



KENYA MODEL UNITED NATIONS

20TH SESSION

CONFERENCE

**THE FIRST UNGA COMMITTEE ON DISARMAMENT AND INTERNATIONAL
SECURITY COMMITTEE**

BACKGROUND GUIDE

LETTER FROM THE DIAS

Honorable Delegates,

We as the dais of the First General Assembly committee, Disarmament and International Security welcome you to the annual Kenya Model United Nations Conference. This 20th Session's dais shall be graced by Oliver Mboya (Chair), Pauline Wambui (Co-Chair) and Michelle Oriedo (Committee Secretary).

The selected topic of discussion has been well thought out by the team and it is our sincere hope that in-depth research shall be carried out not only to understand your foreign policies on the matter, but to also come up with workable solutions for the issue at hand. We hope that this will be a learning experience for you and wish you fruitful deliberations.

This guide is supposed to assist and not limit your research. We encourage you to hone your skills of comprehension and critical thinking as you tackle this topic.

Please send the position papers to: disec@kenyamodel.un.or.ke

Warm Regards,

DISEC Dais



MANDATE OF THE COMMITTEE

The Disarmament and International Security Committee (DISEC) is one of the six subsidiary committees of the General Assembly established by the UN Charter in 1945. DISEC has 193 member states and all have an equal vote in matters raised. Its role is described in Article 11, Chapter IV of the United Nations Charter. Its mandate as a committee of the General Assembly is to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources. It addresses issues relating to disarmament, global challenges, and threats to peace that affect the international community and it seeks out solutions to the challenges in the international security regime. Although the Security Council (UNSC) is the only UN body capable of acting on its decisions, DISEC makes valuable recommendations to the Security Council on all aspects of matters that place global peace at risk.

DEVELOPMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS AND ITS EFFECT ON INTERNATIONAL SECURITY



INTRODUCTION

The United Nations Educational, Scientific and Cultural Organization (UNESCO, 2010) defines ICT as the forms of technology that are used to transmit, process, store, create, display, share or exchange information by electronic means¹. According to the Oxford Learner's Dictionary, Telecommunications is the technology of sending signals, images and messages over long distances by radio, phone, television, satellite, among others.² The global telecom services market size was valued at USD 1.74 trillion in 2019 and is expected to grow at a Compound Annual Growth Rate (CAGR) of 5.0% from 2020 to 2027. There are various factors that fuel the growth of telecommunications which include, but are not limited to, shift in customer inclination towards cloud-based technology and mobile devices, increasing number of mobile subscribers, high demand for high-speed data connectivity, and the growing demand for value-added managed services just to name a few.³

¹Anderson, J. (2010). *ICT TRANSFORMING EDUCATION*. Bangkok: UNESCO

² <https://www.oxfordlearnersdictionaries.com/definition/english/telecommunication>

³ (Telecom Services Market Size, Share & Trends Analysis Report By Service Type (Basic Communication, Value-added), By Transmission, By Product, By Application, By Region, And Segment Forecasts, 2020 - 2027, 2020)

In accordance with the most recent International Standard Industrial Classification of All Economic Activities of the world-wide System of National Accounts, the Information and Communications Sector covers activities such as publishing, motion pictures, video and television program production, sound recording and music publishing programming, broadcasting telecommunications, computer programming, consultancy and related activities and information services⁴. ICT is embedded in numerous aspects of our lives and has produced some positive benefits. It has also created so many opportunities and technical advancements that have widened possibilities.

The global communication network has undoubtedly been one of the prominent areas for continued technological advancements over the past few decades. The industry's product offering began evolving in the late 19th century, from only voice and visual signals in terms of facsimile or telegraphs over wired infrastructure to the current scenario of exchanging audio, video, and text content over numerous wireless infrastructures. The market for telecom services has also witnessed significant improvements in data speeds, from Global System for Mobile communications (GSM) and Code Division Multiple Access (CDMA) to Third Generation (3G), Fourth Generation (4G), and now the commercialization of Fifth Generation (5G) networks⁵. The advent of data connectivity has made possible the reduction in the duration of transferring large chunks of data from days to hours and now to a few seconds.

As people worldwide struggle with the realities of the COVID-19 pandemic, digital entertainment platforms as well as the global telecom service providers have benefitted from the current scenario due to their industry type. In a current worldwide lockdown scenario, a shift among masses to remote working will fuel the demand for network connectivity and infrastructure. The temporary shutdown of multiplexes and other outdoor entertainment avenues due to strict social distancing has increased the usage of various digital platforms, including social media, gaming, and OTT applications. The mobile voice traffic has also witnessed an upsurge during this period with prominent communication operators reporting an enormous escalation

⁴ United Nations, International Standard Industrial Classification of All Economic Activities, Rev.4, New York, 2008.

⁵ Market Analysis Report

in their voice traffic since the outbreak of the pandemic. Social media has been an avenue of release for very many people globally and has helped people deal with the adverse effects the pandemic has come with.

PROBLEM STATEMENT

In as much as ICT has its advantages, its misuse poses potential risk for international peace and security. A security threat is defined as a potential violation of security and may entail unauthorized disclosure of information, theft, removal or loss of information or other resources, unauthorized destruction or modification of data and equipment and impersonation, or masquerading as an authorized entity among others. Threats may be accidental or intentional and may be active or passive. An accidental threat is one with no premeditated intent such as a system or software malfunction or a physical failure. An intentional threat is one that is realized by someone committing a deliberate act which, when achieved, becomes an attack. ICT has created numerous vulnerabilities and has some adverse negative effects and threats. Some of these include cyber warfare, cyber terrorism and attacks on critical information infrastructure. There is a growing concern that vulnerabilities in ICT can be exploited yet there is little understanding of it⁶.

Use of ICT can pose civil and military threats due to its use for military, terroristic and political purposes that have no consideration for maintenance of international security, and which could cause serious political, social and economic consequences. The use of ICT weapons would be dangerous when used against military and civilian facilities, state systems and institutions. This would lead to disruption of normal functioning which could constitute a direct threat to national security. An attack on anti-aircraft, anti-missile and other defense communication and control systems would leave a state defenseless before a potential aggressor, thereby depriving it of the possibility to exercise its legitimate right of self-defense⁷.

Overreliance on social media sites and mobile devices may lead to psychological

⁶ UN document A/RES/57/239, 31 January 2003

⁷ www.unidir.org

and physical issues such as depression especially in developing children, teenagers and the youths. A 2017 study on young adults aged 19–32 years found that people with higher social media use were more than three times as likely to feel socially isolated than those who did not use social media as often⁸. Negative social interactions, which may include cyber bullying, have been seen to bring about an increase in the levels of depression and anxiety while aggravating the suicide rates among users over the years.

Threats can also occur in the finance sector where unauthorized transfer of bank resources, closure of accounts and conducting electronic attacks to block computer networks of central banking institutions, could not only create crisis situations in the given area, but at a wider scale could cripple a country's economy and have detrimental effects on multinational relations.

PAST UN ACTIONS

The UN has been aware of the rapid growth in the IT and Telecommunication industry since long ago. This is looking back to the days when Morse code was one of the most advanced means of telecommunication. The International Telecommunications Union (ITU) was founded in Paris 1865 as the International Telegraph Union. It then went on to take its present name in 1932 and finally became specialized agency of the UN in 1947⁹. Initially this specialized agency of the UN focused on telegraph but has currently expanded its scope of work to the multiple sectors in ICT and telecommunication. ITU mainly focuses on three arms which branch into other components of ICT and telecommunication.¹⁰ These are as follows:

1. Standardization – this entails the setting of international standards of how systems relate with each other throughout the world. It also helps dictate the tariffs and accounting services principles for international telecom services.
2. Radio communication – this ensures and monitors the fair, rational and safe use of radio frequencies and satellites. It also deals with services to do with wireless and radio communication services
3. Development- the ITU says it is committed to connecting the world wherever one

⁸ www.medicalnewstoday.com

⁹ <https://www.itu.int/en/about/Pages/history.aspx>

¹⁰ <https://www.itu.int/en/history/Pages/FocusOnITUAreasOfWork.aspx>

may be. From this they implement projects to help develop communication services and infrastructure.

On 2nd April 2014 the ITU launched a study to assess the status of cyber security worldwide which is one of the biggest threats to international security when it comes to ICT.¹¹

Hackers change their tactics everyday hence it is important that security forces keep up with new developments in the ICT world whether it be systems, viruses or new attack methods.¹² The issue of ICT was adopted in the General Assembly, raised by the Russian federation in 1998 for the first committee and was adopted without vote as resolution 53/70. Since 2004, five Groups of Governmental Experts (GGE) have continued to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed. Furthermore, since the same year, a group of government experts have been studying and identifying threats while providing recommendations that are welcomed by UN member states to do with ICT security and identified threats in the ever-growing ICT world. In particular, the 2015 report of the GGE was adopted by consensus in resolution 70/237. This resolution “calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts.” Annual reports have been produced by the secretary General as from 1998 where members of the general assembly are welcomed to give their recommendations publicly for resolutions 73/27 and 73/266. This widens the scope of the information put together in the field of ICT and telecommunications. United Nations Secretary-General António Guterres has expressed his concerns on malicious acts performed in the ICT sector. This was made one of his key priorities and was included in his ¹³*Agenda for Disarmament* released in May 2018. He notes that “global interconnectivity means that the frequency and impact of cyber-attacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time.” He further states that “in this context, malicious acts in cyberspace are contributing to diminishing

¹¹ <https://news.un.org/en/story/2014/04/465252-un-telecom-agency-launches-study-assess-status-cybersecurity-worldwide>

¹² [Developments in the field of information and telecommunications in the context of international security – UNODA](#)

¹³ <https://www.un.org/disarmament/sg-agenda/en/>

trust among States.” As a result of these, two action points on cyber were included in the ¹⁴*implementation plan* for the Agenda for Disarmament.

¹⁵During the 89th session, an issue was raised concerning critical system failure threats on contingency planning for the year 2000 (YK2). It was realized that this was more of a risk in developing countries and it was agreed that while each organization should make its own assessment of risks and the degree to which it was prepared to invest resources in contingency planning, it was essential that the UN system have an orchestrated approach to the issues and plan a coherent overall response. As a result, recommendation was put forward that discussions at the meeting of the High Level CCAQ to consider the Y2K issue and include the question of which body or bodies should be allocated responsibility for coordinating system-wide contingency plans. Also, it was suggested that responsibility be assigned to management rather than information technology specialists.

The above information is just but a few samples of many more issues already covered or that are being covered by the UN. In light of this we believe you will find it very helpful to use the links provided in the footnotes to expand your knowledge on the same.

POSSIBLE SOLUTIONS

The following recommendations are quite technical. They touch on norm development and new approaches to better address the emerging challenges and opportunities created by new technologies. They are:

- a. Make the UN the depository and safe-keeper of big data: The UN could help gather, collect, and store data, especially from regions where the infrastructure is not safe or sufficient. Member states could give this mandate to the UN, which would have to create and implement safeguards for the data.
- b. Consolidate and build analytical capacity: The UN could help provide greater analytical and statistical capacity when member states lack it. This could facilitate economic and social development, as well as gathering and analyzing necessary data on climate change. This capacity already exists but

¹⁴ <https://www.un.org/disarmament/sg-agenda/en/#actions>

¹⁵ [Information and communications technologies \(ICT\) | United Nations - CEB \(unsceb.org\)](#)

is currently spread throughout the system.

- c. Recognize cyberspace as “global common good”: The UN could formally recognize that cyberspace should be used for “peaceful purposes” in the interests of humanity.
- d. Support confidence-building measures (CBMs): The UN and other multilateral actors could put in place CBMs at the regional and sub-regional levels to ensure the security and sustainability of cyberspace.

CONCLUSION

A new wave of technology is driving rapid global change. Developments in the field of ICT are inevitable. Some developments will be benevolent, while others malevolent. It is therefore important to address the emerging potential threats posed in a bid to maintain international security.

QUESTIONS A RESOLUTION MUST ANSWER

1. In what ways can the UN can keep up with the changing trends of IT and Telecommunications while continuing to maintain international security?
2. What threats are posed by IT and Telecommunications to international security?
3. How can threats posed by IT and Telecommunications to international security be managed?
4. How will the UN take on or delegate the task of educating everyday users on the dangers present in the world of IT and telecommunication?
5. How has abundant access to information affected international security and what should be done about it?
6. Who is responsible for safety in the IT and telecommunication world and how can they be assisted or made aware of this?

REFERENCES

1. Anderson, J. (2010). ICT TRANSFORMING EDUCATION. Bangkok: UNESCO.
2. <https://www.oxfordlearnersdictionaries.com/definition/english/telecommunication>
3. *Telecom Services Market Size, Share & Trends Analysis Report By Service Type (Basic Communication, Value-added), By Transmission, By Product, By Application, By Region, And Segment Forecasts, 2020 - 2027.* (2020).
4. United Nations, International Standard Industrial Classification of All Economic Activities, Rev.4, New York, 2008.(<http://unstats.org/unsd/cr/registry/>)

5. General Assembly, Creation of a Global Culture of Cyber security, UN document A/RES/57/239, 31 January 2003
6. General Assembly, Creation of a Global Culture of Cyber security and the protection of critical information infrastructures, UN document A/RES/58/199, 30 January 2004.
7. <https://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf>
8. <https://www.medicalnewstoday.com/articles/negative-effects-of-technology#psychological-effects>
9. <https://www.itu.int/en/about/Pages/history.aspx>
10. <https://www.itu.int/en/history/Pages/FocusOnITUAreasOfWork.aspx>
11. <https://news.un.org/en/story/2014/04/465252-un-telecom-agency-launches-study-assess-status-cybersecurity-worldwide>
12. Developments in the field of information and telecommunications in the context of international security – UNODA
13. <https://www.un.org/disarmament/sg-agenda/en/>
14. <https://www.un.org/disarmament/sg-agenda/en/#actions>
15. Information and communications technologies (ICT) | United Nations - CEB (unsceb.org)