“The Paris Call for Trust and Security in Cyberspace”

Frequently Asked Questions

1. **Why is France launching the Paris Call for Trust and Security in Cyberspace?**

The digital space, more simply known as “cyberspace”, has become a new place for economic opportunities and social transformations. In recent years, France has made strengthening the stability of this space one of its priorities. Our country aims to enable cyberspace to be a **forum for discussions for all States, their citizens and businesses**. To achieve this, we are promoting a rules-based cyberspace, where international law applies and where fundamental freedoms and human rights are respected.

2. **What is the content of this call?**

The Paris Call for Trust and Security in Cyberspace is a political declaration that will signal a global mobilization for the stability of cyberspace. This Call strengthens the work of the international community and of the many stakeholders involved in digital security.

This text recalls a number of principles which we see as fundamental, such as the implementation of international law and human rights in cyberspace. It also highlights the need for a multistakeholder approach to draw up norms enabling us to take full advantage, i.e. reliably and securely, of the opportunities opened up by the digital revolution.

Finally, the Paris Call promotes strengthening the security of digital products and services, which, for example, we use in our daily lives. Therefore, the text aims to prevent cyberattacks by malicious parties which endanger all individuals in cyberspace.

3. **How was this text prepared?**

Cyberspace is today the meeting place for a wide range of actors, from different backgrounds. To this end, **the Paris Call is the result of a process which includes three types of actors: States, private companies and civil society.** It is the fruit of consultations with France's government partners, first and foremost European ones, but also with digital private sector and NGO actors.

Naturally, within the private sector and civil society, there are varying, sometimes contradictory, voices and interests. We have therefore talked to the broadest possible range of actors in order to reflect this diversity of opinions and to emphasize the main points on which we can all agree.

4. Who can endorse the Paris Call?

States, businesses and civil society organizations are invited to endorse this text via a contact form accessible online, on the site of the Ministry for Europe and Foreign Affairs.

The text will remain open for endorsement after it has been presented at the 13th Internet Governance Forum on 12 November. We hope it can garner as many endorsements as possible.

5. What is the goal of the Paris Call?

This texts aims to highlight issues which do not always get the attention they deserve. Cybersecurity is not just for IT experts or geeks. All of us use cyberspace, whether as consumers, citizens, regulators, political decision-makers, developers or producers of digital products. We all need concrete mechanisms enabling us to operate in a safe cyberspace which respects our freedoms.

This Call highlights the importance we place on the stability of cyberspace and our determination to work well with all parties to provide concrete solutions. The Paris Call will strengthen the legitimacy of actors which endorse it in order to offer ambitious solutions to meet the challenges set out in this text.

This text must also serve to protect the users of IT tools and applications. It recalls that companies must commit to maintaining the security of digital products and services for a sufficient duration during their life cycle. Processes to manage and disclose IT vulnerabilities must also be improved. Finally, the principle of "security by default" must become the norm for all digital products on the market.

6. In concrete terms, what difference will this Call make?

For us, this Call must mark the start of detailed dialogue on everybody's responsibilities as regards cybersecurity and the stability of cyberspace. **Work must continue to implement the various priorities identified in the Call.** We will make a number of proposals within different international organizations regarding the security responsibilities of the makers of digital products and services.

7. How will this initiative be monitored?

We do not want to create a complex system or bureaucracy designed to monitor all the developments resulting from this Call.

It is, **however, important that in a year's time, we meet with our partners and various endorsers, at the next editions of the Paris Peace Forum and the Internet Governance Forum,** in order to make an initial assessment of the progress made. This should allow us to take stock of the concrete ideas, solutions and proposals put forward by the Call's various endorsers, but also to identify the issues which require further work.

8. What role can private stakeholders play in cyberspace?

Private actors have an important responsibility in the digital world due to their widespread presence and the many services they provide. However, **with regard to international peace and security, in both cyberspace and elsewhere, it is indeed States which are currently and must remain at the forefront.**

That is why we wanted to state in the Call that offensive activities by private actors in cyberspace, which sometimes resemble cyber mercenary activities and create risks of escalation and conflict, must be prohibited.

At the same time, we must recognize that most of the infrastructure which allows cyberspace to operate and provides us with access to it is owned by private companies. **Like civil society, companies therefore have a role to play in protecting and defending cyberspace, within the limits prescribed by international law and national legislation and by working in close cooperation with governments.**