**FORUM:** Special Conference 1

**QUESTION OF:** Measures to counter cyber security attacks and establishing cyber security strategies in the digital age

**SUBMITTED BY:** Poland

THE SPECIAL CONFERENCE 1,

*Defining* malware as a software which is specifically designed to disrupt, damage, or gain authorized access to a computer system,

*Reminding* that the term hacking means gaining unauthorized access to data in a system or computer,

*Defining* cyber attack as an attempt by hackers to damage or destroy a computer network or system,

*Defining* cyber warfare as the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes,

*Taking note* of different types of cyber security attacks which include denial-of-service (DoS), drive-by download, phishing and malware attacks,

*Alarmed* that the average cost of cyber attacks on small and medium-sized businesses was an average of $2,235,000 as of 2017,

*Noting* with concern 60% of small businesses say attacks are becoming more severe and more sophisticated,

*Alarmed* of the fact that digital transactions in Europe were hit with 30% more breaches in the first 3 months than the first quarter of 2017,

*Reaffirms* the notion that a targeted cyber attack on a member state’s civilian or military institutions by another member state can be considered an act of war depending on the severity of the attack,

*Alarmed by* member states that indulge in state-sponsored cyber warfare in order to achieve ideological or political goals,

1. Calls for the creation of a special United Nations Council on Cyber Security (UNCCS) composed of cybersecurity experts representing member states whose responsibilities will include:
   1. ensuring a way of communication between institutions in use of a system and the Council
   2. drafting and updating a code of conduct on cybercrime, which will consist of regulations for maintaining Internet integrity, security standards and respect for the benefit of all of its members, clients, and stakeholders
   3. setting penalties depending on the situation at hand for those who fail to comply with the regulations above
   4. understanding the likelihood of scenarios in which a system is under attack and analyzing the risk of said attacks on targets such as but not limited to:
      1. government elections
      2. major transnational corporations
      3. international banks
      4. high profile events
   5. advising member states to take preventative measures against cyber attacks
   6. investigating alongside United Nations (UN) agencies such as Interpol in the aftermath of major cyber attacks
   7. helping member states to work together to solve major cybersecurity breaches in order to avoid geopolitical consequences and damage in diplomatic relations
   8. helping the Least Economically Developed Countries (LDCs) develop their Cybersecurity capabilities;
2. Calls upon Member States to implement educational programs about cybersecurity in public as well as private schools, and to set up public programs by means such as but not limited to having the government and relevant Non-Governmental Organizations (NGOs), such as the Center for Internet Security (CIS) and the Information Systems Audit and Control Association (ISACA), team up to create a beneficial education system for all ages and different types of internet users, in order to:
   1. Teach prevention of threats by various types of cyber security attacks, and the ways in which they can be combated:
      1. Types of cybersecurity attacks would include attacks such as denial-of-service (DoS) and drive-by download
      2. Meeting times for cybersecurity classes would be in the responsibility of those institutions running the classes, with a minimum of a one-hour class per week
   2. demonstrate the different tactics on how to make personal accounts safer on the Internet or other systems that include shared information to the public;
3. Encourages investment by member states in improving cybersecurity for the purposes of:
   1. Preventing major attacks on government institutions
   2. Protecting corporations and businesses from cybercrime
   3. Equipping law enforcement in dealing with cybercrime;
4. Discourages the use of electronic voting machines (EVMs) during major government elections as EVMs are not properly secured;
5. Recommends member states put in place cybersecurity and encryption regulations on institutions such as but not limited to:
   1. Government and private banks
   2. Credit monitoring services
   3. Social security or welfare
   4. Insurance companies
   5. Healthcare services;
6. Proposes a tri-annual United Nations Convention on Cyber Warfare in which member states will have to discuss and agree on:
   1. International rules on the use of cyber warfare during:
      1. Counterterrorism operations
      2. Interstate conflicts
      3. Peacetime
   2. Strategies to counter hacking done by groups such as but not limited to:
      1. Criminal syndicates
      2. Non-state actors
      3. State-sponsored groups
      4. “Lone wolves” or individual cybercriminals
      5. Activist groups
   3. The penalties for a member state using cyber warfare for political or ideological gain
   4. Prohibited targets of state-sponsored hacking such as but not limited to:
      1. Medical services
      2. Charities and aid agencies
      3. UN agencies;
7. Urges member states to place economic sanctions on countries that have been found to be indulging in activities such as:
   1. State-sponsored hacking,
   2. cybercrime for economic gain,
   3. The sabotaging of other member states’ public services,
   4. The manipulation of democratic elections by the use of hacking;
8. Advises member states to develop software designed to protect from dangerous malware, ransomware, and spyware.