MODEL UNITED NATIONS

2020

DIRECTORS WELCOME LETTER:

Dear Delegates and Faculty Advisors,

It is my pleasure to welcome you to the American University of Sharjah Model United Nations (AUSMUN) 2020. This conference has been the home of fruitful debate, practical resolutions, dedicated moderators, spectacular delegates, and diligent advisory and executive boards for the past twelve years and is continuing to do so for its thirteenth year. With 1000 delegates registered from more than 45 national and international educational institutions, this conference will be the biggest one yet!

This year's theme 'Embracing Diversity, Shaping the Future' has been designed to capture the essence of issues that surround our globalized society. Even though we have come this forward in time, there has been little to no improvement in accepting diversity as portrayed by the latest atrocities in several countries around the world. However, the future can be successfully be shaped for us, the youth, only by embracing diversity in every sector of life and we hope to draw attention to this.

This background guide has been formulated by our hard-working chairs and the research team to provide delegates with the starting point of their preparation for this three-day conference. The guide is initially divided into two sections based on the two topics and is further split into logical components. Firstly, the Summary and History section acts as an introduction to the issue by highlighting important events, terms, history, and global implications. Secondly, the Discourse on the Issue section establishes a link between the issue, its implications, significance, and the United Nations Charter. Lastly, the Past International Organization (IO) Actions and Latest Developments section elaborates on the previous action that has been taken and latest development in terms of the last actions taken with regards to the issue. At the end of each issue, delegates will find sections of Questions the Discussions and Resolutions Should Address and Suggestions for Further Research that aim to streamline the process of delegate's research. However, in order to grab a better understanding of the topic and be able to position yourself better to participate during the conference, it is advised to go beyond the background guide since this guide does not encapsulate enough information to be sufficient for every country and is only a brief introduction to the issues at hand. It is highly encouraged for delegates to view the 'Delegate Handbook' on the AUSMUN website and the 'How to Research' video on YouTube created by AUSMUN.

Finally, I would like to extend my sincerest gratitude to all the contributors to this background guide. It is the collaborative work of the Moderators, AUSMUN Research Team, and the AUSMUN Media Team. On behalf of them all, I truly hope that this guide will be of great help to you.

All the very best for the conference and if you have any queries or concerns, please do not hesitate to contact me at research@ausmun.com.

Sincerely,
Manaswi Madichetty
Director of Research
AUSMUN 2020

MODERATORS WELCOME LETTER:

Liana Hajeir

Emad Toubar

Abdulrahman Hamdan

Haneen Shahin

Dear Delegates and Faculty advisors,

It brings me great pride to welcome you to the American University of Sharjah Model United Nations (AUSMUN). This year, the conference has reached its 13th edition, and with that we are delighted to welcome you to the Cyber-Security committee for this year's conference.

State governments face several cybercrime challenges, which is a significant consequence of the rise in cyberspace technology. Cybercriminals have managed to commit numerous cybersecurity breaches in multiple international financial, military, and emergency establishments. Given that, it is essential to discuss these challenges in an international assembly in order to maintain the United Nations' (UN) agenda in preserving human security.

With the introduction of the Internet of Things (IOT), where all devices connect to the internet, it is now more important than ever to protect a user's data and information. The topics of discourse for this committee are 'Cybersecurity for Energy Infrastructure' and 'Collective Defense Against Cyber-Attacks.' These aforementioned topics are of vital importance because energy is significant to world politics, as well as important to cybersecurity defense in the modern world. Therefore, in this committee, we expect nothing less than dedicated and hardworking delegates that will work together to solve issues that are rising during this very technological age.

In order to succeed in this committee, we expect delegates to perform most of their hard work prior to the conference. A delegate must research the two topics of this committee, and write a position paper that outlines their country's stance on each topic. This is very important as it will help delegates understand the topics better, resulting in an improved experience overall. Finally, on behalf of the Cyber-Security chairs, we are very excited to meet each and every one of you!

Should you have any concerns or inquiries, please do not hesitate to contact us at b00069538@aus.edu.

Sincerely,
Cyber-Security Chairs

CS

Cyber-Security

Topic I

Cybersecurity for Energy Infrastructure

1. Summary & History

Cybersecurity is the act of protecting IT systems from cyber-attacks that could inflict physical or digital damage to hardware, software and databases. It deals with the unauthorized use of technology, or the use of technology to harm. As the world of smart devices and internet of things expands, attackers are growing more creative and innovative, which creates a challenge for governments and organizations in controlling cybercrime (Roberts, 2019). As the internet continues to become more widespread in today's society, almost everything has become integrated in a "smart" and wireless fashion. Among the many infrastructures and devices that have been successfully connected to cyberspace, energy infrastructures have become almost completely reliant on wireless connection. This shift has increased efficiency and improved the standard of living for many of the member states that have implemented such systems. However, the rising concerns of hacking and cybercrimes loom over a potentially new frontier for energy production.

Many efforts have been made by member states to ensure that cybercrimes do not become a concern when talking about critical infrastructures such as energy grids. For example, the African Union Convention on Cyber Security drafted (African Union, 2011) was an initiative that demanded that parties undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognizes the importance of Critical Information Infrastructure. The European Union also implemented the Cyber Security Strategy in 2013 which aimed to assess vulnerabilities in the European critical infrastructures and encouraged the development of stronger, more powerful systems (European Commission, 2013).

2. Discourse on the Issue

The significance and impact of the cybersecurity issue is highlighted when noting that the energy infrastructure of a country is responsible for national security, the economic well-being of a country and their residents' safety, according to the office of Cybersecurity, energy, security and emergency response. To put this into perspective, in "Enhancing cybersecurity in the energy sector: a critical priority" Smith (2018) states that, the US electricity grid encompasses 7,000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of miles of low-voltage distribution lines" and is referred to as the world's 'largest interconnected machine.' Any cyber breach in the energy infrastructure would clearly have drastic consequences, regardless of the country in which it occurs. The paper also elaborates that a cyber-attack on a single technological company could spiral out of control and rapidly spread to the energy infrastructure of the entire nation. Furthermore, the global impact of this issue can be additionally stressed when reviewing the quotes made by the department of homeland security secretary at the National Cybersecurity Summit, when he stated "cyber threats collectively now exceed the danger of physical attacks against us" (Homeland Security, 2018). Furthermore, at the same summit, the US Department of Energy secretary also stated that the economy of the world is driven so much by energy. It's our national security interest to continue to protect these sources of energy" (Malik and Nussbaum, 2018) which highlights the economic significance of cybersecurity on energy infrastructure.

3. Past International Organization (IO) Actions & Latest Developments

The energy industry continues to embrace the Internet of Things (IoT) with smart metering as well as other networked technologies that bring forth potential vulnerabilities. This development brings with it concern for nations and particularly, cybersecurity authorities.

The Energy Expert Cyber Security Platform (EESCP), an expert group which provides guidance or recommendations to the European Commission in respect to the energy sector, published the 'Cyber Security in the Energy Sector' report (EESCP, 2017). This report stressed the urgency for the energy sector to rapidly address the major current and forthcoming challenges of cyber threats and the need for cybersecurity to be adequately addressed.

The report further reaffirmed two major pieces of European legislation implemented for the baseline of cybersecurity across the EU Member States; the General Data Protection Regulation (GDPR) (2016), and the Directive on security of Network and Information Systems (NIS Directive) (2016). The EESCP Report settled with four key strategic priorities, but also highlighted that success depended on the capability and readiness of various stakeholders to collaborate and cooperate.

Key recommendations for energy providers included employment of a threat and risk management system, implementation of an efficient and effective cyber-incident response network, improvement in resistance and resilience to cyberattacks, and ensured technical and human competence and capability to address cyber-security issues in the energy sector.

The European Commission has also since published a 'Recommendation on Cybersecurity in the Energy Sector' (European Commission, 2019). The Recommendation stresses and builds on recent EU legislation concerning the energy sector, including the abovementioned. It puts forth guidance that pushes towards achievement of a higher level of cybersecurity. Additionally, taking specific characteristics of the energy sector into account, which include, the usage of legacy technology and interdependent systems across borders.

The Commission in the Recommendation calls on Member States to encourage industry stakeholders to cultivate knowledge and skills relative to cybersecurity and to include these considerations into their national cybersecurity framework where appropriate.

The Recommendation aims to:

- Address real-time requirements of energy infrastructure components.
- Implement relevant cybersecurity preparedness measures related to cascading effects in the energy sector.
- Protect against threats to legacy and state-of-the-art technology.

Additionally, the U.S. Senate passed a bipartisan cybersecurity bill titled 'Securing Energy Infrastructure Act (SEIA)' on June 27, 2019 that will study ways to substitute automated systems that have low-tech redundancies to protect the country's electric grid from hackers (Goud, 2019).

4. Questions the Discussions and Resolutions Should Address

- Who is responsible for ensuring the cybersecurity for the energy sector?
- Where will the funding for these security initiatives come from?
- To what extent will energy conglomerates sacrifice their privacy to ensure their cyber security?

- How should the exchange of data, in these security measures, be controlled and contained (who should have access to them)?

5. Suggestions for Further Research

- Role of energy stakeholders concerning cybersecurity
- Safety concerns

Topic II

Collective Defense Against Cyber-Attacks

1. Summary & History

Using the internet has become almost a necessity for all households in the majority of countries around the world. In fact, 3.9 billion people out of the 7.7 billion currently alive on Earth have daily access to the internet (Clement, 2019). It is safe to say that the internet has become important to keep us connected to our loved ones and with that benefit comes the responsibility of making sure that all web systems are protected against any and all threats.

For almost twenty years, the United Nations has been working continuously to combat many cyber-related issues. However, while protecting our cyberspace is a goal many members share and strive for, many rising challenges have held back progress in achieving that goal. Many member states disagree on how international laws should apply to certain cybercrimes, while others simply lack the capabilities of application and implementation of certain technologies that allow for better cyberspace defense. Despite these issues, the United Nations continues to emphasize and work on solving the issue of cyberspace defense by raising awareness and encouraging member states to strengthen some of their cyber-related policies.

2. Discourse on the Issue

The UN recognizes cybercrime as a breach of international law, and thus has implemented the principles of the law of state to fully address behaviors in cyberspace. The affirmation that the principles of the UN charter are applicable to state activities in cyberspace allows the governments to react to violations efficiently. Wolter (2019), mentions that in cyberspace, states must prohibit the use of force, and respect territorial sovereignty and independence, and must react to settle disputes by the same means as those used in the physical world.

Implications of cybercrime on world affairs could have a variable degree of severity. For example, relatively minor incidents can take place such as, individual company cybersecurity violations through digital transformation that lead to customer and employee data loss, negative exposure and revenue loss. In addition, major implications include the use of e-governments to access sensitive information and inflict harm thousands of miles away to physical infrastructure. (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018). Moreover, some of the biggest bank robberies in recent history have occurred through digital means (e.g. the $ 81 million cyber heist in Bangladesh. Iyengar, 2016).

The countries which are currently considered most vulnerable to cyber-attacks are Belgium, Dominican Republic, Hong Kong, Samoa, China, Afghanistan, Tajikistan, South Africa and Australia. Whereas the top 10 countries that are most prepared for Cyber Attacks include Canada, United States, Brazil, Norway, Germany, Estonia, Oman, New Zealand and Malaysia.

3. Past IO Actions and The Latest Developments

Multiple worldwide international organizations have been working on the issues of cybersecurity, cybercrime and cyber-attack defenses and those include but are not exclusive to the SANS institute, the OWASP (Open Web Application Security Project), WiCyS (Women in CyberSecurity), ISSA (Information Systems Security Association), and Center for Internet Security.

The UN General Assembly committee has previously formed a resolution on the "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures" (General Assembly, 2010), during which it recalled its previous resolutions in 2001, 2002, 2003 and 2004. The committee recognized the increasing use of information technology with average persons and governmental organizations, as well as the rising responsibility of these individuals and organizations to take steps to enhance the security of these ITs. It also focused on the importance of achieving universal access to data, including developing countries. It affirmed that the security of critical information must be addressed by governments systematically and that their national efforts must be supported by international organizations in order to enhance their cyber security.

The issue of cybersecurity was again addressed by the UN in 2018 during a panel discussion entitled "The Application of International Law in Cyberspace: State of Play" (Jabbari, 2018). During which, the representative of Austria to the UN opened the event by asking questions about what laws apply to cyberspace and what additional actions must be taken. The European External Action Service noted that the EU institute for security had been working to implement an active cyber plan for the European union. The conference also discussed cyberspace under international laws and agreements, and what constitutes a cyber-attack, and whether the attacked data is protected by International Humanitarian Law (IHL).

The Global Conference on Cyberspace (GCCS) are conferences where governments, private sectors and members of civil society meet to discuss, promote and enhance the practical cooperation in cyberspace, cyber capacity building, and the norms for behavior in cyberspace.

4. Questions The Discussions and The Resolutions Should Address

- Who is responsible for ensuring the protection against cyberattacks?
- Where will the funding for these security initiatives come from?
- To what extent should the general public sacrifice their privacy for the promise of security?
- How should the exchange of data, in these security measures, be controlled and contained (who should have access to them)?

5. Suggestions For Further Research

- Different approaches to solving cybersecurity issues (multi-sector and individualized)
- Accountability and responsibility of cyber attacks
- Privacy vs. Security Dilemma

References

African Union (2011). African Union Convention on Cyber Security and Personal Data Protection. Retrieved from https://ccdcoe.org/organisations/au/

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1). doi: 10.1093/cybsec/tyy006

Clement, J. (2019, January 9). Number of internet users worldwide 2005-2018. Statista. Retrieved from https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Energy Expert Cyber Security Platform (EESCP) (2017). Cyber Security in the Energy Sector. Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:-52013JC0001.

European Commission (2019). Cybersecurity in the Energy Sector. Retrieved from https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

General Assembly (2010). Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. Retrieved from https://undocs.org/pdf?symbol=en/A/RES/64/211

Goud, N. (2019). Automated US Power grids to be replaced by manual systems to limit Cyber Attacks. Cybersecurity Insiders. Retrieved from https://www.cybersecurity-insiders.com/automated-us-power-grids-to-be-replaced-by-manual-systems-to-limit-cyber-attacks/

Homeland Security (2018). Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech. Retrieved from https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech

Iyengar, R. (2016). FBI Begins Probing Bangladesh's Huge Cyber Heist as Top Crime Expert Gets Kidnapped. TIME. Retrieved from https://time.com/4265625/bangladesh-cyber-heist-81-million-fbi-tanvir-hassan-zoha/

Jabbari, C. (2019). The Application of International Law in Cyberspace: State of Play. UNODA. Retrieved from https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

Malik, N. S. and Nussbaum, A. (2018). Five Months After Energy Cyberattack, U.S. Pushes Collaboration. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2018-07-31/five-months-after-energy-cyber-attack-u-s-pushes-collaboration

Roberts, D. (2019). The Evolving Significance of Cybersecurity. EC-Council Blog. Retrieved from https://blog.eccouncil.org/the-evolving-significance-of-cybersecurity/

Smith, D. C. (2018). Enhancing cybersecurity in the energy sector: a critical priority.

Wolter, D. (2019). The UN Takes a Big Step Forward on Cybersecurity. Arms Control Association. Retrieved from https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity