APPEL DE PARIS

POUR LA CONFIANCE ET LA SÉCURITÉ
DANS LE CYBERESPACE

12 • 11 • 2018

APPEL DE PARIS
POUR LA CONFIANCE ET LA SÉCURITÉ DANS LE CYBERESPACE

12 novembre 2018

Le cyberespace joue désormais un rôle capital dans tous les aspects de notre vie ; il relève de la responsabilité d'un grand nombre d'acteurs, chacun dans son domaine propre, de le rendre plus fiable, plus sûr et plus stable.

Nous réaffirmons notre soutien à un cyberespace ouvert, sûr, stable, accessible et pacifique, devenu partie intégrante de la vie sous tous ses aspects sociaux, économiques, culturels et politiques.

Nous réaffirmons également que le droit international, dont la Charte des Nations Unies dans son intégralité, le droit international humanitaire et le droit international coutumier, s'applique à l'usage des technologies de l'information et de la communication (TIC) par les États.

Nous réaffirmons que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne et que le droit international des droits de l'Homme s'applique au cyberespace.

Nous réaffirmons que le droit international constitue, avec les normes volontaires de comportement responsable des États en temps de paix et les mesures de développement de la confiance et de renforcement des capacités élaborées dans le cadre des Nations Unies, le fondement de la paix et de la sécurité internationales dans le cyberespace.

Nous condamnons les cyberactivités malveillantes en temps de paix, notamment celles qui menacent des individus et des infrastructures critiques ou qui ont pour effet de leur causer des dommages importants, sans discernement ou systémiques, et nous accueillons avec satisfaction les appels invitant à améliorer leur protection.

Nous nous félicitons également des efforts déployés par des États et des acteurs non étatiques pour venir en aide de manière impartiale et indépendante aux victimes de l'usage malveillant des TIC, que celui-ci intervienne en période de conflit armé ou non.

Nous reconnaissons que la menace constituée par la cybercriminalité impose de redoubler d'efforts afin d'améliorer la sécurité des produits que nous utilisons, de renforcer nos défenses face aux criminels et de favoriser la coopération entre toutes les parties prenantes, tant à l'intérieur de nos frontières nationales qu'au-delà de celles-ci, et que la Convention de Budapest sur la cybercriminalité est à cet égard un outil essentiel.

Nous reconnaissons les responsabilités des principaux acteurs du secteur privé pour développer la confiance, la sécurité et la stabilité dans le cyberespace et nous encourageons les initiatives qui visent à accroître la sécurité des processus, produits et services numériques.

Nous nous félicitons de la collaboration entre les pouvoirs publics, le secteur privé et la société civile en vue d'élaborer de nouvelles normes de cybersécurité permettant aux infrastructures et aux organisations d'améliorer leurs systèmes de cyberprotection.

Nous reconnaissons que tous les acteurs peuvent apporter leur soutien à un cyberespace pacifique en encourageant la divulgation responsable et coordonnée des vulnérabilités.

Nous soulignons la nécessité de développer une vaste coopération dans le domaine du numérique et les efforts de renforcement des capacités de tous les acteurs, et nous encourageons les initiatives qui permettent d'accroître la résilience et les compétences des utilisateurs.

Nous reconnaissons la nécessité d'une approche multi-acteurs renforcée et d'efforts supplémentaires afin de réduire les risques qui pèsent sur la stabilité du cyberespace et d'établir davantage de fiabilité, de capacité et de confiance.

À cet effet, nous nous déclarons résolus à agir de concert, au sein des instances existantes et par le biais des organisations, institutions, mécanismes et processus appropriés, pour nous venir mutuellement en aide et mettre en place des actions en coopération afin, notamment :

- d'empêcher les cyberactivités malveillantes qui menacent des individus et des infrastructures critiques ou qui leur causent des dommages importants, sans discernement ou systémiques, et d'y remédier ;

- d'empêcher les activités qui portent atteinte intentionnellement et dans une large mesure à la disponibilité ou à l'intégrité du cœur public de l'internet ;

- de développer notre capacité de prévenir les interférences de la part d'acteurs étrangers destinées à déstabiliser des processus électoraux au moyen de cyberactivités malveillantes;

- d'empêcher le vol de propriété intellectuelle à l'aide des TIC, notamment des secrets industriels ou autres informations commerciales confidentielles, dans l'intention de procurer des avantages concurrentiels à des entreprises ou à un secteur commercial ;

- d'élaborer des moyens d'empêcher la prolifération d'outils malveillants et de pratiques informatiques destinés à nuire ;

- d’accroître la sécurité des processus, produits et services numériques tout au long de leur cycle de vie et d’un bout à l’autre de la chaîne d’approvisionnement ;

- de soutenir les actions visant à développer une hygiène informatique avancée pour tous les acteurs ;

- de prendre des mesures pour empêcher les acteurs non étatiques, y compris le secteur privé, de mener des actions cyber offensives en réponse à une attaque dont ils seraient victimes, pour leur propre compte ou pour celui d’autres acteurs non étatiques ;

- de favoriser une large acceptation et la mise en œuvre de normes internationales de comportement responsable ainsi que de mesures de développement de la confiance dans le cyberespace.

En vue d’assurer le suivi des progrès accomplis sur ces sujets dans le cadre des instances et mécanismes appropriés, nous convenons de nous réunir de nouveau en 2019 lors du Forum de Paris sur la paix et du Forum sur la gouvernance de l’Internet à Berlin.

[Paris, le 12 novembre 2018]