**FORUM:** Disarmament Committee

**QUESTION OF:** Combating the growing threat of cyber warfare

**SUBMITTED BY:** Ukraine

THE DISARMAMENT COMMITTEE,

*Recalling* previous relevant United Nations resolution ‘Technical assistance and training States to improve national legislation and build the capacity of national authorities in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks’, which illustrates the urgency and globalism of the aforementioned question,

*Recognizing* the need for action as a consequence of the many, unregulated acts of cyber warfare,

*Addresses* the efforts of the Budapest Convention and A/RES/57/239 to establish international guidelines and definitions on cyber security,

*Emphasizing* that an acceptable solution to such an issue is urgent,

1. Requests the UN to set the following as a definition of what cyber warfare really is, so it can be expressed to be on the same level as standard war: “A cyber-attack on any major organization or government that can affect a country’s economy and/or infrastructure, can be accompanied with military action’’ and an international cyber defense force to combat issues of cyber terrorism;
2. Suggests that all member states have summits every 1 years in which cyber-warfare related matters should be kept up to date and be enforced by international police forces like INTERPOL;
3. Encourages all member states to increase the security measures against cyber-attacks by improving computer-related items, such as, but not limited to:
   1. improving firewalls
   2. upgrading outdated technology, for example:
      1. hardware
      2. security systems
      3. off-line and backup servers
      4. security programs, such as randomly generated access codes
   3. reducing the number of people who have access to confidential information
   4. anti-zero day systems that:
      1. use reverse engineering and white hat hacking,
      2. have mandatory optional software updates following any found holes,
      3. hired employees to monitor codes (Nigeria),
   5. quantum encryption to replace traditional passwords;
4. Further encourages the creation of intranational emergency hotlines that will rely on backup power grids:
   1. Funded by cyber funding and built by white helmet volunteers,
   2. Overseen and monitored by Intercyber,
   3. Connects governments and large corporations to regional stations to allow for communication in the case of a cyber attack caused power outage;
5. Authorizes the creation of the international cyber committee Inter-cyber who could quickly detect cyber-attacks and respond to any such attacks, as well as recommends tri-annual software assessments for firewalls and anti-virus technologies;
6. Calls upon the creation of a comprehensive international plan to combat cyber warfare including:
   1. international cooperation under the Inter Cyber,
   2. establishing intraweb-servers in nations that will protect private information and that relies on the backup power grids,
   3. mandatory implementation of anti-virus software as previously mentioned
   4. international law and escalating punishments for cyber warfare beginning at two years,
   5. establishing a cyber response center for the Inter Cyber in Ukraine.
7. Urges member states to sanction all countries that use cyber warfare as a military means;
8. Encourages the creation of an anti-warfare organisation as a vigilant medium to detect warfare online, and to remain aware of issues of online warfare rather than waiting for said annual summits;
9. Asks the UN to introduce funding for security measures against cyber warfare for less economically developed countries where NGO’s and MEDC’s will help LEDC’s to be able to implement necessary security measures;