**FORUM:** Special Conference 1

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

**SUBMITTED BY:** France

MAIN-SUBMITTED BY: FRANCE,

CO-SUBMITTED BY: Germany, United Kingdom, Somalia, Czech Republic, Gabon, Denmark, Finland, Cuba, Sweden, Belize, France, Syria, Serbia, Japan, Latvia, Morocco,

THE SPECIAL CONFERENCE 1,

*Noting* that privacy is a fundamental human right,

*Further noting* that most people have a smartphone or computer connected to the Internet,

*Acknowledging* that in 2016 there was an estimated 4,000 cyber attacks committed per day according to the Federal Bureau of Investigation (FBI) and 3.174 billion people (CIA, the World factbook) have access to the internet and all of these people can become a victim of cybercrime,

*Realizing* the fact that cybersecurity threats are broadly available, relatively cheap, and constantly evolving,

*Noting* that 20% of businesses do not have a disaster recovery plan, while 42% of businesses that do have a plan have outdated backup methods,

*Encouraging* all nations to spread awareness of cybercrime throughout their country to help secure the understanding amongst civilians,

*Keeping in mind* that cybercrime is a difficult issue to tackle, but an increasing number of nations are banding together to combat the growing threat to internet security,

*Aware* that as part of an increasingly interconnected world, the state, critical infrastructures, businesses and citizens depend on a reliable functioning of information and communication technology and the internet,

*Alarmed* by that cybercriminals earn 1.5 trillion dollars a year worldwide,

*Fully alarmed* that the goal of cybercriminals is stealing sensitive company information or personal data and generating profit,

*Keeping in mind* that cybercrime is an evolving form of crime,

*Noting with deep concern* that serious cyber attacks have a considerable negative impact on the performance of technology, businesses and the administration and hence on a nation’s social, political and economic lifelines,

*Deeply concerned* about attacks in recent years against information infrastructures which have become ever more frequent, complex and in an increasing professional manner,

*Realising* that criminals, terrorists and spies use cyberspace as a place for their activities and do not stop at state borders and that military operations can also be behind cyber security breaches,

*Taking into* account that cyber security must be in line with the importance of protection whilst at the same time not limiting the opportunities and utilization of cyber-space,

*Emphasizing* that the increasing complexity and vulnerability of information infrastructures the cyber security situation and will continue to remain critical,

*Taking note* that most people see technology (especially internet) as something that is free to use but the internet looks free nevertheless we are paying with our privacy, our personal data, and everything we do on our digital devices is stored anywhere,

*Welcoming* the help of the biggest technology companies,

*Emphasizing* that preventing and detecting are the most important ways to

insure cybercriminals to stop,

1. Suggests that individual nations request big technology companies to collect less data from their customers by means such as asking companies to only take data which is necessary for minimal use through the use of the browser “Silo”, through this:
   1. users would have the possibility to cancel the data collection which:
      1. has to be possible at any moment
      2. has to be simple to understand and the ability to turn it off
   2. users would be the rightful owners of all data that a company collects, being able to have access to this data at any moment in order to easily correct and delete all date if they must;
2. Supports greater science, technology, engineering, and mathematics (STEM) initiatives in order to combat the shortage of talent within the cybersecurity field through the Mentors of Science Program, an initiative to be similar to the ones already sponsored by the RAND Corporation for example, which:
   1. would teach specific skills such as coding, robotics, financing, etc.
   2. would have mentors receive stipends for their efforts and the adolescents receive practical and useful guidance on how to achieve their goals and careers, leading to a rise of those interested in STEM fields, such as cybersecurity,
3. Recommends the education of countries about cybercrime, by means such as but not limited to:
   1. mentoring and encouraging young adolescents enrolled in secondary school for careers in science and technology positions, implemented in schools and volunteers would be allowed to experience their selected career for a month under the supervision of professionals in the technology branch,
   2. teaching children how to use technology in a secure and smart way from a young age, so in the future they will help in preventing cybercrime, by:
      1. implementing such information in the curriculum of primary schools, where they would learn for example how to be aware of privacy
      2. implementing it as well in high schools where the students would learn to program and thus see the risks of technology
   3. teaching about privacy not only in schools but also in local communities for the whole population, by means such as but not limited to:
      1. educating them through main news sources, such as the national and international news
      2. developing a nationwide database about cybersecurity;
4. Emphasizes the importance of international and national cooperation in order to ensure cyber security by:
   1. enforcing rights of citizens
   2. protecting critical information infrastructures
   3. recognizing that incidents in other countries' information infrastructure directly affect one's own nation
   4. cooperating with organizations such as the North Atlantic Treaty Organisation (NATO) to affirm that international laws apply in the cyberspace which:
      1. allows for nations to act as a watchdog and better use their resources to protect and defend themselves and each from cyber breaches
      2. can be implemented as regional blocs or how nations decide with whom to share it with
5. Declares accordingly that in order to achieve the aforementioned cooperation at a national level through the enforcement of international rules of conduct, standards and norms as well as enhancing the framework conditions for drawing up common minimum standards (code of conduct) which includes:
   1. confidence building security measures
   2. signatures by as many countries as possible
   3. shaping of nations' external cyber policies in such a way that interests and ideas concerning cyber security are coordinated and pursued in international organizations
   4. the necessity of sovereign evaluation and decision-making powers
   5. the initiation of projects to support partner countries with know-how in cyber defense strategies;
6. Further invites cooperation at a national level through measures such as but not limited to:
   1. the creation of an enhanced strategic and organizational basis by the public and private sector for closer coordination based on intensified information sharing
   2. the set-up of a National Cyber Response Centre that:
      1. allows the quick and close information sharing on weaknesses of IT products, vulnerabilities, forms of attacks and profiles of perpetrators
      2. helps the analysis of Cyber Security issues
      3. gives consolidated recommendations for counter actions
      4. is coordinated with competent authorities as well as partners from industry and academia
   3. the submission of regular reports on early warning in order to effectively combat cyber security threats, by means such as but not limited to:
      1. the set up of a National Cyber Security center
      2. the establishment and maintenance of cooperation between governments and the public and private sector
      3. bringing together politicians, business representatives, associate members, law enforcement agencies and representatives from academia
      4. coordinating preventative tools
      5. encouraging an interdisciplinary approach to tackling the issue of cyber security;
7. Proposes preventative measures against cyber attacks for companies before they occur including:
   1. Unified Threat Management (UTC) firewalls coupled with the production of honeypot software or red herrings in which:
      1. the UTC firewall will include:
      2. deep packet inspection to detect malware and viruses
      3. a single console in which administrators are able to select specifically which websites and servers their computers have access to
      4. content filtering including spam filtering and web-filtering is implemented to reduce clickbait from potential hackers, viruses and other threats
   2. the production of honeypot software and red herrings that will:
      1. act as decoy pop-ups that will trap and distract hackers from the actual information they desire
      2. gather threat information such as IP addresses of the hackers
      3. alert the owner of the site of the attempted breach so that proper legal action can be taken
   3. implements air gaps for companies’ main computers which are:
      1. isolated networks to reduce the potential threats present on public and insecure servers
      2. flexible enough to couple with UTC firewalls as they are not as secure due to bluetooth capabilities
   4. implements threat removers in the event of attempted cyber attacks such as Webroot, which automatically scans a computer for potential threats and removes them on request of the owner within minutes
   5. implements different strong encryption methods such as:
      1. the Advanced Encryption Standard (AES) which is one of the strongest symmetric encryption methods used to protect the most classified information
      2. similar to the AES, Twofish which s another block cipher based off the earlier version Blowfish in order to have the same number of encryptions as banks so there is less opportunity to have holes in the system;
8. Requests for tactical and strategic planning among allied nations in which:
   1. cyberattacks are viewed in the context of aggressive action by hostile foreign agents or governments
   2. responses must be viewed under the same imperative where an attack on one is an attack on all
   3. they will be notified on the how, where, and the effects of the attack and how the receiving nation could or was able to prevent it
   4. national defense budgets should be adjusted to encompass cybersecurity assets and resources to prevent and combat cyber attacks
9. Reminds that the EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in the last 20 years by ways such as, but not limited to:
   1. the GDPR which should be used outside and in the European Union (EU)
   2. thie rule being used properly and controlled by a worldwide authorised organisation such as:
      1. an organisation that has the right to operate everywhere at all time
      2. that these organizations have to share information about the dangers and methods cyber criminals use
      3. that he cyber criminals have to be convicted by these organisations
   3. the government has to promote this law in their public domain,
10. Requests that countries join cyber security partnerships based on geographical blocks and a larger partnership of the global community:
    1. if countries join cyber security partnerships they can share information on how to combat cyber warfare happening in their regions and help each other if there is a serious attack
    2. examples of partnerships are the Council of Europe Convention on Cybercrime (CEC), Shanghai Cooperation Organization (SOC), and International Multilateral Partnership Against Cyber Threats (IMPACT); these organizations all work with the countries within their block or across the globe to combat cyber warfare and share tactics;
11. Considers it desirable that other nations adopt a Cyber Incident Scoring System (CISS) based off the Department of Homeland Security’s model where:
    1. the system has a range of 1 to 5 with 5 being the most severe and 1 being an insignificant attack
    2. it is classified based on the effects of the incident, the severity, and how damaging they are to national sovereignty, public safety, and the economy
    3. it is based on the classification of the incident, it will allow policy makers and leaders to assess and consider responses which:
       1. acts as a signal to the international community
       2. improves decision making transparency
       3. reduces the odds of misperceptions that can lead to escalation of the event;
12. Endorses a national standard for a victim response plan for data breaches known as the Standard for Victim Response of Cyberattacks in which:
    1. a large breach of data concerning consumer and employee data which can negatively affect organizations but also small to medium sized businesses would be taken into account
    2. the financial security of the victims as well as the victim’s personal security of information would be taken into consideration
    3. quick victim response in the case of a cyberattack data breach would be ensured
    4. public communication in the event of a breach that is both prompt and honest about what information was compromised and the victims that were affected would be advised
    5. companies should consider protective options such as identity theft defenses or credit monitoring;
13. Determines the necessity for individual awareness of cyber security by means such as but not limited to:
    1. practicing adequate personal cybersecurity
    2. utilizing strong authentication or 2-step verification methods for adding layers of security to account for the prevention of breaches of those accounts
    3. utilizing biometrics offered in certain accounts and one time codes
    4. access password managers to securely lock account passwords and prevent unwarranted thefts of personal information
    5. becoming aware of safe browsing tools such as Google’s safe browsing tool that can flag websites that are dangerous to visit
    6. recognizing and avoiding phishing attempts which:
       1. lure people into giving away personal information in order to instal malware onto the device or to gain access to accounts
       2. can be attempted through a variety of means such as emails, text messages, and social media
       3. avoid entering passwords or information on sites that do not seem to be legitimate and observe into questionable links
    7. reporting unwarranted intrusions or attempted instructions to proper authorities or law enforcement;
14. Encourages countries to have an association that can aid not only the corporations within the country but also the people, such as the one introduced in Zimbabwe which helps companies and citizens protect themselves from cyber threats, by means such as but not limited to:
    1. offering services such as seminars for people who want to learn more about cyber security, penetration testing, forensic investigations
    2. encryption services, and Intrusive Detection Systems;
15. Suggests the implementation of Advanced Encryption Standard (AES) technology, which is a symmetric encryption algorithm, for the encryption of sensitive data through the:
    1. the protection of data confidentiality using modern encryption algorithms
    2. organizations that collect personally identifiable information
    3. the option for a 256-bit long key size for encryption and decryption and can be used efficiently for both hardware and software and by businesses to encrypt the sensitive data of their customers;
16. Calls upon Information and Communication Technology (ICT) and content providers to aid the promotion of a safe and reliable cybersafe environment by improving security through:
    1. documenting of past hacking events and their details for efficient discovery and resolving of the cyber attack
    2. an auditable security system to be integrated during the development of an IT structure and not post production
    3. aid regarding password and privacy security for both civilians and governments through means, such as but not limited to:
       1. an alert system if an account is opened in a strange location or other suspicious activity occurs
       2. a guarantee of up to date security which is to be improved upon whenever better technology arises
    4. information provided to subscribers about high risks of a breach of security in the network which can lead to a personal data loss or misuse.