GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

FAIRE PROGRESSER LA CYBERSTABILITÉ

RAPPORT FINAL
NOVEMBRE 2019

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOUVOIR LA STABILITÉ DANS LE CYBERESPACE AFIN DE BÂTIR UN ENVIRONNEMENT DE PAIX ET DE PROSPÉRITÉ

La Commission mondiale sur la stabilité du cyberespace (en anglais Global Commission on the Stability of Cyberspace ou GCSC) développe des propositions de normes et de politiques afin d'améliorer la sécurité et la stabilité sur le plan international et d'encourager le comportement responsable des acteurs étatiques et non-étatiques dans le cyberespace.

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

FAIRE PROGRESSER LA CYBERSTABILITÉ

RAPPORT FINAL
NOVEMBRE 2019

***The Hague* Centre for Strategic Studies**
Lange Voorhout 1
2514 EA La Haye
info@hcss.nl
www.hcss.nl

EastWest Institute
New York | Bruxelles
Moscou | San Francisco
cyber@eastwest.ngo
www.eastwest.ngo

PRÉSIDENTS

Michael Chertoff États-Unis
Latha Reddy Inde
Marina Kaljurand Estonie *(ancienne présidente)*

COMMISSAIRES

Abdul-Hakeem Ajijola Nigeria
Virgilio Almeida Brésil
Isaac Ben-Israel Israël
Scott Charney États-Unis
Frédérick Douzet France
Anriette Esterhuysen Afrique du Sud
Jane Holl Lute États-Unis
Nigel Inkster Royaume-Uni
Khoo Boon Hui Singapour
Wolfgang Kleinwächter Allemagne
Olaf Kolkman Pays-Bas
Lee Xiaodong Chine
James Lewis États-Unis
Jeff Moss États-Unis
Elina Noor Malaisie
Joseph S. Nye, Jr. États-Unis
Christopher Painter États-Unis
Uri Rosenthal Pays-Bas
Ilya Sachkov Russie
Samir Saran Inde
Marietje Schaake Pays-Bas
Motohiro Tsuchiya Japon
Bill Woodcock États-Unis
Zhang Li Chine
Jonathan Zittrain États-Unis

REPRÉSENTANTS ET CONSEILLERS SPÉCIAUX

Carl Bildt Suède
Vint Cerf États-Unis
Sorin Ducaru Roumanie
Martha Finnemore États-Unis

ADMINISTRATEURS

Alexander Klimburg Autriche
Bruce W. McConnell États-Unis

PRÉSIDENTS DES GROUPES CONSULTATIFS DE RECHERCHE

Sean Kanuck États-Unis
Koichiro Komiyama Japon
Marília Maciel Brésil
Liis Vihul Estonie
Hugo Zylberberg France

SECRÉTARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTENAIRES

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

SPONSORS

Département fédéral des Affaires étrangères de Suisse

GLOBSEC

Ministère des Affaires étrangères d'Estonie

Ministère des Affaires internes et des communications du Japon

SOUTIENS

Commission de l'Union africaine

Black Hat USA

DEF CON

Délégation de l'Union européenne des Nations Unies à Genève

Forum Mondial sur la Cyber Expertise

Google

Municipalité de La Haye

Packet Clearing House

Université de Tel Aviv

Institut des Nations Unies pour la recherche sur le désarmement

SOMMAIRE

LETTRE DE LA PRÉSIDENCE

Le cyberespace représente l'une des plus grandes inventions de l'humanité, car il remodèle les relations personnelles, sociales, commerciales et politiques. Malheureusement, en raison des attaques sur et via ce cyberespace, il devient urgent et nécessaire d'agir pour assurer sa stabilité. Le concept de stabilité du cyberespace, comme sa cousine la stabilité internationale, requiert une vision partagée, où toutes les parties reconnaissent que les désaccords et les changements géopolitiques qui affectent le cyberespace doivent être gérés dans une paix relative et que la stabilité du cyberespace doit être assurée.

La Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace ou GCSC) a commencé ses travaux avec la conviction qu'une question traditionnellement réservée aux États, la sécurité et la paix internationales, ne pouvait plus être traitée sans impliquer d'autres acteurs. Le cyberespace est un environnement multipartite : ceux qui construisent et gèrent le cyberespace, et ceux qui répondent aux attaques sur et via celui-ci, peuvent être des acteurs non-étatiques autant que des acteurs officiels issus des gouvernements. Nos commissaires ont été choisis afin de refléter cette caractéristique. Outre d'anciens hauts fonctionnaires de gouvernements ayant une expérience des questions de sécurité internationale, nous comptons dans nos rangs des chefs de file dans les domaines de la gouvernance de l'Internet, des droits de l'homme et du développement, de la technologie et de l'industrie. Ensemble, nos 28 commissaires originaires de 16 pays différents disposent d'une vaste expérience et d'un large éventail de points de vue. Ils ont été assistés par les commentaires du grand public en réponse à l'action de sensibilisation de la Commission.

Le rapport final de la Commission est le fruit de trois ans d'un travail acharné. Nous remercions chaleureusement tous ceux et celles qui ont rendu cela possible : nos commissaires, conseillers et chercheurs (dont de nombreux bénévoles), nos soutiens financiers et notre conseil de direction. Enfin, notre reconnaissance va au Secrétariat, qui a non seulement géré le processus avec beaucoup de compétence, mais a également joué un rôle clé dans la création de la Commission en tant qu'initiative de la société civile.

Tout au long de ses travaux, la Commission est restée consciente des autres initiatives, passées et actuelles, dans le domaine du cyberespace. Notre rapport, *Faire progresser la cyberstabilité (Advancing Cyberstability)*, vient compléter et renforcer ces travaux parallèles en fournissant de nouvelles idées pour faire progresser la stabilité du cyberespace.

Michael Chertoff
Co-Président
Global Commission on the Stability of Cyberspace

Latha Reddy
Co-Présidente
Global Commission on the Stability of Cyberspace

RÉSUMÉ ANALYTIQUE

Nous venons de terminer une période de vingt-cinq ans de stabilité stratégique et de paix relative parmi les puissances majeures. Les conflits entre les États ont pris de nouvelles formes, et les cyberactivités jouent un rôle fondamental dans cet environnement nouveau et volatile. Au cours des dix dernières années, le nombre et la sophistication des cyberattaques par des acteurs étatiques et non-étatiques ont augmenté, ce qui menace la stabilité du cyberespace. Pour le dire plus simplement, les personnes et les organisations ne peuvent plus avoir entièrement confiance en leur capacité à utiliser le cyberespace en toute sécurité, ni être assurées de la disponibilité et de l'intégrité des services et des informations.

Dans ce contexte, la Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace ou GCSC) a été convoquée pour formuler des recommandations visant à faire progresser la cyberstabilité. Nous avons commencé par identifier sept éléments afin de définir un Cadre pour la cyberstabilité. Ce cadre comprend : (1) un engagement multipartite ; (2) les principes de la cyberstabilité ; (3) le développement et la mise en œuvre de normes facultatives ; (4) le respect du droit international ; (5) des mesures visant à renforcer la confiance ; (6) des mesures visant à renforcer les capacités ; et (7) la promulgation ouverte et l'utilisation généralisée de normes techniques afin de garantir la résilience du cyberespace. Après avoir défini ce cadre, la Commission a exploré en détails trois de ces éléments : l'engagement multipartite, les principes et les normes.

L'engagement multipartite est prévu dans de nombreux accords internationaux, mais reste controversé. Certains continuent de croire que la tâche d'assurer la sécurité et la stabilité internationales relève exclusivement de la responsabilité des États. Toutefois, en pratique, le champ de bataille virtuel (autrement dit le cyberespace) est conçu, déployé et géré essentiellement par des acteurs non-étatiques, et nous sommes convaincus que leur participation est nécessaire pour assurer la stabilité du cyberespace. Par ailleurs, leur participation est inévitable puisque les acteurs non-étatiques sont souvent les premiers à répondre aux cyberattaques, et à les attribuer.

La Commission a conclu que ces acteurs non-étatiques étaient non seulement des éléments essentiels pour assurer la stabilité du cyberespace, mais qu'ils devaient également être guidés par des principes et liés par des normes. Les quatre principes reflètent ce point de vue, amenant toutes les parties à se montrer responsables, faire preuve de retenue, agir et respecter les droits de l'homme :

- Responsabilité : Toute personne est responsable d'assurer la stabilité du cyberespace.
- Retenue : Aucun acteur, étatique ou non-étatique, ne devrait prendre de mesures qui nuisent à la stabilité du cyberespace.
- Nécessité d'agir : Les acteurs étatiques et non-étatiques devraient prendre des mesures raisonnables et appropriées pour assurer la stabilité du cyberespace.
- Respect des droits de l'homme : Les efforts pour assurer la stabilité du cyberespace doivent respecter les droits de l'homme et l'État de droit.

S'appuyant sur ces principes, et cherchant à compléter et non à dupliquer le travail d'autres personnes, la Commission a élaboré huit normes destinées à assurer une meilleure stabilité du cyberespace et à répondre aux préoccupations techniques ou aux lacunes des normes précédentes :

1. Les acteurs étatiques et non-étatiques ne devraient ni mener ni autoriser sciemment des activités qui portent intentionnellement et substantiellement atteinte à la disponibilité générale ou à l'intégrité du coeur public de l'Internet, et donc à la stabilité du cyberespace.
2. Les acteurs étatiques et non-étatiques ne devraient pas poursuivre, soutenir ou permettre des cyber opérations visant à perturber l'infrastructure technique essentielle aux élections, référendums ou plébiscites.
3. Les acteurs étatiques et non-étatiques ne devraient pas manipuler les produits et services en cours de développement et de production, ni permettre qu'ils soient manipulés, si cela risque de porter atteinte de manière substantielle à la stabilité du cyberespace.

4. Les acteurs étatiques et non-étatiques ne devraient pas réquisitionner les ressources TIC du grand public pour les utiliser comme botnets ou à des fins similaires.

5. Les acteurs étatiques devraient créer des cadres de procédures transparents pour évaluer s'il convient de divulguer des vulnérabilités ou des défauts dont ils ont connaissance, mais non connus du grand public, dans les systèmes et technologies de l'information, et à quel moment il convient de le faire. La présomption par défaut devrait favoriser la divulgation.

6. Les développeurs et fournisseurs de produits et services dont dépend la stabilité du cyberespace devraient (1) donner la priorité à la sécurité et à la stabilité, (2) prendre des mesures raisonnables pour s'assurer que leurs produits ou services sont exempts de vulnérabilités importantes, et (3) prendre des mesures pour atténuer en temps utile les vulnérabilités découvertes ultérieurement et être transparents quant à leur processus. Tous les acteurs ont l'obligation de partager les informations concernant les vulnérabilités afin d'aider à prévenir ou atténuer la cyberactivité malveillante.

7. Les acteurs étatiques devraient adopter des mesures appropriées, y compris des lois et des règlements, pour assurer une cyber-hygiène de base.

8. Les acteurs non-étatiques ne devraient pas s'engager dans des cyber-opérations offensives, et les acteurs étatiques devraient empêcher de telles activités et réagir si elles se produisent.

Recommandations

Reconnaissant à la fois l'importance de l'engagement multipartite et le fait que déclarer un comportement normatif ne le rend pas pour autant normatif, la Commission fait six recommandations qui se concentrent sur le renforcement du modèle multipartite, la promotion de l'adoption et de la mise en œuvre des normes, et la garantie que celles et ceux qui ne respectent pas ces normes soient tenus responsables.

La Commission recommande en particulier que :

1. Les acteurs étatiques et non-étatiques adoptent et mettent en œuvre des normes permettant d'augmenter la stabilité du cyberespace en favorisant la retenue et en encourageant l'action.

2. Les acteurs étatiques et non-étatiques, selon leurs responsabilités et leurs limites, réagissent de manière appropriée aux violations des normes, en veillant à ce que ceux et celles qui les enfreignent soient confrontés à des conséquences prévisibles et significatives.

3. Les acteurs étatiques et non-étatiques, y compris les institutions internationales, redoublent d'efforts pour former leur personnel, renforcer les capacités et les compétences, promouvoir une compréhension commune de l'importance de la stabilité du cyberespace et prendre en compte les besoins disparates des différentes parties.

4. Les acteurs étatiques et non-étatiques collectent, partagent, examinent et publient des informations relatives aux violations des normes et à l'impact de telles activités.

5. Les acteurs étatiques et non-étatiques établissent et soutiennent les communautés d'intérêt pour aider à assurer la stabilité du cyberespace.

6. Un mécanisme permanent d'engagement multipartite soit établi pour traiter les questions de stabilité ; un mécanisme dans lequel les États, le secteur privé (y compris la communauté technique) et la société civile seraient impliqués et consultés de manière adéquate.

La publication de ce rapport représente à la fois une fin et un début. La Commission a rempli son mandat. Cependant, pour les membres et les soutiens de la GCSC, ainsi que pour tous ceux et celles qui soutiennent ses objectifs, le travail nécessaire à la mise en œuvre de ces principes, normes et recommandations ne fait que commencer. Il doit commencer, car les avantages du cyberespace seront perdus si sa stabilité n'est pas assurée.

1. INTRODUCTION

L'évolution numérique et le cyberespace ont bouleversé l'existence humaine.[1] La capacité à numériser, stocker, analyser et transférer les données dans le monde entier a profondément affecté tous les secteurs de la société et a changé la manière dont nous menons les activités personnelles, professionnelles et politiques. Aujourd'hui, près de la moitié de la population mondiale a accès à Internet[2] et ce nombre augmente rapidement. Même les personnes qui ne sont pas personnellement connectées au cyberespace en ressentent les effets, puisque les entités dont elles dépendent pour leur fournir des biens et des services utilisent souvent le cyberespace pour les communications, la logistique et les finances.

Les avantages du cyberespace, et le besoin d'assurer sa stabilité, ont fait l'objet de nombreux débats, tout comme les défis qu'il pose. Le cyberespace peut notamment soutenir des objectifs à la fois nobles et ignobles. Par exemple, la connectivité globale, l'anonymat et le manque de traçabilité permettent aux individus et aux machines de se connecter à des données et des systèmes sans décliner leur identité, mais les criminels peuvent également tirer parti de ces attributs pour commettre des crimes en toute impunité. Par conséquent, les gouvernements, les entreprises et les personnes du monde entier sont confrontés à des dilemmes. Les gouvernements veulent protéger le cyberespace, fournir des services publics et encourager d'autres activités importantes (par ex. l'éducation et les services bancaires en ligne), mais ils veulent également faire progresser les intérêts de sécurité nationale, en particulier l'application des lois, les services de renseignement et les capacités militaires. Les entreprises, qui cherchent à protéger leurs clients, leur réputation et leurs bénéfices, se trouvent attaquées et enquêtent sur des activités malveillantes, et/ou sont sujettes à des demandes de renseignements de la part des gouvernements. Le grand public, que ces personnes soient ou non elles-mêmes connectées, dépend de plus en plus de la technologie numérique et l'adopte, mais est préoccupé par sa disponibilité et son intégrité. Ces dix dernières années, le nombre et la sophistication des cyberattaques ont beaucoup augmenté, y compris les attaques contre les systèmes gouvernementaux et les infrastructures critiques.[3] De ce fait, ni le statu quo ni les tendances observables ne sont encourageants.

Les cyberattaques, menées à la fois par des acteurs étatiques et non-étatiques, font apparaître la nécessité de définir un Cadre pour la cyberstabilité. Un tel cadre doit permettre de réduire le risque de perturbations importantes du cyberespace qui en compromettraient les avantages et réduiraient le bien-être des personnes, y compris leurs droits et libertés. De toute évidence, des produits et services bien conçus et bien construits, et bien gérés par des professionnels de l'informatique et des utilisateurs d'ordinateurs, permettront d'augmenter la sécurité et la stabilité ; tout comme des produits et services mal conçus ou négligés, ou des pratiques opérationnelles médiocres ou nonchalantes, les compromettront. Cependant, un meilleur développement

1 Le terme « cyberespace » a été défini de diverses manières. https://en.wikipedia.org/wiki/Cyberspace. Le dictionnaire le définit comme « un système électronique qui permet aux utilisateurs d'ordinateurs du monde entier de communiquer entre eux ou d'accéder à des informations pour quelque fin que ce soit. » https://dictionary.cambridge.org/us/dic-tionary/english/cyberspace. Selon le Royaume-Uni, « le cyberespace est le terme utilisé pour décrire le support électronique des réseaux numériques utilisé pour stocker, modifier et communiquer des informations. Il inclut l'Internet, mais aussi d'autres systèmes d'informations qui soutiennent les entreprises, les infrastructures et les services ». https://www.cpni.gov.uk/cyber. En tant que tel, il est sans doute plus large que l'Internet, qui est décrit en termes populaires comme un « système mondial de réseaux informatiques interconnectés qui utilise la suite de protocoles Internet (TCP/IP) pour relier des appareils dans le monde entier ». Voir https://en.wikipedia.org/wiki/Internet. Voir également Union internationale des télécommunications (ITU), « Defining the Internet », document de travail (mai 2013), https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx.

2 « Internet Usage Statistics », Internet World Stats, dernière modification le 4 octobre 2019, https://internetworldstats.com/stats.htm.

3 Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents Since 2006*, https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf; Louis Marinos et Marco Lourenço, ed., *ENISA Threat Landscape Report 2018*, ENISA (janvier 2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018; Abhishek Agrawal et al., *Microsoft Security Intelligence Report*, Vol. 24 (décembre 2018), https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original; Assemblée générale des Nations Unies, *Progrès de l'informatique et des télécommunications et sécurité internationale. Rapport du Secrétaire général*, 24 juin 2019 https://undocs.org/fr/A/74/120.

et une meilleure exploitation ne suffiront pas, surtout si les acteurs étatiques et non-étatiques considèrent le cyberespace comme un champ de bataille où l'on peut obtenir un avantage politique, militaire ou économique. Un agresseur persistant peut mettre en échec les mesures de sécurité, ce qui donne lieu à l'adage « l'attaque bat la défense sur Internet » et crée l'instabilité.[4] Il est donc important de se concentrer non seulement sur la technologie mais aussi sur les comportements : comment encourager tous les acteurs à se comporter de manière responsable afin d'améliorer (et non menacer) la stabilité du cyberespace ?

Pour répondre à cette question, de nombreuses entités gouvernementales et non gouvernementales ont soutenu la création de la Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace ou GCSC),[5] notant que :

> Nous venons de terminer une période de vingt-cinq ans de stabilité stratégique et de paix relative parmi les puissances majeures. Les conflits entre États vont prendre de nouvelles formes, et les cyberactivités sont susceptibles de jouer un rôle prépondérant dans cet environnement nouveau et volatile, augmentant ainsi le risque de compromettre l'utilisation pacifique du cyberespace pour faciliter la croissance économique et l'expansion des libertés individuelles.
>
> Afin de contrer ces développements négatifs, la Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace) développera des propositions de normes et de politiques afin d'améliorer la sécurité et la stabilité sur le plan international et d'encourager le comportement responsable des acteurs étatiques et non-étatiques dans le cyberespace. La GCSC fait appel à l'ensemble des parties prenantes pour développer une compréhension commune, et ses travaux veulent faire progresser la cyberstabilité en soutenant l'échange d'informations et le renforcement des capacités, la recherche fondamentale et la défense des intérêts de chacun.[6]

La Commission est elle-même multipartite et internationale puisqu'elle est constituée de personnes d'origines et de compétences diverses. Certains commissaires ont servi leur gouvernement et étaient engagés dans des négociations bilatérales et multilatérales sur des questions liées au cyberespace, tandis que d'autres ont une expérience dans la construction, la maintenance et la protection de l'Internet. D'autres encore représentent la société civile.

Le travail de la Commission n'est pas le seul ni le premier dans son genre. La GCSC, reconnaissant que de nombreuses autres institutions et processus (passés et présents) partagent son intérêt pour la stabilité du cyberespace, a cherché à ne pas dupliquer le travail effectué par ces autres entités. Au contraire, la GCSC tente plutôt de s'appuyer sur ces autres processus multipartites et gouvernementaux et d'influencer les travaux futurs. Ces processus incluent les travaux fondateurs et en cours du Groupe d'experts gouvernementaux des Nations Unies (GEG de l'ONU),[7] les travaux du Groupe de travail à composition non

4 Voir, par exemple, P.W. Singer et Allan Friedman, « The Cult of the Cyber Offensive », *Foreign Policy* (15 janvier 2014), https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/; World Economic Forum (WEF), *The Global Risks Report 2019*, (2019), http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

5 Pour en savoir plus sur la GCSC, voir Annexe C : Histoire, objectifs et processus de la GCSC.

6 Global Commission on the Stability of Cyberspace, https://cyberstability.org/.

7 Dans une importante résolution de 2015, l'Assemblée générale des Nations Unies a confirmé à l'unanimité la conclusion du GEG de l'ONU Voir la résolution de l'Assemblée générale 70/237, *Résolution adoptée par l'Assemblée générale le 23 décembre 2015 [sur le rapport de la Première Commission (A/70/455)]*, https://undocs.org/fr/A/%20RES/70/237. Ainsi, le droit international et, en particulier, la Charte des Nations Unies établissent un cadre exclusif pour répondre au niveau international aux actes hostiles qui s'applique également aux cyber-opérations. Notre travail s'appuie sur l'accord de tous les États lors de l'Assemblée générale des Nations Unies de 2015, d'être guidé par les normes de comportement responsable afin d'accroître la stabilité et la sécurité dans l'utilisation des TIC et de respecter les engagements pris en vertu du droit international en matière de diligence et de coopération.

limitée des Nations Unies (GTCNL), ainsi que les efforts du Forum mondial sur la Cyber Expertise (GFCE),[8] le Sommet mondial sur la société de l'information (SMSI), la Commission mondiale sur la gouvernance de l'Internet (la Commission Bildt), le Forum sur la gouvernance de l'Internet (IGF), la Conférence mondiale sur le cyberespace (Global Conference on CyberSpace/ London Process), la NETmundial Initiative, l'Organisation pour la sécurité et la coopération en Europe (OSCE), la Commission de l'Union africaine (AUC), la Charter of Trust, les Cybersecurity Tech Accord, le programme de La Haye pour les cyber normes, l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), l'Appel de Paris pour la confiance et la sécurité dans le cyberespace (« Appel de Paris »), et le Groupe de haut niveau sur la coopération numérique créé par le Secrétaire général des Nations Unies. Les travaux de la Commission ont également été éclairés par des recherches commandées et des demandes issues de commentaires du grand public.

Certains des efforts énumérés se sont concentrés, en partie, sur la stabilité du cyberespace, et il est apparu que la stabilité et la gouvernance du cyberespace sont inextricablement liées, ce qui peut être source de préoccupation. En effet, autrement dit, en l'absence d'un modèle de gouvernance solide, la société ne dispose pas des interactions et des processus décisionnels nécessaires pour assurer la stabilité. Par exemple, la Commission Bildt a proposé un pacte social multipartite pour le respect de la vie privée et la sécurité numérique « entre les citoyens et leurs représentants élus, le pouvoir judiciaire, les forces de l'ordre et les services de renseignement, les entreprises, la société civile et la communauté technique de l'Internet, dans le but de restaurer la confiance et de renforcer la foi dans l'Internet ».[9]

Nous saluons ces efforts visant à élaborer des principes, des règles et des normes à appliquer au comportement de chacun dans ce nouveau domaine turbulent qu'est le cyberespace et nous pensons qu'un cadre global est nécessaire pour accroître la stabilité du cyberespace. L'histoire montre que les sociétés et les gouvernements peuvent, dans certains cas, avoir besoin de décennies pour mettre en place des structures de gouvernance internationale formelles et étendues pour les nouvelles technologies qui causent des perturbations importantes.[10] L'émergence du cyberespace, en tant que dimension cruciale de l'interdépendance économique, sociale et sécuritaire mondiale, ne date que de la fin des années 1990, lorsque l'utilisation du « World Wide Web » a commencé à se généraliser. Les processus évolutifs de gouvernance se trouvent aujourd'hui à un stade précoce où coexistent des domaines de cohérence et d'incohérence normatives.[11] Par exemple, si les normes et les institutions liées au système des noms de domaine sont bien développées, il existe des désaccords majeurs entre les États et entre les entreprises en ce qui concerne la réglementation du contenu. Parfois, les acteurs étatiques et non-étatiques appliquent des normes provenant d'autres régimes, tels que la propriété intellectuelle et les échanges commerciaux et, de plus en plus, les entreprises privées établissent elles-mêmes des normes.[12] L'objectif de notre Commission n'est pas de régler ces différentes questions de gouvernance, mais de les inscrire dans un cadre général pour assurer la stabilité du cyberespace.

Nous notons également que celles et ceux qui sont concernés par la stabilité du cyberespace se sont efforcés de suivre ceux qui cherchent à la mettre à mal, ainsi que de suivre le rythme des développements technologiques et de l'évolution des conflits géopolitiques. Une partie du défi est que le cyberespace a transformé la manière dont les acteurs poursuivent leurs objectifs politiques et militaires. Avec de faibles barrières à l'entrée, il est moins difficile de devenir une cyberpuissance qu'une puissance militaire traditionnelle. De plus, avec les nouvelles technologies dans leur manche, certains hésitent à adopter des contraintes, surtout si celles-ci ne sont pas largement respectées. Il faut un Cadre global pour la cyberstabilité pour la communauté internationale, un cadre qui favorise la stabilité du cyberespace tout en restant utile à mesure que le rythme de l'évolution technologique continue de s'accélérer. Nous commençons donc par définir l'objectif principal : protéger la stabilité du cyberespace.

8 Le GFCE a été particulièrement actif dans le domaine du renforcement des capacités. Voir par exemple « Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building », Forum mondial sur la Cyber Expertise (24 novembre 2017), https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

9 Commission globale sur la gouvernance de l'Internet, *One Internet* (2016), p. IX, https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf. « Nous appelons les gouvernements, les entreprises privées, la société civile, la communauté technique et chaque individu à créer ensemble un nouveau contrat social pour l'ère numérique ».

10 L'exemple le plus pertinent d'une structure de gouvernance de ce type concerne peut-être les armes nucléaires, dont la mise en place a demandé beaucoup de temps et d'efforts. Aujourd'hui, 60 ans après le Traité sur la non-prolifération des armes nucléaires, la gouvernance des armes nucléaires continue d'être un problème de sécurité.

11 Cette première étape a été appelée « complexe de régime ». Voir Joseph Nye, « The Regime Complex for Managing Complex Global Cyber Activities », Commission globale sur la gouvernance de l'Internet, No. 1 (mai 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

12 Voir par exemple les normes développées par ISOC et Microsoft : « Mutually Agreed Norms for Routing Security (MANRS) », Internet Society (2014), https://www.manrs.org/; Angela McKay et al., *International Cybersecurity Norms Reducing Conflict in an Internet-dependent World*, Microsoft (décembre 2014), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA; et Scott Charney et al., *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, Microsoft (juin 2016), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

2. QU'ENTEND-ON PAR STABILITÉ DU CYBERESPACE ?

DÉFINITION :

La stabilité du cyberespace signifie que chacun peut avoir une confiance raisonnable dans sa capacité à utiliser le cyberespace en toute sécurité, où la disponibilité et l'intégrité des informations et des services fournis dans et par le cyberespace sont généralement assurées, où le changement est géré dans une paix relative, et où les tensions sont résolues sans escalade.

Si la définition de la Commission s'appuie sur la définition standard de la « stabilité »[13], elle est plus nuancée à deux égards. Premièrement, elle fait référence à la confiance des utilisateurs. La confiance est importante, car les décisions humaines peuvent être basées sur des perceptions, et pas uniquement sur des faits, et si une personne perçoit un manque de stabilité, elle peut être réticente à utiliser le cyberespace et à en tirer des avantages. À titre d'exemple, l'utilisation du cyberespace permet de rationaliser certains processus et les rend plus efficaces, ce qui laisse entendre que certaines fonctions (par ex. l'accès aux services gouvernementaux, les services de banque en ligne) peuvent tirer profit de l'exploitation du cyberespace. Cependant, si ces systèmes ne sont pas fiables (ou si l'on a l'impression qu'ils ne le sont pas), leur utilisation sera limitée et les avantages de cette technologie seront perdus.

Deuxièmement, il faut se rappeler que le cyberespace est un domaine en constante évolution. Il y a des changements dans la technologie elle-même, dans les modèles commerciaux, dans la fonctionnalité et dans les attentes de la société concernant le rôle de la technologie dans la vie quotidienne. Ainsi, à la différence de la définition standard de la « stabilité » qui inclut « un retour à l'état initial », nous avons besoin de mécanismes agiles pour assurer la stabilité du cyberespace à mesure que les technologies évoluent. Pour le dire plus simplement, chacun doit garder confiance dans la disponibilité et l'intégrité du cyberespace, même si celui-ci (et le monde qui l'entoure) change.

13 La « stabilité » est définie comme « l'état de ce qui est stable ». https://www.lexico.com/en/definition/stability. Stable signifie (1) non susceptible de céder ou de se renverser ; fermement fixé ; (2) non susceptible de changer ou d'échouer ; fermement établi ; et (3) non susceptible de subir des changements physiques. Voir https://en.oxforddictionaries.com/definition/stable. Dans les relations internationales, l'une des définitions les plus complètes du terme de stabilité internationale est « la probabilité que le système [international] conserve toutes ses caractéristiques essentielles, qu'aucune nation ne devienne dominante, que la plupart de ses membres continuent à survivre et qu'il n'y ait pas de guerre à grande échelle. » Karl W. Deutsch et J. David Singer, « Multipolar Power Systems and International Stability », *World Politics*, Vol. 16, No. 3 (avril 1964): 390-406, http://users.metu.edu.tr/utuba/Deutsch.pdf.

3. LE CADRE POUR LA CYBERSTABILITÉ DE LA GCSC

Pour relever les défis décrits ci-dessus, la GCSC, comme d'autres l'ont fait avant elle,[14] propose un Cadre complet pour la cyberstabilité. Ce cadre comprend (1) un engagement multipartite ; (2) les principes de la cyberstabilité ; (3) le développement et la mise en œuvre de normes facultatives ; (4) le respect du droit international ; (5) des mesures visant à renforcer la confiance ; (6) des mesures visant à renforcer les capacités ; et (7) la promulgation ouverte et l'utilisation généralisée de normes techniques afin de garantir la résilience du cyberespace. Les efforts de la GCSC se sont axés essentiellement sur trois de ces éléments : l'approche multipartite, les principes et les normes, qui sont traités respectivement dans les chapitres 4, 5 et 6. En ce qui concerne les normes, nous nous sommes concentrés non seulement sur leur élaboration, mais également sur les questions plus difficiles de l'adoption, de la mise en œuvre et de la responsabilité des transgresseurs.

Nous tenons à souligner que de nombreux efforts sont actuellement déployés pour traiter des éléments individuels de ce Cadre pour la cyberstabilité et que ces efforts sont, comme le cyberespace lui-même, décentralisés. Pour progresser, la GCSC estime que des efforts concertés et globaux de toutes les parties prenantes sont nécessaires. C'est pourquoi la GCSC formule, outre les questions de fond, des recommandations de processus pour tenter d'exploiter et de compléter les efforts existants et, peut-être, de leur donner un nouvel élan.

14 Voir, par exemple, *The Age of Digital Interdependence: Rapport du Groupe de haut niveau sur la coopération numérique créé par le Secrétaire général des Nations Unies* (juin 2019), p.39, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf. « Nous recommandons l'élaboration d'un engagement mondial sur la confiance et la sécurité numériques pour façonner une vision commune, identifier les attributs de la stabilité numérique, élucider et renforcer la mise en œuvre de normes pour une utilisation responsable de la technologie, et proposer des priorités d'action. »

Le Cadre pour la cyberstabilité utilise des icônes réalisées par Freepik, monkik, smalllikeart, Eucalyp, Itim2101 de www.flaticon.com.

4. ENGAGEMENT MULTIPARTITE

Malgré une multitude d'accords internationaux conclus entre les États qui citent l'importance d'une approche multipartite, celle-ci reste controversée. Pour certains, le débat est philosophique et se concentre sur les rôles comparatifs des acteurs étatiques et non-étatiques dans la politique sur les technologies et les affaires internationales. Pour d'autres, les processus multipartites sont pratiques : ils estiment que les États qui agissent seuls ou avec une contribution non-étatique minimale ne peuvent pas assurer la stabilité du cyberespace.[15] Nous partageons ce dernier point de vue.

Le débat sur les mérites d'un engagement multipartite dure depuis des décennies. Souvent, la question s'est posée dans le contexte de la gestion des ressources de l'Internet, mais elle a également été soulevée pour les normes et la sécurité nationale. Par exemple, pendant la deuxième phase du Sommet mondial des Nations Unies sur la société de l'information, le Groupe de travail des Nations Unies sur la gouvernance de l'Internet (WGIG) a rejeté le concept de direction d'une seule partie prenante. Il a conclu que l'Internet était trop vaste pour être géré par un seul groupe ou une seule organisation, et a proposé une approche multipartite. Ainsi, en 2005, les chefs d'État ont déclaré dans l'Agenda de Tunis du SMSI qu'« Une définition de la gouvernance de l'Internet est l'élaboration et l'application par les États, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet ».[16]

Ce point de vue a été réaffirmé dix ans plus tard par la Réunion de haut niveau de l'Assemblée générale des Nations Unies sur l'examen global de la mise en œuvre des résultats du SMSI, qui figure également dans la résolution des Nations Unies 70/125 (2015) :

> Nous réaffirmons en outre les valeurs et les principes de coopération et de dialogue entre les diverses parties concernées qui caractérisent depuis toujours les mesures visant à donner suite aux textes issus du Sommet mondial sur la société de l'information sachant que la participation, le partenariat et la coopération véritables des gouvernements, du secteur privé, de la société civile, des organisations internationales, des techniciens et des universitaires et de toutes les autres parties prenantes concernées, selon leurs rôles et leurs responsabilités respectifs, avec une représentation équilibrée des pays en développement, demeurent essentiels à la constructionde la société de l'information.[17]

15 « La définition du SMSI (2005) présente le concept de « rôles respectifs » et la philosophie de « partage ». La déclaration NETmundial (2014) définit les éléments clés comme étant le modèle « bottom up » (du bas vers le haut), l'ouverture, la transparence, l'intégration et les droits de l'homme. En d'autres termes, nous disposons de quelques lignes directrices générales pour une approche multipartite, mais il n'y a pas de modèle unique multipartite. Jusqu'à présent, deux modèles multipartites différents ont émergé : le modèle consultatif et le modèle collaboratif. » Wolfgang Kleinwächter, « Towards a Holistic Approach for Internet Related Public Policy Making, » Global Commission on the Stability of Cyberspace (janvier 2018), https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf. Pour d'autres discussions sur les modèles multipartites, voir Virgilio Almeida et al., « The Origin and Evolution of Multistakeholder Models, » *IEEE Internet Computing*, Vol. 19 (janvier-février 2015) : 74-79, https://doi.ieee-computersociety.org/10.1109/MIC.2015.15.

16 « Agenda de Tunis pour la société de l'information, » SMSI (18 novembre 2005), paragraphe 34, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-fr.pdf.

17 Voir la résolution 70/125 de l'Assemblée générale des Nations Unies, *Document final de la réunion de haut niveau de l'Assemblée générale sur l'examen d'ensemble de la mise en œuvre des textes issus du Sommet mondial sur la société de l'information*, A/RES/70/125 (16 décembre 2015), paragraphe 3, https://undocs.org/fr/A/RES/70/125.

À nouveau, la résolution va au-delà de la gestion des ressources critiques de l'Internet et touche directement au cœur des questions de sécurité nationale :

> Nous estimons que les États jouent un rôle moteur dans le traitement des questions de cybersécurité ayant des incidences sur la sécurité nationale. Nous estimons également que toutes les parties prenantes, chacune selon son rôle et ses responsabilités, participent et contribuent utilement à cette action.[18]

En ce qui concerne plus particulièrement les normes, le Groupe des Huit (G8) a déclaré en 2011 que :

> La sécurité des réseaux et des services sur l'Internet concernent l'ensemble des parties prenantes. Elle nécessite une coordination entre les États, les organisations régionales et internationales, le secteur privé, [et] la société civile… Les États ont un rôle à jouer, éclairés par un large éventail de parties prenantes, pour contribuer à la définition d'approches communes et de règles pour l'utilisation du cyberespace.[19]

Deux ans plus tard, en 2013, le GEG de l'ONU publie son *Rapport sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale*. Dans une section intitulée Renforcer la coopération pour promouvoir un environnement informatique pacifique, sûr, résilient et ouvert), le GEG de l'ONU a noté que « S'il revient aux États de prendre l'initiative pour mener à bien cette tâche, la participation appropriée du secteur privé et de la société civile est à même de rendre la coopération plus efficace ».[20] Le rapport poursuit en disant, dans une section intitulée Recommandations sur les normes, règles et principes de comportement responsable des États que :

> Les États Membres devraient réfléchir à la meilleure façon de coopérer dans l'application des normes et des principes de comportement responsable susmentionnés, tout en s'intéressant au rôle que le secteur privé et les organisations de la société civile pourraient y jouer. Ces normes et ces principes confortent l'action de l'Organisation des Nations Unies et des groupes régionaux et servent de base aux travaux qui devront être entrepris pour instaurer la confiance.[21]

Ces positions sont réaffirmées dans le rapport de 2015 du GEG de l'ONU, où il a été déclaré que :

> C'est aux États qu'il incombe au premier chef de garantir un environnement informatique sûr et pacifique, mais la coopération internationale gagnerait en efficacité si l'on mettait au point des mécanismes pour la participation du secteur privé, des milieux universitaires et de la société civile.[22]

Cette déclaration est reprise dans une résolution de 2018 de l'Assemblée générale sur *Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale*.[23] D'autres accords internationaux expriment clairement le même sentiment, par exemple, l'Appel de Paris déclare, « nous reconnaissons la nécessite d'une approche multi-acteurs renforcée et d'efforts supplémentaires afin de réduire les risques qui pèsent sur la stabilité du cyberespace et pour d'établir davantage de fiabilité, de capacité et de confiance ».[24]

18 Id., paragraphe 50.

19 Groupe de Huit, « Déclaration du G8 : Un nouvel élan pour la liberté et la démocratie », Sommet du G8 de Deauville (27 mai 2011), paragraphe 17, https://www.diplomatie.gouv.fr/IMG/pdf/Declaration_G8_Generale_20110527.pdf.

20 Assemblée générale des Nations Unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, A/68/98 (24 juin 2013), p.7, paragraphe 12, https://undocs.org/fr/A/68/98, (ci-après, Rapport 2013 du GEG de l'ONU).

21 Id., p.8, paragraphe 25.

22 Assemblée générale des Nations Unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, A/70/174 (22 juillet 2015), p.13, paragraphe 31, https://undocs.org/fr/A/70/174, (ci-après, Rapport 2015 du GEG de l'ONU).

23 Résolution 73/266 de Assemblée générale des Nations Unies, *Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale*, A/RES/73/266 (22 décembre 2018), https://undocs.org/fr/A/RES/73/266.

24 Ministère de l'Europe et des Affaires étrangères, Appel de Paris pour la confiance et la sécurité dans le cyberespace (11 novembre 2018), https://pariscall.international/fr/. Voir également, NETmundial, « NETmundial Multistakeholder Statement » (24 avril 2014), http://netmundial.br/wp-content/up-loads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Plus récemment, en juin 2019, le Groupe de haut sur la coopération numérique du Secrétaire général des Nations Unies a déclaré dans son rapport *L'Ère de l'interdépendance numérique* :

> Une coopération numérique efficace exige de renforcer le multilatéralisme, malgré les tensions actuelles. Elle exige également que le multilatéralisme soit complété par une coopération multipartite qui implique non seulement les gouvernements, mais également un éventail beaucoup plus large d'autres parties prenantes telles que la société civile, le monde universitaire, les technologues et le secteur privé.[25]

Si l'idée d'une approche multipartite a fait ses preuves, elle n'est pas universellement soutenue. Certains gouvernements continuent de croire que la tâche d'assurer la sécurité et la stabilité internationales relève exclusivement de la responsabilité des États. Cette conception plus traditionnelle de la sécurité découle de l'idée que les États ont la responsabilité de protéger leurs citoyens contre les attaques par la force, une idée qui se reflète dans les responsabilités du Conseil de sécurité des Nations Unies, telles que codifiées dans l'article 24 de la Charte des Nations Unies.[26] Cette ligne de pensée peut également être renforcée par l'expérience car, dans le domaine physique, les gouvernements n'ont pas seulement le monopole de l'usage légitime de la force, mais ils contrôlent également les armes de qualité militaire (par ex. les avions, les chars) utilisées pour attaquer et défendre.

En pratique, le champ de bataille virtuel (c'est-à-dire le cyberespace) est conçu, déployé et exploité principalement par le secteur privé. Les gouvernements, malgré leurs responsabilités uniques, ne sont pas les protecteurs exclusifs de ce domaine. Même si les gouvernements maintiennent un monopole *de jure* sur l'usage légitime de la force dans le cyberespace, ils n'ont plus en pratique le monopole de l'attaque et de la protection dans ce domaine et ne peuvent pas non plus empêcher la prolifération et l'utilisation de puissantes cyber armes. Au contraire, la communauté technique, la société civile et les individus jouent également un rôle majeur dans la protection du cyberespace, y compris dans la promulgation de normes. Par conséquent, l'approche multipartite est nécessaire pour améliorer les résultats, et garantir que les normes et les politiques soutenant la stabilité du cyberespace sont bien formulées et évitent les conséquences indésirables.

Il est tout aussi important de noter que même si les États souhaitent agir seuls, ils ne peuvent pas le faire. La participation des acteurs non-étatiques aux questions touchant à la stabilité du cyberespace est inévitable. Par exemple, de nombreux membres du secteur privé et de la communauté technique peuvent être responsables de protocoles et de services critiques, et ils peuvent protéger les États qui utilisent leurs produits commerciaux et en source ouverte. De plus, même les enquêtes et l'attribution des attaques, un rôle et une prérogative politique traditionnellement du ressort des gouvernements, ne sont plus leur seul domaine de connaissance et de responsabilité à présent. Certaines attaques d'États notables ont été identifiées et rendues publiques par des entités non-gouvernementales. En résumé, même si les États ont un rôle unique à jouer pendant et après une attaque (y compris l'activité de maintien de l'ordre et/ou la prise de mesures diplomatiques ou d'autres mesures étatiques), ils n'ont pas le monopole de l'enquête et de l'attribution, et ne peuvent pas non plus exclure les acteurs non-étatiques. Par conséquent, l'élaboration de normes et de politiques efficaces pour le cyberespace (et la garantie de leur respect) nécessite la participation de toutes les parties prenantes et relève de leur responsabilité à toutes. Les gouvernements doivent créer des mécanismes qui intègrent effectivement la participation du secteur privé, de la communauté technique, du monde universitaire et d'autres représentants de la société civile. C'est exactement ce que de nombreux gouvernements ont demandé.

25 *The Age of Digital Interdependence*, p. 7, https://digitalcooper-ation.org/wp-content/uploads/2019/06/DigitalCooperation-re-port-web-FINAL-1.pdf.

26 Charte des Nations Unies, « Chapitre 5 – Le Conseil de sécurité » Répertoire de la pratique du Conseil de sécurité, https://www.un.org/securitycouncil/fr/content/repertoire/functions-and-powers#rel1.

5. PRINCIPES

Le comportement normatif est issu de valeurs. Déclarer ces valeurs, qu'elles soient liées ou non aux responsabilités individuelles, aux responsabilités des États ou aux droits fondamentaux de l'homme, doit donc être notre point de départ. En effet, si les valeurs divergent, il peut être difficile d'obtenir un consensus, et cela risque d'entraîner des interprétations et des mises en œuvre différentes des accords internationaux selon les pays ou les régions. Cela ne veut pas dire qu'il est absolument nécessaire de s'accorder sur les principes pour progresser. Parfois, les parties s'entendent sur des comportements acceptables même si leurs motivations diffèrent. Toutefois, les principes partagés et l'interdépendance peuvent mener à des engagements plus profonds et réduire le risque de désaccords ou de conflits futurs. Il est donc important que les parties aient des discussions franches sur les principes qui guident leur réflexion et dont découlent les normes.

Les quatre principes suivants sont essentiels pour assurer la stabilité du cyberespace :

1. **Responsabilité :** Toute personne est responsable d'assurer la stabilité du cyberespace.
2. **Retenue :** Aucun acteur, étatique ou non-étatique, ne devrait prendre de mesures qui nuisent à la stabilité du cyberespace.
3. **Nécessité d'agir :** Les acteurs étatiques et non-étatiques devraient prendre des mesures raisonnables et appropriées pour assurer la stabilité du cyberespace.
4. **Respect des droits de l'homme :** Les efforts pour assurer la stabilité du cyberespace doivent respecter les droits de l'homme et l'État de droit.

A. Le principe de responsabilité

Le premier principe concerne la nature décentralisée et distribuée du cyberespace. Il réaffirme la nécessité d'une approche multipartite pour assurer la stabilité du cyberespace et, notamment, étend les « parties prenantes » à chaque individu. Chaque individu a la responsabilité, à titre personnel et/ou professionnel, d'assurer la stabilité du cyberespace. S'il est évident que les responsables des politiques gouvernementales en matière de cyberespace et les employés qui gèrent les services du cloud ont un rôle important à jouer, chaque individu connecté au cyberespace doit faire des efforts raisonnables pour s'assurer que ses propres dispositifs ne sont pas compromis et, peut-être, utilisés dans des attaques. Même celles et ceux qui ne sont pas connectés à l'Internet peuvent dépendre des capacités de celui-ci pour recevoir des biens et des services, et ils ont eux aussi intérêt à s'assurer que la politique du cyberespace est traitée de manière appropriée dans leurs communautés.

B. Le principe de retenue

Le deuxième principe concerne une exigence générale de retenue. Pour les États, ce principe est conforme aux résolutions de 2018 de l'Assemblée générale des Nations Unies (AGNU) concernant le comportement responsable des États dans le cyberespace[27] et au rapport du GEG de l'ONU de 2015 qui note que « conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États devraient coopérer ... à prévenir les pratiques informatiques jugées nocives qui peuvent compromettre la paix et la sécurité internationales »[28] Cependant, il n'est pas uniquement question des États, car les acteurs non-étatiques peuvent également engager des actions, comme le piratage de leurs agresseurs, qui pourraient également miner la stabilité du cyberespace.

27 Résolution 73/27 de l'Assemblée générale des Nations Unies, *Progrès de l'informatique et des télécommunications et sécurité internationale*, A/RES/73/27 (5 décembre 2018), https://undocs.org/fr/A/RES/73/27; and Résolution de l'Assemblée générale des N.U. 73/266, https://undocs.org/fr/A/RES/73/266.

28 Rapport 2015 du GEG de l'ONU, p.7, paragraphe 13(a), https://undocs.org/fr/A/70/174.

C. Le principe de nécessité d'agir

Le troisième principe prévoit une obligation générale de prendre des mesures positives pour préserver la stabilité du cyberespace. Lors de leurs actions, les États doivent veiller à éviter d'aggraver les tensions ou d'accroître l'instabilité par inadvertance. Ce principe reprend l'obligation notée dans le rapport du GEG de l'ONU de 2015 de « coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des TIC. »[29] Encore une fois, il n'est pas seulement question des États, car les entreprises privées et les particuliers peuvent également prendre des mesures de coopération pour contribuer à assurer la stabilité du cyberespace. Par exemple, les entreprises privées peuvent travailler ensemble pour atténuer les menaces virtuelles, et les particuliers peuvent s'assurer qu'ils utilisent les meilleures pratiques, comme la mise à niveau, les correctifs et l'authentification multifactorielle, pour réduire le risque que des réseaux de botnets ne prennent le contrôle de leurs appareils et soient ensuite utilisés pour lancer des attaques à grande échelle qui menacent la stabilité du cyberespace.

D. Le principe des droits de l'homme

Le quatrième principe reconnaît l'importance de la sauvegarde et du respect des droits de l'homme comme un élément important de la stabilité du cyberespace. Plus les individus dépendent des technologies de l'information et des communications, plus les perturbations sur l'activité humaine résultant des menaces qui pèsent sur sa disponibilité ou son intégrité sont amplifiées. Il est donc impératif qu'en poursuivant leurs intérêts stratégiques nationaux dans le cyberespace, les États tiennent dûment compte de l'impact sur les individus, en particulier sur leurs droits fondamentaux. Dans le même ordre d'idées, les acteurs non-étatiques devraient considérer et minimiser les risques que leurs activités font courir aux individus dans l'exercice de leurs droits en ligne et hors ligne. Le respect du principe des droits de l'homme exige au minimum que les États respectent leurs obligations en matière de droits de l'homme en vertu du droit international lorsqu'ils s'engagent dans des activités dans le cyberespace.

Les droits de l'homme universellement acceptés sont inscrits dans la Déclaration universelle des droits de l'homme.[30]De plus, un grand nombre d'accords internationaux prévoyant toute une série de droits de l'homme spécifiques ont été adoptés et créent des obligations juridiques contraignantes pour les États. Dans le contexte du cyberespace, l'application des droits universels de l'homme a été confirmé ouvertement à de nombreuses occasions par l'Assemblée générale des Nations Unies,[31] le Conseil des droits de l'homme des Nations Unies (CDH)[32] ainsi que par les rapports de 2013 et de 2015 du GEG de l'ONU.[33]Pour assurer la stabilité du cyberespace, il est essentiel de défendre les droits fondamentaux et de faire en sorte que les utilisateurs aient la certitude que leurs droits sont respectés.

Nous précisons que les quatre principes ne sont pas destinés à être exhaustifs ou à couvrir tous les aspects de la politique du cyberespace, et de nombreuses organisations ont produit des ensembles de principes généraux couvrant une grande variété de questions. Il existe également d'autres organisations qui se concentrent sur des questions relatives à la gouvernance de l'Internet et aux droits de l'homme en ligne (notamment la vie privée, la liberté d'expression et la liberté d'association). Notre objectif est de parvenir à une large acceptation des principes qui soutiennent la stabilité du cyberespace, en particulier à une époque d'activités hostiles sophistiquées sans précédent où les règles peuvent être floues ou, même si elles sont claires, ne sont ni adoptées ni appliquées.

29 Id.

30 Résolution 217 A (III) de l'Assemblée générale des Nations Unies, *Déclaration universelle des droits de l'homme* (10 décembre 1948), https://www.un.org/fr/universal-declaration-human-rights/.

31 Voir Résolution 68/167 de l'Assemblée générale des Nations Unies, *Le droit à la vie privée à l'ère du numérique*, A/RES/68/167 (18 décembre 2013), https://undocs.org/fr/A/RES/68/167; et la Résolution 69/166 de l'Assemblée générale des Nations Unies, *Le droit à la vie privée à l'ère du numérique*, A/RES/69/166 (18 décembre 2014), https://undocs.org/fr/A/RES/69/166.

32 Conseil des droits de l'homme des Nations Unies, *La promotion, la protection et l'exercice des droits de l'homme sur Internet*, A/HRC/20/L.13 (29 juin 2012), https://undocs.org/fr/A/HRC/20/L.13.

33 Rapport 2013 du GEG de l'ONU, https://undocs.org/fr/A/68/98 et Rapport 2015 du GEG de l'ONU, https://undocs.org/fr/A/70/174.

6. NORMES

Si les principes constituent un point de départ essentiel pour établir une politique et orienter les actions tactiques, leur haut degré d'abstraction exige qu'ils soient complétés par des accords plus granulaires qui définissent les comportements acceptables. Cela signifie que les principes doivent être complétés par des normes. Les normes représentent des comportements sociaux attendus et appropriés.[34] Il est impossible de discuter des normes sans se référer aux travaux d'autres organisations, en particulier le Groupe d'experts gouvernementaux (GEG) des Nations Unies et son rapport de 2015.[35] Le GEG de l'ONU a reconnu que « compte tenu de la spécificité du domaine informatique, de nouvelles normes pourraient être élaborées au fil du temps »[36], et le mandat de la GCSC était, en fait, d'« élaborer des propositions de normes et de politiques pour renforcer la sécurité et la stabilité internationales. » Afin de s'appuyer sur les travaux antérieurs et d'identifier les domaines dans lesquels des normes supplémentaires pourraient être justifiées, il est important de commencer par les normes convenues en 2015, qui figurent, dans leur intégralité, à l'annexe A.

Comme l'a noté le GEG de l'ONU en 2015, il a été chargé, entre autres, « de préciser dans quel domaine il pouvait être nécessaire d'élaborer des normes supplémentaires qui tiennent compte de la complexité et de la spécificité des technologies de l'information et des communications ».[37] Depuis lors, les produits et services des TIC (ainsi que leur utilisation abusive) n'ont cessé d'évoluer. Pour faire face à cette situation, la GCSC s'est attachée à combler les lacunes de l'ensemble actuel de normes, à ajouter une spécificité technique à la discussion sur les normes et à traiter les questions de mise en œuvre. Pour combler les lacunes, par exemple, la GCSC a approuvé une norme visant à protéger le coeur public de l'Internet[38]et une norme pour protéger les systèmes électoraux.[39]De la même manière, alors que la norme du GEG de l'ONU se rapporte à « l'intégrité de la chaîne logistique »[40], une norme de la GCSC parle plus précisément des types d'attaques des chaînes logistiques qui doivent être traitées.[41]

34 https://en.oxforddictionaries.com/definition/norm.
35 Rapport du GEG de l'ONU 2015, https://undocs.org/fr/A/70/174.
36 Id., p. 8, paragraphe 15.
37 Id., p. 7, paragraphe 11.

38 Global Commission on the Stability of Cyberspace (GCSC), *Call to Protect the Public Core of the Internet* (New Delhi, novembre 2017), https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf. Dennis Broeders, un chercheur néerlandais, a été un promoteur précoce de l'identification du coeur public de l'Internet pour protection spéciale. Voir Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam Univer-sity Press, 2015), http://www.oapen.org/download?type=docu-ment&docid=610631.
39 Global Commission on the Stability of Cyberspace (GCSC), *Call to Protect the Electoral Infrastructure* (Bratislava, mai 2018), https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.
40 Rapport du GEG de l'ONU 2015, p. 8, paragraphe 13(i). « Les États devraient prendre des mesures raisonnables pour assurer l'intégrité de la chaîne logistique, afin que les utilisateurs finaux puissent avoir confiance en la sécurité des produits informatiques. Les États devraient s'attacher à prévenir la prolifération des techniques et outils informatiques malveillants et l'utilisation de fonctionnalités cachées nuisibles ».
41 Global Commission on the Stability of Cyberspace (GCSC), *Norms Through Singapore* (novembre 2018), https://cyberstabil-ity.org/wp-content/uploads/2019/04/singaporenew-digital.pdf. « Les acteurs étatiques et non-étatiques ne devraient pas manipuler les produits et services en cours de développement et de production, ni permettre qu'ils soient manipulés, si cela risque de porter atteinte de manière substantielle à la stabilité du cyberespace. »

L'autre différence majeure entre les normes du GEG de l'ONU et celles proposées par la GCSC est que cette dernière estime que des responsabilités devraient également être imposées aux acteurs non-étatiques, notamment en matière de retenue ou des mesures positives pour assurer la stabilité du cyberespace. Nous ne faisons pas référence ici aux cyberattaques des criminels. Les criminels qui ne sont pas dissuadés par les actions gouvernementales ne le seront pas par les normes. Cependant, comme la technologie évolue rapidement et que les lois ne le font pas, il est utile de préciser quels comportements non-étatiques doivent être encouragés ou découragés, même en l'absence de lois. Par exemple, certains préconisent que les victimes de piratage informatique soient autorisées à « pirater en retour » (hack back). Même en l'absence de lois autorisant ou interdisant ce type de comportement, la GCSC estime qu'il est déconseillé de le faire, et ce pour plusieurs raisons, notamment le fait que l'agresseur initial peut faire passer son attaque par des systèmes tiers (par ex. un fournisseur de services cloud ou un hôpital) et que le piratage peut donc avoir un impact sur des utilisateurs innocents (par ex. des clients dans le cloud ou des patients). De plus, en raison de ces attaques contre des victimes innocentes, le piratage peut être perçu comme une escalade ou la provoquer. En résumé, en raison des complexités soulevées, même en l'absence de lois, une norme limitant les acteurs du secteur privé peut influencer le comportement, et donc servir un objectif salutaire.

A. Normes proposées par la GCSC

En gardant à l'esprit les points soulevés ci-dessus, la GCSC a élaboré les propositions de normes suivantes :

1. Les acteurs étatiques et non-étatiques ne devraient ni mener ni autoriser sciemment des activités qui portent intentionnellement et substantiellement atteinte à la disponibilité générale ou à l'intégrité du coeur public de l'Internet, et donc à la stabilité du cyberespace.

2. Les acteurs étatiques et non-étatiques ne devraient pas poursuivre, soutenir ou permettre des opérations virtuelles visant à perturber l'infrastructure technique essentielle aux élections, référendums ou plébiscites.

3. Les acteurs étatiques et non-étatiques ne devraient pas manipuler les produits et services en cours de développement et de production, ni permettre qu'ils soient manipulés, si cela risque de porter atteinte de manière substantielle à la stabilité du cyberespace.

4. Les acteurs étatiques et non-étatiques ne devraient pas réquisitionner les ressources TIC du grand public pour les utiliser comme botnets ou à des fins similaires.

5. Les acteurs étatiques devraient créer des cadres de procédures transparents pour évaluer s'il convient de divulguer des vulnérabilités ou des défauts dont ils ont connaissance, mais non connus du grand public, dans les systèmes et technologies de l'information, et à quel moment il convient d'en parler. La présomption par défaut devrait favoriser la divulgation.

6. Les développeurs et fournisseurs de produits et services dont dépend la stabilité du cyberespace devraient (1) donner la priorité à la sécurité et à

la stabilité, (2) prendre des mesures raisonnables pour s'assurer que leurs produits ou services sont exempts de vulnérabilités importantes, et (3) prendre des mesures pour atténuer en temps utile les vulnérabilités découvertes ultérieurement et être transparents quant à leur processus. Tous les acteurs ont l'obligation de partager les informations concernant les vulnérabilités afin d'aider à prévenir ou atténuer la cyberactivité malveillante.

7. Les acteurs étatiques devraient adopter des mesures appropriées, y compris des lois et des règlements, pour assurer une cyber-hygiène de base.

8. Les acteurs non-étatiques ne devraient pas s'engager dans des cyber-opérations offensives, et les acteurs étatiques devraient empêcher de telles activités et réagir si elles se produisent.

Il convient de noter qu'il peut être difficile de trouver les mots les plus appropriés pour exprimer une norme. Si les normes sont trop précises et ne laissent aucune place à l'interprétation, il peut être difficile de parvenir à un consensus et les lacunes de couverture peuvent devenir importantes. D'un autre côté, si les normes sont trop vagues, elles ne fournissent pas l'orientation nécessaire pour guider le comportement et fixer des attentes claires pour un groupe spécifique d'acteurs. L'objectif est de trouver le bon équilibre et de développer d'autres normes, si nécessaire, pour garantir que les comportements indésirables sont pris en compte. Pour prendre un exemple, les normes du GEG de l'ONU adoptées en 2015 protégeaient les infrastructures critiques, mais il n'est pas certain que le coeur public de l'Internet soit couvert par ces termes. De nombreuses personnes pensent que les infrastructures critiques sont des services et des équipements publics (par ex. l'électricité, les communications, ou les services bancaires).[42] De plus, le GEG de l'ONU n'a pas fait spécifiquement référence aux systèmes électoraux, une préoccupation qui s'est accentuée après 2015.[43]

Si les systèmes électoraux sont couverts dans certains pays par référence (c'est-à-dire que certains États considèrent désormais les systèmes électoraux comme des infrastructures critiques, les faisant ainsi entrer dans le champ d'application des normes relatives aux infrastructures critiques),[44]d'autres pays n'ont pas forcément cette approche. Ainsi, si le cyberespace est mondial, les protections normatives ne le sont pas forcément. Pour aider à résoudre les problèmes d'interprétation des normes de la GCSC, la Commission a décidé de fournir un contexte de référence pour chaque norme décrite ci-dessus (voir annexe B).

Enfin, les normes de comportement dans le cyberespace ne peuvent pas être statiques. Les normes de la GCSC reflètent un moment dans le temps dans un paysage technologique en constante évolution. Les acteurs étatiques et non-étatiques doivent être prêts à développer de nouvelles normes au fur et à mesure que les technologies progressent et que notre compréhension des implications des technologies existantes évolue.

Qu'elles soient axées sur les normes du GEG de l'ONU, les normes de la GCSC ou sur d'autres propositions, il faut savoir que, pour que les normes soient efficaces, il est nécessaire qu'elles soient adoptées et appliquées, et que ceux qui les enfreignent soient redevables et reconnus responsables. Nous abordons maintenant ces questions, avant de nous pencher sur la manière dont les acteurs non-étatiques, qui sont décentralisés et répartis dans le monde entier, peuvent se réunir pour travailler avec les gouvernements sur des solutions pratiques aux défis soulevés par la cyberstabilité.

B. Adoption des normes

Pour qu'une norme soit efficace, elle doit être acceptée par le plus grand nombre. Cette acceptation, même par des acteurs que certains considèrent comme des contrevenants potentiels, renforce la légitimité des actions qui dénoncent le non respect des normes et des actions collectives appropriées prises pour répondre à ces violations. Bien que l'adoption généralisée soit la meilleure solution, il est possible pour de petits groupes d'États ou d'autres entités partageant le même

42 Les infrastructures critiques ont été définies comme incluant « des systèmes et actifs, qu'ils soient physiques ou virtuels, si indispensables que leur incapacité ou destruction pourrait avoir un impact déstabilisant sur la sécurité, la sécurité économique nationale, la santé ou la sûreté de la population ou une combinaison de ces éléments. » *Critical Infrastructures Protection Act of 2001*, 42 Code des États-Unis § 5195c(e), (2001). Elles ont également été définies comme « des actifs ou systèmes qui sont vitaux au maintien des fonctions de la société, de la santé, de la sécurité et du bien-être économique ou social de la population. » Conseil de l'Union européenne, *directive du Conseil 2008/114/CE du 8 décembre 2008 sur le recensement et la désignation des infrastructures critiques*
européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, Journal officiel de l'Union européenne, (8 décembre 2008), https://eur-lex.europa.eu/legal-content/FR/TXT/%20PDF/?uri=CELEX:32008L0114.

43 Erik Brattberg et Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks,* Carnegie Endowment for International Peace (23 mai 2018), https://carnegieendowment.org/2018/05/23/russian-election-int europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435. Voir aussi Michael McFaul, ed., *Securing American Elections*, Stanford Cyber Policy Center (juin 2019), https://cyber.fsi.stanford.edu/securing-our-cyber-future.

44 Voir, par exemple, U.S. Department of Homeland Security, « Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsec-tor » (6 janvier 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastruc-ture-critical.

état d'esprit de se mettre d'accord sur des normes particulières et de les faire appliquer. Pour remédier à cette situation, la GCSC propose une approche souple et extensible qui permet aux États et aux autres parties prenantes d'adopter certaines normes tout en rejetant ou en s'abstenant d'en adopter d'autres. Cette approche permet non seulement de clarifier les choses en mettant en évidence les domaines spécifiques d'accord et de désaccord, mais aussi d'adopter, d'affiner et de mettre en œuvre des normes particulières, même s'il faut plus de temps pour en évaluer certaines autres. Dans tous les cas, l'adoption généralisée de normes est un effort à long terme.

Promouvoir l'adoption de normes présente également des défis uniques et concrets. Le défi principal est que nous essayons de faire face à des comportements perturbateurs relativement nouveaux. Dans la mesure où une norme est « quelque chose d'habituel, de typique ou de standard »[45], élaborer des normes concernant le comportement futur est un exercice intéressant. Si tout le monde se comporte déjà d'une certaine manière, alors une norme écrite ne fait que codifier une pratique existante. Cependant, s'il n'y a pas de « comportement typique », alors l'élaboration d'une norme est une tentative visant à encourager un comportement commun à l'avenir, même si ce comportement n'existe pas encore aujourd'hui. Le simple fait de déclarer un comportement souhaitable ne le rendra pas normatif, il faut donc en promouvoir l'adoption.

Deuxièmement, il est nécessaire de mieux sensibiliser les entités capables de mettre en œuvre les normes proposées, ainsi que celles que ces normes sont censées protéger. Même avec une activité importante au sein des Nations Unies et une multitude d'autres forums, l'adoption des normes en est encore à ses débuts et il reste beaucoup à faire pour promouvoir les normes proposées et les faire accepter, en particulier dans certaines régions du monde. C'est pourquoi les efforts de renforcement des capacités dans ce domaine sont si essentiels. Les organisations dotées de plus grandes capacités sont plus susceptibles de soutenir efficacement l'adoption de normes, et obtenir une meilleure adhésion est un élément fondamental de toute structure normative mondiale. De plus, il faut s'adresser à ceux qui sont protégés par les normes, car ils peuvent ne pas avoir conscience de leur impact potentiel. Par exemple, il ne semble pas que les centres d'alerte et de réaction aux attaques informatiques (CSIRT/CERT) soient largement sensibilisés à la norme du GEG de l'ONU recommandant aux États de n'utiliser les CSIRT nationaux qu'à des fins défensives. Comme nous le verrons plus loin, les entités protégées ont souvent un rôle à jouer dans la mise en œuvre et la responsabilité ou redevabilité (ainsi que dans la conception de la norme proposée), mais elles ne peuvent pas remplir ces rôles si elles n'ont pas conscience ou connaissance des propositions faites par les acteurs étatiques et non-étatiques. Il est clair que les gouvernements et les organisations internationales doivent faire davantage pour toucher les communautés que les normes proposées sont censées aider.

45 Voir https://www.lexico.com/en/definition/norm.

C. Mise en œuvre des normes

Après l'adoption d'une norme, les acteurs étatiques et non-étatiques doivent prendre des mesures concrètes pour la mettre en œuvre. Il semble y avoir un consensus croissant dans les processus des Nations Unies en cours (GTCNL et GGE) et dans les efforts régionaux pour que la mise en œuvre devienne une priorité.[46] Pour certains, la mise en œuvre fait référence à l'adoption de la norme, à l'engagement d'efforts de renforcement des capacités et de mesures de confiance, ou à l'obtention d'un consensus à plus petite échelle sur la signification d'une norme convenue.[47] Ces étapes sont des conditions préalables importantes à la mise en œuvre des normes, mais elles ne servent pas à la mise en œuvre en soi. Par exemple, le renforcement des capacités est nécessaire pour que les pays puissent se sécuriser et disposer de la largeur de bande nécessaire pour s'engager au niveau international, mais il est possible de renforcer les capacités sans adopter ou mettre en œuvre des normes. De la même manière, les mesures de confiance peuvent contribuer à maintenir la stabilité du cyberespace en facilitant l'échange des points de vue nationaux sur les décisions numériques, en établissant des lignes directes pour des communications rapides entre les cyberexperts nationaux et en encourageant le partage des meilleures pratiques et des normes de

46 Résolution 73/266 de l'Assemblée générale des Nations Unies, p. 3, paragraphe 1(b), https://undocs.org/fr/A/RES/73/266 ; résolution 73/27 de l'Assemblée générale des Nations Unies, p. 5, paragraphe 5, https://undocs.org/fr/A/RES/73/27. Voir aussi l'Organisation pour la sécurité et la coopération en Europe (OSCE), *remarques introductives par le secrétaire général Thomas Greminger*, présidence 2019, conférence de l'OSCE sur la sécurité cyber/des TCI (Bratislava, 2019). « Des organisations régionales … peuvent être des incubateurs pour de nouvelles idées et d'efforts pratiques liés aux mesures de renforcement de la confiance, ainsi que des organismes de mise en œuvre d'accords mondiaux, comme les rapports du GEG. Les organisations régionales sont donc à la fois des incubateurs et des organismes de mise en œuvre. »

47 L'Assemblée générale des Nations Unies a invité tous les États membres à continuer de communiquer au Secrétaire général, en tenant compte des constatations et recommandations qui figurent dans les rapports du GEG et du Groupe de travail à composition non limitée (GTCNL), à continuer à communiquer au Secrétaire général leurs vues et leurs évaluations sur *entre autres* « les mesures prises au niveau national pour renforcer la sécurité de l'information et promouvoir la coopération internationale dans ce domaine » et « les mesures que la communauté internationale pourrait prendre pour renforcer la sécurité numérique au niveau mondial ». Voir le rapport du Secrétaire général de l'ONU 74/120, https://undocs.org/fr/A/74/120. Pour une présentation des opinions supplémentaires des États membres, voir https://www.un.org/disarmament/ict-security/.

sécurité, mais encore une fois, cela peut être fait sans normes. La mise en œuvre d'une norme implique plutôt de prendre des mesures concrètes pour lui donner de la force. Au niveau national, cela peut consister à intégrer les normes proposées dans la politique, la législation et la doctrine militaire nationales. Sur le plan international, cela peut consister à citer les dispositions d'une norme lorsque l'on attribue des attaques ou que l'on met en place une action diplomatique. L'exécution d'une norme de cette manière sert également à lui donner une définition plus précise.

D. Responsabilité

Lorsque les normes sont adoptées et mises en œuvre, il faut que ceux et celles qui les enfreignent aient à répondre de leurs actes. Cela soulève les questions complexes de l'attribution et de la réponse, qui se sont toutes deux révélées difficiles dans la lutte contre les cyberattaques.

Pour affirmer qu'un acteur étatique ou non-étatique a agi de manière illicite, il faut une attribution crédible. Cela commence par la collecte et l'analyse des preuves. Un travail technique et procédural peut être effectué dès maintenant pour améliorer la qualité et la rapidité de l'attribution. Plus précisément, comme pour d'autres disciplines techniques, il est important de disposer de protocoles bien acceptés pour la collecte et l'analyse des preuves afin d'améliorer la qualité des enquêtes. La normalisation des méthodes d'enquête est importante, car elle permet de réduire les inquiétudes sur l'intégrité des preuves, même si l'attribution doit être décidée au cas par cas. Outre l'amélioration de l'attribution (qui est une question technique), il est possible de faire beaucoup de choses pour raccourcir la durée des processus bureaucratiques associés à la prise de décisions d'attribution et ensuite, le cas échéant, les rendre publiques. Le délai souvent long entre un évènement et une déclaration de responsabilité est dû, en grande partie, au manque de clarté ou à la lourdeur des processus permettant de prendre les décisions au niveau national, et cela s'accentue encore lorsque plusieurs pays sont impliqués dans des déclarations d'attribution collectives. La conception et l'application des processus pour parvenir à l'attribution au niveau national et international, ainsi que l'optimisation du partage des informations entre les pays, peuvent améliorer considérablement la rapidité et l'efficacité des déclarations d'attribution et faciliter toute autre action appropriée.

Même après que les preuves aient désigné un acteur donné, l'étape suivante (l'attribution) peut rester difficile. Par le passé, certains acteurs étatiques et non-étatiques ont affirmé que l'attribution était impossible ou exigeait une preuve absolue. Cependant, il n'est pas nécessaire d'avoir une preuve absolue, et si l'attribution peut être difficile, la situation n'est pas aussi insurmontable que certains l'ont suggéré. Dans le contexte de l'État-nation, l'attribution, que ce soit dans le domaine virtuel ou physique, est souvent un acte politique. Bien qu'aucune norme particulière de preuve n'ait été convenue, les pays sont toujours fortement incités à ne pas faire d'allégations fallacieuses, de peur de perdre leur crédibilité. En résumé, il faut que l'attribution soit convaincante pour les autres pays et le grand public.

Même si une partie lésée est satisfaite de voir qu'un acteur est déclaré responsable (l'attribution s'est en fait produite dans des cas internationaux), il s'est également avéré difficile de tenir les acteurs véritablement redevables, ce qui a sapé la valeur des normes. Après tout, s'il n'y a pas de conséquences négatives pour ceux qui violent les normes acceptées, ces normes ne sont guère plus que des mots, et il est peu probable qu'elles découragent les activités perturbatrices.

La responsabilité des cyberattaques menées par des acteurs non-étatiques est relativement simple et se fait principalement en imposant une responsabilité civile ou pénale en vertu des lois nationales des États concernés. Il y a certainement là des défis à relever, car la nature internationale de nombreuses cyberattaques et les défis techniques liés à la collecte de preuves peuvent constituer des obstacles à l'action des États. Cependant, la voie à suivre est claire en théorie : rationaliser les processus internationaux d'application de la loi et veiller à ce que les cybercriminels soient identifiés et poursuivis.

Il est plus difficile de tenir les États responsables de violations de normes.[48] En effet, la réponse à une attaque dans le cyberespace dépend fortement du contexte. Pour savoir si une responsabilité est exigée, les acteurs étatiques et non-étatiques évalueront différents facteurs. Par exemple, un État qui réagit à une violation des normes peut prendre en compte les implications politiques, tandis qu'une entreprise du secteur privé peut prendre en compte les répercussions sur les affaires et la réputation. Pour traiter une violation, les mesures prises par l'État en réponse à une violation des normes peuvent être considérées comme un continuum, car la réponse peut être mineure (par ex. une plainte privée), importante (par ex. des sanctions économiques) ou dramatique (par ex. une réponse cinétique très visible). Bien qu'il n'y ait pas et qu'il n'y aura pas de réponse unique, il est clair que les violations des normes et du droit international doivent avoir des conséquences significatives. Les efforts passés

48 Les États peuvent être tenus responsables des cyber-opérations qu'ils conduisent, dirigent ou autorisent. Le principe de diligence raisonnable peut également s'avérer utile pour définir le niveau de soin requis des États dans le cyberespace. Joanna Kulesza, *Due Diligence in International Law*, (Leiden: Brill Nijhoff, 2016), https://doi.org/10.1163/9789004325197. Voir aussi, *Articles sur la responsabilité de l'État pour fait internationalement illicite*, adoptés par la Commission du droit international lors de sa cinquante-troisième session en 2001, annexés à la résolution 56/83 de l'Assemblée générale des Nations Unies du 12 décembre 2001, et corrigés par le document A/56/49(Vol I)/Corr4, Articles 4 et 11, https://legal.un.org/docs/index.asp?path=%2E%2E%2Filc%2Ftexts%2Finstruments%2Ffrench%2Fdraft%5Farticles%2F9%5F6%5F2001%2Epdf&lang=EF&referer=http://legal.un.org/cod/.

pour faire respecter les normes ont eu un succès limité, et des réponses plus efficaces et plus rapides sont nécessaires. Nous reconnaissons également que ces réponses devraient chercher à éviter une plus grande instabilité.

Les acteurs non-étatiques s'efforcent de faire en sorte que les contrevenants aux normes soient tenus responsables de leurs actes. Par exemple, le GFCE[49] associe des membres du gouvernement, de la société civile et du secteur privé pour aider à coordonner les efforts de renforcement des capacités, ce qui est une condition préalable à l'adoption et à la mise en œuvre des normes, ainsi qu'à la responsabilité pour violation de ces normes. De plus, le secteur privé a assumé un rôle important dans l'attribution des attaques, en utilisant à la fois des informations exclusives et publiques pour exposer les acteurs et décrire les dommages qu'ils ont causés. Enfin, certaines entités du secteur privé ont proposé ou lancé des initiatives, telles que le « CyberPeace Institute »[50], qui sont conçues pour surveiller et exposer les grands cyberévènements de manière plus systématique et, potentiellement, à plus grande échelle.

Les acteurs non-étatiques devraient jouer un rôle accru pour que ceux qui enfreignent les normes soient tenus responsables de leurs transgressions. L'idée de faire respecter des normes par le secteur privé n'est pas nouvelle : par exemple, en 1977, lors de la lutte contre l'apartheid en Afrique du Sud, General Motors a promu un ensemble de principes largement adoptés définissant les conditions pour faire des affaires dans ce pays, ce qui a entraîné le désinvestissement de plus de 125 entreprises étrangères.[51] Plus récemment et plus symboliquement, de nombreuses entreprises (et gouvernements) ont répondu au meurtre saoudien du reporter de l'opposition Jamal Khashoggi en boycottant la Future Investment Initiative pour marquer leur désapprobation.[52]Ces types d'efforts devraient faire l'objet d'un examen plus approfondi.

E. Communautés d'intérêt

Alors qu'une approche multipartite de l'adoption et de la mise en œuvre des normes ainsi que de la responsabilité pour leur violation est essentielle, il est difficile de mobiliser les énergies et les capacités de ces groupes. Les gouvernements utilisent souvent le terme « like-minded nations » (nations partageant le même état d'esprit) pour parler d'un groupe d'États ayant des opinions semblables, mais il n'existe aucun terme équivalent qui englobe un ensemble d'États, d'entreprises privées, d'organisations à but non lucratif (y compris des organismes de normalisation), la société civile et des personnes qui partagent les mêmes points de vue sur un sujet particulier. Ceci est important, car les normes qui ont été proposées par le GEG de l'ONU et la GSGC peuvent affecter différentes circonscriptions, et des organisations et des membres de la société différents pourraient s'intéresser à la défense de certaines normes plus que d'autres. Puisque les gouvernements, le secteur privé, la communauté technique, le monde universitaire et la société civile ne sont pas des entités monolithiques, il est important de réfléchir à la manière de créer un effort concerté plutôt que concentré : un effort qui fasse collaborer des communautés diverses sur les sujets liés aux normes.[53]La création de communautés d'intérêt permet à ceux qui ont une expertise dans des normes particulières de travailler à leur développement et à leur mise en œuvre. Par exemple, les équipes d'intervention en cas d'urgence informatique (CERT/CSIRT) pourraient s'intéresser particulièrement à la mise en œuvre et à la surveillance des normes du GEG de l'ONU visant à protéger cette communauté, tout comme les responsables des systèmes électoraux pourraient s'intéresser particulièrement aux normes de la GCSC sur les systèmes électoraux. De même, la communauté de l'Internet pourrait aider à faire progresser, à mettre en œuvre et à surveiller des normes proposées par la commission sur la protection du coeur public de l'Internet, et les développeurs pourraient s'intéresser davantage aux normes concernant la manipulation de produits.

La formation d'une communauté d'intérêt pourrait être dirigée d'en haut ou résulter d'un processus ponctuel initié par les utilisateurs finaux. Le fait que les membres eux-mêmes puissent former une communauté n'implique pas que leur développement et leur succès doivent être laissés au hasard. Au contraire, il est important de s'intéresser tout particulièrement à ce qui fait le succès d'une communauté : (1) des principes partagés ; (2) sa consécration à une question particulière ; (3) des connaissances spécialisées ; (4) un soutien financier et administratif ; et (5) un processus transparent. En fait, il est sans doute possible d'identifier un modèle de bonnes pratiques de création et de mise en œuvre de communautés, ce qui permettrait à des processus d'établissement de normes divers de s'appuyer sur un modèle communautaire similaire. Cela permettrait de réconcilier différents flux de travail pour garantir l'efficacité et le ciblage des efforts, et de tirer parti des meilleures pratiques en matière d'adoption et de mise en œuvre des normes, ainsi que de responsabilité pour leur violation.

49 Global Forum on Cyber Expertise, https://www.thegfce.com/.
50 CyberPeace Institute, https://cyberpeaceinstitute.org/.
51 Voir, pour une explication générale, « Sullivan Principles », Wikipedia, 12 août 2018, https://en.wikipedia.org/wiki/Sullivan_principles.
52 Voir « Western boycott of Future Investment Initiative 2018 », *Royal News*, 16 octobre 2018, https://en.royanews.tv/news/15500/2018-10-16.
53 Voir, pour une explication générale, *The Age of Digital Interdependence*, https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf.

7. RECOMMANDATIONS

Nos six recommandations visant à assurer la stabilité du cyberespace découlent de nos principes sur la responsabilité, la retenue, la nécessité d'agir et le respect des droits de l'homme. Si chacun est responsable d'assurer la stabilité du cyberespace, et qu'une approche multipartite est essentielle à celle-ci, nos recommandations visent également à s'appuyer sur les capacités des acteurs étatiques et non-étatiques, en partie par l'intermédiaire des communautés d'intérêt. En résumé, nous mettons l'accent sur ce qui *devrait* être fait et sur la manière dont cela *pourrait* être fait.

1. **Les acteurs étatiques et non-étatiques doivent adopter et mettre en œuvre des normes permettant d'augmenter la stabilité du cyberespace en favorisant la retenue et en encourageant l'action.** Les acteurs étatiques qui ont précédemment accepté des normes doivent définir plus clairement les termes utilisés, un résultat qui pourrait être obtenu par de nouvelles négociations et par l'expérience pratique de mise en œuvre des normes existantes. Les acteurs tant étatiques que non-étatiques devraient fournir des preuves claires de l'adoption et de la mise en œuvre des normes par des déclarations publiques, et par des changements des politiques et des actes.

2. **Les acteurs étatiques et non-étatiques, selon leurs responsabilités et leurs limites, doivent réagir de manière appropriée aux violations des normes, en veillant à ce que ceux et celles qui les enfreignent soient confrontés à des conséquences prévisibles et significatives.** L'élaboration et la mise en œuvre des normes ne seront pas efficaces si ceux qui les violent savent qu'ils peuvent le faire impunément. Par conséquent, les acteurs étatiques et non-étatiques devraient développer des capacités internes afin d'évaluer les transgressions, et de décider et de prendre rapidement les réponses individuelles et collectives appropriées, conformément au principe de nécessité d'agir.

3. **Les acteurs étatiques et non-étatiques, y compris les institutions internationales, devraient redoubler d'efforts pour former leur personnel, renforcer les capacités et les compétences, promouvoir une compréhension commune de l'importance de la stabilité du cyberespace et prendre en compte les besoins disparates des différentes parties.** Accroître les capacités, les compétences et la compréhension permettront aux acteurs partout dans le monde de mieux appliquer les lois et normes internationales, et les autres mesures de renforcement de la confiance conçues pour améliorer la stabilité du cyberespace tout en respectant les droits de l'homme. Toutes les parties devraient s'appuyer sur les organisations existantes, notamment le Forum mondial sur la Cyber Expertise, qui concentrent leurs efforts sur le développement des capacités, puisqu'il s'agit d'une condition préalable à l'adoption et à la mise en œuvre de normes, à la responsabilité pour violation, à la prise d'autres mesures de stabilité et au respect des droits de l'homme.

4. **Les acteurs étatiques et non-étatiques devraient collecter, partager, examiner et publier des informations relatives aux violations des normes et à l'impact de telles activités.** Bien qu'il se produise des actions qui constitueraient une violation des normes édictées par les Nations

Unies et proposées par la GCSC, leur déclaration tend à être anecdotique plutôt qu'exhaustive. Les organisations, en particulier celles qui sont indépendantes de tout intérêt d'État ou commercial, devraient recueillir et publier systématiquement des informations sur les violations des normes et leur impact. Cela permettrait de catalyser les réponses des acteurs étatiques et non-étatiques aux violations des normes et d'améliorer le respect des normes.

5. **Les acteurs étatiques et non-étatiques devaient établir et soutenir les communautés d'intérêt pour aider à assurer la stabilité du cyberespace.** L'établissement et le soutien des communautés permettront de s'assurer que toutes les parties intéressées, notamment les États, le secteur privé, la communauté technique, le monde universitaire et la société civile remplissent tous leurs responsabilités pour garantir la stabilité du cyberespace. Ces communautés peuvent s'intéresser en particulier, entre autres, à l'interprétation, l'adoption et la mise en œuvre des normes de cybersécurité présentées dans le présent rapport et ailleurs, lorsque les standards en matière de preuve pour l'attribution sont robustes, et lorsque les contrevenants aux normes sont tenus responsables rapidement et efficacement.

6. **La GCSC recommande l'établissement d'un mécanisme permanent un engagement multipartite pour traiter des questions de stabilité, dans lequel les États, le secteur privé (y compris la communauté technique) et la société civile sont suffisamment impliqués et consultés de manière adéquate.** Le principe de responsabilité reconnaît que chacun a un rôle à jouer pour assurer la stabilité du cyberespace et met l'accent sur la nécessité d'approches multipartites. À partir de 2011-17, la Conférence mondiale sur le cyberespace (GCCS) a fourni une plateforme pour un tel engagement, qui a réuni des participants membres de ministères des Affaires étrangères et de la Sécurité chargés d'assurer la stabilité mondiale dans d'autres contextes. Cela a aussi été le moment du lancement du Forum mondial sur la Cyber Expertise, un effort de renforcement des capacités important. Le Forum sur la gouvernance de l'Internet (IGF) a aussi offert une plateforme importante pour les discussions multipartites. Plus récemment, l'Appel de Paris a réuni la plus grande communauté multipartite jamais organisée de soutiens des normes de cybersécurité. Ces efforts suggèrent qu'il est temps de développer une communauté multipartite mondiale, inclusive, orientée vers l'action, consacrée à la mise en œuvre pratique des normes de cybersécurité présentées dans le présent rapport et ailleurs. Ce mécanisme devrait être supporté par une structure permanente pour garantir un effort soutenu et continu.

ANNEXE A : NORMES ADOPTÉES PAR LE GEG DE L'ONU[54]

a. Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États devraient coopérer à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des TIC et à prévenir les pratiques informatiques jugées nocives qui peuvent compromettre la paix et la sécurité internationales ;

b. En cas d'incident informatique, les États devraient examiner toutes les informations utiles, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans cet environnement et la nature et l'ampleur des conséquences de l'incident ;

c. Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications ;

d. Les États devraient réfléchir à la meilleure façon de coopérer pour échanger des informations, s'assister mutuellement, engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies de l'information et des communications et appliquer d'autres mesures collectives afin de parer à ces risques ; à cet égard, les États peuvent être amenés à déterminer si de nouvelles mesures doivent être élaborées ;

e. Les États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression ;

f. Un État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public ;

g. Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des communications, en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions pertinentes ;

h. Les États devraient répondre aux demandes d'aide appropriées formulées parun autre État dont une infrastructure essentielle a été exposée à des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté ;

i. Les États devraient prendre des mesures raisonnables pour garantir l'intégrité de la chaîne logistique, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits informatiques. Les États devraient s'attacher à prévenir la prolifération des techniques et des outils informatiques malveillants et l'utilisation de fonctionnalités cachées malveillantes ;

j. Les États devraient encourager le signalement responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent ;

k. Les États ne devraient pas mener ou soutenir sciemment des activités visant à porter atteinte aux systèmes d'information des équipes d'intervention d'urgence agréées (parfois également appelées équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité informatique) d'un autre État. Un État ne devrait pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des activités internationales malveillantes.

54 Voir Assemblée générale des Nations Unies, *Rapport du Groupe d'experts gouvernementaux sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, A/70/174 (22 juillet 2015), https://undocs.org/fr/A/70/174.

ANNEXE B :
LES NORMES DE LA GCSC

1. NON-INGÉRENCE DANS LE NOYAU PUBLIC

NORME :

Les acteurs étatiques et non-étatiques ne devraient ni mener ni autoriser sciemment des activités qui portent intentionnellement et substantiellement atteinte à la disponibilité générale ou à l'intégrité du coeur public de l'Internet, et donc à la stabilité du cyberespace.

CONTEXTE

Définir le coeur public de l'Internet est difficile, car différents types d'attaques peuvent finir par nuire à la disponibilité ou à l'intégrité générale d'Internet (l'issue à éviter). Cela dit, il existe clairement certains composants qui seraient ciblés pour avoir un tel impact large, et il est au moins possible de fournir une liste non exhaustive de ces éléments critiques. De manière générale, la Commission définit l'expression « disponibilité générale » comme signifiant que le comportement de l'acteur a un impact substantiel sur la population en général. Par conséquent, cette norme reconnaît que les États qui l'appuient peuvent quand même s'engager dans des activités dont l'objectif et la portée sont plus limités, et qui n'ont pas d'impact substantiel sur la population en général.

Pour la Commission l'expression « coeur public de l'Internet » inclut les éléments critiques des infrastructures de l'Internet comme le routage et le transfert de paquets, les systèmes de désignation et de numérotation, les mécanismes de chiffrement de sécurité et d'identité, les supports de transmission, les logiciels et les centres de données.

Les éléments de routage et de transfert de paquets comprennent notamment : (1) l'équipement, les installations, les informations, les protocoles et les systèmes qui facilitent la transmission de communications en paquets de leurs sources vers leurs destinations ; (2) les points d'échange de l'Internet (les sites physiques où la bande passante de l'Internet est produite) ; (3) les routeurs d'appairage et de base des principaux réseaux qui transportent cette bande passante aux utilisateurs ; (4) les systèmes nécessaires pour assurer l'authenticité du routage et défendre le réseau contre les comportements abusifs ; (5) la conception, la production et la chaîne d'approvisionnement des équipements utilisés aux fins susmentionnées ; et (6) l'intégrité des protocoles de routage eux-mêmes et de leurs processus de développement, de normalisation et de maintenance.

Les systèmes de désignation et de numérotation comprennent notamment : (1) les systèmes et les informations utilisés dans le fonctionnement du système de noms de domaine d'Internet (y compris les registres, les serveurs de noms, le contenu de zone, les infrastructures et les processus tels que les DNSSEC utilisés pour signer des dossiers de façon chiffrée) ; (2) les services d'information WHOIS pour la zone racine, la hiérarchie d'adresses inverses, le code pays, les domaines géographiques et internationalisés de premier niveau et pour les nouveaux domaines génériques et non militaires génériques de premier niveau ; (3) les résolveurs DNS récursifs publics fréquemment utilisés ; (4) les systèmes de l'« Internet Assigned Numbers Authority » et des registres régionaux de l'Internet qui rendent disponibles et maintiennent l'attribution unique d'adresses de protocole Internet, de numéros de système autonomes et d'identificateurs de protocole Internet ; et (5) les protocoles de désignation et de numérotation eux-mêmes et l'intégrité des processus de normalisation et des résultats pour l'élaboration et la maintenance des protocoles.

Les mécanismes de chiffrement de sécurité et d'identité comprennent notamment : (1) les clés de chiffrement utilisées pour authentifier les utilisateurs et les appareils et sécuriser les transactions Internet ; (2) l'équipement, les installations, les informations, les protocoles et les systèmes qui permettent la production, la communication, l'utilisation et la dépréciation de ces clés ; (3) les serveurs de clés PGP, les autorités de certification et leur infrastructure à clé publique ; (4) DANE et ses protocoles et infrastructures connexes ; (5) les mécanismes de révocation de certificats et les journaux de transparence ; (6) les gestionnaires de mots de passe ; (7) les authentificateurs d'accès en itinérance ; (8) les mécanismes de temps précis et d'établissement de la priorité temporelle, tels que le protocole de temps de réseau (NTP, Network Time Protocol) et son infrastructure ; (9) l'intégrité des processus de normalisation et des résultats pour l'élaboration et la maintenance d'algorithmes et de protocoles de chiffrement ; et (10) la conception, la production et la chaîne d'approvisionnement de l'équipement utilisé pour mettre en œuvre les processus de chiffrement.

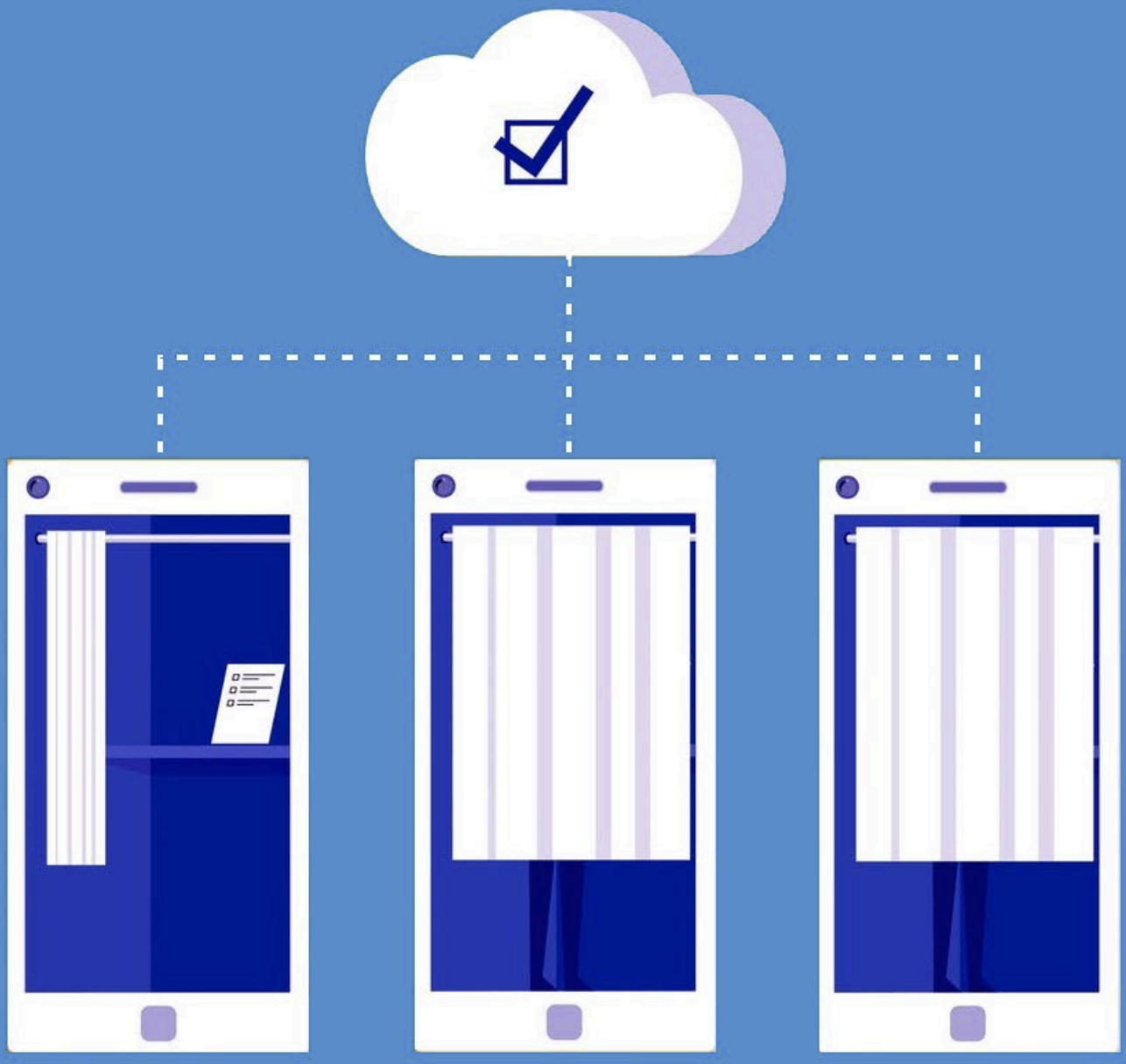
Les supports de transmission comprennent notamment : (1) les infrastructures, les systèmes et les installations de communications desservant le public, par cuivre, fibres optiques ou sans fil ; (2) les câbles terrestres et sous-marins et les stations d'atterrissage, les centres de données et autres installations physiques qui les soutiennent ; (3) les communications vocales et de données cellulaires et autres communications sans fil ; (4) les communications de radiodiffusion réglementées et non réglementées ; (5) les systèmes de soutien pour la transmission, la régénération du signal, l'arborescence, le multiplexage et la discrimination signal-bruit ; et (6) les systèmes de câble qui desservent des régions ou des populations, mais pas ceux qui servent les clients de chaque entreprise individuellement.

Les logiciels comprennent notamment la disponibilité et l'intégrité des processus de développement, du code source et des infrastructures de distribution de correctifs des logiciels utilisés dans le coeur de l'Internet et par une grande partie du public utilisant Internet.

Les centres de données comprennent notamment : (1) les installations physiques qui hébergent les serveurs, le contenu et les infrastructures de l'Internet ; (2) le système utilisé pour assurer la sûreté, la sécurité, le contrôle d'accès physique, les systèmes d'exploitation, de gestion, de maintenance et de redondance des centres de données ; et (3) les systèmes de communication utilisés pour transmettre des communications en provenance, au sein et vers des centres de données.

Les experts estiment que de nombreuses autres catégories d'infrastructures de l'Internet et tributaires de systèmes informatiques méritent une protection, cette définition pourrait donc être élargie à l'avenir.

2. PROTÉGER LES INFRASTRUCTURES ÉLECTORALES



NORME :

Les acteurs étatiques et non-étatiques ne devraient pas poursuivre, soutenir ou permettre des cyber opérations visant à perturber l'infrastructure technique essentielle aux élections, référendums ou plébiscites.

CONTEXTE

De toutes les règles, préceptes et principes qui guident la conduite des États dans le concert des nations, la norme de non-ingérence est peut-être la plus sacrée. L'article 2(4) de la Charte des Nations Unies définit cette norme et lui attribue un statut légal et donc contraignant :

> Les membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies.

Par cette disposition, les auteurs de la Charte ont reconnu que les menaces les plus graves contre le principe de non-intervention provenaient de mesures coercitives visant l'autonomie physique ou politique d'un État, car en fait, les deux sont essentielles à sa souveraineté. Le territoire contrôlé par un État peut être une manifestation de sa capacité souveraine, mais il est sans valeur sans la jouissance de l'autorité politique et de l'indépendance. En outre, rien ne reflète davantage une véritable indépendance politique que des processus nationaux participatifs, comme des élections, organisés librement et équitablement. La Charte des Nations Unies a cherché à accorder des protections solides contre les interférences extérieures indues. Ces mesures de protection sont de nouveau attaquées à l'ère numérique.

Les experts ont débattu de la question de savoir si le type d'interférence électorale liée à la cybercriminalité récemment constaté équivaut à une violation illégale de la souveraineté (parce qu'elle interfère avec l'exercice d'une fonction intrinsèquement gouvernementale) ou à une intervention illégale.[55] Qu'une violation du droit international soit survenue ou non, cependant, il est clairement possible que des acteurs malveillants, agissants seuls, collectivement ou pour le compte d'États, manipulent des élections par des moyens numériques. Les processus nationaux participatifs devenant de plus en plus complexes tant par leur taille que leur sophistication, les données, institutions et infrastructures pour les gérer se sont multipliées. Aujourd'hui, de nombreux pays publient en ligne leurs listes électorales (une garantie traditionnelle fondamentale contre la manipulation ou la fraude électorales), exposant ces bases de données à des cyberattaques et une exploitation via Internet. De même, les instruments de vote électoral sont utilisés dans des régions reculées d'un pays, où ses opérateurs ne sont pas pleinement informés des risques et des problèmes associés à leur manipulation numérique. Les fournisseurs de logiciels de vote et les systèmes informatiques aux niveaux local ou « des kiosques » restent également susceptibles de telles intrusions.

Face aux menaces toujours plus nombreuses et intenses contre les processus participatifs, et reconnaissant que de telles attaques sont inacceptables, la GCSC recommande des mesures nationales et une coopération internationale plus robustes et efficaces pour prévenir, atténuer et réagir aux intrusions cybernétiques contre les infrastructures électorales techniques. La Commission reconnaît que la tenue effective des élections ou des processus participatifs au niveau régional, local ou fédéral est définitivement du ressort des États, et doit se dérouler conformément à leurs lois nationales respectives. Néanmoins, les cyberattaques contre leurs infrastructures électorales peuvent provenir de l'extérieur de leurs frontières, ce qui nécessite une résolution par la coopération multilatérale. À mesure que davantage de pays optent pour la numérisation de leurs systèmes électoraux, les vulnérabilités et les risques associés à ces infrastructures sont multipliés, tout comme la perspective d'une cyberattaque majeure. Les gouvernements doivent donc s'engager à s'abstenir de mener des cyberopérations contre les infrastructures électorales techniques d'un autre État. En recommandant cette norme, la Commission affirme simplement que l'ingérence électorale est intolérable, qu'elle soit considérée comme une violation du droit international ou non.

55 Voir Michael N. Schmitt, « 'Virtual' Dis-enfranchisement: Cyber Election Med-dling in the Grey Zones of International Law », *Chicago Journal of International Law*, Vol. 19, No. 1, et Nicholas Tsagourias, « Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace », https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-princi-ple-of-non-intervention-in-cyberspace/.

3. NORME VISANT À ÉVITER TOUTE MANIPULATION

NORME :

Les acteurs étatiques et non-étatiques ne devraient pas manipuler les produits et services en cours de développement et de production, ni permettre qu'ils soient manipulés, si cela risque de porter atteinte de manière substantielle à la stabilité du cyberespace.

CONTEXTE

Dans une norme consacrée à la « non-ingérence dans le coeur public de l'Internet », la GCSC a appelé les acteurs étatiques et non-étatiques à ne pas nuire intentionnellement et substantiellement à la disponibilité ou à l'intégrité générale du coeur public de l'Internet. À l'appui de cette norme, la Commission a noté la dépendance croissante d'autres infrastructures à l'égard d'un Internet stable et sécurisé, et les conséquences dramatiques potentielles de sa perturbation. Alors que la norme relative au coeur public était consacrée au « coeur de l'Internet », les individus et les organisations dépendent fortement de certains produits commerciaux pour accéder à ce coeur public et tirer parti de la connectivité qu'il fournit. Par conséquent, la manipulation de composants clés de produits logiciels et matériels informatiques (les systèmes d'exploitation, systèmes de contrôle industriels, commutateurs, routeurs et autres équipements de réseau critiques, les produits et normes cryptographiques critiques, la conception de puces et les applications grand public largement utilisées par les utilisateurs finaux, etc.) peuvent également priver la société de la capacité d'utiliser et d'exploiter Internet en toute sécurité, et sapent de manière générale la confiance dans son bon fonctionnement. Bien que de telles attaques soient souvent mentionnées dans les médias, ce qui reçoit moins d'attention est le fait qu'une attaque peut se produire avant même qu'un produit ou sa mise à jour ne soient sur le marché. Par exemple, un produit peut être attaqué en insérant une vulnérabilité, ou en supprimant secrètement une fonction de sécurité, pendant la phase de conception et de fabrication ou pendant l'une de ses mises à jour. En d'autres termes, un produit peut être manipulé avant sa sortie ou sa production, ce qui a des conséquences pour le grand public. Le délai entre l'insertion d'une vulnérabilité et son activation pour une utilisation malveillante peut varier.

Les États ont des intérêts et des responsabilités contradictoires dans la gestion des produits de la technologie de l'information. D'un côté, ils ont l'obligation de promouvoir la résilience et l'intégrité des infrastructures cybernétiques afin de contribuer à contrecarrer les futures cyberattaques d'acteurs malveillants et de rendre l'écosystème numérique dans son ensemble plus sûr. D'autre part, le devoir des États est de protéger la sécurité nationale pour leurs citoyens et de combattre les criminels et autres acteurs malveillants dans le cyberespace. Des États se sont appuyés sur l'exploitation des vulnérabilités des produits et services numériques utilisés par des adversaires pour accomplir leur mission de sécurité nationale et publique. Ainsi, dans la mesure où les États considèrent l'exploitation de vulnérabilités comme une approche efficace pour assumer leurs responsabilités, ils peuvent également trouver utile d'introduire intentionnellement des faiblesses ou des portes dérobées dans des produits et services utilisés par leurs adversaires. Les acteurs non-étatiques peuvent à leur tour également manipuler des produits et services, car leurs objectifs peuvent être facilités par leur capacité à perturber la stabilité du cyberespace. Il est important de noter que cette norme interdit toute manipulation d'une ligne de produits ou services qui mettrait en danger la stabilité du cyberespace. Cette norme n'interdirait pas une action ciblée d'un État qui ne présente que peu de risque pour la stabilité globale du cyberespace ; par exemple, l'interception et la manipulation ciblées d'un nombre limité d'appareils d'utilisateurs finaux afin de faciliter l'espionnage militaire ou les enquêtes criminelles. Ce type d'activité, à moins qu'il ne se produise au sein de l'infrastructure de base du coeur public lui-même, ou qu'il n'affaiblisse de manière critique la confiance des utilisateurs dans Internet mondialement, est peu susceptible d'affaiblir la confiance globale dans le cyberespace qui est une condition de la cyberstabilité. Bien qu'un acteur non-étatique puisse également cibler des systèmes de manière limitée, une telle activité pourrait violer les lois pénales et civiles existantes.

Alors que des acteurs étatiques et non-étatiques ne devraient pas manipuler sciemment des produits en cours de développement ou de production, les acteurs de l'industrie ont également la responsabilité d'empêcher de telles activités. Par conséquent, ceux qui créent des produits et services doivent s'engager à exercer une diligence raisonnable dans la conception, le développement et la livraison de produits et services qui accordent la priorité à la sécurité, et qui réduisent ainsi la probabilité, la fréquence, l'exploitabilité et la gravité des vulnérabilités. Les acteurs concernés doivent également rejeter tout effort apparent, étatique et non-étatique, de compromission des produits et services, et doivent adopter des pratiques qui réduisent le risque de manipulation et leur permettent de réagir si une telle pratique est découverte.

4. NORME VISANT À LUTTER CONTRE LA RÉQUISITION DE DISPOSITIFS TIC DANS DES BOTNETS

NORME :

Les acteurs étatiques et non-étatiques ne devraient pas réquisitionner les ressources TIC du grand public pour les utiliser comme botnets ou à des fins similaires.

CONTEXTE

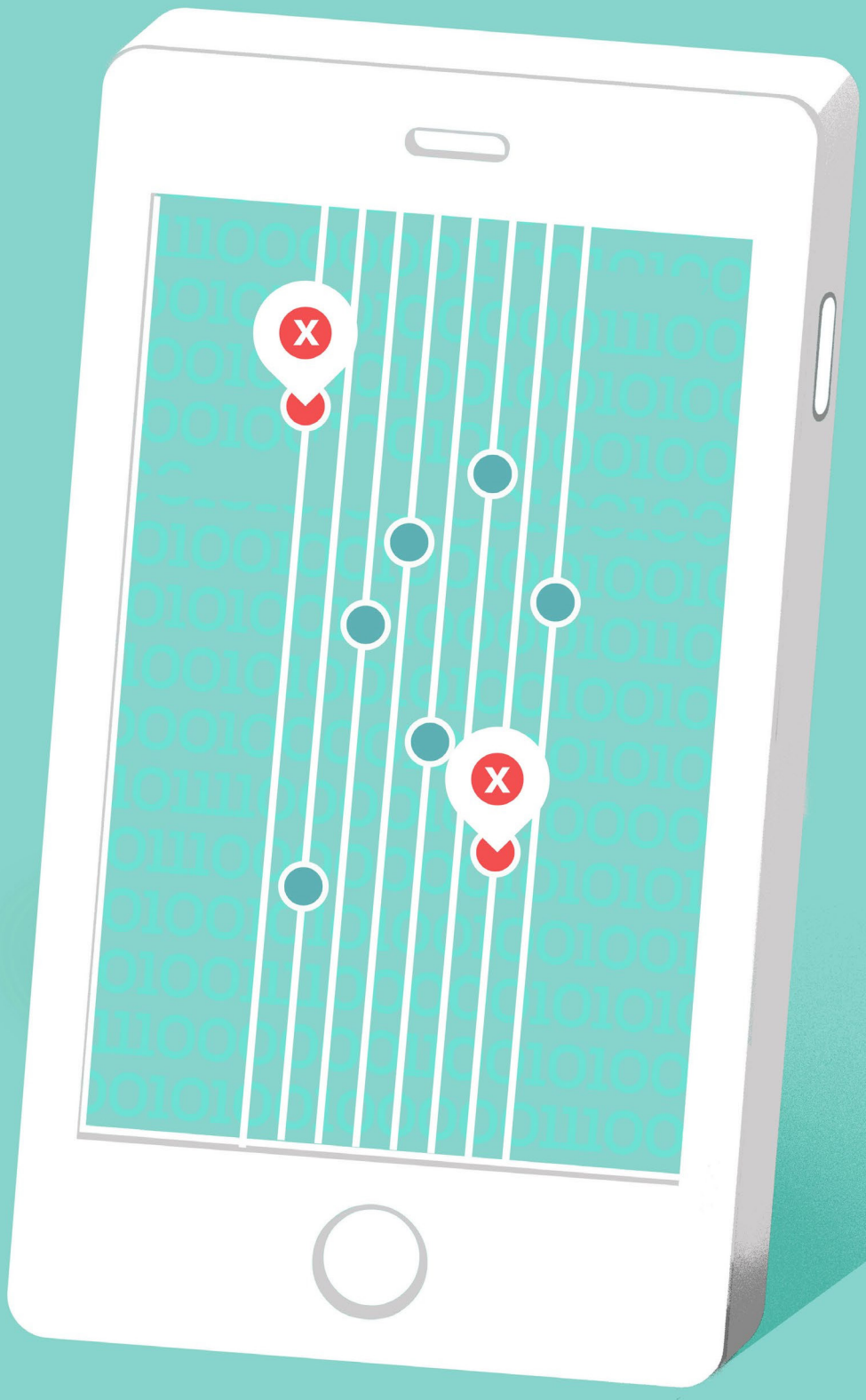
Les appareils connectés à l'Internet font désormais partie intégrante de la vie quotidienne partout dans le monde. Nous sommes entourés d'appareils dotés d'une multitude de capacités de calcul, de mise en réseau, de détection et de déclenchement. Les thermostats, téléviseurs, dispositifs médicaux, réveils et automobiles ont une capacité de calcul, de stockage et d'accès au réseau susceptible d'être appropriée et abusée. L'exploitation des vulnérabilités de leur code sous-jacent peut entraîner des problèmes de sécurité physique pour les personnes utilisant le dispositif : un appareil fonctionnant en dehors de ses paramètres de conception peut prendre feu ou créer d'autres conditions dangereuses, telles que des portes déverrouillées inopinément, une diffusion vidéo depuis l'intérieur du domicile ou la défaillance d'un équipement (médical).

Le terme de botnets est utilisé lorsque des agents logiciels sont installés, en masse et sans consentement, pour utiliser les ressources de calcul, de stockage ou de réseau des appareils. Ces botnets peuvent ensuite servir à avoir des effets directs sur un autre système ciblé, notamment sur la confidentialité, la disponibilité et l'intégrité des données des cibles finales. Par conséquent, un appareil « tiers » potentiellement non impliqué, et son propriétaire/opérateur, sont rendus partis à une cyberactivité malveillante à leur insu. La compromission d'appareils pour installer des agents logiciels malveillants non seulement affaiblit leurs défenses contre d'autres attaques (par exemple contre des criminels) ou perturbe leur fonctionnement normal, mais rend également le propriétaire/l'opérateur potentiellement coupable des dommages infligés à la cible finale. Ceci est particulièrement grave dans les cas où la compromission de l'appareil pourrait par inadvertance faire de l'appareil et de son propriétaire/opérateur un belligérant involontaire dans des hostilités entre États, et par conséquent inviter des représailles ou engager la responsabilité.

Alors que nous devenons de plus en plus dépendants de la technologie dans notre environnement personnel et que toujours plus d'appareils connectés sont introduits sur le marché, l'exploitation d'appareils grand public et leur utilisation comme botnets sapent de plus en plus la confiance et déstabilisent la société. La Commission reconnaît qu'il existe des cas, par exemple pour faire appliquer la loi, dans lesquels des acteurs étatiques autorisés peuvent trouver nécessaire d'installer des agents logiciels sur des appareils d'un adversaire particulier spécifiquement ciblé ou d'un groupe d'adversaires. Toutefois, les acteurs étatiques et non-étatiques ne devraient pas réquisitionner les appareils civils du grand public (en masse) pour faciliter ou exécuter directement des cyberopérations offensives, quels qu'en soient les motifs.[56]

56 Cette norme complète la précédente norme proposée pour les acteurs étatiques et non-étatiques visant à éviter toute manipulation des produits avant leur sortie, qui est consacrée aux aspects de la chaîne d'approvisionnement, tandis que la présente norme concerne des appareils déjà déployés.

5. NORME VISANT À CE QUE LES ÉTATS CRÉENT UN PROCESSUS DE DIVULGATION DES VULNÉRABILITÉS



NORME :

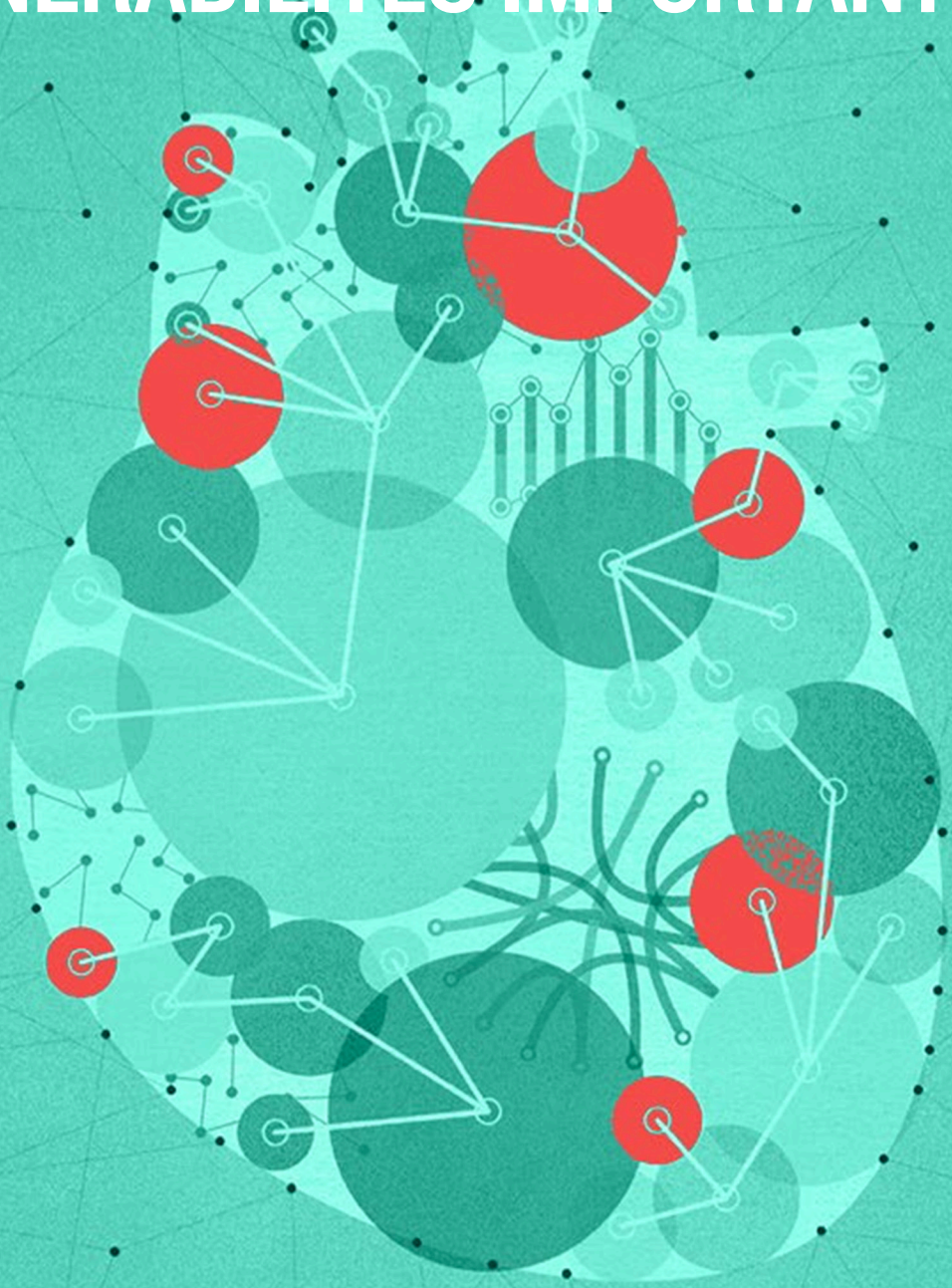
Les acteurs étatiques devraient créer des cadres de procédures transparents pour évaluer s'il convient de divulguer des vulnérabilités ou des défauts dont ils ont connaissance, mais non connus du grand public, dans les systèmes et technologies de l'information, et à quel moment il convient d'en parler. La présomption par défaut devrait favoriser la divulgation.

CONTEXTE

Plus les systèmes d'exploitation, les logiciels critiques et les matériels informatiques deviennent complexes, plus ils contiennent de vulnérabilités. Celles-ci peuvent être exploitées par des acteurs étatiques et non-étatiques. Les États ont quelquefois des intérêts et des responsabilités contradictoires dans la gestion de vulnérabilités nouvellement découvertes. D'un côté, ils ont l'obligation de promouvoir la résilience et l'intégrité des infrastructures essentielles à la stabilité du cyberespace, et en contribuant à contrecarrer les activités cyber malveillantes, de rendre l'écosystème numérique dans son ensemble plus sûr pour tous les utilisateurs. Cela va dans le sens d'une divulgation rapide par un État des vulnérabilités nouvellement découvertes aux fournisseurs et fabricants afin que des correctifs soient appliqués, ainsi que de divulgations à un public plus large au besoin, pour protéger ce dernier. D'autre part, les États ont le devoir de protéger leurs citoyens des criminels, d'enquêter sur la cybercriminalité et d'en poursuivre les coupables, et se réservent le droit d'imposer des sanctions qui servent de moyen de dissuasion spécifique et général à l'égard d'activités malveillantes futures. L'exploitation des vulnérabilités des infrastructures numériques dont ils dépendent est un outil essentiel pour poursuivre les acteurs malveillants, et en particulier les acteurs sophistiqués tels que les États voyous. Les États font donc souvent valoir qu'ils doivent préserver au moins certaines capacités spécifiques, notamment l'utilisation de vulnérabilités non divulguées, sinon des acteurs malveillants extrêmement capables ne pourraient pas être découverts et surveillés.

Bien qu'il soit peu probable que les États divulguent volontairement chaque vulnérabilité qu'ils découvrent, plusieurs États ont récemment évolué dans le sens d'une divulgation plus systématique des vulnérabilités qu'ils connaissent, afin de promouvoir une plus grande cybersécurité systémique. Pour ce faire, les États devraient créer un processus décrit publiquement destiné à évaluer les avantages et les inconvénients d'une divulgation, qui tienne compte de toute une série de considérations politiques, économiques, sociales et techniques. Plus précisément, ce processus devrait être transparent sur le plan de la procédure et devrait tenir compte de tous les points de vue, notamment des facteurs comme la sécurité et la résilience des réseaux, la sécurité des utilisateurs et de leurs données, les besoins policiers et de sécurité nationale, et les implications diplomatiques et commerciales. Les États-Unis ont récemment promulgué une nouvelle version d'un tel processus et d'autres pays envisagent de créer leurs propres politiques de processus de divulgation des vulnérabilités (Vulnerability Equities Process ou VEP). Étant donné que la découverte et la divulgation de vulnérabilités couvrent plus d'un État, afin de promouvoir la résilience des réseaux tout en préservant la sécurité nationale, il serait dans l'intérêt de la stabilité à long terme du cyberespace que chaque État ait un tel processus en place. De plus, les États devraient travailler au développement de processus compatibles et prévisibles. L'existence de tels processus peut servir de mesure de renforcement de la confiance entre États dans le sens où ils fournissent une certaine assurance que les considérations pertinentes et les intérêts contraires sont pleinement pris en compte. Bien sûr, chaque État dispose de capacités différentes et de structures administratives uniques, cependant, un processus VEP efficace devrait être conçu pour tenir compte d'un large ensemble de points de vue et de considérations. De plus, même si les décisions finalement prises dans des cas particuliers pourraient, par nécessité, rester confidentielles, les procédures générales et le cadre permettant de prendre ces décisions devraient être transparents. Finalement, la présente norme traite uniquement de l'établissement d'un processus encadrant les prises de décisions de divulgation. Si un gouvernement ou une autre entité décide de divulguer une vulnérabilité, cette divulgation devrait être effectuée d'une manière responsable, qui améliore la sécurité du public, et ne prête pas à l'exploitation de cette vulnérabilité.

6. NORME VISANT À RÉDUIRE ET À ATTÉNUER LES VULNÉRABILITÉS IMPORTANTES



NORME :

Les développeurs et fournisseurs de produits et services dont dépend la stabilité du cyberespace devraient (1) donner la priorité à la sécurité et à la stabilité, (2) prendre des mesures raisonnables pour s'assurer que leurs produits ou services sont exempts de vulnérabilités importantes, et (3) prendre des mesures pour atténuer en temps utile les vulnérabilités découvertes ultérieurement et être transparents quant à leur processus. Tous les acteurs ont l'obligation de partager les informations concernant les vulnérabilités afin d'aider à prévenir ou atténuer la cyberactivité malveillante.

CONTEXTE

Certains produits ou services informatiques sont essentiels à la stabilité du cyberespace en raison de leur utilisation au sein d'infrastructures techniques fondamentales, comme la résolution de noms et le routage de base, parce qu'ils facilitent de manière générale l'utilisation d'Internet par les utilisateurs ou parce qu'ils sont utilisés au sein d'infrastructures critiques. Ceux qui créent des produits et services doivent s'engager à exercer une diligence raisonnable dans la conception, le développement et la livraison de produits et services qui accordent la priorité à la sécurité, et qui réduisent ainsi la probabilité, la fréquence, l'exploitabilité et la gravité des vulnérabilités.

En raison de la complexité croissante des logiciels et du matériel, ces produits présentent communément certaines vulnérabilités. Bien que celles-ci soient généralement involontaires, des acteurs étatiques et non-étatiques malveillants les exploitent souvent lorsqu'elles sont découvertes de manière à compromettre la stabilité du cyberespace.

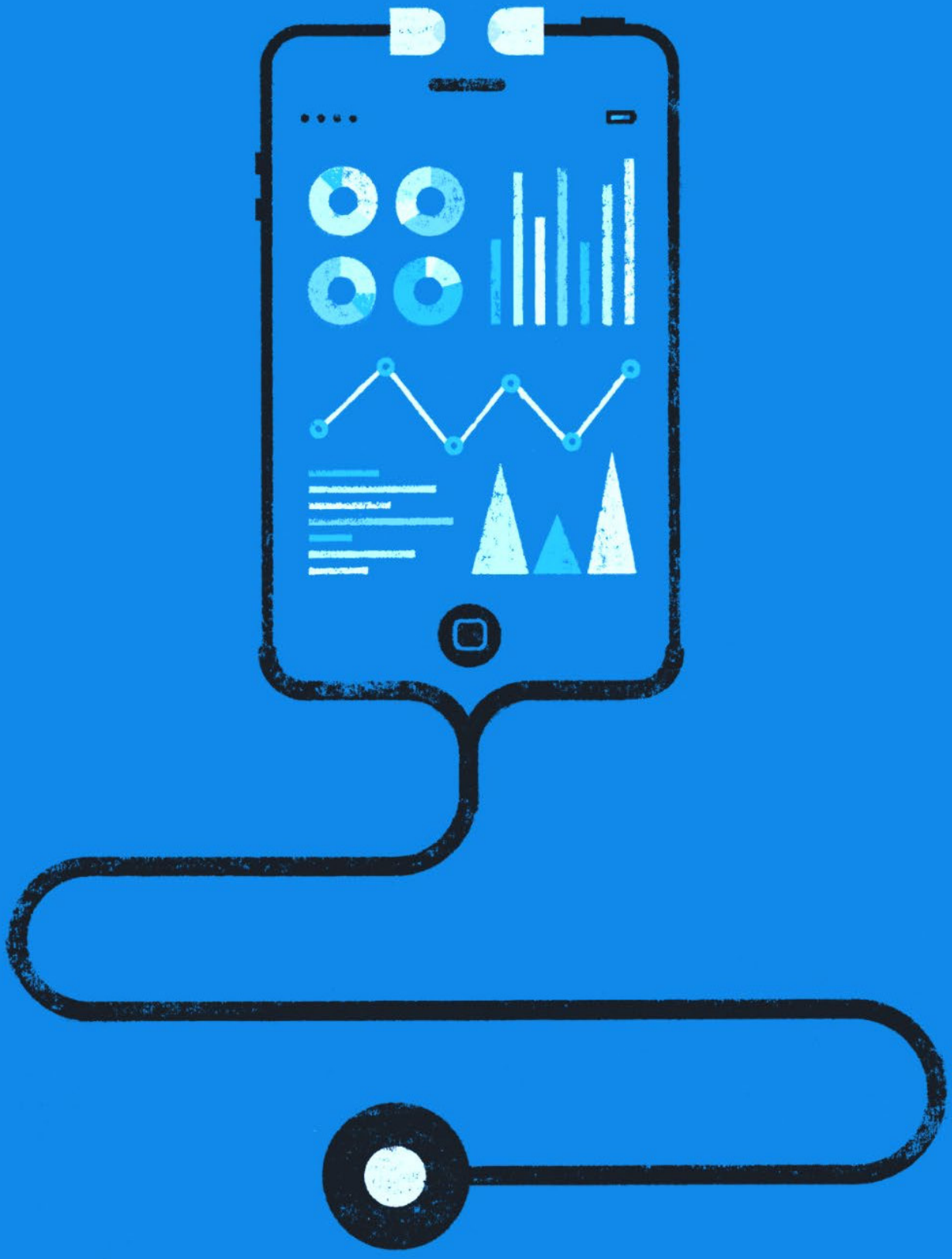
De plus, dans un monde hyperconnecté et hyperdépendant, une vulnérabilité découverte peut affecter plusieurs produits et services de différents producteurs et dans différents environnements. Appliquer des correctifs à un produit sans révéler la vulnérabilité sous-jacente aux autres pourrait protéger ce produit, mais pas la stabilité du cyberespace dans son ensemble. Les acteurs les mieux placés pour évaluer l'impact d'une vulnérabilité donnée sont souvent ceux qui développent, produisent, installent ou opèrent les produits qui sont affectés par ces vulnérabilités. Il est important de partager les informations qui pourraient aider à corriger les vulnérabilités de sécurité ou aider à prévenir, limiter ou atténuer une attaque.[57]

Bien qu'il soit actuellement très difficile de garantir qu'il n'existe aucune vulnérabilité dans les produits commercialisés ou mis à jour récemment, cette norme proposée suggère plutôt que ceux qui participent au développement ou à la production de tels produits devraient prendre des « mesures raisonnables » réduisant la fréquence et la gravité des vulnérabilités qui apparaissent effectivement.

Tout comme la norme de « non-manipulation » traite de l'insertion intentionnelle de vulnérabilités dans des produits et services critiques, et que la norme d'hygiène traite finalement des devoirs des utilisateurs finaux, la présente norme proposée vise à ce que ceux qui développent ou produisent des produits critiques prennent des mesures raisonnables pour s'assurer que le nombre et la portée des vulnérabilités critiques sont minimisés et qu'elles sont atténuées efficacement et rapidement, et au besoin, divulguées lorsqu'elles sont découvertes. Le processus utilisé devrait être transparent pour créer un environnement prévisible et stable.

57 L'une des normes relatives au comportement responsable des États dans le rapport de 2015 du GEG de l'ONU (A/70/174) affirme que « les États devraient encourager le signalemen responsable des failles informatiques et partager les informations correspondantes sur les moyens permettant de les corriger, afin de limiter et éventuellement d'éliminer les risques pour les systèmes qui utilisent les technologies de l'information et des communications et pour les infrastructures qui en dépendent ».

7. LA NORME SUR LA CYBER-HYGIÈNE DE BASE COMME DÉFENSE FONDAMENTALE



NORME :

Les acteurs étatiques devraient adopter des mesures appropriées, y compris des lois et des règlements, pour assurer une cyber-hygiène de base.

CONTEXTE

Plus la connectivité Internet se propage partout dans le monde et touche tous les aspects de la vie moderne, plus les utilisateurs, quel que soit leur type (individus, organisations, entreprises et gouvernements), dépendent de la technologie et de l'accès aux informations disponibles sur Internet. La politique, l'économie, l'information publique, l'éducation, le développement et tous les autres types d'interaction sociale dépendent étroitement de l'Internet et des technologies associées. Néanmoins, cette merveille moderne reste globalement peu sûre, et personne n'échappe à ses dangers.

Il n'existe toujours pas de consensus sur le meilleur moyen d'optimiser les technologies prometteuses du cyberespace tout en protégeant le public. Cependant, il est généralement admis que les avantages de nos vies connectées numériquement ne dureront pas si des normes agréées de sécurité essentielle dans le cyberespace ne sont pas adoptées. À cette fin, la Commission soutient fermement l'adoption généralisée et la mise en œuvre vérifiée d'une cyber-hygiène de base : un régime de mesures fondamentales qui couvre des tâches essentielles classées par priorité à effectuer pour prévenir, atténuer rapidement et se défendre contre les dangers dans le cyberespace.

En effet, étant donné l'étendue de l'interconnectivité en ligne, ces mesures constituent un devoir de vigilance fondamental qui devrait être exigé de tous les utilisateurs. Les régimes d'hygiène devraient incorporer des mesures fiables de mise en œuvre, prévoir un partage généralisé des informations techniques et des meilleures pratiques, et être soumis à une surveillance appropriée. Des appareils et processus de plus en plus intelligents nécessitent des lois et des réglementations bien pensées. En renforçant la responsabilité pour ce devoir de cyber-vigilance fondamentale, les gouvernements ne devraient pas freiner l'innovation ou altérer les propriétés essentielles de l'Internet.

Les normes de cyber-hygiène existent déjà sous diverses formes.[58] Elles sont de mieux en mieux acceptées mondialement, car les gouvernements et les entreprises comprennent de plus en plus l'importance de prendre des mesures éprouvées pour aider à prévenir et à atténuer rapidement les dangers des programmes malveillants connus. De plus, ces normes reflètent les meilleures pratiques, soulignent l'importance d'une surveillance raisonnable régulière, et mettent l'accent sur l'importance de partages d'informations automatisés lorsque c'est possible pour alerter les autres utilisateurs des problèmes. Les cyber-défenses de base décrites dans ces approches tiennent compte du fait qu'aucun gouvernement, groupe d'utilisateurs ou aucune organisation ne peut pallier seul à tous les risques cybernétiques. Elles reconnaissent aussi que les utilisateurs à tous les niveaux ont des rôles importants à jouer pour renforcer la cybersécurité.

La GCSC est convaincue que la défense fondamentale de la cybersécurité par l'adoption généralisée de la cyber-hygiène est devenue essentielle à une utilisation responsable et une croissance bénéfique d'Internet. La sécurité doit être considérée comme un processus continu dont les responsabilités sont partagées entre les acteurs, et disposant de mécanismes, comme les déclarations automatisées et le partage des informations, pour assurer une redevabilité appropriée.

La Commission reconnaît également que de nombreuses sociétés de par le monde font face à des défis considérables dans l'utilisation des technologies de l'information et des communications, et appelle les États à partager leurs connaissances et à offrir de développer des capacités pour exemplifier des processus pour l'application efficace de régimes de cyber-hygiène de base afin d'élargir l'effet de la présente norme.

58 Cela inclut, par exemple, l'Institut européen des normes de télécommunication (ETSI), le *Center for Internet Security* (CIS) à but non lucratif et l'*Australian Signals Directorate* (ASD), entre autres.

8. NORME CONTRE LES CYBER-OPÉRATIONS OFFENSIVES MENÉES PAR DES ACTEURS NON-ÉTATIQUES

NORME :

Les acteurs non-étatiques ne devraient pas s'engager dans des cyber-opérations offensives, et les acteurs étatiques devraient empêcher de telles activités et réagir si elles se produisent.

CONTEXTE

Bien que les technologies de l'information et des communications aient transformé favorablement nos sociétés, elles posent également de nouveaux défis en matière de sécurité. La rapidité et l'omniprésence des cyber-opérations posent souvent des problèmes considérables aux systèmes judiciaires des États et à la coopération policière internationale. Malgré ces difficultés, il ne faut pas oublier que la souveraineté est la pierre angulaire du système international de paix et de sécurité fondé sur des règles. Les États ont le monopole de l'utilisation légitime de la force, dans le cadre strict du droit international. Certains acteurs non-étatiques, principalement des entreprises privées, militent pour le droit de conduire des cyber-opérations offensives au-delà des frontières nationales, prétendant que cela constitue une action défensive nécessaire puisque les États ne sont pas capables de les protéger adéquatement contre les cyber-menaces. Ces cyber-opérations offensives des acteurs non-étatiques sont quelquefois appelées par euphémisme de la « cyber-défense active »[59], notamment ce que l'on appelle le « piratage inverse » (hack back), puisqu'elles sont menées à des fins défensives.

Certains États ne contrôlent pas et peuvent choisir d'ignorer ces pratiques, malgré le risque qu'elles posent pour la stabilité et la sécurité du cyberespace. Cependant, dans de nombreux États, de telles pratiques seraient illégales, et même punies pénalement, alors que dans d'autres États, elles ne semblent ni interdites ni explicitement autorisées. Quelques États envisagent néanmoins de légitimer les cyber-opérations offensives des acteurs non-étatiques. Le fait est que certains ont décidé ou proposé des législations nationales pour permettre des opérations offensives par des acteurs non-étatiques.

La GCSC estime que de telles pratiques fragilisent le cyberespace. Elles peuvent entraîner des perturbations et des dommages graves, notamment pour des tiers, et sont donc susceptibles de déclencher des litiges juridiques complexes et d'aggraver les conflits. Les États qui accorderaient explicitement ou autoriseraient sciemment des acteurs non-étatiques à mener des opérations offensives, pour leur propre compte ou celui de tiers, créeraient un dangereux précédent et risqueraient d'enfreindre le droit international. La Commission estime que les mesures offensives devraient être réservées aux États et rappelle que le droit international établit un cadre strict et exclusif pour les réponses des États aux actes hostiles qui s'appliquent également aux cyber-opérations. De même, dans le cadre du droit international, les acteurs non-étatiques agissant au nom des États doivent être considérés comme leurs agents, et sont donc réputés être des prolongations de l'État.[60]

Si des États permettent de telles actions, ils pourraient donc être tenus responsables en vertu du droit international.[61] Les États doivent agir, au niveau national et international, pour empêcher les cyber-opérations offensives menées par des acteurs non-étatiques.

59 La cyber-défense active doit être entendue comme un ensemble de mesures allant de la légitime défense sur le réseau d'une victime aux activités destructrices sur le réseau d'un attaquant. Les cyber-opérations offensives au sein de ce continuum impliquent que le défenseur agisse en dehors de son propre réseau, indépendamment de son intention (attaque ou défense) et de la qualification juridique de ses actes. Des travaux supplémentaires devraient être menés sur la définition des cyber-opérations offensives et de la cyber-défense active.

60 Voir la « note supplémentaire » pour un traitement plus large de ce cas dans le cadre du droit international, disponible ici : https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Of-fensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf. 61 Id.

ANNEXE C : HISTOIRE, OBJECTIFS ET PROCESSUS DE LA GCSC

Depuis son lancement à la Conférence sur la sécurité de Munich en février 2017 sous le patronage du ministre néerlandais des Affaires étrangères Bert Koenders, la Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace) a été considérée comme l'une des premières initiatives multipartites de ce genre à se concentrer spécifiquement sur la stabilité du cyberespace. Présidée par Michael Chertoff, ancien secrétaire américain à la Sécurité intérieure, Latha Reddy, ancien conseiller adjoint à la sécurité nationale indien et précédemment par Marina Kaljurand, membre du Parlement européen et ancien ministre des Affaires étrangères estonien, la Commission comprend 28 personnalités de régions et d'horizons divers liés à la cybersécurité internationale.[62] Elle est soutenue par des conseillers spéciaux, un Secrétariat, composé du *Centre d'études stratégiques de La Haye* et de l'EastWest Institute, un Groupe consultatif de recherche, ainsi que par des partenaires et sponsors, dont les ministères des Affaires étrangères néerlandais et français, la Cyber Security Agency de Singapour, Microsoft, l'Internet Society et Afilias.

La Commission est née du désir de poursuivre les travaux des précédentes commissions de la société civile, notamment de la Commission mondiale sur la gouvernance de l'Internet, et de s'associer aux travaux de la Conférence mondiale sur le cyberespace (GCCS). En 2015, *le Centre d'études stratégiques de La Haye* (HCSS) a été invité à organiser une session préparatoire de la réunion de La Haye de la GCCS consacrée à la paix et à la sécurité internationales. Une grande partie de la déclaration de la GCCS s'est inspirée directement des travaux de la réunion préparatoire, soulignant clairement la nécessité d'un format multipartite pour discuter des questions de cybersécurité internationale. En conséquence, le HCSS a réuni un groupe central de supporteurs et de bailleurs de fonds (à l'origine Microsoft, l'Internet Society et le ministère des Affaires étrangères des Pays-Bas) et a élaboré un plan stratégique. En août 2016, l'EastWest Institute (EWI) l'ayant rejoint en tant que partenaire du secrétariat, le HCSS a organisé une réunion du Groupe fondateur de la GCSC à la Harvard Kennedy School, qui a rédigé les principales exigences relatives à son fonctionnement, ses membres, sa structure et ses objectifs, ainsi que son énoncé de mission.

Cet énoncé de mission stipule :

> La Commission mondiale sur la stabilité du cyberespace (en anglais Global Commission on the Stability of Cyberspace ou GCSC) développe des propositions de normes et de politiques afin d'améliorer la sécurité et la stabilité sur le plan international et d'encourager le comportement responsable des acteurs étatiques et non-étatiques dans le cyberespace. La GCSC fait appel à l'ensemble des parties prenantes pour développer une compréhension commune, et ses travaux veulent faire progresser la cyberstabilité en soutenant la recherche, l'échange d'informations et le développement des capacités.

Dès ses débuts, la GCSC a été conçue pour influencer les priorités liées à la paix et la sécurité internationales dans le domaine du cyberespace, désignées généralement par le terme « cybersécurité internationale ». Le Groupe fondateur a identifié le besoin de solliciter des points de vue divers, en particulier des communautés techniques et de gouvernance de l'Internet, lors des discussions en cours sur la cybersécurité internationale. L'objectif était d'éclairer les délibérations sur la maîtrise des armements et les communautés sur la paix et la sécurité, dans lesquelles la plupart du bon travail, particulièrement sur les normes, était considéré comme ralenti par l'absence de contribution et d'acceptation des acteurs de la société civile et du secteur privé. C'est donc pour des raisons pratiques plutôt qu'idéologiques qu'une approche multipartite a été considérée.

62 La liste complète des commissaires est présentée à la page 4.

La GCSC a organisé ses délibérations selon une approche « bottom-up to top-down » (ascendante puis descendante). En premier lieu, elle a identifié les normes opérationnelles qui répondent aux besoins les plus urgents en matière de cybersécurité exprimés par ses membres et auxquels il n'a pas été apporté de réponses ailleurs. Deuxièmement, elle a extrapolé à partir de ces normes et des normes existantes une définition de travail de la cyberstabilité et de ses principes. Troisièmement, un cadre de stabilité a été élaboré pour mieux comprendre ce que l'architecture de paix et de sécurité internationales doit accomplir pour répondre à cette définition. Enfin, elle a développé des recommandations à l'intention des parties prenantes étatiques et non-étatiques sur la façon d'y parvenir.

Pour atteindre ces objectifs, les commissaires ont fait participer aux délibérations des parties prenantes de différents groupes et diverses origines géographiques. Dès le départ, la Commission a insisté sur la tenue de ses réunions en marge des conférences pertinentes, afin de faciliter les contributions de nombreuses parties prenantes.[63] Elle a également sollicité activement les contributions des chercheurs et de la communauté dans son ensemble. Pour relier le travail de la GCSC à celui de la communauté universitaire en général, le Groupe consultatif de recherche a été formé, disposant d'un président et de quatre vice-présidents[64] responsables de la gestion d'une liste d'emails de plus de 200 experts. Ce Groupe a aussi été à l'origine d'un vaste programme de recherche, qui a finalement commandité plus de 20 études d'instituts de recherche et de chercheurs du monde entier.[65] La majeure partie de ce travail a été présentée directement aux commissaires lors des « Audiences sur la cyberstabilité » qui lui ont été consacrées.

Avant la publication du présent rapport et des normes publiées précédemment, la Commission a toujours sollicité les contributions d'un large ensemble d'intervenants gouvernementaux, de la société civile et de l'industrie. En échelonnant la livraison pendant toute la durée de la Commission, il a été possible d'inviter constamment des contributions et commentaires extérieurs. Des demandes de consultations en ligne ont été émises sur les normes de la GCSC et la définition de la cyberstabilité. Plus de 23 communications ont été reçues d'acteurs du monde entier, qui ont contribué à éclairer les délibérations des commissaires. De plus, la Commission a activement participé à plus de 70 conférences et événements, et a organisé des tables rondes, des événements secondaires et des audiences sur la cyberstabilité spécifiques réunissant de nombreuses parties prenantes étatiques et non-étatiques.

Enfin, les commissaires eux-mêmes ont maintenu des liens actifs avec leurs propres communautés respectives. Les contributions et commentaires de ces groupes ont constitué le socle des interactions avec la communauté plus large d'experts étatiques et non-étatiques et constitueront le fondement de la promotion du présent rapport à l'avenir.

63 Des réunions officielles des commissaires ont été organisées lors des événements suivants : Conférence sur la sécurité de Munich 2017 (Munich, Allemagne) ; CyCon (Tallinn, Estonie) ; BlackHat USA (Las Vegas, États-Unis) ; Conférence mondiale sur le cyberespace (New Delhi, Inde) ; Forum international sur la cybersécurité FIC 2018 (Lille, France) ; Conférence sur la sécurité de Munich 2018 (Munich, Allemagne – délégation) ; GLOBSEC (Bratislava, Slovaquie) ; Semaine de la cybernétique d'Israël (Tel Aviv, Israël – délégation) ; Semaine de la cybernétique internationale de Singapour (Singapour) ; Forum de la paix et de la gouvernance de l'Internet (IGF) (Paris, France – délégation) ; Institut des Nations Unies pour la recherche sur le désarmement 2019 (Genève, Suisse) ; Forum communautaire ICANN 64 (Kobe, Japon) ; EuroDIG (La Haye, Pays-Bas) ; Réunion annuelle du GFCE (Addis Ababa, Éthiopie).

64 Portant sur quatre domaines, dont la paix et la sécurité internationales, le droit international, la gouvernance de l'Internet et la technologie.

65 Voir la section des remerciements.

REMERCIEMENTS

La Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace ou GCSC) tient à remercier les nombreuses institutions et personnes qui ont soutenu, contribué et facilité le travail de la Commission, notamment ses sponsors, le Groupe consultatif de recherche, les auteurs de documents de recherche et les pairs évaluateurs, ainsi que le personnel de soutien. Quelques-unes des personnes et institutions ayant contribué au succès de la Commission sont mentionnées ci-dessous.

Secrétariat

THE HAGUE CENTRE FOR STRATEGIC STUDIES (HCSS)

Alexander Klimburg, directeur, Global Commission on the Stability of Cyberspace Initiative and Secretariat
Louk Faesen, chef de projet, Global Commission on the Stability of Cyberspace Secretariat
Elliot Mayhew, assistant de projet, Global Commission on the Stability of Cyberspace Secretariat

Avec le soutien supplémentaire de : **Timon Domela Nieuwenhuis Nyegaard**, **Koen van den Dool**, **Niels Renssen et Kaja Karlson**.

EASTWEST INSTITUTE (EWI)

Bruce W. McConnell, co-directeur, Global Commission on the Stability of Cyberspace Secretariat
Anneleen Roggeman, chef de projet, Global Commission on the Stability of Cyberspace Secretariat

Avec le soutien supplémentaire de : **Abagail Lawson**, **Dragan Stojanovski** et **Conrad Jarzebowski**.

Partenaires, sponsors et soutiens

Le Centre d'études stratégiques de La Haye, l'EastWest Institute et les commissaires tiennent à mentionner et à remercier en particulier les organisations suivantes pour leur soutien :

PARTENAIRES :

- **Ministère des Affaires étrangères des Pays-Bas**, **Timo Koster** et **Dimitri Vogelaar**
- **Microsoft**, **Jan Neutze** et **Kaja Ciglic**
- **Agence de cybersécurité de Singapour**, **David Koh** et **Sithuraj Ponraj**
- **Internet Society (ISOC)**
- **Ministère des Affaires étrangères de France**, **Henry Verdier** et **David Martinon**
- **Afilias**, **Ram Mohan** et **Philipp Grabensee**

SPONSORS :

- **Département fédéral des Affaires étrangères de la Suisse**
- **GLOBSEC**
- **Ministère des Affaires étrangères d'Estonie**
- **Ministère des Affaires internes et des communications du Japon**

SOUTIENS :

- **Commission de l'Union africaine**
- **Black Hat USA**
- **DEF CON**
- **Délégation de l'Union européenne aux Nations Unies à Genève**
- **Forum mondial sur la Cyber Expertise**
- **Google**
- **Municipalité de La Haye**
- **Packet Clearing House**
- **Université de Tel Aviv**
- **Institut des Nations Unies pour la recherche sur le désarmement**

Ces organisations et institutions se sont engagées à faire avancer le débat et à proposer des solutions créatives à certains des défis les plus urgents auxquels est confrontée la stabilité du cyberespace.

Chercheurs

La Commission tient à remercier les membres de son Groupe consultatif de recherche, un groupe de plus de 200 membres en ligne qui a relié la GCSC au monde universitaire. En particulier, nous tenons à remercier les chercheurs qui ont été mandatés pour rédiger des exposés et des notes afin d'éclairer les délibérations des commissaires.

DOCUMENT D'INFORMATION N° 1 DE LA GCSC (NOVEMBRE 2017)

Alex Grigsby, ancien membre du Council on Foreign Relations (CFR)
Deborah Housen-Couriel, Konfidas Digital Ltd.
Joanna Kulesza, Université de Lodz et **Rolf H. Weber**, Université de Zürich
Oluwafemi Osho, **Joseph A. Ojeniyi**, et **Shafi'i M. Abdulhamid**, Université fédérale de technologie, Minna
Analía Aspis, Université de Buenos Aires
Robert Morgus, ancien membre de New America, **Max Smeets**, ancien membre du Center for International Security and Cooperation, Université de Stanford et **Trey Herr**, Harvard Kennedy School
Arun Mohan Sukumar, **Madhulika Srikumar** et **Bedavyasa Mohanty**, Observer Research Foundation (ORF)

DOCUMENT D'INFORMATION N° 2 DE LA GCSC (MAI 2018)

Shen Yi, **Jiang Tianjiao** et **Wang Lei**, Centre de recherche pour la gouvernance du cyberespace, Université de Fudan
Elana Broitman, **Mailyn Fidler** et **Robert Morgus**, anciens membres de New America
Elonnai Hickok et **Arindrajit Basu**, Centre for Internet and Society
Thomas Uren, **Bart Hogeveen** et **Fergus Hanson**, Australian Strategic Policy Institute (ASPI)
Dragan Mladenović et **Vladimir Radunović**, DiploFoundation
Thomas Reinhold, Institute for Peace Research and Security Policy, Université de Hamburg

Consultations

La Commission tient à remercier les personnes et les organisations suivantes d'avoir soumis de nombreux commentaires en réponse à la demande de consultations sur le régime de normes de Singapour (du 17 décembre 2018 au 17 janvier 2019) et la définition de la stabilité du cyberespace (du 14 août 2019 au 6 septembre 2019) :

Hussein Abul-Enein, Access Partnership
Kayode Akanni, DesignIT
Jonathan D. Aronson, University of Southern California (USC)
Aviram Atzaba, Direction de la cybernétique nationale d'Israël
Arindrajit Basu, **Gurshabad Grover**, **Elonnai Hickok** et **Karan Saini**, Center for Internet & Society
Vytautas Butrimas, Centre d'excellence pour la sécurité énergétique de l'OTAN
Cybersecurity Tech Accord
Michael Daniel, Cyber Threat Alliance
Global Partners Digital
Arvind Gupta et **Dickey Kumar**, Fondation internationale Vivekananda
Tara Hairston et **Anastasiya Kazakova**, Kaspersky
Sven Herpig, Stiftung Neue Verantwortung
Drew Mitnick, Access Now
George M. Moore, Centre James Martin d'études sur la non-prolifération
Brett van Niekerk et **Trishana Ramluckan**, Université de KwaZulu-Natal
Peter Swire, **Justin Hemmings** et **Sreenidhi Srinivasan**, Georgia Tech Scheller College of Business
Johan de Wit, Siemens/TU Delft

Enfin, la Commission tient à remercier les experts suivants, dont le travail et l'expertise ont guidé et éclairé les délibérations de la Commission :

Dennis Broeders, Université de Leiden
Deborah Brown et **Verónica Ferrari**, Association pour le progrès des communications
Michael Daniel, Cyber Threat Alliance
François Delerue, Institut de Recherche Stratégique de l'École Militaire – IRSEM
Akhil Deo et **Arun Mohan Sukumar**, Observer Research Foundation (ORF)
Martha Finnemore, Université George Washington
Aude Géry, Université de Rouen
Duncan Hollis, Temple Law School
Joanna Kulesza, Université de Lodz
Peter Rowland, Packet Clearing House
Michael Schmitt, Exeter Law School

Patra Kongsirimongkolchai/EyeEm/Getty Images

SECRÉTARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTENAIRES

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

SPONSORS

Département fédéral des Affaires étrangères de Suisse

GLOBSEC

Ministère des Affaires étrangères d'Estonie

Ministère des Affaires internes et des communications du Japon

SOUTIENS

Commission de l'Union africaine

Black Hat USA

DEF CON

Délégation de l'Union européenne des Nations Unies à Genève

Forum Mondial sur la Cyber Expertise

Google

Municipalité de La Haye

Packet Clearing House

Université de Tel Aviv

Institut des Nations Unies pour la recherche sur le désarmement