Committee: General Assembly 1st commission

Issue: The issue of state sponsored Cyberwarfare

Main-submitter: Germany

*Recognizing* that the evolution of cyberspace and information and communication technologies (ICT) has led to great opportunities for the international community,

*Observing* increased connectivity, innovation and access to the ICT have been of great importance in reaching the Millennium Development Goals

*Noting* with deep concern that the evolution of technology also shows a disturbing growth in the risk international peace and security of the individual,

*Deeply disturbed about* Spain being the victim of 70,000 cyber attacks in the previous calendar year alone,

*Recalling* the reports of other countries such as Germany, who have disclosed that they reportedly get 5 cyber-attacks a day on its government or other attacks and continues cyber-harassment, which have been noted in countries such as Estonia in 2009, Israel in 2009 and Canada in 2011,

*Having studied* the 2016 Internet Security Report regrettably recognizing that over half a billion personal records have been stolen or lost in 2015 alone,

*Emphasizing* that cyber-attacks have become an international disturbance to an abundance of governments and the international population as a whole,

*Alarmed* by the fact that there are no clear international regulations regarding the legal and illegal use of cyberspace and ICT,

*Articulates* the need to aspire to create an international consensus on cybersecurity, in which the topic of state-sponsored cyber warfare is breached and the use of ICT in offensive and threatening or/and attacking purposes versus defensive/responsive purposes of the fundamental rights and freedom of the individuals is addressed.

1. Urgescollaboration between member states in combating state sponsored cyberwarfare, by the creation of internationally recognized guidelines, which will outline but not be limited to;

a. The rules of engagement of state sponsored cyber warfare, including but not limited to;

i. Banning the use of such warfare on citizens deemed innocent to any ongoing conflict,

ii. Banning wide range distribution of any information alquired from such form of warfare, except with allied nations,

iii. Allowing the use of such warfare only on nations deemed in conflict with one another,

iv. Banning the use of “Boomerang Routing”, due to its destructive nature and infringement on privacy,

b. Prohibiting the monitoring of data passing through a country which is not its final destination;

c. Defining cyberspace sovereignty;

d. The issue of UN-provoked offensive cyber warfare;

e. The creation of a “Freedom of Cyberspace” act, which will include but not be limited to;

i. Limiting a nation's rights and jurisdiction to data passing through it,

ii. Listing cyberspace as common property, that is not under any country’s sovereignty, and is hence free to use,

iii. Limiting a nations ability to launch cyberwarfare attacks,

iv. Creating guidelines and regulations for infringements of the freedom of cyberspace act,

f. The consequences of not adhering to the above mentioned clauses, to be decided by the UN Security Council;

2. Calls for the creation of a United Nation Cyber Warfare Regulatory Committee (UNCWR) with representatives taken from impartial private security agencies (PMC’s), with oversight of this committee (where any confidential data found is not presented to this committee), whose tasks will include but not be limited to:

a. Holding an international cyber warfare conferences, held in a quarter year basis, where delegations from member states will be given the opportunity to raise concerns to do with cyberwarfare with the goal being;

i. Improving communication with member states about this issue,

ii. Allowing LEDCs to raise concerns and learn from nations with better cyber-defenses,

iii. Creating a platform where these issues can be debated by the international community to come up with solutions and guidelines to the use of cyberwarfare,

b. Prevention of inter-state cyber-warfare, through;

i. Cataloging reports of interstate cyber warfare, to be presented in conferences to be held every six months, to discourage such attacks,

ii. Regulating member states cyber warfare capabilities,

iii. The enforcement of relevant consequences, to be decided in future cyber warfare conferences, should member states use techniques and cyberwarfare that is deemed counterintuitive to sustaining peaceful relations,

c. Accumulation of information about cyber terrorist organisations from different delegation’s cyber programs;

i. Where such information will be centralized and available for member states should there be just cause for requiring such information,

ii. To start developing projects and programs to help develop better defenses against cyberterrorism,

d. Presenting possible alterations to the guidelines presented in clause 1, should the need arise, which will be;

i. Done in an attempt to keep up with the latest cyberwarfare attacks and developments,

ii. Presented to the Security Council for debate with regards to rules of engagement,

iii. Used to aid member states with collaboratively achieving the goal of protecting citizens and anyone else considered to be innocent in the conflict, which will be debated within the above mentioned conferences,

e. Requests that the UNCWR have permission to enforce the amended laws mentioned in clause 7;

3. Requestsmember states to raise awareness of the dangers of cyberwarfare infiltrations to both private co-operations and governmental organizations, through;

a. Holding seminars where protective protocols can be presented to these organizations;

b. Requiring firms to boost their cyber security when dealing with confidential information;

c. Collecting data regarding cyberwarfare regularly, which is to be presented in seminars to raise awareness and the prevalence of the issue to such organizations;

4. Further Urgesthe use of state sponsored cyberwarfare to be used only at times of conflict, with the exception of use for self-defense purposes, which will be defined as;

a. Any time concrete evidence is present that information retrieved is vital to a nations security which can be evaluated at the request of the attacked nation by the UNCWR, and which if done unsubstantiated will force the attacking nations to adhere to the consequences outlined in the treaty mentioned in clause 1;

b. Not any continuous and prolonged attack with the pure goal of disrupting regular operations within a country;

c. To be used only when provoked, in defensive use, where use in prevention is not included;

5. Encouragesall governments to invest in higher internet security for protection against cyber-attacks from smaller terrorist groups.

6. Further requeststhat responsibility is taken in terms of the use of a nation’s own cyberwarfare usage;

7. Further encourages revising and amending of current laws in place, regarding cyberwarfare, laws of which will be upheld under the watch UNCWR