Cette traduction est disponible grâce à la contribution volontaire de Mme Afi Edoh et Mme Muriel Alapini.
L'IGF leur en est reconnaissant.

IGF 2020 Messages

CONFIANCE

Quels sont les éléments essentiels pour garantir le fonctionnement, la stabilité et la résilience de l'internet et du monde en ligne, aujourd'hui et à l'avenir, indépendamment de l'évolution constante de l'environnement et du paysage des menaces ?

Le COVID-19 bouleverse nos vies et les restrictions pour contrôler la propagation de la pandémie nous limitent dans nos activités quotidiennes les plus normales. Les solutions électroniques qui nous permettent de continuer à travailler ou à étudier à domicile nécessitent une connectivité sécurisée et stable à un Internet fiable. Un Internet fiable nécessite une infrastructure Internet bien protégée et renforcée.

Les pays qui établissent un plan d'urgence national sont mieux placés pour gérer plus efficacement les interventions en cas de catastrophe ou en temps de crise. Les stratégies d'intervention en cas de catastrophe garantissent la coordination et l'alignement à tous les niveaux de gouvernement. Les partenaires fédéraux, étatiques, locaux, tribaux et territoriaux sont importants pour développer une réponse cohérente et significative aux catastrophes nationales, y compris dans les situations où l'infrastructure n'est pas touchée, comme ce fut le cas avec la crise du COVID-19.

La pandémie COVID-19 est l'occasion d'évaluer et d'identifier les lacunes et les goulots d'étranglement dans l'infrastructure numérique, de commencer à préparer des plans d'action pour une connectivité abordable et fiable, en garantissant une bande passante suffisante à travers chaque tronçon du réseau et en étendant la connectivité à ceux qui ne sont pas encore connectés ou pas encore bien connectés.

La nature transfrontalière mondiale de l'Internet remet en question la notion de souveraineté. La collaboration transfrontalière devient la nouvelle norme. L'Internet a été explicitement conçu pour encourager l'interconnectivité mondiale et inconscient des frontières internationales. C'était et continue d'être un objectif central de connecter autant de personnes, d'appareils et de réseaux que possible dans un réseau mondial de réseaux.

Une grande partie de la main-d'œuvre travaille actuellement à domicile, mesure abrupte et imprévue pour lutter contre le covid. Les employés se connectent à leur réseau domestique au lieu du réseau bien protégé de l'entreprise, ce qui crée de nouveaux risques de sécurité et augmente les risques existants. Cela nécessite des efforts particuliers pour renforcer leur préparation à la cybersécurité. Un renforcement des capacités, une éducation et une formation améliorées et continues contribuent à la création d'une culture de la cybersécurité.

La croissance rapide des appareils IoT pour la maison soulève des inquiétudes quant aux implications en matière de sécurité et de confidentialité pour leurs utilisateurs. Les directives,

publications et recommandations doivent être publiées dans un format convivial et utiliser un langage avec moins de jargon et de terminologie technique.

Que peuvent faire les parties prenantes, allant des modèles gouvernementaux aux initiatives concrètes pour créer un Internet qui soit un espace en ligne sûr et sécurisé pour tous, soutenu par le respect des droits de l'homme et la protection de nos enfants, minimiser les risques et les préjudices potentiels pour les utilisateurs, et éradiquer la discrimination ?

Les gouvernements doivent accélérer leur transformation numérique et développer les canaux en ligne qui sont essentiels pour communiquer et garantir que les citoyens aient accès à des informations importantes en temps de crise.

La vérification des faits nécessite une coopération locale et internationale, ainsi que les compétences et les ressources nécessaires pour faire face à une avalanche d'informations, à une variété de sources et à la diversité des langues. Une vérification adéquate des faits est entravée par la pression politique et les menaces financières et juridiques.

La vérification des faits restera inefficace s'il n'y a aucune confiance dans les vérificateurs de faits. La participation du gouvernement aux initiatives de vérification des faits peut renforcer ou miner cette confiance.

Les robots sont des outils importants, innovants et convaincants pour automatiser les tâches de lutte contre la désinformation. Les ressources économisées peuvent être concentrées sur des tâches nécessitant une surveillance humaine. La transparence est essentielle pour éviter que les robots ne limitent les droits essentiels, tels que la liberté d'expression et l'accès à l'information. La transparence comporte plusieurs niveaux : le fonctionnement interne de l'outil, les critères utilisés et leurs effets, mais aussi les personnes qui déploient l'outil et leur objectif.
La production et la diffusion de contenus illicites et préjudiciables sont deux choses différentes qui nécessitent toutes deux un haut niveau de vigilance. L'amplification algorithmique risque d'automatiser la diffusion du mauvais.

L'éducation aux médias et un dialogue public qui favorise le respect des faits et de la science contribuent à lutter contre la désinformation en ligne, tout comme le rétablissement de la confiance dans le journalisme et une plus grande transparence dans la manière dont les entreprises de médias sociaux (et leurs algorithmes) traitent l'information. La formation des compétences des jeunes à la pensée critique devrait commencer dès le plus jeune âge.

Les parties prenantes, les chercheurs et les développeurs devraient s'associer pour développer des outils techniques et appliquer l'IA et l'apprentissage automatique, pour reconnaître et lutter contre les discours de haine en ligne et la diffusion de désinformation et de fausses informations en ligne.

Le débat et la sensibilisation sur la lutte contre la désinformation et les discours de haine ne peuvent être reportés et doivent être renforcés. Lutter contre les fausses nouvelles est une responsabilité partagée et individuelle. Les utilisateurs doivent être vigilants et se tenir responsables de ce qu'ils partagent en ligne, et ne pas se cacher derrière la technologie ou transférer toute responsabilité sur les plateformes de médias sociaux.

La technologie résout et crée des problèmes. Le monde numérique regorge d'opportunités pour les enfants d'apprendre, de jouer, de développer leur potentiel et de protéger leurs droits, mais il est également plein de dangers qui peuvent nuire ou porter atteinte à leurs droits. Les universitaires et les spécialistes des sciences du comportement et de la santé mentale doivent amplifier leurs recherches sur l'impact positif et négatif des activités en ligne, y compris l'influence du jeu sur le développement et le bien-être des enfants, afin que leurs conclusions puissent guider l'élaboration des politiques et les pratiques de l'industrie. Les enfants, les parents, les éducateurs, l'industrie et les décideurs doivent participer à l'élaboration d'une approche équilibrée qui gère les risques tout en maximisant les opportunités,

---

Comment créer un environnement qui favorise un dialogue avec les parties prenantes, où la méfiance, la peur et l'incompréhension font place à la confiance mutuelle et à la reconnaissance du rôle de chacun, et où les acteurs collaborent pour trouver des réponses globales aux défis de sécurité et de sûreté de notre monde en ligne?

Les entreprises, le gouvernement, la communauté technique et les organisations multilatérales devraient collaborer pour développer des réponses adéquates aux défis aux niveaux national, international et mondial, résultant de crises telles que le COVID-19.

La pandémie a montré comment la technologie et les médias sociaux peuvent être une bouée de sauvetage pour rester en contact avec les amis et la famille, pour poursuivre l'activité économique et pour recueillir des informations. L'IGF devrait faciliter le dialogue sur la responsabilité partagée et les actions des parties prenantes, y compris la réglementation le cas échéant, pour s'assurer que les utilisateurs sont en mesure d'interagir et de communiquer dans un environnement en ligne sécurisé à tout moment.

Les initiatives visant à inclure les points de vue et les perspectives multipartites dans les dialogues de l'ONU sur la cybersécurité sont bien accueillies, mais des efforts supplémentaires sont nécessaires pour rendre les dialogues et les opportunités de fournir des contributions plus visibles, y compris le soutien et le renforcement des capacités pour impliquer les nations et les communautés à travers la fracture numérique. Les initiatives de renforcement des capacités des gouvernements des pays en développement devraient les préparer à participer aux discussions et aux initiatives internationales et mondiales sur les cyber-normes et refléter la perspective et les intérêts des communautés locales et des nations.

La protection des enfants en ligne, y compris dans les jeux en ligne, est un domaine politique émergent et en évolution rapide, et un élément indispensable de la gouvernance mondiale de l'internet. Toutes les parties prenantes doivent assumer leurs responsabilités, renforcer la coopération et coordonner une combinaison adéquate de mesures publiques, privées, juridiques et volontaires aux niveaux national et international. Comme pratique courante, les parties prenantes devraient consulter les enfants sur les questions qui ont un impact sur leur vie, y compris leur vie en ligne.

Les différences entre les régions (géographie, économie, politique, culture) peuvent être importantes et font que les meilleures pratiques ne sont pas directement applicables à chaque région. L'implication de multiples partenaires est bénéfique pour un renforcement durable des cyber capacités. La coopération et le partage de bonnes pratiques entre des régions et des pays plus et moins avancés sont aussi importants que le partage interrégional entre des régions partenaires également avancées. La confiance entre les parties prenantes au sein des régions et entre elles favorisera l'échange de bonnes pratiques. La confiance, la légitimité et l'implication de toutes les parties prenantes concernées sont les piliers de tout projet bénéfique de renforcement des capacités.

Les mécanismes de confiance dans le cyberespace, fondés sur les principes de responsabilité, de transparence, de respect, de consultation mutuelle et de compréhension mutuelle, devraient établir une coopération ouverte entre les parties, y compris les gouvernements, les organisations internationales, les entreprises, les communautés techniques, les instituts de recherche scientifique et les particuliers, et explorer un large éventail d'outils tels que les lois et règlements, les capacités informatiques, la responsabilité sociale, l'éthique, la supervision et l'autodiscipline, ainsi que les normes et standards.

Garantir la sécurité et la confidentialité est essentiel pour que l'écosystème IoT prospère, tandis que les lignes directrices et le processus de prise de décision associé doivent impliquer diverses parties prenantes, y compris la société civile et les décideurs. Il y a un manque de connaissances sur les risques associés à l'IoT et la nécessité d'actions de renforcement des capacités pour présenter les meilleures pratiques et prévenir les menaces. L'IGF est bien placé pour être intermédiaire d'un tel processus.