Manifeste Multipartite

Donner la priorité aux intérêts des personnes dans la prochaine convention des Nations Unies sur la cybercriminalité

Le monde assiste aujourd'hui à une évolution rapide des cybermenaces : les attaques sont de plus en plus nombreuses, graves et complexes et compromettent ainsi notre sécurité collective. Les cybercrimes engendrent de nouveaux risques et défis pour la sécurité, la dignité et l'équité humaines – des défis transnationaux qu'aucun acteur ne peut relever seul. Une approche multipartite est essentielle pour lutter contre l'utilisation malveillante des technologies de l'information et de la communication (TIC) et pour protéger et renforcer les utilisateurs de ces technologies.

Nous suivons de près le processus de négociation de la nouvelle convention internationale sur la lutte contre l'utilisation des TIC à des fins criminelles, telle que prévue dans la résolution 74/247 de l'Assemblée générale des Nations Unies. Compte tenu des instruments qui existent déjà aux niveaux régional et international pour combattre la cybercriminalité, nous exhortons la communauté internationale à éviter les doubles emplois et à s'attacher en particulier à renforcer la mise en œuvre effective et le respect des cadres établis.

Dans ce contexte, eu égard au vote à la majorité à l'Assemblée générale des Nations Unies, nous énonçons un ensemble de principes qui, selon nous, devraient être appliqués par les acteurs participant au processus de négociation de ce nouvel instrument. Ces principes sous-tendent les droits et les libertés indispensables pour réaliser un cyberespace libre, ouvert, sûr et pacifique et pour renforcer le respect du droit dans le cyberespace.

Protéger les victimes

Le nouvel instrument international pour lutter contre la cybercriminalité doit viser avant tout à protéger les cibles et les victimes des cybercrimes, et à proposer des voies de recours effectives ainsi qu'un ensemble de mesures adéquates pour préserver les droits de l'homme. De nombreux gouvernements ont longtemps abusé des mesures de lutte contre la cybercriminalité et se sont servis de la législation en la matière pour étendre le contrôle de l'État et ériger en infraction la publication et la diffusion d'informations gênantes, et pour imposer une surveillance généralisée et restreindre la vie privée de leurs citoyens au nom de la lutte contre le terrorisme. Le nouvel instrument doit garantir la protection de la sécurité, de l'équité et de la dignité humaines, conformément aux obligations des États à l'égard de leurs citoyens. Pour protéger les victimes des cybercrimes tout en empêchant que des comportements qui ne sont autres que l'exercice des libertés fondamentales et des droits de l'homme ne soient érigés en infractions, le nouvel instrument juridique doit garantir que la définition d'un comportement comme « criminel » se base sur des critères à la fois souples et restreints.

Lutter efficacement contre la cybercriminalité en renforçant la coopération internationale

Le but de la nouvelle convention des Nations Unies sur la cybercriminalité doit être avant tout de lutter contre les cybercrimes tout en donnant la priorité aux intérêts des personnes. La convention doit reposer principalement sur la défense des droits de l'homme et sur la mise en œuvre efficace de solutions existantes pour renforcer la coopération internationale entre les autorités judiciaires et les organes chargés de faire respecter la loi dans le cadre d'un contrôle transparent. Elle doit mettre en avant la nécessité de renforcer la collaboration internationale et intersectorielle et d'harmoniser les cadres existants pour enquêter sur les cybercrimes et en poursuivre les auteurs.

Maintenir intactes les obligations internationales existantes

La nouvelle convention sur la cybercriminalité ne doit pas permettre aux États de réduire les obligations qui leur incombent en vertu du droit international et en particulier des instruments relatifs aux droits de l'homme. Dans cet esprit, la nouvelle convention ne doit pas remplacer, mais compléter ou rendre plus percutantes les obligations que les États ont contractées les uns envers les autres. Elle doit renforcer les obligations imposées par le droit international et mettre en lumière l'impact positif de ces obligations.

Mettre l'accent sur les mécanismes de responsabilisation

La nouvelle convention doit mettre l'accent sur la responsabilisation basée sur des éléments de preuve, afin de permettre aux victimes de cybercrimes d'avoir accès à des recours et à une réparation. Les États doivent réduire la marge de manœuvre des criminels non seulement en mettant en œuvre les cadres juridiques internationaux convenus et en collaborant pour poursuivre les auteurs des crimes, mais aussi en encourageant l'établissement de partenariats public-privé pour lutter contre la cybercriminalité. Lorsque les responsables sont amenés à rendre compte de leurs actes, c'est l'impact de la cybercriminalité sur l'ensemble de la société qui doit être pris en compte.

Faire en sorte que la convention soit intemporelle

Étant entendu que la cybercriminalité évolue rapidement et que les définitions y relatives devront probablement être adaptées en conséquence, le champ d'application de la convention doit être défini sans référence aucune à des technologies particulières.

Préserver l'ouverture d'Internet

Les pays sont de plus en plus nombreux à vouloir fractionner Internet en différentes sphères d'influence et de contrôle nationales. La nouvelle convention sur la cybercriminalité ne doit pas fournir aux régimes non démocratiques un motif ou un prétexte pour compromettre l'ouverture d'Internet en fermant leurs frontières numériques au reste du monde au nom de la prévention de la cybercriminalité. Dans cette optique, la nouvelle convention doit prévoir que les règles de compétence puissent être adaptées de manière à tenir compte du caractère mondial d'Internet et de la libre circulation de l'information.

ÉTABLIR DES PROCESSUS APPROPRIÉS

Appliquer en tout temps une approche multipartite

Toutes les parties prenantes doivent être consultées et impliquées efficacement à tous les stades du processus de négociation. Les intérêts de la société civile, des entreprises, des universitaires, des chercheurs, des experts techniques et des institutions scientifiques et de recherche doivent être pris en compte. Pour assurer une représentation équilibrée des intérêts, des experts dans les domaines de la cybersécurité, de la gouvernance d'Internet, du droit international et des droits de l'homme, entre autres, doivent s'asseoir à la table des négociations.

Promouvoir la transparence

Les négociations sur la nouvelle convention doivent être aussi transparentes que possible. Les organisations, les personnes et les États dont les intérêts et les droits peuvent être mis en cause doivent avoir l'opportunité de s'exprimer et d'être entendus. Le calendrier des négociations, la liste des participants et tous les projets de textes, par exemple, doivent être rendus publics.

Donner une définition précise du cybercrime

En définissant le cybercrime d'une manière trop générale, on crée le risque que des activités très diverses et dépassant largement le cadre du cybercrime soient érigées en infractions. Les négociateurs doivent veiller à formuler une définition précise des crimes qu'ils veulent sanctionner, afin d'éviter que la convention soit utilisée pour justifier des mesures de répression contre des opposants politiques, des défenseurs des droits de l'homme ou la société civile.

Adopter une approche axée sur la recherche d'un consensus

La nouvelle convention sur la cybercriminalité doit être le fruit d'un consensus. Ses dispositions doivent être convenues d'un commun accord par différents pays et régions, et basées sur des consultations intenses associant des groupes d'experts et les parties prenantes concernées.

Signatories

Organisations :

7amleh
The Arab Center for Social Media Advancement

Africa Freedom of Information Centre

Asia Internet Coalition

Atlassian

The Azure Forum for Contemporary Security Strategy

Big Cloud Consultants

Castroalonso LET

Center for Democracy and Technology

The Centre for Internet and Society

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Cyber Governance and Policy Center
at the University of Oklahoma

Cyber Project at the Belfer Center

Cyber Threat Alliance

CyberPeace Foundation

CyberPeace Institute

Cybersecurity Advisors Network (CyAN)

Cybersecurity Coalition

Cybersecurity Tech Accord

CyberSolace Limited

Cyberspace Cooperation Initiative
at Observer Research Foundation America

Derechos Digitales

Digital Peace Now

Diplowomen

Dragos

ESET

FIRST

Fundación Karisma

F-Secure

GitHub

HackerOne

Hitachi

Identity Valley

Institute for Security and Technology

International Service for Human Rights (ISHR)

Internet Sans Frontieres

Jokkolabs Banjul

Media Matters for Democracy

Microsoft

Myanmar Center for Responsible Business

Luta Security

NetApp

Ostrom Workshop Program on Cybersecurity and Internet Governance
Indiana University

Packet Clearing House

Paradigm Initiative

R Street's Cybersecurity & Emerging Threats

Ranking Digital Rights

Rapid7

Redes Ayuda

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa

SAP

Silverado Policy Accelerator

Stiftung Neue Verantwortung (SNV)

Swiss Digital Initiative

Tech Policy Design Centre
Australian National University

USM Technology

Wisekey

World Wide Web Foundation
via The Contract for the Web

Personnes signant à titre personnel :

Luca Belli
Director of the Center for Technology and Society at Fundação Getulio Vargas

Vinton G. Cerf
Vice president and Chief Internet Evangelist, Google

Fergus Hanson
Director, International Cyber Policy Centre

Katie Moussouris
Founder and CEO, Luta Security

Marc Rogers
Founder, CTI League

Anne-Marie Slaughter
Bert G. Kerstetter '66 University Professor Emerita of Politics and International Affairs, Princeton University

Cris Thomas
Security Researcher, Space Rogue

Christopher Painter
President of The Global Forum on Cyber Expertise Foundation, signing in personal capacity.

Eneken Tikk
Cyber Policy Institute

Jokkolabs Banju
Gambia