Consultation des soutiens de l'Appel de Paris

Annoncée au Forum international de la cybersécurité (FIC) à Lille le 30 janvier 2020 par l'Ambassadeur pour le numérique, cette consultation vise à recueillir les préoccupations et sujets d'intérêt de la communauté de l'Appel de Paris afin de mieux les relayer sur la scène internationale.

La consultation sera ouverte jusqu'au 16 mars 2020. Une synthèse des contributions sera présentée par la France à partir du mois d'avril lors des prochains rendez-vous de la communauté de l'Appel de Paris.

Les réponses brutes seront publiées en open data sur data.gouv.fr, à l'exception des noms et courriels des organisations.

Pour plus d'informations sur l'Appel de Paris, rendez-vous sur pariscall.international.

Pour toute question, écrivez à : contact@pariscall.international

1. Prospective

a. Selon vous, quelle innovation technologique risque d'avoir des implications particulièrement déstabilisatrices dans les mois ou années à venir ? *(500 signes maximum)*

1b. Selon vous, quelle innovation technologique dispose des applications les plus prometteuses en matière de cybersécurité ? *(500 signes maximum)*

c. Avez-vous mis en place des actions particulières en réaction à ces nouvelles menaces et opportunités ?

☐ Oui
☐ Non

d. Si oui, lesquelles ? *(500 signes maximum)*

2. Droits individuels

a. Selon vous, les droits des citoyens sont-ils suffisamment protégés face aux pratiques dangereuses qui se développent dans le cyberespace (cybercriminalité, vol d'informations personnelles, manipulation de l'information, interférences électorales...) ?

☐ Oui, absolument
☐ Oui, en partie
☐ Non, pas suffisamment
☐ Non, pas du tout

b. Comment mieux les protéger ? *(500 signes maximum)*

c. Selon vous, comment garantir l'application du droit international des droits de l'Homme et du droit international humanitaire au cyberespace ?

☐ En faisant davantage confiance aux acteurs privés

☐ En ouvrant des discussions à ce sujet qui associeraient l'ensemble des acteurs du cyberespace

☐ En menant des négociations au sein des organisations internationales (ONU, OCDE, UE, etc.)

☐ En créant des outils permettant de sanctionner les acteurs qui ne respecteraient pas ces normes

☐ Autre : … (réponse libre)

d. Les fournisseurs de services et produits numériques devraient-ils avoir un devoir de diligence pour protéger leurs utilisateurs des risques en ligne (« duty of care ») ?

☐ Oui, absolument
☐ Oui, en partie
☐ Non, sans doute pas
☐ Non, pas du tout

3. Sécurisation

a. Prenez-vous des mesures particulières pour garantir la cybersécurité de vos produits et services ?

☐ Oui
☐ Non

b. Selon vous, quelles normes ou standards minimaux les entreprises qui commercialisent des produits et services numériques devraient-elles respecter ? *(500 signes maximum)*

c. Selon vous, quelles mesures pourraient être prises au niveau national ou international par les États afin de garantir la protection des infrastructures critiques civiles ? *(500 signes maximum)*

d. Pensez-vous que ces mesures devraient être obligatoires ?

☐ Oui
☐ Non

3e. De quel dispositif ou procédure disposez-vous en cas d'attaque ou d'incident cyber sur vos infrastructures ? *(500 signes maximum)*

f. Avez-vous les moyens d'informer vos autorités d'un incident cyber qui vous affecterait ?

☐ Oui
☐ Non

4. Renforcement capacitaire et coopération technique

Le renforcement capacitaire consiste à apporter un soutien au développement des capacités de cyberdéfense des entités publiques et privées à travers des programmes de formation et d'entraînement, de l'assistance technique, et des échanges de ressources et de compétences.

a. Quels sont les besoins en matière de renforcement capacitaire de votre organisation ou de votre pays ? *(500 signes maximum)*

b. Avez-vous les moyens de contribuer au renforcement capacitaire de votre écosystème, de votre pays ou d'autres pays ?

☐ Oui
☐ Non

c. Si oui, comment êtes-vous prêt à contribuer ? *(500 signes maximum)*

d. Quelle initiative de renforcement capacitaire ou coopération internationale vous a le plus marqué l'année dernière ? *(500 signes maximum)*

e. Quel est, à votre avis, le manque principal de votre organisation en matière de cybersécurité ? *(500 signes maximum)*

5. Coopération multi-acteurs

a. Collaborez-vous, à votre niveau, avec des autorités publiques, des entreprises et/ou des organisations de la société civile ?

☐ Oui
☐ Non

b. Si oui, comment ? *(500 signes maximum)*

c. Quels obstacles freinent selon vous la coopération entre États, secteur privé et société civile ? *(500 signes maximum)*

d. Quelle est, selon vous, l'enceinte multi-acteurs la plus adaptée aux discussions sur le cyberespace ? *(500 signes maximum)*

6. Les principes de l'Appel de Paris et le processus ONU

Deux processus de négociations ont débuté à l'ONU en 2019 sur la sécurité du cyberespace. Les groupes de travail établis traitent de l'application du droit international au cyberespace, de la production de normes relatives au comportement responsable des États, et du développement de mesures de confiance et de renforcement capacitaire.

a. Parmi les 9 principes de l'Appel de Paris, quels sont les 3 qui vous semblent les plus essentiels pour le maintien de la paix et de la sécurité dans le cyberespace ?

Le détail des principes est disponible ici.

Choisissez-en 3 :

- ☐ Protéger les individus et les infrastructures critiques
- ☐ Protéger le cœur public de l'internet
- ☐ Défendre les processus électoraux
- ☐ Défendre la propriété intellectuelle
- ☐ Empêcher la prolifération de pratiques informatiques et logiciels malveillants
- ☐ Accroître la sécurité des processus, produits et services numériques
- ☐ Développer une hygiène informatique avancée
- ☐ Empêcher les acteurs non étatiques de mener des cyber-ripostes
- ☐ Favoriser des normes internationales de comportement responsable

b. Parmi ces principes, quels sont ceux que vous souhaiteriez voir traiter à l'ONU ?

Le détail des principes est disponible ici.

Choisissez-en autant que vous voulez :

- ☐ Protéger les individus et les infrastructures critiques
- ☐ Protéger le cœur public de l'internet
- ☐ Défendre les processus électoraux
- ☐ Défendre la propriété intellectuelle
- ☐ Empêcher la prolifération de pratiques informatiques et logiciels malveillants
- ☐ Accroître la sécurité des processus, produits et services numériques
- ☐ Développer une hygiène informatique avancée
- ☐ Empêcher les acteurs non étatiques de mener des cyber-ripostes
- ☐ Favoriser des normes internationales de comportement responsable

c. Selon vous, d'autres sujets devraient-ils être traités à l'ONU en matière de cybersécurité ? *(500 signes maximum)*

d. Quel niveau de connaissance pensez-vous avoir concernant les travaux passés et en cours à l'ONU sur les questions de cybersécurité ?

- ☐ 0 (Aucun)
- ☐ 1
- ☐ 2 (Moyen)
- ☐ 3
- ☐ 4 (Très bon)

7. A propos de vous

a. Nom de votre organisation*

Cette information ne sera pas rendue publique.

b. Email de contact*

Cette information ne sera pas rendue publique.

c. Vous êtes soutien de l'Appel de Paris*

☐ Oui
☐ Non

d. Vous êtes*

- Un Etat
- Un organisme public ou une collectivité territoriale
- Un représentant du secteur privé
- Un représentant de la société civile

**Champs obligatoires*