Draft Resolution for the Disarmament and International Security Committee

1-2-3: Regulation, Prevention, Response

Signatories: Afghanistan, Algeria, Antigua and Barbuda, Austria, Azerbaijan, Bangladesh, Belarus, Belize, Bolivia, Botswana, Bulgaria, China, Costa Rica, Cuba, Cote d'Ivoire, Cyprus, Democratic Republic of Congo, Equatorial Guinea, Ethiopia, Fiji, Gambia, Guinea, Hungary, Indonesia, Iran, Kyrgyzstan, Lithuania, Madagascar, Maldives, Montenegro, Morocco, Nicaragua, Niger, Nigeria, Palestine, Panama, Peru, Qatar, Republic of Congo, Republic of Korea, Russia, Rwanda, South Africa, Swaziland, Tanzania, Thailand, Tonga, Togo, Tunisia, Turkmenistan, Ukraine, Uruguay, Venezuela, Zambia

Topic B: Cyber Warfare

The General Assembly,

Recalling its resolutions 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 64/25 of 2 December 2009 and 67/2 of 3 December 2012 on developments in the field of information and telecommunications in the context of international security, 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and 64/211 of 21 December 2009 on the creation of a global culture of cybersecurity and building on national efforts to protect critical information infrastructures,

Deeply conscious of the fact that variations exist in the national laws of States in relation to what constitutes criminal conduct,

Recognizing the paramount importance of the legal statutes at the international level, including the UN Charter and other universally recognized norms governing international relations,

Expecting Member States to actively promote the prosecution of violators of such laws,

Expressing its satisfaction with regional efforts to combat cyber-threats, in particular within the Shanghai Cooperation Organization, the Organization of American States, the Asia-Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Economic Community of West African States, the African Union, CARICOM, NATO, the European Union, the Organization for Security and Cooperation in Europe and the Council of Europe,

Recognizing the global and open nature of the Internet as a driving force in accelerating progress towards development and the damaging potential it possesses,

Acknowledging the consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies,

Noting that cyber-power has become an indispensable element of modern technology-based military capability,

Recognizing the complementarity of bilateral, regional and multilateral cooperation for the prevention of cyber-warfare,

Definitions

1. *Endorses* the following definitions of "cyber-crime", "cyber-attacks", and "cyber-warfare":
    a. Cyber-crime: an aggressive action in the cyber-domain by a non-political actor towards another non-political actor, being a violation of criminal law, committed by means of a computer system,
    b. Cyber-attack: any action taken to undermine the functions of a computer network for a political or national security purpose, such as the disruption of dams, dikes, nuclear power plants and medical facilities, and banks particularly as defined by the Geneva convention, whereby bearing in mind that:
        i. Any aggressive action taken by a state actor in the cyber-domain implicates national security, and therefore will be regarded as a cyber-attack,
        ii. A cyber-crime committed by non-state actors or a group who intrudes national or international cyber-systems with the intention to create fear or instability and which deliberately targeted without regard to safety of non-combatants, perpetrated for religious, political or ideological goals, will be considered as a cyber-terrorist attack,
        iii. A cyber-crime committed not for a political or national security purpose, such as internet fraud or identity theft, will not be viewed as a cyber-attack,
    c. Cyber-warfare: a cyber-attack as defined here above,
        i. Whose effects are equivalent to a conventional armed attack or a use of force, causing damage, destruction or casualties for political effect, or,
        ii. That occurs in the context of armed conflict;

2. *Recommends* that a panel of experts in cyber security, under the authority of the UN Institute for Disarmament Research, with the help of the International Telecommunications Union, which shall be referred to as the Panel of Technical Experts on Cyber Security:

a. Consist of experts nominated by any member state, based on equitable geographical representation, and confirmed by a vote of the majority of nations, including:
    i. Government officials,
    ii. White-hat hackers,
    iii. Cyber security defense experts,
    iv. International law experts, and
    v. Other relevant persons as needed,
b. Reconvene every 2 years, except when a special emergency session is requested by the General Assembly or Security Council, to reevaluate and update the definitions of cyber-crime, cyber-attacks, cyber warfare, and cyber espionage;

Regulation

3. *Recommends* the drafting by an established Panel of Governmental Experts of a UN Manual on the application of international law with regard to cyber warfare, aimed at identifying the main rules of cyber warfare regarding international law, explaining their legal basis and normative content and addressing their practical implications in the cyber context, in areas such as but not limited to:
    a. Encourages the UN Manual to be focused on substantive issues such as but not limited to:
        i. Determine under which circumstances, if any, cyber operations can amount to an internationally wrongful threat or use of force, an armed attack justifying the resort to necessary and proportionate force in self-defence or a threat to international peace and security under the law governing the resort to force (*jus ad bellum*), and if so, aimed at determining the specific threshold at which cyber attacks amount to a use of force,
        ii. Determine the applicability of the law of neutrality and whether belligerents can lawfully use the telecommunications infrastructures of neutral states for cyber-attacks and what are the responsibilities of the neutral state, regarding non-state actors conducting attacks within or through its territory or infrastructure,
    b. The Panel shall be composed as following:
        i. Considering equitable geographical distribution,
        ii. Open to the joining of willing states,
        iii. Experts are appointed as designated by the above-defined states,
    c. Gathering regularly,
    d. Headed by a rotating chair, changed yearly;

4. *Emphasizes* that governments are responsible for non-state actors when those actors are under the direct control or fall under the authority of the state, often as characterized by funding and direct oversight;

5. *Reaffirms* the importance of coordinating policies dealing with cyber-attacks and cyber-warfare, both on a national and an international level:
    a. Nationally, by combining both defense and foreign affairs policy,
    b. Regionally, as a first step toward international cooperation and as an efficient level to take into account regional specificities,
    c. Internationally, by encouraging cooperation between member nations;

6. *Urges* states to introduce national legislation and appropriate internal measures to regulate cyber crimes and attacks according to the aforementioned definition, including but not limited to:
    a. Through the criminalization of, inter alia:
        i. Illegal access to devices, information or communications,
        ii. Illegal interception of information or communications,
        iii. Attacks on data integrity,
        iv. Attacks on system integrity,
        v. Device abuse,
        vi. Computer counterfeiting,
        vii. Computer fraud,
        viii. Attempts against intellectual property and related rights, and against the right to privacy,
        ix. State financial or other support for non-governmental groups and/or individuals involved in the abovementioned actions,
    b. And by implementing internal cyber-security structures, such as:
        i. Cyber Forensics Labs,
        ii. Cyber Security Incident Response Teams;

7. *Recommends* that activities referred to as "cyber-attacks", carried out by or suffered by a state actor, will be regulated in the following way:
    a. States carrying out cyber-attacks shall be held responsible in accordance with the general principles of international public law, insofar that the cyber-operation be attributable to it and constitute a breach of its international obligations,
    b. To the extent that cyber-attacks do not qualify as armed attacks triggering the right of self-defense, but yet violate an international obligation of the perpetrating state, such as the customary international law norm of non-intervention, states suffering from a cyber-attack may employ limited and proportional counter-measures, in line with the general principles of public international law;

8. *Urges* States to adopt a responsible behavior and actions consistent with norms, rules and principles of such a responsible behavior, including the above-mentioned applicability of international law to the cyber-sphere and the respect of national sovereignty, territorial integrity and political independence, such as but not limited to:
    a. The adoption of effective safeguards for:
        i. Confidentiality, understood as the prevention for information from being used by unauthorized individuals or processes,
        ii. Integrity, viewed as safeguarding accuracy and completeness of anything of value to an organization,
        iii. Availability, which is to ensure that information is accessible and usable on demand by authorized entities,
    b. The non-use of non-State actors as proxies for the commitment of malicious Information and Communication Technology, (ICT) related actions, and therefore
    c. The responsibility of all State to fight non-State actors' ICT-related malicious actions, including to find, deny safe haven to, and bring to justice and prosecute any non-State actor who supports, facilitates, participates, or attempts to participate in the financing, planning, preparation, or commission of cyber warfare acts or provides safe haven pursuant to the resolution of the Security Council 1624 (2005);

Prevention

9. *Endorses* creating a Prevention & Trust-building program using the Public Health model as a role model, which researches, monitors and makes recommendations to states, groups and individuals to empower them to guard their citizens and themselves against cyber-attacks by focusing on:
    a. Incident watch, to monitor cyber sphere activities from botnets, malware, crime and attacks from trusted partners such as United Nations of Internal Oversight Service and UNDIP Disaster Risk Assessment, and the scientific community,
    b. Threat analysis and building a Cyber Risk Assessment & Management Matrix,
    c. Data dissemination, that provide information for states, critical infrastructures, private groups and individuals on topics including, but not limited to:
        i. Current developments in the cyber sphere,
        ii. Best practices for protecting and defending systems,
        iii. How to assess infrastructures to find vulnerabilities, assessment that could have for basis the self-assessment tool annexed in resolution 64/211 of the General Assembly,
        iv. How to best address these vulnerabilities,
        v. How governments can target denial of service issues and cybercrime;

10. *Recommends* that a Cyber Risk Assessment & Management MATRIX be created under the aegis of the United Nations of Internal Oversight Service in order to prevent the cyber-attacks from happening, strengthen our resilience, deter malicious actions
    a. With the eventual objectives of:
        i. Understanding the current situation, needs and gaps to assess already existent threats,
        ii. Building on existing information and capacities,
        iii. Providing available data and information on the current institutional framework and capabilities,
    b. Should follow the following steps:
        i. Systematic inventory and evaluation of existing risk assessment studies
        ii. Hazard assessment to identify the nature, location, intensity and likelihood of major hazards prevailing in a community or society,
        iii. Vulnerability analysis to determine the capacity or lack of capacity of elements at risk to withstand the given hazard scenarios,
        iv. Loss/impact analysis to estimate potential losses of exposed population, poverty, services, live hoods and environment, and assess their potential impacts on society,
        v. Risk profiling and evaluation to identify cost-effective risk reduction options in terms of the socio-economic concerns of a society and its capacity for risk reduction,
        vi. Formulation or revision of the Cyber Risk Assessment Matrix strategies and action plans that include setting priorities, allocating resources;

11. *Recommends* to adopt transparency and confidence-building measures (TCBMs) in ICT-related activities, in order to increase predictability of cyber incident, to reduce misperception among ICTs-related States activities and to create a global cyber-security culture for settling the appropriate conditions toward a peaceful, secure, open and cooperative ICT environment, measures in which stand:
    a. The exchange of national views on the use of ICTs for defense matters, including in conflict situation and in counter-terrorism programs, either in national initiatives, through the UN by providing a report to the Secretary-General or through national publications such as *White Papers*, or in workshops,
    b. The exchange of information on national legislation on cyber-security and on cyber-security strategies and policies, including prevention and response to cyber-incident, either in national initiatives such as *White Papers*, through the UN by providing a report to the Secretary-General or in workshops,
    c. The organization international seminars, conference cycles and workshops, with the participation of States, private sector and the scientific and legal community;
    d. The harmonization of national legal frameworks about ICT-related actions, through incentives to make those frameworks in compliance with international

principles, in order to facilitate cooperation and to reduce incidents that could otherwise be misinterpreted as hostile State actions;

12. *Encourages* further research into a system with a defensive advantage, by
    a. Requesting NGOs, states, and private corporations to offer cash prizes and incentives to reward the development of a system which privileges defense, in contrast to the current cyberspace, which is weighted towards offensive capabilities,
    b. Offering to subsidize the installation of new cyber-infrastructure in nations without preexisting extensive internet infrastructure, with the understanding that such infrastructure would function as a test case;

13. *Authorizes* the United Nations Office for Disarmament Affairs, in cooperation with the existing resources of the International Telecommunications Union, to construct a database, known as the International Preventative and Response Database for Cyber Warfare, which shall:
    a. Use the existing database structure of the United Nations Office for Disarmament Affairs for the UN Register of Conventional Arms,
    b. Offer data to all stakeholders, including private corporations,
    c. Gather information from voluntary participants, with a particular emphasis on working with:
        i. Private corporations, including mass-media channels, and financial institutions which are targeted by state or non-state actors,
        ii. States which are targeted in a variety of forms, as defined above;

Response

14. *Urges* all member states to participate in, contribute to, and make use of the resources currently available for combating cybercrime, including, but not limited to, Interpol and IMPACT;

15. *Calls upon* Interpol to facilitate the identification and punishment of non-state cyber-criminals through:
    a. Formalizing existing Mutual Legal Assistance Treaties, by:
        i. Aiding in bilateral or multilateral information sharing, and coordination particularly when cybercriminals use proxies, in order to better determine the origin of the attacks,
        ii. Encouraging openness when nations detect cyber-attacks, in order to better detect patterns,

b. Facilitating extradition of criminals in order to address jurisdictional conflicts in cases including, but not limited to:
    i. Cyber-attacks carried out against multiple countries simultaneously,
    ii. Attacks which utilize proxies in multiple countries,
c. Providing response strategies for state and non-state interventions upon detecting an attack or suspecting an attack, including, but not limited to,
    i. Tracer bugs to find the root of the infiltration,
    ii. Backup programs to protect critical information and remove access to critical information from hackers;

16. *Encourages* private companies to share information with their respective national governments and the international community with regards to attacks on their resources in the form of:
    a. Information about the technical aspects of the malware and attack, without providing sensitive information about the content targeted in the attack,
    b. A program modeled after of the Malware Information Sharing Program, as used by NATO;

17. *Reaffirms* the right of nations to self-defense in response to both conventional war and cyber-war, while emphasizing that nations ought to:
    a. Exercise such rights in proportion to the magnitude of the attack, as defined by the UN Charter,
    b. Make use of international information sharing resources, as outlined above, in order to:
        i. Ensure accurate attribution through measures outlined above,
        ii. Secure international support for any response to cyber-attacks,
    c. Consult Interpol and/or the Panel of Technical Experts on Cyber Security for guidance as needed,
    d. Focus on defensive strategies first, rather than offensive responses;

18. *Encourages* states with advanced cyber technology to assist developing nations and Small Island and Developing States (SIDS) with creating tools for the development of cyber defense systems, through mechanisms including but not limited to:
    a. The establishment of centralised training unit where states would voluntarily contribute cyber expertise and resources to facilitate the training of cyber experts in developing nations and SIDS, which would:
        i. Invite promising STEM (Science, Technology, Engineering, and Math) and computer science students and professionals from a variety of nations to training camps,
        ii. Focus on developing tools for unique, individual, sustainable strategies rather than replicating the existing technology of developed nations,

iii. Meet regularly in rotating host nations to remain impartial,
iv. Focus on education of individuals and corporations to increase awareness of information usage and leakage,

b. The creation of infrastructure in developing nations and SIDS which would:
i. Not contain easily accessed hubs which are susceptible to physical attack or physical upload of viruses or spyware,
ii. Consist of durable, sustainable physical infrastructure tailored to the climate and needs of each nation;

19. *Further encourages* states to develop contingency measures in case of the breakdown of national infrastructure due to attacks on cyber and information systems, including, but not limited to:
a. Smart Power Grids, which minimize the scope of a blackout attack,
b. Backup Generators for critical infrastructure,
c. Paper records of sensitive or important documents necessary to the effective functioning of the government,
d. Training exercises for police and other critical government employees to respond in cases of a lack of power and/or internet resulting from a cyber attack;

20. *Recommends* that an International Code of Conduct for Information Security be drafted complying with the following requirements:
a. The Code will operate with the stated purposes of:
i. Identifying states' rights and responsibilities in information space,
ii. Promoting their constructive and responsible behaviors within cyber space,
iii. Enhancing their cooperation in addressing the common threats and challenges in information space, to ensure the Information and Communication Technology, or ICTs, networks are solely used to be consistent with the aim of maintaining international stability and security,
iv. Enhancing their cooperation in addressing the common threats and challenges in information space, so as to ensure the ICTs, including networks to be solely used in a method consistent with the aim of maintaining international stability and security,
b. The adherence of this Code should be voluntary and open to all states, based on an equal representation of geography and other factors;
c. In accordance with the following steps:
i. Cooperating in combating criminal and terrorist activities with the use of ICTs, including dissemination of information inciting terrorism, extremism, national division, likely to undermine states' political, economic and social stability and territoriality,

ii. Reaffirming all State's rights and responsibilities to protect their information space, critical information infrastructure,
iii. Encouraging assistance to developing countries in their efforts to enhance capacity-building on information security with the eventual aim of closing the digital gap between states,
iv. Respecting the rights and freedom in information space, including rights and freedom of searching for, acquiring and disseminating information on the premise of complying with relevant national laws and regulations,
v. Prioritizing the work of regional bodies,

21. *Encourages* all member states to further strengthen their capacity in incident management building measures and information sharing for the purpose of warning, response and recovery among the following actors:
    a. Government agencies,
    b. Non-governmental organizations,
    c. Other actors involved;

22. *Calls for* strengthening solidarity and effective defense for critical infrastructure by establishing a voluntary database system, with achieving transparency and confidence building on prevention of cyber attacks with the following purposes:
    a. Sharing information about potential hackers or groups,
    b. Sharing information about confirmed regional or international hackers,
    c. Technology sharing for system security reinforcement and bridging digital divide by countries;

23. *Recommends* member states to strengthen capacity building of developing countries and bridge the digital divide between states by technological assistance and sharing;

Conclusion

24. *Calls upon* the United Nations Fifth Committee to delegate funding for the programs outlined in this resolution;

25. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats of cyber warfare, as well as new strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

26. *Decides* to include in the provisional agenda of its twenty-fifth session the item entitled "Cyber Warfare".