Non-paper listing specific language proposals under agenda item “Rules, norms and principles” from written submissions received before 2 March 2020

China
- States should pledge not to use ICTs and ICT networks to carry out activities which run counter to the task of maintaining international peace and security.

State sovereignty in cyberspace
- States should exercise jurisdiction over the ICT infrastructure, resources as well as ICT-related activities within their territories.
- States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens’ legitimate interests in cyberspace.
- States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability.
- States should participate in the management and distribution of international Internet resources on equal footing.

Critical infrastructure protection
- States have the rights and responsibilities regarding legal protection of their critical ICT infrastructures against damage resulting from threats, interference, attack and sabotage.
- States should be committed to refraining from launching cyber attacks on the critical infrastructures of other states.
- States should not exploit policy and technical advantages to undermine the security and integrity of critical infrastructures of other states.
- States should increase exchanges on standards and best practices with regard to critical infrastructure protection and encourage enterprises to embark on such exchanges.

Data security
- States should take a balanced approach with regard to technical advancement, business development and safeguarding national security and public interests.
- States have the rights and responsibilities to ensure the security of personal information and important data relevant to their national security, public security, economic security and social stability.
- States shall not conduct or support ICT-enabled espionage against other states, including mass surveillance and theft of important data and personal information.
- States should pay equal attention to both development and security, and push for the lawful, orderly and free flow of data. States should facilitate exchanges of best practices and cooperation in this regard.

Supply chain security
- States should not exploit their dominant position in ICTs, including dominance in resources, critical ICT infrastructures and core technologies, ICT goods and services to undermine other states’ right to independent control of ICT goods and services as well as their security.
- States should prohibit ICT goods and services providers from illegal obtainment of users’ data, control and manipulation of users’ devices and systems by installing backdoors in goods. States should also prohibit ICT goods and services providers from seeking illegitimate interests by taking advantage of users’ dependence to their products, or forcing users to upgrade their systems or devices. States should request ICT goods and services providers to make a commitment that their cooperation partners and users would be noticed in a timely manner if serious vulnerabilities are detected in their products.
- States should be committed to upholding a fair, just and non-discriminatory business environment. States should not use national security as a pretext for restricting development and cooperation of ICTs and limiting the market access for ICT products and the export of high-tech products.
Counter-terrorism

- States should prohibit terrorist organizations from using the Internet to set up websites, online forums and blogs to conduct terrorist activities, including manufacturing, publication, storage, and broadcasting of terrorist audio and video documents, disseminating violent terrorist rhetoric and ideology, fund-raising, recruiting, inciting terrorist activities etc.
- States should conduct intelligence exchanges and law-enforcement cooperation on countering terrorism. For instance, one state should store and collect relevant online data and evidence in a timely manner upon request from other states for cyber-related terrorism cases, provide assistance in investigation and deliver prompt response.
- States should develop cooperative partnership with international organizations, enterprises and citizens in fighting cyber terrorism.
- States should request Internet service providers to cut off the online dissemination channel of terrorist content by closing propaganda websites and accounts and deleting terrorist and violent extremist content.

Croatia, Finland, France and Slovenia

- States should be encouraged to take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State’s territory.
- This aim could be achieved by working with the private sector to define permissible actions using a risk-based approach and to develop concrete tools - certification processes, best-practices guides, response mechanisms to incidents and, as appropriate, national regulations.

Cuba

This situation calls for the implementation of specific regulations complementary to international law aimed, among others, at the following equally important elements:

- Preventing the application of unilateral measures and measures against states measures that hinder universal access to the benefits offered by ICTs.
- Mitigating the malignant effects of attribution in the face of cyber-attacks.
- Preventing the militarization of cyberspace.
- Protecting citizens’ private data more effectively by promoting international regulations in this respect.
- Complementing legislation on cyberterrorism in order to face cybersecurity incidents and problems, such as cyberattacks.
- Define by consensus what is understood by a cyberattack. Operationalizing the application, with greater objectivity, of the principles of international law in this area.

Islamic Republic of Iran

- The roles of States, with the primary responsibility for maintaining a secure, safe and trustable ICT environment, should be enhanced in ICT environment governance, including policy and decision making, at global level. The envisaged governance should be realized in a manner which strengthen state sovereignty and shall not affect rights of the states in making their choice of development, governance and legislation models in the ICT environment.
- States should refrain from the threat or use of force against the territorial integrity or political independence of any state within and through ICT environment.
- No state has the right to intervene through cyber-related ways and means, directly or indirectly and for any reason, in the internal or external affairs of other states. All forms of intervention and interference or attempted threat against political, economic, social and cultural systems as well as cyber-related critical infrastructure of the States shall be condemned and prevented. (UNGA resolution 2131 of 21 December 1965)
- States shall not use ICT advances as tools for economic, political or any other type of coercive measures, including limiting and blocking measures against target states. (UNGA resolution 2131 of 21 December 1965)
- States should ensure appropriate measures with a view to making private sector with extra-territorial impacts, including platforms, accountable for their behaviour in the ITC environment. States must exercise due control over ICT companies and platforms under their Page 8 of 11 jurisdiction, otherwise they are responsible for knowingly violating national sovereignty, security and public order of other states.
• States should refrain from, and prevent, abusing ICT supply chains developed under their control and jurisdiction, to create or assist development of vulnerability in products, services and maintenance compromising sovereignty and data protection of the target states.

Netherlands

• “State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace” [would be] guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g)

• “State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites,” [would be] guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g)