MUN

DIRECTORS' WELCOME LETTER

Dear Delegates and Faculty Advisors,

On behalf of the organizers, the Advisory Board, and the Executive Board of AUSMUN 2019, it is my greatest pleasure to welcome you to the 12th annual AUSMUN Conference. With over 900 delegates registered from more than 40 national and international educational institutions, this conference will be the biggest one yet!

This year's background guide was diligently written to provide delegates with enough guidance for their research. It will act as a great starting point for delegates to familiarize themselves with the topics of their respective committee. After a short letter that gives the chairs a chance to welcome their delegates, a summary, a brief history, a discourse on the issue, and the latest developments of the issue will be presented. In the summary, delegates will have their first quick briefing on the issue were concerns will be defined. Followed by that, the guide delves into the root causes of the issue by identifying its history. Then, a discourse section will look into the issue with further scrutiny by presenting both sides of the topic's debate and examining some of its challenges and influences. Finally, it will aim to provide delegates with the latest activities in regards to the matter and any progressions in its respect. At the very end of the guide, delegates will find questions that will guide their thinking, some suggestions that will guide their research, and references that they can use for further relevant information. However, it is important to point out that depending solely on the guide will not be sufficient enough to prepare delegates for the conference. It is highly encouraged for delegates to look at the Delegate Handbook on the AUSMUN website and to view the "How to Research" video created by AUSMUN.

The theme of this year's conference is youth empowerment. This is very important as we are the children of tomorrow. Even if delegates are not necessarily planning on pursuing an occupation in the field of law or politics, MUN is an enriching experience to all. MUN is supposed to teach more than just details on a certain crisis, it educates them to work harder, to think on their feet, to learn from others and from themselves, to fall and to fail, and to break free from their fears. It dares them to be without hesitation. It dares them to add to the world. To Speak. To act. To know. We all understand how difficult it is to be a delegate. It requires a suspicious load of work and consumes most of one's energy. But we want delegates to give it their all and to get what they came here for.

Finally, I would like to conclude this letter by extending my gratitude to everyone who has contributed to this background guide in any way or form. It is the collaborative work of the chairs, the AUSMUN Research Team, and the AUSMUN Media Team. On behalf of them all, we truly hope that you find this background guide of great help and use.

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

Nada Nassereddin
Director of Research
AUSMUN 2019

WORLD CONFERENCE
ON CYBERSECURITY

Emad Toubar

Hamed Ali

Tasnim Elzini

MODERATOR'S WELCOME LETTER

Dear Delegates,

It is our privilege to welcome you to the twelfth conference of the American University of Sharjah's Model United Nations Conference (AUSMUN). As chairs of the Cyber Security Committee, we look forward to hearing your insights and ideas on our related topics. We also hope that our delegates grow from the debates and discussions they share throughout this experience.

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.

Since 2011, the Global Conference on Cyberspace (GCCS) has been held biennially to facilitate discussions between international leaders, policymakers, and industry experts to establish internet policies and enhance cyber capacity building. The conference welcomes over 2000 delegates, around 100 government representatives, and multiple keynote speakers, all with the shared aspiration of resolving current global cyberspace issues. Countries such as the United States, India, China, and Russia alongside multinational corporations (MNCs) such as Google, Apple, and Microsoft are all essential participants.

The GCCS discusses important topics such as the construction of standardized internet norms, which would be classified under internet rights or security. This is crucial as it is one of the many 'grey zones' that lacks sufficient regulation in criminalizing potentially harmful operations, which can have drastic implications on societies. Therefore, it is crucial to build consensus on the two topics discussed during this year's AUSMUN, which are both broad enough to be applied globally yet specific enough to cover all the pillars of human rights and human security.

The chairs hope that with the help of this background guide, our dear delegates will be able to conceptualize constructed research, arguments, and resolutions. We also hope you do not forget about the most important part of MUN, which is to make friends and enjoy yourselves.
If you have any concerns or inquiries, feel free to contact us at b00070346@aus.edu.

Best Regards,
The Cybersecurity Committee Chairs

TOPIC 1

Defining and Classifying Cyberspace Security Threats and Attacks

SUMMARY

"Cyberspace" is often defined as a globally interconnected network of digital information and communication infrastructures, including the internet, telecommunication networks, computer systems, and the information resident therein (Ottis, & Lorents, 2010). "Cybersecurity" can be defined as the protection of information systems from theft or damage, information on hardware and software, as well and the disruption or misdirection of the services they provide. Cybersecurity strategies include identity management, risk management, and incident management. (Espinoza, & Moditsi, 2016). However, while these definitions are encompassing of different notions, it is still difficult to pinpoint and to classify cyberspace security threats and attacks.

HISTORY

While cybercrime has become more prevalent than ever, hacking is not a recent phenomenon. Hacking was first used for large-scale attacks back in 1988 when 70 million dollars were stolen from the First Bank of Chicago (Secter, 1988). This resulted in widespread mayhem across the world and subsequently resulted in the establishment of the Computer Misuse Act of 1990 in the United Kingdom (UKPGA, 1990). In 2002, alarming statistics demonstrating the escalating rate of security incidents and cyber-attacks emerged – wherein the security incidents almost doubled (Byres, Leversage, Kube, 2007). This exploitation subsequently shed light on the vulnerability that the infrastructures businesses were based on (Coleman & Sapte, 2003).

In 2013, Edward Snowden's case caused a global uproar that alerted people once again of the lack of privacy online. It was revealed that breaches made by security agencies enabled them to tap into the servers of major internet firms including Google, Microsoft, and Facebook (Greenwald, 2014). The revelation made it clear that advances in cybercrime laws and enforcement alone will not be sufficient. Instead, organizations need to identify system vulnerabilities and implement protective measures to combat security threats and attacks (Coleman, & Sapte, 2003). Nielsen (2012) illustrates the domain that is cyberspace as a borderless, rapidly changing and growing. As such, it remains an ongoing

challenge that needs to be resolved to make it a habitable space that is suitable to everyone – organizations, internet providers, and internet users alike.

DISCOURSE ON THE ISSUE

Cyberspace can be accessed by everyone with internet access. As of June 2018, the number of people with internet access is 55.1% of the world population (Statista, 2018), where the number crossed the four billion people mark in October of 2018. That is a 1,066% increase from 2000 and comes to show the fast speed in which cyberspace is growing. However, a growing space naturally means that new things are added and internet policing is getting more challenging. This makes the space more vulnerable to cyber-attacks and security threats. Every encoded piece of information over the internet has a decryption key, and with available and developing software today, that key can be found relatively with ease. This, in turn, brings the question of how organizations and people alike are meant to safely store and transmit their data.

PAST IO ACTIONS AND THE LATEST DEVELOPMENTS

Crimes committed explicitly over the internet were first officially addressed in late September of 2001 at the UN Convention on Cybercrime in Budapest – though it was only made effective in 2004. A treaty opened for signatures to both Member States and non-Member States; the treaty specifically focused on infringements of copyright, computer-related fraud, child pornography, and violations of network security. It was initiated in aims of pursuing a common criminal policy aimed at the protection of society against cybercrime through adopting appropriate legislation and fostering international co-operation (Council of Europe, 2004). While that was the first convention devoted to cybercrimes, cyberspace problems were brought up in the General Assemblies prior to that. Russia submitted a resolution in the First Committee in 1998 to resolve global issues concerning internet security, of which the United States refused to support until 2009, where they become co-sponsors of the same resolution drafted in 1998.

QUESTIONS THE DISCUSSIONS AND THE RESOLUTIONS SHOULD ADDRESS

- Where does your country stand on the international measures and efforts taken to ensure cybersecurity?
- How has breach of cybersecurity affected your country's sovereignty and what were the changes made to prevent such attacks?
- What exactly constitutes cyber threats and attacks?
- Has your country been a subject of cyber terrorist attack in the past?
- Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.
- What entities should be placed in control of cyber security threat? Are the current frameworks such as the BSA and the global cybersecurity index sufficient?

SUGGESTIONS FOR FURTHER RESEARCH

- Asses your national participation in international efforts to combat cybercrime, such as the round the clock Cybercrime Point of Contact Network.
- Determine the cyber security and critical information infrastructure protection risks to your economy, national security, critical infrastructures, and civil society that must be managed.

-

REFERENCES

Byres, E., Leversage, D., & Kube, N., (2007). Security incidents and trends in SCADA and process industries. Network Security. Retrieved from: https://pdfs.semanticscholar.org/be64/146dadde896ba21c9be738ca8b9df2c7e8ff.pdf

Coleman, C., & Sapte, D. W., (2003). Cyberspace security. Computer Law & Security Review, 19(2), 131-136. doi:10.1016/S0267-3649(03)00208-5

Computer Misuse Act 1990. (1990, June 29). Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/contents

Council of Europe (2004). Convention on Cybercrime: Details of Treaty No.185. Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Espinoza, J., Moditsi, K., (2016). Combating Cyber Security Threats. Old Dominion University Model United Nations Society. Retrieved from: https://www.odu.edu/content/dam/odu/offices/mun/issue-briefs-2016/ib-cyber-intelligence-gathering.pdf

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state (First ed.). New York, NY: Metropolitan Books/Henry Holt.

Nielsen, S. (2012). Pursuing security in cyberspace: Strategic and organizational challenges. Orbis, 56(3), 336-336.

Ottis, R. & Lorents, P. (2010). Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, pp 267-270.

Secter, B. (1988, May 19). 7 Charged in $70-Million Chicago Bank Embezzlement Scheme. Retrieved from http://articles.latimes.com/1988-05-19/news/mn-4838_1_embezzlement-scheme

Statista, (2018). Global digital population as of October 2018 (in millions). Retrieved from: https://www.statista.com/statistics/617136/digital-population-worldwide/

USEFUL SOURCES

Jouini, M., Rabai, L., & Aissa, A. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489-496. doi:10.1016/j.procs.2014.05.452

Coleman, C. (2003). Cyberspace security:securing cyberspace — new laws and developing strategies. Computer Law and Security Review: The International Journal of Technology and Practice,19(2), 131-136. doi:10.1016/S0267-3649(03)00208-5, retrieved from https://www.odu.edu/content/dam/odu/offices/mun/issue-briefs-2016/ib-cyber-intelligence-gathering.pdf

United States. Department of Homeland Security. (2003). The national strategy to secure cyberspace. Washington, D.C.: Department of Homeland Security.

TOPIC 2

Safeguarding Privacy in the Digital Age

SUMMARY

In 2018, it was recorded that approximately 4.2 billion individuals have access to the internet (Internet World Stats, 2018). To put that into perspective, this means that every 1 in 2 people is a user of the internet. The internet has become an extremely essential part of many people's lives to the extent that it could be identified as a human right. It has become such an important medium for communication, business, entertainment, and much more. As this cyberspace medium continues to become more important and relevant in the lives of many citizens, more issues and threats arise alongside its evolution. Among the most important of these issues is the issue of digital privacy in the modern age. Many users continue to put their blind trust in the internet every day by sharing and storing their personal information on various websites. For example, websites such as Facebook and Instagram have amassed a large database of personal information shared by their users over the span of almost a decade. Since the internet is easily accessible by anyone, malicious criminals are able to also access these websites for their own personal gain. This puts the information of many users at risk and could also pose problems at a larger scale (i.e. governmental agencies' confidential information). With that in mind, digital privacy has become an essential topic to be discussed amongst countries to figure out the proper way to protect all the information found on the cyberspace.

HISTORY

In the past, the only methods of invading someone's privacy were through physical means. With the introduction of computers, however, invading personal privacy became a much easier task for criminals and organizations. Today, hackers simply access someone's computer and they can find a surplus of information that users trustingly store. That was until 1976 when two individuals, Martin E. Hellman and Whitfield Diffie, created the public-key encryption, which helped secure users' information from any invasion of privacy. Recently, in 2014, the European Union adopted the "Right to Be Forgotten". This states that "personal data must be erased immediately where ... the data subject has withdrawn his consent and there is no other legal ground for processing, the data subject has objected and there are no overriding legitimate grounds for the processing or erasure is required to fulfill a statutory obligation

under the EU law or the right of the Member States" (GDPR, 2018). Although a lot has been done to adapt privacy rights to evolving technologies, a permanent solution has yet to be found to the issue of technologies evolving at a rate beyond that of which governments are able to keep up with.

DISCOURSE ON THE ISSUE

From electronic communication to cloud computing, all cyberspace systems require the transmission of data from one entity to another, which is why in the current digital age protecting such information is crucial. In the current era, technology at its essence is both a problem and a solution for the issues brought up by information systems. Information saved in Data Warehouses can be easily misused if not managed properly as it can facilitate the accumulation of large amounts of data. As the details of our lives become more digitized, privacy concerns start to appear as soon as technology is involved. These technological advancements that are essential also introduce concerns for confidentiality and information security, and as such, confidentiality has become a pillar in our modern society (Singhal, 2007). For example, the e-commerce industry boosts marketers to capture consumer's marketing habits and form Data Warehouses about each person and later sold to the highest bidder. This however does not stop here which is why protecting such information is a major issue that has to be resolved. The National Institute of Standards and Technology (NIST) provides encryption standards for government agencies. Encryption, if properly implemented, is a powerful tool that allows organizations to safely secure sensitive data (CSRC, 2018). There are multiple approaches to securing data either by encryption or through following one of the published information security standards. In properly determining how best to enhance security, it is useful to have some basic principles for assessing data protection technologies. The data protection technology should allow for clear audit tracks to prevent data alteration or to identify when data have been changed. Not to mention, the technology should have the means to provide graduated levels of access to the data. However, as long as governments and private companies continue to collect information about people, there will be individuals attempting to access it.

INTERNATIONAL ORGANIZATIONS' PAST ACTIONS AND RECENT DEVELOPMENTS

The United Nations have introduced several resolutions towards improving the international state of digital privacy. One of its most recent actions has been the implementation of Resolution 68/167 in

December of 2013, which was done through the General Assembly. Resolution 68/167 aimed to modernize Member States' approach to privacy rights for the digital age. It also stated that "While the right to privacy under international human rights law is not absolute, any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy, and proportionality" (United Nations, 2014). The Human Rights Council later improved upon the digital privacy laws by adopting Resolution 28/16 in April 2015. The resolution, adopted by the Human Rights Council, called for the appointment of a Special Rapporteur on the right to privacy. The Special Rapporteur was given the task of reporting any violations of privacy and especially those linked with the rising new technologies, with the full assistance of all Member States (United Nations, 2014). On November 21, 2016, the General Assembly adopted another resolution to the right of digital privacy that aimed to specifically address private sectors. The resolution called for Member States to place stricter regulations on their privacy laws to prevent the private sector from violating the privacy of any citizen (Brown, 2016). The Cambridge Analytica scandal, which involved an app harvesting data beyond the scope of the terms and conditions, managed to use it for its political campaign and bank off easy consumers (Reichel, 2018). Another concerning development in the issue also occurred when it was discovered that Facebook has been giving companies such as Nike and Spotify wide access to users' personal information.

QUESTIONS THE DISCUSSIONS AND RESOLUTIONS SHOULD ADDRESS

- To what extent could privacy be compromised for the sake of security?
- How could user information be protected?
- Should governments and organizations have access to user information?

SUGGESTIONS FOR FURTHER RESEARCH

- Public Key Encryption.
- The Eraser Law.
- Edward Snowden and the NSA.

REFERENCES

Brown, D. (2016). New UN resolution on the right to privacy in the digital age: Crucial and timely. Retrieved from https://policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436

CSRC. (2018). NIST. Retrieved from https://csrc.nist.gov/

GDPR. (2018). Right to be Forgotten. Retrieved from https://gdpr-info.eu/issues/right-to-be-forgotten/

Internet World Stats. (2018). Retrieved from https://www.internetworldstats.com/stats.htm

Singhal, A. (2007). Data warehousing and data mining techniques for cyber security (Vol. 31). Springer Science & Business Media.

United Nations. (2018). The Right to Privacy in the Digital Age. Retrieved from https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx