Topic: The Question of State Sponsored Cyber Terrorism

The Political Committee,

Acknowledging the exponential growth in the number of individuals using the Internet, resulting in an increase from an estimated 16 million in 1995, to over 1 billion in 2010,

Defines cyber terrorism as the "politically motivated use of computers and information technology to cause severe disruption in society",

Defines critical infrastructures as those who physical or online systems are crucial to the operations of a nation's economy and government,

Recognizing the risk of cyber attacks due the dependence of critical infrastructure on technology,

Alarmed that state-sponsored cyber attacks have increased by 38% in 2015 compared to the previous year,

Deeply concerned by the twenty countries who have announced their objective to strengthen offensive cyber capabilities,

Recalling resolution 58/199, which calls for the creation of a global culture of cybersecurity and the protection of critical information infrastructures,

Desiring international cooperation amongst nations to increase awareness of the dangers of cyber terrorism and share strategies for defence programs,

Aware of a potential cyber arms race for an increase in cyber capabilities and the danger that follows it,

Further alarmed of a terrorist's ability to have access to the systems which control nation's entire critical infrastructures.

1. Urges The formation of UNSUCT (United Nations Summit on Understanding Cyber Terrorism), to meet biannually in Geneva with roles of but not limited to:
    a. Investigating and reporting on cases of International Cyber Terrorism,

    b. Forming a proposed treaty on the legalities of international cyber terrorism to be published within three years of this resolution passing,
    c. Advising nations on how to prevent their institutions from being victims of International Cyber Terrorism,
    d. Refers to countries who are strongly suspected of sponsoring cyber terrorism to the security council for economic sanctions,
    e. Provide financial means to members unable to invest in protective technologies in order to prevent underdeveloped countries from becoming victims of cyber terrorism;

2. Strongly recommends the creation of a sub-department (named Office of Cybersecurity- OCS), of the OCT (Office of Country Terrorism) to specialise in countering cyber terrorism by,
    a. Establishing a team of specialists to locate all sources of terrorist sites that could later be used to find locations of terrorist parties or organizations,
    b. Initiating a program serving to protect civilians and their personal information in companies' database by:
        i. Informing companies annually of the danger s of cyber terrorism and the importance of protecting their clients,
        ii. Providing work conference for company security teams on the protection of their clients' needs and personal information,
    c. Encouraging government forces for government intelligence agencies to address the issue of cyber terrorism by:
        i. Aiding civilians to understand the problem and to take preventative measures to protect themselves against it,
        ii. Monitoring how the companies and third parties organizations utilize civilians' personal information;
3. Encourages all member states to strengthen their central government's cyber security by:
    a. Implementing national cyber-terror threat protocols, which would include how to combat cyber attacks as well as the necessary software needed for devices containing sensitive and confidential government information,
    b. Establishing a more secure system for government employees, following Russia's example of using government encrypted networks which can only be accessed using certain IP addresses,
    c. Training government officials in order to ensure the correct use of all public cyber security infrastructure,
    d. A minimum standard level of security of confidential information, located at banks, government facilities, hospitals, etc. to prevent hacks into weak computing systems,
    e. Introducing different levels of encryption for sensitive files;
4. Calls for the IMF to provide funding, the use of which is to be monitored by Transparency International Observers, to provide better protection against

cyber-attacks by covering possible failures with additional infrastructure such as but not limited to:

a. Emergency generators in all strategically relevant buildings, for instance, hospitals, or government agencies,
b. Storages of national important resources, for instance, oil, and nourishments which will be distributed by the government in case of emergency,
c. Intranets which are in no way connected to the internet in all strategically and economically relevant agencies, organizations, and companies, for instance, military, state banks, or nuclear plants,
d. Radio-based equipment for all strategically relevant agencies and organizations for instance, the police, military or train operators,
e. Power plants which do not heavily rely on electronic steering systems, for instance, wind turbines, or solar power plants.