G7 DECLARATION
ON RESPONSIBLE STATES BEHAVIOR IN CYBERSPACE

LUCCA, 11 APRIL 2017

INTRODUCTION

We remain committed to an accessible, open, interoperable, reliable and secure cyberspace. We recognize the enormous benefits for economic growth and prosperity that we and all others derive from cyberspace as an extraordinary tool for economic, social and political development.

We are concerned about the risk of escalation and retaliation in cyberspace, including massive denial-of-service attacks, damage to critical infrastructure, or other malicious cyber activity that impairs the use and operation of critical infrastructure that provides services to the public. Such activities could have a destabilizing effect on international peace and security. We stress that the risk of interstate conflict as a result of Information and Communication Technology (ICT) incidents has emerged as a pressing issue for consideration. Furthermore, we are increasingly concerned about cyber-enabled interference in democratic political processes.

We encourage all States to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT. Cooperative approaches would also contribute to the fight against the use of cyberspace by non-State actors for terrorist and other criminal purposes.

For these reasons, the G7 set an ambitious course in promoting security and stability in cyberspace and the protection of human rights, through *"The Principles and Actions on Cyber"* endorsed in Ise-Shima on 26 and 27 May 2016.

We continue to call upon all States to be guided in their use of Information and Communications Technologies (ICTs) by the cumulative reports of the United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN-GGE).

Reaffirming our commitment to contribute to international cooperative action and the protection against dangers resulting from the malicious use of ICTs, we support the following Declaration, and encourage similar commitments from other States:

DECLARATION

We recognize the urgent necessity of increased international cooperation to promote security and stability in cyberspace, including on measures aimed at reducing the malicious use of ICTs by State and non-State actors;

We are committed to promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States;

We reaffirm and note with approval the widespread affirmation by other States that international law and, in particular, the United Nations Charter is applicable to the use of ICTs by States. This affirmation is essential to maintaining peace and security and promoting an open, secure, stable, accessible and peaceful ICT environment;

We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties;

We reiterate the responsibility of States to refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations;

We note that, in the interest of conflict prevention and peaceful settlement of disputes, international law also provides a framework for States' responses to wrongful acts that do not amount to an armed attack - these may include malicious cyber activities. Among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures, including measures conducted via ICTs, against the State responsible for the wrongful act in order to cause the responsible State to comply with its international obligations;

We note that the customary international law of State responsibility supplies the standards for attributing acts to States, which can be applicable to activities in cyberspace. In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When attributing an internationally wrongful act to another State, or when taking action in response, a State must act in accordance with international law. In this context, a State assesses the facts and is free to make its own determination in accordance with international law with respect to attribution of a cyber-act to another State;

In 2016, we affirmed that, under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognized that States may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace;

To increase predictability and stability in cyberspace, we call on States to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible in order to improve transparency and give rise to more settled expectations of State behavior;

We believe that confidence building measures on States' use of ICTs are also an essential element to strengthen international peace and security. We continue to support the development and implementation of such practical CBMs, including communication channels among States for crisis management, in relevant bilateral, regional and multilateral forums, including the Organization for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum (ARF);

In addition, we support the promotion of voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime, which can reduce risks to international peace, security and stability. Such norms do not seek to limit or prohibit any action that is otherwise consistent with international law. Nor do norms limit a State's obligations under international law, including with regard to human rights. Norms reflect the current expectations of the international community, set standards for responsible State behavior, and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.

The following voluntary, non-binding norms of State behavior during peacetime were articulated in the 2015 GGE report and the 2015 G20 Leaders' Communiqué:

1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
2. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;
5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;
8. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;
9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
10. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;
11. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should

not use authorized emergency response teams to engage in malicious international activity.

12. No country should conduct or support 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 sectors.