Southern China International MUN

Security Council: On measures to preserve information security considering the threat of data breaches
Agenda overseen by: Jennifer Wang

1. Description of the Issue

1.1 History of the Issue

In today's increasingly globalized society, much of the world's information is experiencing a shift to being stored in cyberspace databases. This shift has proven to be revolutionary, but also dangerous; the cybercrime that has followed this shift has begun to establish itself as an increasingly prominent issue. Data breaching is a persistent threat to all governments and organizations. Cybercrime does not pertain to borders, and thus is not limited by them; such attacks spark chain reactions that can have staggering economic costs and may even wreak consequential damage on an individual scale. All states should find the preservation of information security to be important regardless of their socioeconomic status, and such an effort is only achievable through geopolitical collaboration.

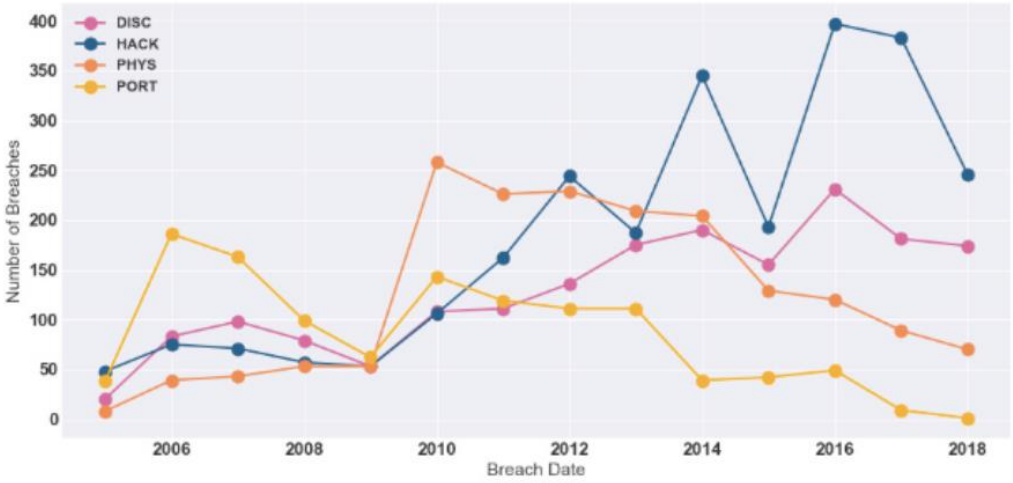
Data breaches are officially defined as "a cyber-attack in which sensitive, confidential or otherwise protected data has been accessed or disclosed in an unauthorized fashion. Data breaches can occur in any size organization, from small businesses to major corporations"[12]. There have been several major data breaches over the years and affected parties have ranged from individual citizens to national governmental organizations. For instance, one of the worst incidents which have involved data breaching was the United States' Equifax data breach in 2017. There were 148 million affected records, and individuals' personal information such as Social Security numbers, addresses, driver license numbers, and credit card numbers were compromised. The breach had been undiscovered for months before $700 million was used to compensate those who had been affected by the data breach after its discovery. Equifax not only suffered from this breach financially, but they also underwent reputational damage and was faced with congressional inquiries as well. [21] The Equifax data breach is only one of countless ruthless cyber-attacks that have triggered massive consequences on every level.

Consequently, this has given way to increased attention to the governing of **cyberspaces,** known officially as the "technical architecture that allows the global internet to function"[17].

For digital safety, states, industries, and individuals that use technology may find it in themselves to look towards international laws that determine permissions, regulations, and prohibitions on the use of technology.

The countries of the United Nations have put a particular emphasis on the significance of furthering information security through various policies and treaties. One of these treaties (and the most influential one currently) is the *Council of Europe Convention on Cybercrime*, also known as the **"Budapest Convention."** This convention has been ratified by 67 countries, including Australia, Canada, the European Union, Japan, the U.K., the U.S., and more.[1] This convention aims to harmonize national law, promote international cooperation, and define criminal offenses among other things.

Information security first posed to be a threat in 2005, according to breach records provided by **Privacy Rights Clearinghouse (PRC);** since then, there have been more than 9000 breaching incidents archived with around 12 billion records.[16]



(b) Breaches type evolution over time

Fig. 1: Data breaches by type

Although the issue of data breaching was discovered relatively recently, the number of data breaches around the world have been increasing at an alarming rate. A historical analysis of breach records shows that health organizations have been the most targeted, as it contains sensitive personal information that easily allows for identity theft. Multinational companies come next, with NGOs being the least attacked type of organization. Government and military breaches take up a small percentage, presumably due to their strong security frameworks—however the breached data results in dire repercussions.[16]

Table 1: Number of Hacking Breaches recorded by type of Organization

Type of Organization	Number of Hacking Breaches	Proportion
BSF	214	8.21%
BSO	**619**	**23,76%**
BSR	301	11.55%
EDU	295	11,32%
GOV	148	5,68%
MED	**952**	**36,54%**
NGO	38	1,45%

In response to these attacks, several different treaties were proposed. The Budapest Convention is the first of these treaties. It not only serves as a legal document, but it is also a framework for involving parties to create partnerships that encourage cooperation in cases such as emergency situations. The convention has been praised for being a "golden standard" due to its intricacy and comprehensiveness.

The 2018 U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD) is another such treaty. This treaty "transformed the system for cross-border access to data in criminal investigations. It empowers U.S. authorities to order U.S. service providers to turn over data regardless of storage location and authorizes law enforcement in one country to directly serve requests for the production of data […] once an executive agreement between the U.S. and another country is in place"[5]. While the intentions of this act come from a place of cyber-security, it has been argued that this act weakened the privacy of global citizens.

1.2 Recent Developments

Information security has been regarded as an issue of higher priority in recent years. In the December 2019, the U.N. General Assembly took action and voted on the adoption of a resolution that had kickstarted a process that involved drafting a comprehensive treaty on handling cybercrime. Negotiations were expected to commence in January of 2022 and conclude in 2023. The negotiations had revealed a serious unanimity regarding the issue, and competing proposals were put out.

This controversy of cybersecurity is not to go unnoticed. Many countries that have signed the Budapest Convention made up the opposition against the final draft of the resolution, yet the treaty still passed. "Leading digital rights organizations warned against rushing ahead with the treaty because the proposal's treatment of cybercrime is extremely vague and open to abuse, it supplants ongoing work elsewhere in the U.N., and the process so far has excluded civil society"[5]. This divide on the treaty exposed key disagreements, such as the specific definition of what constitutes cybercrime, how law enforcement may be involved in cross-

border investigations, and to what extent should governments have a role in regulating the internet. There are several questionable implications to the treaty regarding human rights, freedom of speech, and privacy. While international cooperation will be important in ensuring accountability to abolish cybercrime, it will also prove to be a challenge if states' opposing views continue to clash.

Key Terms

Data – Facts and statistics collected together for reference or analysis; the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media (Oxford Languages).

Data breach - a cyber-attack in which sensitive, confidential or otherwise protected data has been accessed or disclosed in an unauthorized fashion. Data breaches can occur in any size organization, from small businesses to major corporations.[12]

Cyberspace – The technical architecture that allows the global internet to function.[17]

Cybercrime – Any criminal activity that involves a computer, networked device, or a network.[6]

Hacking – The gaining of unauthorized access to data in a system or computer (Oxford Languages).

ICTs (Information and Communication Technologies) – The combination of manufacturing and services industries that capture, transmit and display data and information electronically.[13]

Global Cybersecurity Index (GCI) – The most trusted reference that measures the commitment of countries to cybersecurity at a global level.[14]

2. Emphasis of the Discourse

2.1 Stance of Intergovernmental Organizations

In addition to the UN's continued efforts in combatting this issue through the drafting of resolutions, other intergovernmental organizations have also contributed.
The African Union drafted a convention regarding protecting cyber-security. Titled "African Union Convention on Cyber Security and Personal Data Protection," these 37 page-long treaties are a legal framework for cyber security and personal data protection for the African Union member states. It considers how it should regulate an ever-evolving technological domain by strictly defining terms related to cybercrime, detailing the boundaries of what

should be considered cybercrime, and how each individual crime shall be considered. The Convention was adopted in June of 2014.[4]

In furthering international cooperation on this matter, the African Union Commission and the Council of Europe have also organized workshops on cyber-security policies. The workshop brought "e-diplomacy" to global attention, illustrating how the use of technologies could have an impact on diplomacy. The participating countries have since pronounced their commitments to "accelerate their partnership on cyber security"[2].

The Council of Europe has been one of the key players in working against cybercrime. They have joined with the European Union to create CyberEast—a project aimed at "adopting legislative and policy frameworks compliant to the Budapest Convention on Cybercrime and related instruments, reinforcing the capacities of judicial and law enforcement authorities and interagency cooperation, and increasing efficient international cooperation and trust on criminal justice"[9].The project will be extended until the end of 2023, with a budget of 5.3 million Euros, and six countries (Moldova, Armenia, Belarus, Georgia, Azerbaijan, and Ukraine) participating.
While the intent of many intergovernmental organizations comes from the same place, each state has their underlying desires and motives. There are various differences when it comes to an individual country's perspective on the specifics of cybercrime. Intergovernmental organizations must seek a way to standardize certain definitions regarding cyber-security in order to move forward and create clear-cut treaties that will serve to be productive rather than superficial.

2.2 Stance of Developed Countries

In a predominantly digitizing world, cybersecurity comes as a necessary part of the development of all countries. Developed countries have the resources, technological advancements, and the economic assets necessary to install digital infrastructure which guarantees cyber-security. In particular, the United States and European countries have been seen as "prominent models of cyber security strategies"[7], score high on the Global Cybersecurity Index, and they are constantly looked towards by developing countries as examples of how to implement legislations and large-scale propositions. From recent data collected by the United Nations Conference on Trade and Development (UNCTAD), 71% of the world's nations have cyber-security legislations, with a big portion of that percentage being developed countries. Cyberlaw statistics on electronic transactions, consumer protection, privacy and data protection, and cybercrime show that most developed nations have adopted these laws. Nevertheless, the industries and governments of developed countries are still distinguished targets for malicious cybercrime organizations, due to the very fact that these nations are socioeconomically accomplished. With higher incomes, more advanced technologies, urbanization, and greater digitization, developed nations are found to be more likely to become victims of cybercrime. According to the Cyber Risk Index developed by Nord VPN, countries such as Iceland, Sweden, the United States, and the United Kingdom were among the list of nations that have the highest cyber risk.[20] The index

takes into account certain significant factors such as urban population, internet penetration, crime index, and the global cybersecurity index as well.

2.3 Stance of Developing Countries

For developing countries, cyber-security may pose as a challenge. Many nations lack the resources and economic capabilities to provide adequate cyber-security for their industries, government, and citizens. Statistics show that unsurprisingly, the Least Developed Countries (LDCs) and developing countries have the lowest percentage of cyberlaw implementation regarding electronic transactions, consumer protection, privacy and data protection, and cybercrime. 15% of the world's countries have no legislations on data protection. Some of these countries include Venezuela, Cuba, Libya, Afghanistan, etc. In fact, there are even countries that lack data on cyber-security. However, such is rarely the case, as many of the developing countries provided on the country list (e.g., Gabon, Ghana, Kenya, Mexico, India) all have some sort of legislation implemented. Indeed, countries that are developing tend to have lower cyber risks. Iran, China, India, and Nigeria are among the countries with the lowest cyber risk, according to Nord VPN's cybersecurity index.[20] The index considers certain significant factors such as urban population, internet penetration, crime index, and the global cybersecurity index as well. However, the existing problem for developing nations currently is the fact that cybercrimes are harder for such nations to absolve, and it is more difficult for them to hold these criminals accountable without the competency in digital forensics.[7]

3. Possible Solutions

3.1 In Favor of Developed Countries

Developed countries have the advantage of economic capability, newer technologies, and the resources available at their hands to pursue information security. Since developed countries are highly at risk of experiencing cybercrime attacks, it is in their best interests to devise plans to ensure the safety, privacy, and security of their cyberspaces.

Developed nations will find it helpful to establish a uniform system to fight cybercrimes. The best way to stop cybercrime is through either prevention or precaution—it is much easier to prevent a cybercrime than it is to investigate it.[18] Governments can **fund projects that work towards anti-hacking and cyberspace safety, or they can choose to develop cybercrime centers as divisions of their governmental organizations.** There are various technical methods that can be applied by IT specialists in criminal investigation, and organizational methods that can be put towards arranging inter-authority cooperation when it comes to cybercrime fighting.[18]

3.2 In Favor of Developing Countries

Developing countries face many challenges when it comes to establishing information security, however that does not render it impossible.

Developing nations may find it necessary to **educate their population and raise awareness on ICTs and cybercrime in general.** This will ensure engagement and cooperation among the private, academic, and technical communities and will help populations become more readily available to embrace cybersecurity.[8] Increased awareness to all ages and levels, regardless of industry, is of utmost importance; after all, a nation's development often starts with education.
Cybercrime is an issue that does not pertain to borders; therefore, it is only sensible that the solutions to this issue will not be limited by borders either. **Developing countries must increase international cooperation and encourage developed countries to contribute to a worldwide effort.** Collaboration at the policy, technical, and law enforcement levels are detrimental to protect the world from the common enemies and criminals found in cyberspaces.

4. Keep in Mind the Following

When researching this topic, it is paramount to consider your country's socioeconomic status and how it may affect your nation's political perception towards cybercrime and cyber-security. Make sure to investigate to what extent your country is affected by cybercrime, and their capabilities in establishing data security to prevent it. Then, expand your perspective to how your country has and can contribute to the global discussion of cyber-security on an international level. Cyber-security is an international issue, and it is important to keep that in mind while you are covering your country's stance on this topic. Here are some questions to guide you through your research:

1. *How has your country been affected by data breaching, hacking, and cybercrime historically?*
2. *What has your country done to combat cybercrime and ensure the technological security of its government, its firms, and its people?*
3. *How does the political stance (right wing, conservative/left wing, liberal) of your country affect its policymaking when it comes to preserving information security?*
4. *Where does your country stand when it comes to the Budapest Convention, and how do they justify this stance?*
5. *In what ways does your country work to preserve data security in international cyberspaces?*
6. *How can the world work as a whole to bring more information security to developing or Least Developed Countries, and what can your country offer?*
7. *Are the policies your country is currently adopting or the legislations your countries are participating in controversial? If so, in what ways and why?*

8. *To what extent is your country willing to infringe on the boundaries of human rights (particularly regarding privacy and cross-border investigations) to obtain cyber-security?*

5. Evaluation

Information security has become increasingly important as recent years have shown the world an acceleration of a digital transformation happening upon the global society. Cyberattacks have increased worldwide, causing huge losses in economic, healthcare, and security sectors. Developed nations have been especially at risk and targeted by cybercriminals due to their extensive wealth and rapid digitization, whereas developing nations are struggling to put up frameworks that will protect themselves. To combat the issue of cybercrime and ensure secure cyberspaces around the world, developed and developing countries alike must come together and increase international cooperation, help each other develop sustainable cyber-security frameworks, and create productive legislations. It is imperative to consider what information security implies for the world in a holistic viewpoint, not just from an individual country's perspective. Increasing international cooperation and finding common ground on this issue will be no easy task. Remember to consider the views of many and think laterally. Good luck, delegates.

6. Bibliography

1. 17, Christian Ohanian October, et al. "The UN Cybercrime Treaty Has a Cybersecurity Problem in It." *Just Security*, 17 Oct. 2022, https://www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it/.
2. "African Union Commission and Council of Europe Join Forces on Cybersecurity." *African Union Commission and Council of Europe Join Forces on Cybersecurity | African Union*, 15 Mar. 2023, https://au.int/en/pressreleases/20180412/african-union-commission-and-council-europe-join-forces-cybersecurity.
3. "African Union Convention on Cyber Security and Personal Data Protection." African Union.
4. "African Union." *CCDCOE*, https://ccdcoe.org/organisations/au/.
5. Brown, Deborah. "Cybercrime Is Dangerous, but a New UN Treaty Could Be Worse for Rights." *Human Rights Watch*, 13 Aug. 2021, https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.
6. Brush, Kate, et al. "What Is Cybercrime? Definition from Searchsecurity." *Security*, TechTarget, 23 Sept. 2021, https://www.techtarget.com/searchsecurity/definition/cybercrime#:~:text=Cybercrime%20is%20any%20criminal%20activity,to%20damage%20or%20disable%20them.
7. Cacacho, Mars. "Cyber Security Policy in Developing Countries: Rowing an Unfamiliar World without a Paddle." *Secon*, 17 Nov. 2022, https://seconcyber.com/cyber-security-developing-countries/.

8. Contreras, Belisario. “3 Ways Governments Can Address Cybersecurity in the Post-Pandemic World.” *World Economic Forum*, https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/.
9. “CyberEast - Cybercrime - Publi.coe.int.” *Cybercrime*, https://www.coe.int/en/web/cybercrime/cybereast.
10. “Data and Privacy Unprotected in One Third of Countries, despite Progress.” *UNCTAD*, 29 Apr. 2020, https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress.
11. “Data Protection and Privacy Legislation Worldwide.” *UNCTAD*, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
12. Froehlich, Andrew, et al. “What Is a Data Breach?” *Security*, TechTarget, 27 July 2022, https://www.techtarget.com/searchsecurity/definition/data-breach.
13. Giles, John. “What Is ICT? What Is the Meaning or Definition of ICT?” *Michalsons*, 20 Dec. 2022, https://www.michalsons.com/blog/what-is-ict/2525.
14. “Global Cybersecurity Index 202.” *ITU Publications*, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.
15. “Global Cybersecurity Index.” *ITU*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
16. Hammouchi, Hicham, et al. “Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches over Time.” *Procedia Computer Science*, Elsevier, 21 May 2019, https://www.sciencedirect.com/science/article/pii/S1877050919306064.
17. Hollis, Duncan. *A Brief Primer on International Law and Cyberspace*. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.
18. Murashbekov, Olzhas B. “Methods for Cybercrime Fighting Improvement in Developed Countries.” Journal of Internet Banking and Commerce.
19. Russu, Catalina. “The Impact of Low Cyber Security on the Development of Poor Nations | Experts' Opinions.” *Developmentaid*, 12 Sept. 2022, https://www.developmentaid.org/news-stream/post/149553/low-cyber-security-and-development-of-poor-nations.
20. Whitney, Lance. “Why Developed Countries Are More Vulnerable to Cybercrime.” *TechRepublic*, 27 May 2020, https://www.techrepublic.com/article/why-developed-countries-are-more-vulnerable-to-cybercrime/.
21. Todd, Drew. “Top 10 Data Breaches of All Time.” *SecureWorld*, 14 September 2022, https://www.secureworld.io/industtry-news/top-10-data-breaches-of-all-time.