**COMMITTEE:**  Human Rights

**QUESTION OF:** Establishing Cyber Rights for Individuals

**MAIN SUBMITTER:** Russia

**CO-SUBMITTERS:** Luxembourg, Afghanistan, Thailand, Rwanda

THE GENERAL ASSEMBLY,

***Defining*** Cyber rights as the rights of individuals while online,

***Wishing to notify*** that the most common form of cyber right violation is sending viruses,

***Appalled*** that over 3,000,000 users of Snapchat have had their personal details copied and used against them,

***Noting with satisfaction*** that APEC, ASEAN and IGF have started to spread awareness of cyber crimes,

***Fully aware*** that the first step to cyber rights was the recent ‘National Cyber Security Policy 2013’; it was successful,

1. ***Encourages*** member nations with the help of NGOs to increase awareness on cyber rights and ways to improve individuals’ knowledge of cyber safety through ways such as but not limited to:
2. Hold global awareness days,
3. Speeches and courses at school,
4. Online safety course,
5. Different forms of media;
6. ***Requests*** NGOs and the UN to take action against governments or any body of authority that tries to hack or access personal or restricted information through means of disciplinary measures such as but not limited to;
 a) Condemning,
 b) Requests a re-election, as the government proves to be inadequate in terms of improving international relations;
7. ***Recommends*** every single electronic appliance would need to be sold with a package informing and equipping the user with programs such as, but not limited to:
 a) Spam blockers,
8. Firewall protection,
9. Anti-virus software,
10. Encryption software;
11. ***Urges*** member nations to increase their ability to respond efficiently to the threat of cybercrime through means such as but not limited to:
 a) Governments to hire more IT specialists,

 b) Increase training facilities,

c) Create a division in the Government which targets the improvement and implementation of cyber rights for individuals and firms in order to improve safety online;

1. ***Requests*** member nations to prevent cybercrime by educating the youth on how to protect their cyber appliances and how to defend their cyber rights;
2. ***Suggests*** new cyber laws to be implemented with harsh enforcement to follow those who break the laws. Harsh enforcement includes but are not limited to:
3. Prison sentences,
4. Fines;
5. ***Endorses*** the creation of a fully committed cyber police whose duties include but are not limited to:
6. Creating programs to stop and track down cyber criminals,
7. Arresting criminals;
8. ***Recommends*** the public to refrain from giving too much personal information on social networking sites;
9. ***Declares*** that social network sites such as Facebook and Twitter have a time limit set for keeping the public’s personal details and not distribute the information;
10. ***Strongly suggests*** that governments do not store people’s personal information due to the fact that it goes against basic privacy rights.