PARIS CALL
FOR TRUST AND SECURITY IN CYBERSPACE

12th November 2018

Cyberspace now plays a crucial role in every aspect of our lives and it is the shared responsibility of a wide variety of actors, in their respective roles, to improve trust, security and stability in cyberspace.

We reaffirm our support to an open, secure, stable, accessible and peaceful cyberspace, which has become an integral component of life in all its social, economic, cultural and political aspects.

We also reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States.

We reaffirm that the same rights that people have offline must also be protected online, and also reaffirm the applicability of international human rights law in cyberspace.

We reaffirm that international law, together with the voluntary norms of responsible State behavior during peacetime and associated confidence and capacity-building measures developed within the United Nations, is the foundation for international peace and security in cyberspace.

We condemn malicious cyber activities in peacetime, notably the ones threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure and welcome calls for their improved protection.

We also welcome efforts by States and non-state actors to provide support to victims of malicious use of ICTs on an impartial and independent basis, whenever it occurs, whether during or outside of armed conflict.

We recognize that the threat of cyber criminality requires more effort to improve the security of the products we use, to strengthen our defenses against criminals and to promote cooperation among all stakeholders, within and across national borders, and that the Budapest Convention on Cybercrime is a key tool in this regard.

We recognize the responsibilities of key private sector actors in improving trust, security and stability in cyberspace and encourage initiatives aimed at strengthening the security of digital processes, products and services.

We welcome collaboration among governments, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections.

We recognize all actors can support a peaceful cyberspace by encouraging the responsible and coordinated disclosure of vulnerabilities.

We underline the need to enhance broad digital cooperation and increase capacity-building efforts by all actors and encourage initiatives that build user resilience and capabilities;

We recognize the necessity of a strengthened multistakeholder approach and of additional efforts to reduce risks to the stability of cyberspace and to build-up confidence, capacity and trust.

To that end, we affirm our willingness to work together, in the existing fora and through the relevant organizations, institutions, mechanisms and processes to assist one another and implement cooperative measures, notably in order to:

- Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;

- Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;

- Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;

- Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;

- Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;

- Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;

- Support efforts to strengthen an advanced cyber hygiene for all actors;

- Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors ;

- Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

In order to follow-up on the progress made to advance these issues in the appropriate existing fora and processes, we agree on reconvening at the Paris Peace Forum in 2019 and at the Internet Governance Forum in Berlin in 2019.

[Paris, 12th of November, 2018]