FORUM: General Assembly 1

QUESTION OF: The issue of state-sponsored cyber warfare

SUBMITTED BY: The Republic of the Congo

THE GENERAL ASSEMBLY,

*Alarmed* by the growing threat that cyberwarfare, left unregulated, poses to humanity,

*Concerned* that acts of cyberwarfare could lead to a proportionate response in the form of conventional warfare,

*Noting* *with deep concern* the lack of action by the international community on this issue in recent years,

*Recalling* the technological advancements brought on by the advent of the Internet and the need for it to remain free, secure and open, while balancing this with the need to maintain national security,

*Taking* into consideration the sovereignty of individual member states,

*Recognising* the urgent need for member states to act collectively to resolve this issue,

1. Defines state-sponsored cyberwarfare as when a sovereign state, or organisation with the implicit support and/or funding of a sovereign state, deliberately accesses and interferes with another sovereign state’s cyberspace, with intentions including, but not limited to;
   1. engaging in inter-state espionage within another sovereign state’s cyberspace,
   2. engaging in industrial espionage within another sovereign state’s cyberspace,
   3. initiating hostilities with another sovereign state through cyber-attacks, further defined as an offensive manoeuvre that, through mechanisms such as hacking, causes significant disruption to a sovereign state’s infrastructure and/or computer network;
2. Asks that individuals and organisations undertaking acts of cyberwarfare on behalf of member states are subject to the same restrictions and regulation as the activities of sovereign nations would be;
3. Calls upon the need for states participating in cyberwarfare, both directly and indirectly, to act in accordance with all international humanitarian law;
4. Urges the illegality of cyber-warfare when not conducted in accordance with international humanitarian law;
5. Authorises the foundation of the United Nations Panel on Cyberwarfare (UNPC), a new UN panel that will aim to resolve disputes and conflicts arising from state-sponsored cyberwarfare by:
   1. Establishing the United Nations Convention on the Regulation of Cyberwarfare (UNCRC), within 5 years, with objectives including, but not limited to:
      1. Applying existing rules of engagement to non-conventional warfare within cyberspace,
      2. Creating an appropriate international dispute resolution mechanism that will be assigned the settlement of specific disagreements,
      3. Establishing an enforcement body and suitable procedures for non-compliance with articles within the UNCRC,
   2. Suggesting amendments to the Geneva Conventions, regarding the criminalisation of cyberwarfare that is not in accordance with all existing international humanitarian law,
   3. Operating under the following principles, until such as time as the UNCRC is set up:
      1. A sovereign state, directly or indirectly, engaging in cyberwarfare not in accordance with all existing international humanitarian law would be liable to be referred to the Security Council for appropriate economic and other sanctions,
      2. A sovereign state’s cyberspace consists of cyber infrastructure located within a state’s territory or cyber infrastructure located outside of a state’s territory that is otherwise protected under the existing principle of territorial sovereignty,
      3. Any foreign internet traffic passing through a sovereign state is passing through said state’s sovereign cyber territory, as according to the principle of territorial jurisdiction, and, as such, is able to be intercepted and analysed, provided there is reasonable suspicion of illegal activity,
      4. Any internet traffic may be manipulated by a sovereign state, or actors on behalf of said state, to pass through its sovereign territory, but only in cases where there is probable cause for criminal activity that would threaten the security of a sovereign state,
   4. Organising a biannual conference of all sovereign member states to allow for the discussion of how best to respond and/or regulate new advances in cyberwarfare, as well as information sharing in the area of cyber defence;
6. Further authorises the foundation of the United Nations Cyber Defence Fund (UNCDF), a new UN fund that will aim to reduce the size of the threat posed by state-sponsored cyberwarfare by measures, including but not limited to:
   1. Allocating funds to research projects that aim to sufficiently improve cyber defence mechanisms and cyber security, subject to approval from the UNCDF with the amount of funds to be determined by the UNCDF on a case by case basis,
   2. Further allocating funds to low income member states in accordance with World Bank thresholds, defining a low income member state as a member state with a per capita gross national income of less than USD 1035, to improve protections on their sovereign cyberspace, with the amount of funds to be determined by the UNCDF on a case by case basis;
7. Calls for the establishment of a biennial international conference of eminent mathematicians and computer scientists, as well as member states, to develop standards for end-to end encryption that allows for improved protection against cyber-attacks and considerations of the privacy and security of the individual to be balanced against the need for states to be able to safeguard their own security.