**FORUM:** Special Conference II

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

**MAIN SUBMITTER:** The Russian Federation

THE SPECIAL CONFERENCE 2,

*Noting with concern* the increasing occurrence of cyber-attacks, in India the number went from 20 security breaches in 2004, to over 13,000 in 2011,

*Further Noting with concern* the 2007 Estonian cyber attacks and urging all countries to take immediate and definite measures to prevent such attacks from occurring again,

*Realising* that cyber terrorism is less expensive, easier, safer and more anonymous than traditional terrorism, and it can affect a larger number of people; therefore it is more accessible for terrorists,

*Bearing in mind* that besides technical measures, collateral legal measures should be employed as well, in order to prevent and deter criminal behaviour,

*Recognising* the Convention on Cybercrime and all its achievements and efforts,

*Seeking* to decrease the threat of cyber terrorism

*Convinced* that the full co-operation of the United Nations (UN) member states will ensure a total elimination of the growth of cyber threats,

*Recognising* the increased use of the cyberspace by Violent Non-State Actors (VNSA),

1. Proclaimsthe universal definition of cyber terrorism to be: “the intentional use of electronic information systems for the perpetration of terrorist acts inspired by certain motives, such as, but not limited to:
   1. political
   2. ideological
   3. religious with the aims of, but not limited to:
      1. death
      2. serious bodily injury
      3. serious material damage
      4. creating a state of fear
      5. compel a government and/or international organisation to do or abstain from any act
   4. breaching bank security systems
   5. breaching national websites and/or federal agencies;
2. Calls all member states and NGO’s such as but not limited to, Interpol, Europol, CODEXTER, and OSCE to consider taking part in existing international conventions and implementing UN resolutions concerning cyber terrorism such as but not limited to:
   1. The Octopus Conference (a conference which discusses cyber terrorism and means to solving it) with certain reforms such as:
      1. meeting once a year as opposed to every five years
      2. including government officials and more cyber terrorism experts within the conference;
3. Encourages all member states to invest in the research of preventing cyber terrorism, and if solutions are found implementing them;
4. Recommendsthe cooperation between countries, since terrorism is a transnational crime, and encourages to:
   1. create a international legal framework which will deal with mutual judicial assistance, extradition agreements and jurisdictional issues
   2. develop domestic laws to include the establishment of terrorist acts as serious criminal offences and the creation of adequate punishments
   3. to strengthen coordination among states in combating crimes that might

be connected with terrorism, such as:

* + 1. illegal drug trafficking, in order to counter the phenomenon of narcoterrorism, through the help of the United Nations Office on Drugs and Crime (UNODC)

* + 1. money-laundering, which is connected to drug trafficking and is fought by law enforcement and the anti money laundering Unit of UNODC
    2. smuggling and spreading of nuclear, chemical and biological arms and materials and conventional weapons

4d) to add in the United Nations Convention against Transnational Organised Crime (UNCTO) a protocol against cyber terrorism as there is none whilst cyber terrorism is considered a transnational crime

1. Encouragesthe monitoring of online hacking forums in an attempt to limit the trade of illegal malware, such as but not limited to:
   1. Distributed Denial of Service (DDOS)
2. Requestsall governments to implement a routine check of information infrastructures for any signs of cyber activity which is suspicious, if signs are found the government may intervene;
3. Further encourages all member states to consider the guidance offered by the UNODC 2012 report which states and describes the key issues concerning cyber terrorism;
4. Calls upon the international community to establish a comprehensive international legal instruments against the use of cyberspace by terrorists;
5. Solemnly affirms the criminalisation of cyber terrorism to establish jurisdiction and prosecution of the accused;
6. Urges all member states tosupport international cooperation and technical assistance in the providing of ample responses to all criminal challenges in the cyberspace;
7. Authorizes all network operators of Wireless Fidelity (Wi-Fi) networks and cyber access to require users to register and identify themselves to ensure that all internet users are identifiable in an attempt to making the recognising of cyber criminals an easier process;
8. Calls forthe balancing of the law enforcements and human rights considerations to avoid tedious discussion of the infringement of privacy;
9. Further recommends organisations and departments susceptible to cybercrime, including but not limited to:
   1. the United Nations Department for Safety and Security to make use of multiple proxy servers to protect their secure information and prevent cyber terrorists from being successful;

14. Encourages educating the public on:

1. the dangers of cyberterrorism
2. how to protect themselves from cyberterrorism

consequences of cyberterrorism.

15. Further encourages the increasing of sentence length for convicted cyber terrorists and the force finding the criminals in order to discourage further crimes for those convicted and those considering commiting an act of cyber terrorism;

16 . Requests the establishment of the United Nations Cyber Terrorism Unit (UNCTU) to monitor and deal with all aspects of the war on cyber terrorism in order to:

a) effectively assemble a long term plan for the elimination of cyber terrorism

b) establish short term goals to minimize the current reach of cyber terrorism as:

i. current computer systems are the least protected against threats like these, and will take more time to update and secure