Paris Call Community Consultation

Announced at the International Cybersecurity Forum (ICF) in Lille, France, on January 30, 2020, by the French Ambassador for Digital Affairs, this consultation aims at better understanding the concerns and interests of the Paris Call community in order to better relay them on the international stage. The consultation will be open until March 16, 2020. A summary of the contributions will be presented by France as from April during the next meetings of the Paris Call community.

Raw contributions will be published on the French open data platform data.gouv.fr, except for organizations' names and email addresses.

For more information on the Paris Call, visit pariscall.international.

If you have any question, please write to: contact@pariscall.international.

1. Foresight

a. In your opinion, which technology may have the most destabilizing impact in the coming months or years? *(500 character limit)*

b. In your opinion, which technological innovation has the most promising cybersecurity applications? *(500 character limit)*

c. Have you put in place specific actions in response to these new threats and opportunities?

☐ Yes
☐ No

d. If yes, which actions? *(500 character limit)*

2. Individual rights

a. In your opinion, are citizens' rights sufficiently protected in the face of dangerous practices developing in cyberspace (cybercrime, theft of personal information, information manipulation, electoral interference...)?

☐ Yes, absolutely
☐ Yes, partially
☐ No, insufficiently
☐ Not at all

b. If no, how can they be better protected? *(500 character limit)*

c. In your opinion, how can we guarantee the application of international human rights law and international humanitarian law to cyberspace?

☐ By placing more trust in private actors
☐ By opening discussions on this topic that would involve all relevant stakeholders
☐ By conducting negotiations within international organizations (UN, OECD, EU, etc.)
☐ By creating tools for imposing sanctions on actors who do not respect these norms
☐ Other: …

d. Should providers of digital services and products have a duty of care to protect their users from online risks?

☐ Yes, absolutely
☐ Yes, possibly
☐ Probably not
☐ Absolutely not

3. Advancing security

a. Do you take any special measures to ensure digital security of your products and services?

☐ Yes
☐ No

b. In your opinion, what minimum norms or standards should companies selling digital products and services adhere to? *(500 character limit)*

c. In your opinion, what measures could be taken at the national or international level by states to ensure the protection of civil critical infrastructure? *(500 character limit)*

d. Do you think these measures should be mandatory?

☐ Yes
☐ No

e. What mechanism or procedure do you have at your disposal in the event of a cyber-attack or incident on your infrastructures? *(500 character limit)*

f. Do you have the ability to inform your authorities of a cyber incident that would affect you?

☐ Yes
☐ No

4. Capacity building and technical cooperation

Capacity building refers to supporting the development of cyber defense capabilities of public and private entities through training and coaching programs, technical assistance, and the exchange of resources and expertise.

a. What are the capacity building needs of your organization or country? *(500 character limit)*

b. Do you have the resources to contribute to capacity building in your community, in your country or in other countries?

☐ Yes
☐ No

c. If yes, how are you willing to contribute? *(500 character limit)*

d. Which capacity building or international cooperation initiative impressed you the most last year? *(500 character limit)*

e. What, in your opinion, is your organization's main weakness in terms of cybersecurity? *(500 character limit)*

5. Multi-stakeholder cooperation

a. Do you collaborate, on your level, with public authorities, businesses and/or civil society organizations?

☐ Yes
☐ No

b. If yes, how? *(500 character limit)*

c. What obstacles do you think impede cooperation between governments, the private sector and civil society? *(500 character limit)*

d. What do you think is the most appropriate multi-stakeholder forum for discussions on cyberspace? *(500 character limit)*

6. The principles of the Paris Call and the UN process

Two negotiation processes have begun at the United Nations in 2019 on the security of cyberspace. Established working groups deal with the application of international law to cyberspace, the production of norms for responsible behavior by states, and the development of confidence-building and capacity-building measures.

a. Among the 9 principles of the Paris Call, which 3 seem to you the most fundamental for the maintaining of peace and security in cyberspace? *(Choose 3)*

Full version of the principles is available here.

☐ Protect individuals and critical infrastructures
☐ Protect the public core of the Internet

- □ Defend electoral processes
- □ Defend intellectual property
- □ Prevent the proliferation of malicious software and practices
- □ Strengthen the security of digital processes, products and services
- □ Strengthen an advanced cyber hygiene for all actors
- □ Prevent non-state actors from hacking back
- □ Promote international norms of responsible behavior

b. Which of these principles would you like to see addressed at the UN? *(Choose as many as you like)*

Full version of the principles is available here.

- □ Protect individuals and critical infrastructures
- □ Protect the public core of the Internet
- □ Defend electoral processes
- □ Defend intellectual property
- □ Prevent the proliferation of malicious software and practices
- □ Strengthen the security of digital processes, products and services
- □ Strengthen an advanced cyber hygiene for all actors
- □ Prevent non-state actors from hacking back
- □ Promote international norms of responsible behavior

c. In your opinion, are there other cybersecurity issues that should be dealt with at the UN? *(500 character limit)*

d. What level of knowledge do you think you possess about past and ongoing work at the UN on cybersecurity issues?

- □ 0 (None)
- □ 1
- □ 2 (Average)
- □ 3
- □ 4 (Very good)

7. About your organization

a. Name of your organization*

This information will not be made public.

b. Contact email*

This information will not be made public.

c. Are you a supporter of the Paris Call?*

☐ Yes
☐ No

d. You are*

☐ A government
☐ A public or local authority
☐ A company or trade association
☐ A civil society organization

** These questions are mandatory.*