General Assembly

The question of improving cybersecurity and protection of sensitive data in an increasingly digitised world.

Introduction:

This research paper will address the question of improving cybersecurity and protection of sensitive data in an increasingly digitised world. This paper will aim to define the issue, discuss major countries involved, relevant UN treaties, historical events, its causes, and draw conclusions, with possible resolutions.

Definition of Key Terms:

Cybersecurity:
The protection of devices, networks and sensitive data from unauthorized access and possible criminal use.

Hacker:
A person who is able to illegally access private and restricted data or devices.

Global Cybersecurity Index (GCI): (Global)
Reference used globally to compare countries' commitment to cybersecurity, it takes into account: legislative, technical, organizational measures that countries have put in place, as well as their commitment to international cooperation and capacity development.

Ransomware:
A malicious software which blocks access to a device or a system until a sum of money is paid.

Cyber extortion:
When sensitive data, devices or systems are being held hostage by a hacker until their demands are met.

Background Information:

Currently, approximately 57% of the world population are also internet users (Individuals, 2021). This increasing interconnectivity has resulted in growing cybercrime threats which most of the time are done from the comfort and security of home. As the internet continues to evolve more users rely on digital keychains to store sensitive information, such as but not limited to, banking information, and credit card details. This has left an open door for cyber-criminals who take advantage of the situation by leaking data or reselling it to third parties.

Globally, the most common forms of cybercrime are phishing, identity theft, hacking, and online intellectual property infringements. Phishing scams refer to criminals who trick internet users into giving away personal information, such as baking details. The most common method used by these thieves is impersonating popular brands, such as Google, to lure people into fake websites, and uploading their sensitive data. Similarly, identity theft criminals use forms, or emails to make people upload their personal information. Hacking instead is based on a larger scale, therefore, criminals commonly known as hackers managed to shut down, or misuse in their favour websites or computer networks.

Furthermore, online intellectual property infringements are a very common crime but difficult to discover online. This crime refers to the misuse of trademarks and can be seen in multiple forms, such as but not limited to, impersonation of a brand or person, deliberate use of proprietary images or videos, and use of similar marks for counterfeit sales purposes (Forms, 2021).

Lastly, the quickly evolving digital world has allowed for cybercrime to evolve to extents that make it difficult to contain. On the other hand, current developments in cybersecurity are allowing for better protection of internet users, especially raising awareness on how to protect sensitive data, and better measures to protect computer networks (Digital, 2021).

Major Countries and Groups Involved in the Issue:

Russia:

Russian hackers are considered by many as some of the most dangerous cybercriminals. As the years have passed they have adapted to bypass many systems, especially European and American banking systems which seem to be their favourite

target. Russian cyberattacks are often large-scale attacks which are frequently driven by political reasons.

Brazil:

Cybercriminals in Brazil take advantage of the relatively new “quantum digital leap”, their constantly evolving methods force Latin American organizations to develop anti-cyber plans much faster which could result in the unintentional creation of loopholes for hackers to use to their advantage.

United Nations Office on Drugs and Crime (Index):

The UNODC works towards the creation of sustainable and lasting measures to fight cybercrime by supporting national structures. Their expertise on criminal justice systems allows even less developed countries to raise awareness on the issue of cybercrime, promote prevention and international collaboration.

International Telecommunication Union (About):

ITU is a UN specialised agency for information and communication, their goal is to allow communication networks to connect worldwide protecting everyone’s right to communicate and exchange information regardless of the geographical area where they live.

Timeline of Events:

1984 - US secret service gains jurisdictional power over digital fraud thanks to the U.S. Comprehensive Crime Control Act (Cyber)

1987 - The first commercial antiviruses were created (Freeze)

1990’s - Introduction of email as a communication medium allowed hackers and viruses new entry points to personal and sensitive data (Freeze)

1999 - NASA and the US Defence Department was breached by 15 years old Jonathan James who accessed personal accounts and information, tried to steal NASA's software the International Space Station (Top)

2009 - Google China was attacked by hackers who accessed personal information of many users including important Chinese Civil rights activists (Top)

2011 - Sensitive data from the Paris G20 summit was accessed through a PDF document containing malware which was sent to members of the French Ministry of Finance (The 7)

2021 - Hackers gained access and downloaded 11 terabytes of data and photos from the Israeli Defence Ministry (Significant)

Main Issues:

In an increasingly digitised world, it goes without saying that the international community as a whole has faced a new dawn in challenges that have required the world's attention. Accelerated by the Covid-19 pandemic, global cyber risks continue to rank amongst top emerging and future challenges. The top issues that the General Assembly will have to face include the following (Pipikaite):

1. **More complex technology = Overdependence:**

The rapid adoption of machine learning and artificial intelligence has made our society increasingly dependent on software, hardware and online infrastructure that as it expands, it becomes more vulnerable.

Critical infrastructure and protocols are at risk. The issue of fake news from influencing elections is a prime example of something that is beyond our control in the free world. Or cyber-attacks on web services critical to the functioning of government such as Italy's Lazio region vaccine portal attack which put a hold on vaccine bookings for days.

2. **Fragmented and Complex Regulations:**

It is obvious that challenges with cybersecurity do not respect borders nor boundaries, likewise with the fragmented plethora of organisations that regulate such internet traffic without a coherent approach when it comes to tackling the issue as a community.

Ranging from the General Data Protect Regulation in the US, the California Consumer Privacy Act or the Cybersecurity Law of the People's Republic of China.
This disconnected approach hinders the international community's ability to counter the issue. Individual enterprises must balance their defense against cyber attacks while complying with law and regulations, sometimes where it just isn't compatible.

3. **Difficult process in identifying/tracking Cyber Criminals:**

Cyber criminals have the added advantage that they have a screen in front of them and many defenses which conventional investigations and policing do not have the capabilities for. Yet this does not mean they do not leave traces.
To that end, the likelihood of detection and prosecution of a cybercriminal was estimated by the World Economic Forum to be as low as 0.05% in the United States for example.

4. **Lacking Expertise in the field:**

As mentioned the Covid-19 pandemic has increased the threat of Cyber crime (more specifically Ransomware) considering the diverted attention for more pressing issues such as contrasting the virus.
Preventive measures are a possible solution (further explained in the Possible solutions section) which business and governments alike can adopt to improve cyber security. Organisational priorities should include a proactive plan to respond to threats. It goes without saying that such a new form of criminal activity is met with lacking experience on how to deal with such an issue (Upadhyay).

Relevant UN Resolutions:

The following resolutions represent previous measures taken and attempts to solve the question of cybersecurity and data protection. It goes without saying that given the complexity and recent nature of the issue, the resolutions are quite recent. It can be seen that the following resolutions build on one another (ITU).

All of the following were adopted by the General Assembly under the guidance of the **International Telecommunication Union**:

Resolution 55/63 - January 2001: Combatting the criminal misuse of information technologies:

- Limited Resolution: in essence, it recognises the issue without properly addressing it.
- First ever awareness of the issue made public (i.e Clause 1, subclause ‘h’)

Resolution 56/121 - January 2002: Combatting the criminal misuse of information technologies:

- Limited Resolution: Re-iteration of Resolution 55/63.

Resolution 57/239 - January 2003: Creation of a global culture of cybersecurity:

- Suggests the enhancement of cooperation between relevant UN agencies and international organisations to tackle the issue (i.e clause 4).

Resolution 58/199 - January 2004: Creation of a global culture of cybersecurity and the protection of critical information infrastructures:

- Invites member states to cooperate and aid least economically developed states.
- Please note the elements in the annex for measures states could take for the protection of critical information infrastructures.

Resolution 64/211 - March 2010: Creation of a Global culture of cybersecurity and taking stick of national efforts to protect critical information infrastructures:

- Very comprehensive resolution: Most actions are targeted at cooperation with different entities. These can be found in the annex which act as operative clauses.

Possible Solutions:

In response to the **main issues** that the international community faces and that the General Assembly could therefore evaluate, here are some possible solutions:

- In accordance with the Fragmented and Complex regulations: Polcymakers need to evaluate their decisions based on the impact and possible consequences. Individual regulations and regulating bodies might offer relief on the local level, but the **need for an international/cross-border regulating body** enhancing data protection, preventing cyber attacks and responding to attacks is necessary.

    - The creation of an international organisation, or expansion of the International Telecommunications Union is one such example (Pipikaite).
- In regards to the issue of detecting and prosecuting cyber criminals: Policymakers can help by enhancing cooperation between law-enforcement agencies and developing a unique and single framework by which convicted criminals are to be charged. Always bearing in mind the attribution of evidence, and bringing them to justice in accordance with national legislation (Pipikaite).
- School instruction could be the way forward in teaching middle and high schoolers the issue of cybersecurity as it becomes increasingly important. National and regional education systems could evaluate the imposition of mandatory advisory sessions relating to cyber security. How to protect data: such as password management lessons, illegal sites to avoid, benefits of a VPN and criminals who 'fish' for easy bait, or victims.
- In accordance with the Lacking expertise: Delegates could evaluate the formulation and imposition of Cyber security preemptive measures such as Data backing, continuity of operations protocols in case of attack, staff training and drills to allow for better response plans. In addition, the designing of the frameworks and business models with security in mind might be the new way forward (Upadhyay).
    - The resilience to cyber attacks depends on the speed, scale and flexibility states and companies alike take in order to prevent attacks is fundamental.

Works Cited:

"About International Telecommunication Union (ITU)." *ITU*, www.itu.int/en/about/Pages/default.aspx.

"Cyber CEO: The History of Cybercrime, from 1834 to Present." *Herjavec Group*, 14 Sept. 2021, www.herjavecgroup.com/history-of-cybercrime/.

"Digital." OECD - Topics, OECD, www.oecd.org/digital/. Accessed 24 Dec. 2021.

"Forms of Cybercrime." Information from the Government of the Netherlands, Government of the Netherlands, www.government.nl/topics/cybercrime/forms-of-cybercrime. Accessed 24 Dec. 2021.

Freeze, Di. “The History of Cybercrime and Cybersecurity, 1940-2020.” *Cybercrime Magazine*, 5 Dec. 2020, cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

“Global Cybersecurity Index.” *ITU*, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

“Index.” *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/index.html.

"Individuals using the Internet (% of population)." World Bank Open Data, The World Bank, data.worldbank.org/indicator/IT.NET.USER.ZS. Accessed 24 Dec. 2021.

ITU. "UN Resolutions Related to Cybersecurity." *International Telecommunication Union*, United Nations, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx. Accessed 24 Dec. 2021.

Pipikaite, Algirde, et al. "These are the top cybersecurity challenges of 2021." *World Economic Forum*, 21 Jan. 2021, www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/.

“Significant Cyber Incidents.” *Significant Cyber Incidents | Center for Strategic and International Studies*, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

“The 7 Biggest Government Cyberattacks since 2011.” *Swivel Secure*, 2 Apr. 2019, swivelsecure.com/solutions/government/top-cyber-attacks/.

“Top 5 Most Notorious Attacks in the History of Cyber Warfare.” *Fortinet*, www.fortinet.com/resources/cyberglossary/most-notorious-attacks-in-the-history-of-cyber-warfare.

Upadhyay, Isha, et al. "Top 10 Challenges of Cyber Security Faced in 2021." *Jigsaw*, 28 Aug. 2020, www.jigsawacademy.com/blogs/cyber-security/challenges-of-cyber-security/.