to state-sponsored cyberattacks targeting foreign governments and organizations. The country's cybersecurity presence is marked by a focus on cyber espionage and asymmetrical cyber capabilities, which it uses to exert influence and gather intelligence.

    Iran's Dual Strategy for National Security

    Iran Cyber Threat Overview and Advisories

13. **Iraq-** Iraq's cyber warfare and cybersecurity efforts are primarily focused on internal security and combating extremist groups' online presence. Although it has limited cyber warfare capabilities on a global scale, Iraq's stance centers on improving cybersecurity to protect national infrastructure and prevent cyber threats from destabilizing the country.

    Cybersecurity is a critical

    Summary of Iran

14. **Ireland-** Ireland has been increasing their cyber security efforts. Partnering with South Korea, Ireland took part in a seven-day event in order to test their systems' strength and ability to protect against cyber attacks. Cyber attacks have greatly impacted Ireland, costing them millions of dollars in repairs. In regards to healthcare, Ireland faced a major setback in 2021 due to an intensive cyber attack. Overall, Ireland's attempts to protect itself have fallen short in the past.

    Ireland's National Cyber Security Centre

    Ireland- Cybersecurity

15. **Israel-** Israel is renowned for its sophisticated cyber warfare capabilities and advanced cybersecurity infrastructure. Its proactive stance on cybersecurity involves significant investments in technology and a focus on both defensive and offensive cyber operations, establishing the country as a global leader in the field.

National Cyber Security in Israel

Israel's National Cybersecurity and Cyber Defense Posture

16. **Italy-** Since the COVID-19 pandemic, Italy has been exposed to a greater number of cyber attacks. Over seventy-five percent of Italian organizations have been or are expecting to be hit by a cyber attack. The Italian government is currently working on laws to increase and strictly enforce punishments for cyber attacks, specifically regarding warfare.

    Italian Government Proposes Much Harsher Jail Sentences for Cyber Criminals

    Italy cyber security and crime statistics and trends (2020-2024)

17. **Japan-** Japan has a comprehensive approach on cybersecurity, focusing on defense against cyber threats and promoting innovation and technology development. The country's cyber warfare stance is predominantly defensive, with policies aimed at protecting critical infrastructure and enhancing national security through international cooperation and partnerships.

    National Security Strategy

    CYBERSECURITY STRATEGY

18. **Mexico** - Mexico's thriving economy and strategic geographical position make it an enticing target for illicit cyber activities. Despite significant Foreign Direct Investment (FDI) and robust GDP growth, Mexico remains relatively vulnerable

in terms of cybersecurity and cyber defense. A recent major breach involving the exposure of classified government information, including thousands of emails from the armed forces, underscored the country's susceptibility to cyberattacks. According to experts, this can be attributed to under-investment and inadequate technological readiness.

Cyber Security in Mexico

Mexico Data Hacked

19. **Mongolia**- On January 18, 2021, NATO celebrated the completion of a multi-year project aimed at enhancing Mongolia's cyber defense capabilities, a valued partner of NATO worldwide. Since 2013, the frequency of cyber-attacks has risen annually, with an average of approximately 4 billion potential cyber-attacks recorded. The center's primary responsibility involves monitoring and responding to these attacks, a task diligently carried out by its team of engineers.

    NATO Helps Strengthen Mongolia

    4 Billion Cyber Attacks In Mongolia

20. **North Korea-** North Korea has been using cyberattacks as a powerful weapon in contemporary warfare, employing its skilled hacker networks to target enemies. North Korea, which is well-known for its prowess in cyberspace, has been linked to a number of well-publicized events. The dictatorship uses these attacks for both

ideological and strategic reasons, allowing it to project authority internationally, influence opponents, and wield influence.

North Korea Cybersecurity

North Korea's Cyber Capabilities

21. **Pakistan-** Cyber Security threats in Pakistan include hacking, identity theft, cyber-bullying, and more. The Economic Coordination Committee (ECC) has allocated Rs10 billion (approx. US $36 million) for cybersecurity. To address legal aspects of cyber warfare and International Humanitarian Law (IHL) in cyberspace, the International Committee of the Red Cross (ICRC) in Pakistan and the Research Society of International Law held an expert round table titled "Cyber Security and the Law" on May 17, 2023.

    Protecting Civilian of Cyber Warfare

    Pakistan's Cyber Security.

22. **South Korea-** South Korea is a leader in cybersecurity, putting a strong emphasis on technological innovation and robust defense against cyber threats. The country is known for its advanced cyber capabilities and proactive stance aimed at protecting its critical infrastructure and safeguarding against potential cyber warfare from neighboring states.

    South Korean Cybersecurity

    South Korean Cyber Laws

23. **Spain-** Spain has a strategic location, plays a major role in international affairs, and needs to be on guard against cyber threats that aim to compromise its government institutions, business sector, and vital infrastructure. Spain's defensive capacities must adapt with the digital environment in order to protect its interests in national security from cyberattacks.

    Distribution of cyber attacks in Spain in 2023, by type

    Global Cybercrime Report: Which Countries Are Most at Risk in 2023?

24. **Syria-** Syria's cyber warfare presence is centered on domestic control and surveillance, with the regime leveraging cyber tactics to monitor and suppress internal dissent. Syria's cyber security measures underscore a strong focus on maintaining internal stability through digital means.

    Syria Sanctions

    Syrian Cybercrime Law

25. **Turkey-** According to Ahmet Arslan, the Turkish Minister for Transportation, Maritime Affairs, and Communications, the Turkish government is gearing up to establish a national cyber 'army' to counteract the rising tide of cyber threats facing the nation. As cyberspace continuously evolves, connecting new devices, systems, and users at an unprecedented rate, the nature of the threats it poses is in constant flux, necessitating collaborative efforts for effective mitigation. The

onset of the COVID-19 pandemic further accelerated this dynamic, prompting swift and profound transformations in both government and private sector operations.

Turkey Establishes Cyber System.

In Cyber Security, Turkey Leads The Way

26. **Russia-** Russia's cyber presence is characterized by advanced technical capabilities and a controversial reputation due to its suspected involvement in international cyberattacks. The blurred lines between state-sponsored and independent cyber activities make Russia's cyber operations a complex and often ambiguous aspect of global cybersecurity.

    Russia Cyber Overview

    NATO Cyber Overview

27. **Ukraine-** During the Russia-Ukraine war, Ukraine has faced the imminent threat of Russian state-sponsored cyber attacks. While there have yet to be any extreme cyber attacks on Ukraine, the country is taking the necessary precautions to minimize technological vulnerabilities. Additionally, Ukraine has increased its public-private partnerships with cybersecurity organizations to develop new approaches to counter potential attacks.

    Cyber Operations During the Russia-Ukrainian War

    How Cyber Support to Ukraine can Build its Democratic Future

28. **United Kingdom-** With a rise of state-aligned cybercrime groups that target the UK, the country's parliament has been working to quickly improve its cyber security sectors. The government has hustled to implement regulations and sponsor government departments dedicated to enhancing cybersecurity. Additionally, the United Kingdom has adopted a 'whole of society' approach to continue to improve cyber safety. This works to shift the burden of cyber security from individual citizens to organizations.

    Cybersecurity in the UK

    NCSC Warns of Enduring and Significant Threat to UK's Critical Infrastructure

29. **United States-** With one of the most powerful militaries, the US is largely capable of launching and protecting itself from cyber attacks. The United States is currently the world's top cyber superpower as the US Department of Defense is very well funded. In recent years, the development of cyber technologies in the US has shifted from the defensive to the offensive in order to keep up with rival countries that pose potential threats to the American people.

    Cyber Warfare and U.S. Cyber Command

    Cybersecurity

30. **Venezuela-** As part of an alliance with Russia and China, Venezuela has become a hub for Russian and Chinese cyber technologies. Some have accused Venezuela

of abusing these technologies to surveil and control its population, going as far as to falsify votes in the 2018 elections. In 2019, Venezuela was the victim of a cyberattack, causing power and communication outages.

How Venezuela is Being Used as a Cyber "Hub"

Venezuela's 2019 "Cyber Blackout"

Works Cited

Buxton, Oliver, and Step Guide. “What Is Cyber Warfare and How Does It Work?” *Avast*, 14 July 2023, https://www.avast.com/c-cyber-warfare. Accessed 17 April 2024.

Gillis, Alexander S. “What is Cyberwarfare? | Definition from TechTarget.” *TechTarget*, https://www.techtarget.com/searchsecurity/definition/cyberwarfare. Accessed 17 April 2024.

“A Guide to State-Sponsored Cyber Threats .” *Radware*, https://www.radware.com/blog/wp-content/uploads/2019/12/rad1867_GuideToStateSponsoredCyberthreats_v6_FIN.pdf. Accessed 17 April 2024.

“"How War Has Changed Over Time."” *Wikipedia*, https://delfino.cr/2023/01/how-war-has-changed-over-time. Accessed 17 April 2024.

“Know the Risk: The Best and Worst Countries for Cybersecurity.” *BroadbandSearch*, 15 January 2024, https://www.broadbandsearch.net/blog/best-worst-countries-cybersecurity. Accessed 17 April 2024.

“Significant Cyber Incidents | Strategic Technologies Program.” *CSIS*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 17 April 2024.