Research Report

General Assembly 1

The issue of the urgent need to simmer geopolitical tensions and end terrorist groups foray into cybercrime

Student Officers:
Tirsa Los & Thijmen van der Meijden

Introduction

Due to the COVID-19 pandemic, a lot of people have started to feel bored. Everyone is spending more time at home and therefore the crime rates have, generally speaking, decreased. Also, the possibilities for terrorists to attack are being diminished. Thus, the United Nations is now attempting to prevent terrorist groups from expressing their political views into cybercrime.

The Committee

Our committee will be GA1, formerly known as the United Nations General Assembly First Committee. The First Committee deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime.

The issues of GA1 fall under seven thematic clusters.

- Nuclear weapons
- Other weapons of mass destruction
- Outer space (disarmament aspects)
- Conventional weapons
- Regional disarmament and security
- Other disarmament measures and international security
- Disarmament machinery

The GA1 is the only Main Committee of the General Assembly entitled to verbatim records coverage.

Historical fact: GA1's first resolution was created in 1946 in London.

Keywords

Cybercrime = Crime or illegal activity that is done using the Internet.

Terrorist attack = An attack with a violent action, or threats of violent action, for political purposes.

Phishing attack = An attempt to trick someone into giving information over the Internet or by email that would allow for someone else to take money from them, for example by taking money out of their bank account.

Cyberspace = The Internet considered as an imaginary area without limits where you can meet people and discover information about any subject.

Database = A large amount of information stored in a computer system in such a way that it can be easily looked at or changed.

Overview

As the world is currently tackling the COVID-19 pandemic, new threats are rising. The threat of cybercrime is 'popular' as everyone is doing more things online and the online world is expanding every moment that the pandemic is still relevant. The pandemic has led to the biggest number of employees globally bound to work remotely. The people working from home need to have awareness for and knowledge about phishing scams, the fastest growing type of cybercrime. Significantly, many of these scams are now playing on the fears of people for being infected by the COVID-19 virus. Employees from organizations of all sizes and types now have minimal cybersecurity resources, if any, compared to what is normally available to them.

Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the Official Cybercrime Report, which is published annually by Cybersecurity Ventures. The most effective phishing attacks play on emotions and concerns, and that coupled with the thirst for urgent information around COVID-19 virus, makes these messages hard to resist. According to the report, cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

People working from home should be aware of how to detect and react to phishing frauds, and other types of cyber-attacks. If they act immediately and thoroughly, then cybercrime damage costs can be contained and kept at the current level. If the carelessness due to lack of awareness will continue, it may cause heavy loss globally. As per the Cybersecurity Ventures' estimation that cybercrime damage costs could potentially double during the COVID-19 outbreak period is concerned not only with phishing scams, but also with ransomware attacks, insecure remote access to corporate networks, remote workers exposing login credentials and confidential data to family members and visitors to the home, and other threats.

Transnational criminal organizations and terrorist groups are driving illicit arms transfers and weaponing cyberspace while geopolitical tensions increase the risk of nuclear escalation. Simmering the current heightened tensions hinged on crafting effective frameworks to address shortcomings, from protecting the digital realm from criminals to harnessing the spread of conventional weapons is necessary. Perhaps applying existing provisions of landmark disarmament and non-proliferation agreements, such as the Treaty on the Non-Proliferation of Nuclear Weapons, would be a solution.

Arguments

The issue is not whether there is a need to simmer geopolitical tensions and end terrorist groups foray into cybercrime. The issue is discussing how this can be achieved.

Cybercrime costs include damage and destruction of data, forensic investigation, restoration and deletion of hacked data and systems, fraud, post-attack disruption to the normal course of business, stolen money, lost productivity, theft of personal and financial data, embezzlement, and reputational harm and theft of intellectual property. Phishing emails usually want you to click on something, for instance to update your payment details, or access the latest information on COVID-19. This however, is not considered to be a terrorist attack. Shutting down an Internet provider or intruding a nation’s top-secret database would be considered a terrorist attack.

The importance of preventing such an attack is immense. The places where people can be attacked are growing, especially the government since conferences etc. are also online nowadays. Furthermore, currently terrorists have a lot of time to plan and learn the ways to create such an attack. The technology is developing at all times. People have become more dependent on the Internet, according to a Montenegrin UN delegate cyberspace has become a backbone of society. The consequences of such an attack are increasing.

However, it is important to take into account that the possibilities are limited due to privacy laws that some countries are extremely strict about. Certain security measures go against government policy. It is like a scale with privacy on one side and security on the other.

When discussing how geopolitical tensions can be simmered it is important to look at the actual facts. Currently a lot of newspapers are twisting certain facts to make it more interesting for people to read. This is something that needs to be addressed as well, especially since it causes a lot of distress between countries.

Resolution

In order to solve this issue, we must agree upon a resolution. It is therefore your task to write a resolution that could find a balance between the two sides of privacy and security.

In your resolution you must include an image of your stands of this issue.

We would like you to represent your country with its norms and values and not your personal ideas and values. You must therefore research how your country looks upon this issue on economic, cultural and ethical factors.

If this issue does not immediately affect your country, research all of the countries you are allied with and the stance they take on this issue so you know which resolutions to help with and vote on.

Furthermore your resolution must also include possible solutions, which are clearly elaborated.

Links and Sources

https://www.un.org/press/en/2020/gadis3653.doc.htm

https://cyware.com/category/geopolitical-terrorism

https://www.bleepingcomputer.com/news/security/russian-government-warns-of-us-retaliatory-cyberattacks/?&web_view=true

https://www.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F94219-terrorism-and-security-threat-trends-in-2021

https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm