Forum: General Assembly 1, Disarmament and International Security Committee

Student Officer(s): Ga Young Choi, Se In Lee, Giang Chau Tran

Position(s): Head Chair of GA1, Deputy Chair of GA1, Procedural Chair of GA1

TOPIC 1: The question of defining and regulating cyber operations, cyber warfare, and autonomous weapons

I. Introduction to the Topic

In the world of development the pervasive use of Information and Communication Technologies (ICT) serves both as an enabler of growth and innovation in the world as well as the source of cyber threats. Today, more than 2 million people have access to the Internet and with the increasing dependency on ICT, all of us have become alarmingly vulnerable to possible disruption and exploitation by malicious cyber activity which has been long affecting individuals, private entities, government institutions, and non-governmental organizations. Governments need to ensure that their infrastructure is secure against various types of cyber threats and that their legal and policy frameworks would allow them to effectively defend and mitigate possible cyberattacks—as the unpredictable nature of cyber attacks can appear to be an act of hacktivism at the start, but eventually escalate into something more serious such as cyberwar and potentially threaten national security.

II. Definition of Key Terms & Concepts

Autonomous Weapon

Weapons that can operate and engage targets without the control of humans.

Cyber Security

The state or process in which information and communication systems are protected against unauthorized use or modification, and resiliency of the computer operating system is enhanced.

Cyber operations

The activities of gathering evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or support other intelligence activities.

Cyber warfare

Cyberattacks against computer systems, damaging the critical infrastructure of the nation-state and can develop into an armed attack.

Hacktivism

Intentional access or interference–without or with exceeding authorizations–to systems, websites, and/or data, in order to affect social or political change.

Information warfare

The collection, distribution, modification, interference, and degradation of information in order to gain advantage over adversaries or to disseminate a perception with a certain motive.

Automated (bot) accounts

Inauthentic accounts that imitate the tasks and actions of users and are usually used for nefarious purposes (eg: spreading spam)

III. Key Stakeholders

United Nations Institution for Disarmament Research (UNIDIR)

The UNIDIR is an institution within the United Nations for conducting independent research on the topic of disarmament and international security. This institute handles issues strongly related to the topic such as cyberwarfare and autonomous weapons, especially through its Security and Technology Programme (SecTec). This program aims to build knowledge and awareness of the risk of technological innovation and international security implications and some of its current research includes ‘Artificial Intelligence and the Weaponization of Increasingly Autonomous Technologies’ and ‘Cyber Stability’. This is significant and relevant as it is directly connected to the topics covered in this conference.

United Nations Office of Counter Terrorism (UNOCT)

UNOCT was adopted through resolution 71/291 on July 15th, 2017, by the General Assembly. It collaborates with the security council of the United Nations in order to maintain global security. It also addressed cybersecurity issues that relate to the topic of cyberwarfare and cyber operations.

Stop Killer Robot

Stop Killer Robot is a non-governmental organization that calls for the ban of lethal autonomous weapons and a new international law on autonomy in weapon systems. This organization was formed in October 2012 and was officially launched in 2013. The organization supports the ban on autonomous weapons as it dehumanizes people by giving the decision of life and death to technologies. This organization closely connects to the HRW explained below, as autonomous weapons can cause mass killing and puts human rights at risk.

Human Rights Watch (HRW)

The HRW is a non-governmental organization that conducts research and advocates for human rights. HRW also shows concern towards autonomous weapons, such as the so-called ‘Killer Robots’, supporting the ban of those technologies as well. Additionally, it has proposed key elements and models for a treaty on this issue, on October 20th, 2020.

IV. Key Issues including Background Information

Threat to individual and national security

Cyber attacks can cause interference with the everyday lives of the people in ways such as electrical blackouts, failure of military equipment, and leak of national secured documents. These can result in the theft of delicate data such as medical records of the high officials of the nation. Not only this, they can also disrupt phone or computer networks, as well as paralyze systems to make certain data unavailable. These issues can further extend to national security as they can be the cause of warfare between nations which also raises concerns about the security of the people. Additionally, the concern over the misinformation of technologies (ICT) can also be mentioned. This is even more amplified especially when it comes to terrorists using the Internet and new digital technologies to commit, recruit, or fund terrorist acts. This causes extreme vulnerability to the security of the people, and member states have stressed the importance of cooperation between the stakeholders in tackling this threat efficiently.

Human rights at risk

As autonomous weapons take control over the decision of life and death of humans, this raises a fundamental ethical question of whether the human decision regarding the use of force can be successfully replaced with computer-controlled processes, as well as the life-and-death decisions can be ceded to robots. Another key difference that should be recognized is that the force and weapon systems are designed to kill or injure humans, rather than destroy or damage objects, already being considered to a limited extent.

Disinformation and fake news

False information is prominently spread on social media, which is further assisted by automated (bot) accounts by disseminating it at a large scale and faster rate. Being frequently exposed to such information, readers' perception and behaviors are influenced, shaped, and manipulated according to it. Not only does it compromise the public knowledge on important social and political matters, but it also habors scepticism towards authentic news. With the majority of the public following a destructive manner, cyber tools may imperil geopolitics stability and international ability to cope with cyberthreats.

Electoral fraud

Election facilities encompass polling, votes registration, tabulation, and display, which mostly operate on the online medium, making them susceptible to cyber attacks. Party members have been reported to utilise this by modifying voting results without authorised access to the system. In addition, voters' behaviors and opinions are also manipulated through the means of fake news as mentioned above or the popularisation of particular mindsets, beliefs and ideologies that support one side of the election. An instance of this can be seen in the 2016 US presidential election where 20% of political posts are generated and proliferated by automated (bot) accounts.

Hacktivism

Hacktivism poses severe threats from individual to international scale. Cybercriminals may commit website defacements, endangering the livelihood of its staff and contributors, and attack the service of industries, causing great disturbance to national security. Big banks, for example, have experienced cyber attacks and bank users have consequently encountered identity theft, posing a major economic impairment to a country. Furthermore, hacking methods have progressed and developed significantly, meaning that users and even firewalls are not aware or cannot detect any abnormal activities running in the background.

V. Timeline of Resolutions, Treaties, and Events

These were politically motivated destructive attacks aimed at sabotage and espionage.

Date	**Description of event**
2007	Cyberattacks on Estonia, a wide-ranging attack targeting government and commercial institutions
2008	Cyberattacks during the Russo-Georgian War, the attacks were initiated three weeks before the shooting war began in what is regarded as “the first case in history of a coordinated cyberspace domain attack synchronised with major combat actions in the other warfighting domains
2009	DDoS (Distributed Denial of Service) attacks against South Korea, a series of coordinated cyberattacks against major government, news media, and financial websites in South Korea and the United States
2009	Shadow Network, China-based computer espionage operation that stole classified documents and emails from the Indian government, the office of the Dalai Lama, and other high-level government networks
2010	Japan-South Korea cyberwarfare
2011	Canadian government hackings, hackers using IP addresses from China infiltrated 3 departments within the government and exfiltrated classified data. The attacks resulted in the government cutting off internet access in the departments affected and various responses from both the Canadian government and the Chinese government
2017	Cyberattacks on Ukraine, a series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers, and electricity firms. Similar infections were reported in France, Germany, Italy, Poland, Russia, the United Kingdom, the United States, and Australia.

Dec 2019	The UN General Assembly adopted a resolution on "countering the use of information and communications technologies for criminal purposes", and introducing an Ad Hoc Committee.
2022	Ukrainian cyberattacks, undertaken during the prelude to the 2022 Russia invasion of Ukraine
2022	Cyberattacks on Romania, which occurred after a visit of Romanian officials to Kyiv where more support against Russia was promised while the invasion was taking place

VI. Possible Challenges & Solutions

Threat to individual and national security

As mentioned previously, one possible solution is to encourage strong cooperation between the stakeholders. As cyber attack and warfare can occur at any place and at anytimes, it is important for the stakeholders to get together to make agreements regarding the issue. As most of the presented stakeholders in this report are against cyber warfare along with autonomous weapons, it is also important to recognize the perspective of the stakeholders that are for or neutral to the topic. Furthermore, by knowing so, a more efficient and reasonable resolution can be constructed. With that being said, inefficient cooperations of certain stakeholders can be a possible challenge in coming to an agreement.

Human rights at risk

Some possible solutions for the destructive violation towards human rights would also include efficient communication and cooperations between the stakeholders in the forms of nations, organizations, or communities. Once agreements are set, the possible policies could be discussed which would again lead to an efficient resolution regarding this issue. However, some challenges that should be addressed are the perspectives that are for autonomous weapons. According to the ICRC report on the Ethics and Autonomical Weapon System Report as of April 2018, the potential precision and reliability of autonomous weapons may strengthen the international law and ethical values of humans, which results lower humanitarian consequences.

VII. Recommendations for Resolution Writing including Research

The chair would like to strongly recommend the delegates to deeply research their countries' position on the issue before they start writing the resolution so that they fully understand what stances their country holds and write operative clauses accordingly. It would also be easier for delegates to work with other delegates with similar perspectives on the issue so that the resolution as a whole offers strong and coherent solutions. If you are unsure about the (whole) concept of a resolution or are stuck on how to start writing a resolution/operative clause, the chairs would like to highly recommend the delegate to check out and infer by having a read of the resolution manual which is on the UNISMUN website. Even if you have had a read of the resolution manual and are still lost, please do not hesitate to reach out to any of the chairs!

VIII. Bibliography

-
- "Security and Technology | Programmes | UNIDIR." *Security and Technology | Programmes | UNIDIR*, unidir.org/programmes/security-and-technology. Accessed 13 Oct. 2022.
- "Stop Killer Robots." *Stop Killer Robots*, www.stopkillerrobots.org/about-us. Accessed 13 Oct. 2022.
- "Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control | HRW." *Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control | HRW*, 10 Aug. 2020, www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and.
- "New Weapons, Proven Precedent: Elements of and Models for a Treaty on Killer Robots | HRW." *New Weapons, Proven Precedent: Elements of and Models for a Treaty on Killer Robots | HRW*, 20 Oct. 2020, www.hrw.org/report/2020/10/20/new-weapons-proven-precedent/elements-and-models-treaty-killer-robots.
- "Cybersecurity: How the EU Tackles Cyber Threats - Consilium." *Cybersecurity: How the EU Tackles Cyber Threats - Consilium*, 2 Sept. 2022, www.consilium.europa.eu/en/policies/cybersecurity.
- "Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control | HRW." *Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control | HRW*, 10 Aug. 2020,

www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and.

- Carol, Malaguti, Maria Chiara,Delort,Dorothee,Lee,Yejin. "Legal Framework for Cybersecurity in the Financial Sector : A Comparative Study on Existing Domestic or Regional Legislation on Cybersecurity." *World Bank*, documents.worldbank.org/en/publication/documents-reports/documentdetail/099735005172232846/p1647700ca3dbe0b30a3680c806c4563a93. Accessed 13 Oct. 2022.

IX: Additional Resources

Youtube Links:

- The future of modern warfare: How technology is transforming conflict | DW Analysis