Mr Chairman,

France stands behind the statement of the European Union, and would like to present additional remarks in a national capacity.

In a rapidly changing world, the civilian and military uses of cyber space are increasing, representing important factors for development but also posing new security challenges. Cyber attacks are increasingly frequent, complex and costly, reminding us of the extent to which cyber security is a legitimate priority for governments. States must therefore show their determination to address these challenges through cooperation and law.

To this end, France issued a call to the international community nearly a year ago: the Paris Call for Trust and Security in Cyberspace. This call, which reaffirms our support for a cyber space that is open, secure, stable, accessible and peaceful received very wide support and we are delighted. Some 68 States, 358 private sector actors, and 142 organizations joined us to reaffirm that international law, including the Charter of the United Nations in its entirety, international humanitarian law and international customary law should be applied to the use of information and communication technology.
Every State must therefore respect the obligation to resolve international disputes using peaceful means, without negating its right to take counter-measures in response to internationally illegal actions and with the sole objective of putting an end to such actions, in compliance with its international law obligations.

Also, in order to ensure that people’s rights are respected and protected online as they are in the physical world, States must work together, but also with private-sector partners, academia and civil society.

Mr Chairman,

For many years now, cyber space has been a place of confrontation. That is why France has chosen to adopt a doctrine for using its defensive and offensive cyber warfare capabilities, a doctrine officially presented in January by the Minister for the Armed Forces, Florence Parly. In September 2019, the Ministry for the Armed Forces also published a report that set out France’s position with regard to applying international law to operations in cyber space. This transparency that France is promoting shows that it is a responsible State. It is in keeping with its conception of a cyber space that is free, secure, open, stable and based on trust and the rules of international law.

It is by being transparent that we will succeed in building the necessary trust for cooperation. France therefore encourages every State to publicly present its interpretation of how international law should be applied in cyber space or even its doctrine for using cyber capabilities as we ourselves have done.

Mr Chairman,

As you know, France has actively participated in the various UN Groups of Governmental Experts on cyber security. These groups made progress possible, in 2013 and 2015, on the applicability of international law in cyber space, and the development of important norms and recommendations for responsible behaviour by States in this area. Each State now has a responsibility to implement these recommendations and respect these standards.
France welcomes the resumption of the Group of Governmental Experts’s work on cyber security issues. This new group should help develop norms and recommendations on responsible behaviour of States identified by previous GGEs.

France is also engaged in the negotiations of the open-ended working group (OEWG) on issues related to cyber space security. By nature, this group allows all willing States to join and contribute to better common understanding of threats and solutions. This group has been able to involve the private sector, academia and international organizations in our reflection. They have their own responsibilities and an unprecedented but crucial role in supporting States so as to create a more secure and stable cyber space.

In order to ensure shared security and equal access to an open free and secure cyber space, reflection should be conducted within these mechanisms on a strategy to deploy with a view to building capacity of countries expressing cyber security needs.

Mr Chairman,

France considers that regular institutional multi-stakeholder dialogue on cyber security issues is necessary to build trust and cooperation between States in this area. It is our responsibility and in our interest to defend frameworks for action and rules of law that are collectively established, by committing to strengthening the role of the United Nations system in this regulation while including other digital stakeholders to develop new forms of global governance.

Thank you.