ZYGMUN

DISARMAMENT
(GA1)

COMBATING THREATS TO INTERNATIONAL SECURITY IN CYBERSPACE

MELISA CAKIM
LUANA OLTEANU
SHEMOILA SAINI

Table of Contents

I. Introduction

With the rapid development of new technologies, leaders of the world are confronted with issues that must be handled in order to maintain both national and international security. Cyberspace in particular is considered by many member states to be an integral factor in upholding security, with efforts being concentrated on improving cyber capabilities especially in military or government-related areas. According to ENISA (European Union Agency for Cybersecurity), in 2019 about 11% of cyber-related incidents were motivated by cyber espionage, and about 38% of "malicious actors" were linked to nation-states. These types of attacks have therefore increased concerns of member states, building on already-existing anxieties developed during the Cold War era.

II. Definition of Key Terms

a) Cyberspace - The space produced by the network of digital devices and software.

b) **Cyber warfare** - The act of disrupting or damaging a nation's cyber systems (whether through viruses, hacking, bugs, or other such methods), done by a nation or group of nations.

c) Whistleblowing - The act of releasing secret information (especially that of the state or an influential company) to the general public.

d) "Denial of service" attack - A type of cyberattack that targets a specific service (e.g., banking service), making it unavailable to its intended users.

III. General Overview

There are three main areas that can be considered on the issue of cybersecurity:

a) Strengthening national defense systems to protect against cyberattacks. There are multiple sub-topics that can be considered in turn when it comes to this issue, such as whistleblowing and using cybertechnology in the context of the military.

i. Over the past decades programmers from private companies have been increasingly involved in the process of facilitating cyberspace use in military operations; this is known as the military-digital complex. Although this is not the only way to protect against cyberwarfare in the military sector, this method is especially popular among member states such as the United States,

who has admitted to having over 143 private partnerships of this nature. One other aspect to be aware of is information warfare, which can be part of cyberwarfare. This type of warfare is characterized by aiming to gain a tactical advantage over an opponent by means of gathering intelligence or providing the opposing side with falsified information. Cyberattacks can be used to interfere with a nation's information database, thereby compromising its defensive capabilities for the duration of the cyberattack. Additionally, a cyberattack can be used to gather intelligence from the database itself.

ii. The most famous case of whistleblowing in the past few years has been that of Edward Snowden, a private contractor to the National Security Agency (NSA) who made available a portion of confidential data to the public. While delegates should not focus on this particular case or the ethics of whistleblowing itself, they should consider how whistleblowing might affect cybersecurity, and whether member states should develop further regulations to protect the confidentiality of sensitive data within cyberspace.

b) There are also more indirect approaches to cybersecurity. Cyberattacks can be carried out on companies or executive government branches, with the goal of destabilizing the economy or order of a nation, or leaking citizen information. One such example is the cyberattack on the Estonian government networks from 2007, where online banking was stopped and a part of the nation's government online services couldn't be used. Although this lasted for a period ranging from a few hours for some services and a few days for others, this window of forced inactivity can be detrimental to the organization of a nation and potentially its defensive capabilities as well through this distraction.

c) Another key area in which cyberspace has been used to maintain national security is counter-terrorism. It has been observed that one of the ways in which terrorists recruit new members is through the Internet, or through otherwise digital interfaces. This has been brought to the Security Council as an agenda issue in 2017, and the conclusion has been that cooperation between member states as well as different national sectors is imperative to counteract these issues in the cybersphere. As this is part of the other agenda issue at this conference, it is advisable that delegates keep this aspect in mind but do not address it extensively in their resolutions or in the debate.

IV. Major Parties Involved and their Views

a) China - In December of 2016 China released a document titled "National Cybersecurity Strategy", giving its stance on the matter. The report made clear that China's goals in the future would be to increase protection of cyberspace under its domain in order to preserve national security. Furthermore, it aimed to develop its technological capabilities in this area, stating the strengthening of defenses against cyber warfare as the reason for doing so. From a military point

of view, China also has emphasized the importance of using cyberspace in future military conflicts and has highlighted the need to adapt technology to fit a modern context. This is relevant considering that China has been able to gather one of the largest cyber expert groups working for the military. About 30% of cyberattacks can be traced to China, which has led to multiple accusations of state-sponsored cyberwarfare against other governments.

b) **United States** - The official statement of the NSA CSS (National Security Agency Central Security Service) affirms the growing influence of cyberspace in the modern world, as well asserting the importance of developing improved cybertechnology to resist "very real, very grave national security threats". These threats are considered by the agency to be comprised of hostile foreign governments, terrorists, and "bad actors [...] criminals motivated by profit". In 2015, the Department of Defense released a detailed report on the plan for increasing cybersecurity in the United States, emphasizing, much like other member states, its plan to use cyber technologies for the purpose of safeguarding the nation's vital interests. The report

also noted that the security agencies of the United States would be increasing private partnerships to improve cybersecurity, but that international partnerships should also be maintained, focusing in particular on areas such as the Middle East, Asia Pacific, and key NATO allies. However, the United States also has a high number of cyberattacks originating from it, perpetrators ranging from individuals to government-led programs.

c) **Russia** - The official statement on Russia's cyber policy identifies the main threats to its national security in the cybersphere: the dissemination or promotion of material that supports "the ideology of fascism, extremism, terrorism, and separatism, and [which endangers] the civil peace and political and social stability in society". The statement focuses specifically on how this information can be a danger to Russian citizens, and notes that it is a priority to offer safety and protection from dangerous information to the general public. Another priority, as is the case for many other member states, is creating a strong defense with the use of cybertechnology. In particular, there is a focus on information technology and how it can be used to aid in military strategy and prevent international conflicts. It is also notable that Russia has been accused of perpetrating many cyberattacks, and as a result of this, is perceived by some nations to be a threat on this front. Organizations like NATO, for example, would consider Russia a threat to the safety of its members.

V. Relevant United Nations Documents

- - General Assembly Resolution 58/199 (2004)
- - General Assembly Resolution 64/211 (2010)
- - Security Council Resolution 2341 (2017)

- - General Assembly Resolution 73/27 (2018)
- - General Assembly Resolution 73/266 (2018)

VI. Questions to Consider

- Should the flow of information accessible to the public through cyberspace be restricted to prevent breaches of national security?
    - In this case, how can freedom of speech be preserved?
    - What kinds of restrictions should be applied?
- How can diplomatic international relations be maintained while also upholding national security?
    - Which information relating to the cybersecurity of a nation should be shared with

      other nations (for mutual defense purposes), and which should be kept secret?

- To what extent should nations aim to strengthen their cyber defenses, without

  building an atmosphere of distrust between member states?

- Should there be regulations with regards to how far a nation can develop its cyberspace

  defenses/to what extent it uses cybertechnologies in its military strategies?

- In times of conflict, what types of cyberwarfare are acceptable to use, if any?

VII. Conclusion

Due to the nature of issues pertaining to national security, it is important that member states are able to share their viewpoints and intentions transparently, as well as to cooperate with each other in finding solutions and compromising where necessary. While national security is an important element to uphold, it is the responsibility of member states to ensure a basic international level of safety.

VIII. Bibliography

"Cyber Warfare." *RAND Corporation*, www.rand.org/topics/cyber-warfare.html.

China Publishes First National Cybersecurity Strategy. www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.

Jinghua, Lyu. "What Are China's Cyber Capabilities and Intentions?" *Carnegie Endowment for International Peace*, carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pu b-78734.

Wikipedia contributors. "Information Warfare." *Wikipedia*, 31 Dec. 2020, en.wikipedia.org/wiki/Information_warfare.

"Military-Digital Complex." *Wikipedia*, 5 June 2020, en.wikipedia.org/wiki/Military-digital_complex.

"Cybersecurity." *United Nations Office of Counter-Terrorism*, www.un.org/counterterrorism/cybersecurity. Accessed 30 Jan. 2021.

"ENISA Threat Landscape 2020 - Cyber Espionage." *ENISA*, 20 Oct. 2020, www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage.

"Edward Snowden, Whistleblowing and National Security | Counter-Terrorism Ethics." *EDWARD SNOWDEN, WHISTLEBLOWING AND NATIONAL SECURITY*,

counterterrorismethics.com/edward-snowden-whistleblowing-and-national-securit y. Accessed 30 Jan. 2021.

The history of cyber attacks - a timeline. by Paul King. *NATO Review*, 2013, www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.

CISA. "Security Tip (ST04-015)." *Cybersecurity and Infrastructure Security Agency CISA*, 2009, us-cert.cisa.gov/ncas/tips/ST04-015.

"Understanding the Threat." *National Security Agency Central Security Service > What We Do >* www.nsa.gov/what-we-do/understanding-the-threat/.

"UN Resolutions Related to Cybersecurity." *ITU*, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx.

Zhang, Denise E. "2015 DOD Cyber Strategy." 2015 DOD Cyber Strategy | Center for Strategic and International Studies, 31 July 2019, www.csis.org/analysis/2015-dod-cyber-strategy.

"Cybercrime Top 10 Countries Where Attacks Originate." BBA, 2015.

UNIDIR, 2020, *Russian Federation*, ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf.

"A Tale of Two N Resolutions on Cyber-Security." *Vivekananda International Foundation*, 24 Apr. 2019, www.vifindia.org/2019/april/24/a-tale-of-two-un-resolutions-on-cyber-security#:~:text=In %20December%202018%2C%20the%20UN,the%20Context%20of%20International%20Security'.

Dupuy, Arnold C. "Energy Security in the Era of Hybrid Warfare." *NATO Review*, 13 Jan. 2021, www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfar e/index.html.