Fragmentation de l'Internet et cybersécurité : Une introduction

Samuele Dominioni

Résumé des points clés

- La promotion d'un environnement des TIC ouvert, sûr, stable, accessible et pacifique est un objectif récurrent dans les processus multilatéraux relatifs à la sécurité internationale et à la sécurité des TIC au sein des Nations Unies. Le GTCNL lui-même représente une étape importante dans la coopération internationale vers un tel environnement des TIC.
- L'Internet reste stable, généralement ouvert et sûr dans ses fondements. Cependant, la fragmentation de l'Internet est un phénomène croissant et préoccupant. La fragmentation peut être comprise de différentes manières selon la nature des parties prenantes. Néanmoins, il est possible d'en identifier une dimension technique. Dans ce cas, la fragmentation peut affecter des composants essentiels de l'Internet qui garantissent l'interopérabilité des réseaux et des dispositifs.
- La dimension technique de la fragmentation de l'Internet comporte trois grands domaines de préoccupation, à savoir l'adressage, le nommage et le routage. Certaines de ces préoccupations concernent des innovations nécessaires que la communauté multipartite a dû élaborer pour répondre à l'utilisation croissante des technologies TIC mais qui ne sont pas encore totalement mises en œuvre (par exemple, IPv4 et IPv6) ; d'autres concernent des tendances émergentes dans le développement de composants techniques critiques qui divergent des normes et protocoles internationaux actuels (par exemple, dans le système de noms de domaine) ; et enfin, d'autres font référence à des défauts techniques ou à des limitations dans la conception et le développement de composants critiques de l'Internet (par exemple, le routage).
- Ces zones de fragmentation nuisent non seulement à l'ouverture, à la stabilité et à l'accessibilité de l'Internet mondial, mais ont également des répercussions sur la cybersécurité. Certaines d'entre elles concernent la cybersécurité des normes et des protocoles eux-mêmes (par exemple, les protocoles de routage), qui peuvent être affectés par un large éventail d'activités malveillantes liées aux TIC. D'autres font référence à l'accessibilité, à la disponibilité et à la sécurité des données menacées (par exemple, les systèmes de noms alternatifs). Globalement, en raison de la complexité et de l'interdépendance de la structure de l'Internet, la fragmentation de la dimension technique peut entraîner des risques complexes et multiformes (les « problèmes pernicieux ») pour la cybersécurité.
- Les recherches futures porteront sur la manière dont les risques et les tendances identifiés dans cette introduction pourraient avoir un impact sur la mise en œuvre du cadre pour un comportement responsable des États dans le cyberespace, et donc sur la paix et la sécurité internationales.

Introduction

La promotion d'un environnement des TIC ouvert, sûr, stable, accessible et pacifique est un objectif récurrent dans les processus multilatéraux relatifs à la sécurité internationale et à la sécurité des TIC au sein des Nations Unies. Par exemple, le rapport final du Groupe d'experts gouvernementaux (GEG) 2021 sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale affirme qu'"un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies numériques est

essentiel pour toutes et tous et nécessite une coopération efficace entre les États afin de réduire les risques pour la paix et la sécurité internationales».[1] Le rapport final du groupe de travail à composition non limitée (GTCNL) sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale a rappelé que « La création du Groupe de travail est une étape importante en matière de coopération internationale en vue de l'instauration d'un environnement numérique ouvert, sûr, stable, accessible et pacifique».[2] En outre, les deux rapports soulignent l'importance de protéger l'infrastructure technique essentielle à la disponibilité générale et à l'intégrité d'Internet.[3] La résolution de l'Assemblée générale qui a créé l'actuel GTCNL (2021-2025) a confirmé « la conclusion à laquelle est parvenu le Groupe d'experts gouvernementaux dans ses rapports de 2013 et 2015, à savoir que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique».[4] Cependant, la fragmentation de l'environnement des TIC, et plus particulièrement de l'Internet, est devenue une menace de plus en plus préoccupante, qui se manifeste déjà dans certains contextes. En effet, la fragmentation de l'Internet peut avoir des effets à différents niveaux, parfois imbriqués, notamment politique, commercial et technologique.[5] Un nombre croissant d'États et d'autres acteurs s'inquiètent d'un scénario de fragmentation de l'Internet. Le document du Secrétaire général, Notre Programme commun, mentionne la prévention de la fragmentation de l'Internet comme une action à envisager, et cette question figure parmi les principaux thèmes à inclure dans le prochain Pacte numérique mondial.

La présente introduction est le premier résultat d'un projet plus large sur la fragmentation de l'Internet et la sécurité internationale. Elle vise à présenter le sujet de la fragmentation de l'Internet et à souligner les principaux défis qui peuvent être posés à la cybersécurité au sens large. Sur la base de ce premier résultat, la deuxième partie du projet de recherche examinera l'impact de la fragmentation de l'Internet sur la sécurité internationale et, en particulier, sur la mise en œuvre du cadre de comportement responsable des États dans le cyberespace (ci-après dénommé « le cadre »). Cette introduction est destinée à fournir aux décideurs politiques, aux diplomates et autres acteurs non techniques intéressés une vue d'ensemble de l'évolution de la fragmentation de l'Internet et de ses implications en matière de cybersécurité. Les informations présentées ici proviennent de sources accessibles au public, d'entretiens avec des experts (menés entre septembre et novembre 2023) et de dialogues multipartites avec des intervenants du secteur privé, du monde universitaire et de la société civile, qui se sont tenus en ligne le 17 octobre 2023.

Définition de la fragmentation de l'Internet

La fragmentation de l'Internet est un concept contesté qui peut donner lieu à différentes interprétations selon la nature de la partie prenante. Néanmoins, selon certaines études, il est possible d'identifier une tendance dans la compréhension tripartite de la fragmentation de l'Internet, qui peut se référer à la fragmentation technique, commerciale et gouvernementale.[6] D'autres conçoivent la fragmentation tripartite selon une approche légèrement

[1] Assemblée générale, 2021, A/76/135, https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135.
[2] Assemblée générale, 2021, A/75/816, https://undocs.org/Home/Mobile?FinalSymbol=A%2F75%2F816.
[3] Selon le rapport 2021 du GGE, « à la disponibilité générale ou à l'intégrité de l'Internet ». Voir Assemblée générale, 2021, A/76/135, par. 10.
[4] Assemblée générale, 2020, A/RES/75/240, https://docs.un.org/en/A/Res/75/240
[5] William J. Drake, Vinton G. Cerf et Wolfgang Kleinwächter, 2016, « Internet Fragmentation: An Overview » (Fragmentation de l'Internet : aperçu), Future of the Internet Initiative White Paper, Forum économique mondial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.
[6] Ibid.

différente.[7] Étant donné que cette introduction se concentre sur l'impact de la fragmentation de l'Internet sur la cybersécurité, l'analyse est axée sur la dimension technique.[8]

Selon un livre blanc du Forum économique mondial (FEM) sur la fragmentation de l'Internet, la fragmentation technique survient lorsqu'il existe « des conditions dans l'infrastructure sous-jacente [c'est-à-dire les couches de l'Internet] qui empêchent les systèmes d'interopérer pleinement et d'échanger des paquets de données et l'Internet de fonctionner de manière cohérente à tous les points d'extrémité ».[9] L'encadré 1 donne un bref aperçu des couches de l'Internet et de leurs fonctions.

Encadré 1 : les couches de l'Internet.

Les modèles OSI (Open System Interconnection) et TCP/IP (Transmission Control Protocol/Internet Protocol) comptent parmi les méthodes les plus utilisées pour classer la structure en couches de l'Internet. Ces modèles sont généralement représentés sous la forme d'une pile verticale. Chaque couche est chargée de fonctions différentes mais interconnectées qui transforment un élément d'information (par exemple, une requête textuelle dans un navigateur) en paquets de données afin de rendre possible la communication entre deux (ou plusieurs) dispositifs.

Le **modèle OSI** comprend sept couches : application, présentation, session, transport, réseau, liaison de données et physique.

1. La **couche application** fournit des services aux applications réseau qui utilisent l'Internet, tels que les navigateurs, le courrier électronique et les applications de télécommunication.
2. Au niveau de la **couche présentation**, les informations provenant de la couche d'application sont formatées pour être affichées (en cas de réception) ou pour être traitées ultérieurement (en cas d'envoi).
3. Les processus d'authentification et d'autorisation se déroulent au niveau de la **couche session**. Par exemple, l'authentification (c'est-à-dire la connexion à une application) établit la connexion entre l'utilisateur et le serveur d'application, initiant ainsi une session.
4. La **couche transport** assure la fiabilité de la communication entre les dispositifs et les réseaux. Deux protocoles principaux permettent ce « transport » : le TCP (Transmission Control Protocol) et l'UDP (User Datagram Protocol). Le premier protocole est utilisé pour établir des connexions qui transfèrent de manière fiable des informations entre les dispositifs, mais il peut être lent. Le second, l'UDP, est utilisé pour les connexions qui nécessitent une plus grande vitesse mais moins de précision dans le transfert des données (par exemple, les vidéos en continu).
5. La **couche réseau** facilite la transmission des données entre les dispositifs de différents réseaux. L'une des fonctions de cette couche est l'adressage logique, qui associe l'adresse IP de chaque utilisateur au paquet de données pour s'assurer qu'il atteindra la bonne destination. Ces données sont ensuite transmises d'un réseau à l'autre par l'intermédiaire de routeurs. Cette couche utilise la détermination du chemin pour trouver le meilleur chemin possible pour l'acheminement des données.
6. La **couche liaison de données** aide à préparer les informations à envoyer entre différents réseaux et tente d'éviter les erreurs qui peuvent se produire en transit dans la couche suivante.
7. Dans la dernière couche du modèle OSI, la **couche physique**, les données sont converties en code binaire qui est à son tour transformé en signaux à transmettre sur les supports locaux (ou l'inverse en cas de réception de paquets), qui constituent la connexion physique entre les dispositifs (par exemple, le fil de cuivre, la fibre optique ou l'air pour les signaux radio).

[7] Par exemple, le document de discussion du FGI concernant le réseau de politiques sur la fragmentation de l'Internet (PNIF, pour Policy Network on Internet Fragmentation) adopte les dimensions suivantes : fragmentation de l'expérience de l'utilisateur, fragmentation de la couche technique de l'Internet et fragmentation de la gouvernance et de la coordination de l'Internet ; PNIF, 2023, document de discussion sur le PNIF (contribution au FGI 2023), 15 septembre, https://www.intgovforum.org/en/filedepot_download/256/26218.

[8] Les effets de la fragmentation politique et commerciale sur la cybersécurité seront examinés dans de futures publications.

[9] William J. Drake, Vinton G. Cerf et Wolfgang Kleinwächter, 2016, « Internet Fragmentation: An Overview » (Fragmentation de l'Internet : aperçu), Future of the Internet Initiative White Paper, Forum économique mondial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p. 14.

Le **TCP/IP** est similaire au modèle OSI mais il synthétise les couches application, présentation et session du modèle OSI en une seule couche, appelée la couche application dans le modèle TCP/IP. Les autres couches portent le même nom que celles du modèle OSI, à savoir transport, réseau, liaison de données et physique.

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Application
(interaction personne-machine)</td><td rowspan="3">Application
(présentation des données, encodage et contrôle des sessions)</td></tr>
<tr><td>Présentation
(représentation des données et chiffrement)</td></tr>
<tr><td>Session
(communication entre hôtes)</td></tr>
<tr><td>Transport
(TCP et UDP)</td><td>Transport
(TCP et UDP)</td></tr>
<tr><td>Réseau
(routage et adresses IP)</td><td>Réseau
(routage et adresses IP)</td></tr>
<tr><td>Liaison de données
(récupération des erreurs et retransmission)</td><td>Liaison de données
(récupération des erreurs et retransmission)</td></tr>
<tr><td>Physique
(envoi des données par voie électronique, optique ou par ondes radio)</td><td>Physique
(envoi des données par voie électronique, optique ou par ondes radio)</td></tr>
</table>

En fait, l'Internet peut fonctionner comme un bien public ouvert et mondial grâce à plusieurs infrastructures et propriétés qui permettent la communication et l'échange d'informations (sous forme de paquets de données) indépendamment de l'endroit où l'on se trouve, de qui l'on est et des dispositifs à travers lesquels on se connecte à l'Internet. Parmi ces éléments, certains sont essentiels pour garantir l'interopérabilité des réseaux et des dispositifs (voir encadré 2).

Encadré 2 : les composants essentiels de l'Internet.

Les initiatives suivantes ont contribué à mettre en évidence les composants essentiels de l'Internet.

La Commission mondiale sur la stabilité du cyberespace a élaboré le concept de « noyau public » de l'Internet, qui comprend les éléments suivants :

1. Routage et transfert de paquets
2. Systèmes de dénomination et de numérotation
3. Mécanismes cryptographiques de la sécurité et de l'identité
4. Supports de transmission
5. Logiciels
6. Centres de données[10]

L'Internet Society a proposé cinq propriétés critiques qui définissent les fonctions essentielles des réseaux

[10] Commission mondiale sur la stabilité du cyberespace, « Advancing Cyberstability » (Faire progresser la cyberstabilité), novembre 2019, https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

Internet :

1. Une infrastructure accessible avec un protocole commun ouvert et des barrières mineures à l'entrée.
2. Une architecture ouverte de modules interopérables et réutilisables basée sur des processus de développement aux normes ouvertes volontairement adoptées par une communauté d'utilisateurs.
3. Une gestion décentralisée et un système de routage distribué unique, évolutif et souple.
4. Des identifiants globaux communs, sans ambiguïté et universels.
5. Un réseau généraliste, neutre sur le plan technologique, simple et adaptable.[11]

Le document de discussion du Forum sur la gouvernance de l'Internet concernant le réseau de politiques sur la fragmentation de l'Internet (PNIF) affirme que la fragmentation de l'infrastructure technique de l'Internet est liée à « une série de défis posés à cette interopérabilité au niveau de la couche technique de transport qui permet à l'Internet de fonctionner ».[12] En effet, l'Internet mondial est « fondamentalement ancré dans la conception de la couche de transport de l'Internet et l'utilisation commune des mêmes protocoles techniques (TCP/IP, DNS, BGP, HTTP, IPv4&6, etc.), sur la base d'un système de serveurs racine unifié mais décentralisé pour tous les types de communication sur l'Internet ».[13] Par conséquent, en raison des caractéristiques essentielles relatives aux composants critiques de l'Internet, les actions visant à fragmenter cette dimension technique constitueraient une menace très sérieuse pour son ouverture et son interopérabilité.

Domaines exposés au risque de fragmentation technique de l'Internet

La fragmentation technique est une préoccupation récurrente, en particulier pour la communauté multipartite qui gère les composants essentiels de l'Internet. Le livre blanc du FEM sur la fragmentation de l'Internet, publié en 2016, affirme que « l'Internet reste stable et généralement ouvert et sûr dans ses fondements ».[14] Près de huit ans plus tard, une période très courte à l'échelle d'une technologie, ces fondations restent solides, même si elles présentent des fragilités et des risques croissants.[15] Dans un souci de cohérence avec la littérature existante et, en particulier, avec le livre blanc du FEM, le présent document utilise les mêmes domaines de risque, à savoir l'adressage, le nommage (le système de noms de domaine) et le routage (l'interconnexion) de l'Internet,[16] pour déterminer les tendances actuelles qui affaiblissent les fondements de l'Internet.

[11] Internet Society, « The Internet Way of Networking: Defining the Critical Properties of the Internet » (Le réseau selon l'Internet : définir les propriétés essentielles de l'Internet), septembre 2020, https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/.
[12] PNIF, 2023, document de discussion sur le PNIF (contribution au FGI 2023), 15 septembre, https://www.intgovforum.org/en/filedepot_download/256/26218, p. 12.
[13] Wolfgang Kleinwächter et Alexander Klimburg, 2023, « Fragment or Not Fragment – Is This the Question? Will the "One World-One Internet" Survive Today's Geopolitical Stress Test » (Fragmenter ou ne pas fragmenter - telle est la question ? Le projet "Un monde, un Internet" survivra-t-il au test de résistance géopolitique d'aujourd'hui ?), CircleID, 6 juin, https://circleid.com/posts/20230606-fragment-or-not-fragment-is-this-the-question-will-one-world-one-internet-survive-todays-geopolitical-stress-tests.
[14] William J. Drake, Vinton G. Cerf et Wolfgang Kleinwächter, 2016, « Internet Fragmentation: An Overview » (Fragmentation de l'Internet : aperçu), Future of the Internet Initiative White Paper, Forum économique mondial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p. 8.
[15] Entretien de l'auteur avec M. Vinton G. Cerf, l'un des auteurs du Livre blanc du FEM sur la fragmentation de l'Internet, 26 octobre 2023.
[16] Une façon simple de comprendre l'adressage, le nommage et le routage est de considérer ces termes ainsi : « le nom d'une ressource indique ce que nous cherchons, une adresse indique où elle se trouve et un itinéraire nous indique comment y arriver » ; John F. Schoch, 1978, « A Note on Inter-Network Naming, Addressing, and Routing » (Note sur le nommage, l'adressage et le routage inter-réseaux), Internet Experiment Note # 19, Notebook Section 2.3.3.5, https://www.rfc-editor.org/ien/ien19.txt.

Adressage

L'adressage concerne les identificateurs uniques, également appelés adresses IP, exprimés en valeurs décimales, qui désignent des points uniques sur l'Internet. Les deux principaux problèmes concernent les adresses IP et la fragmentation. Le premier concerne l'adoption et la compatibilité de deux versions d'IP (IPv4 et IPv6), et le second concerne la gestion des numéros IP.

Il existe actuellement deux versions principales d'adresses IP : IPv4 et IPv6. La première est composée d'un espace d'adressage de 32 bits et peut générer jusqu'à environ 4,3 milliards d'adresses. En raison de l'augmentation considérable du nombre de points d'extrémité (par exemple, les dispositifs) sur l'Internet au cours des dernières décennies, l'IPv4 a maintenant épuisé ses combinaisons possibles. Par conséquent, pour répondre à ce besoin de nouveaux identifiants uniques, une nouvelle version de l'IP (IPv6) avec un espace d'adressage de 128 bits a été introduite. IPv6 peut couvrir jusqu'à 340 billions de billions de billions de points d'extrémité.[17] Cependant, IPv4 et IPv6 ne sont pas directement interopérables. Cela signifie que les dispositifs des réseaux IPv4 ne peuvent pas communiquer avec les dispositifs des réseaux IPv6.[18] La compatibilité n'est possible que grâce à des technologies de transition, telles que les réseaux à double pile. La fragmentation peut se produire en cas de divergences dans les versions IP non prises en charge par les technologies de transition entre les différents pays et les régions du monde. Le niveau d'adoption de l'IPv6 augmente régulièrement[19] avec des variations entre les pays.

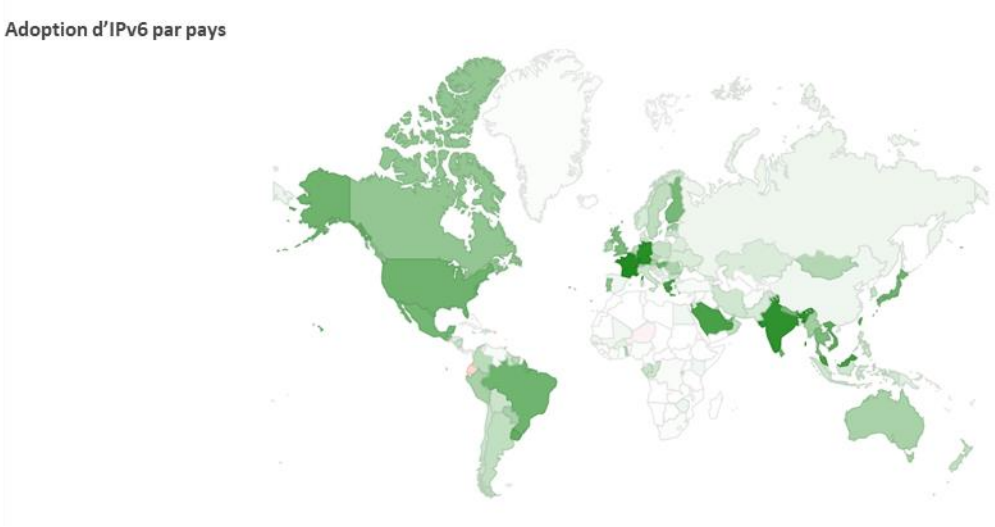

Figure 1 : adoption d'IPv6 par pays : plus la couleur est foncée, plus la connectivité IPv6 est développée (source : Google Statistics)

Par conséquent, la fragmentation résultant de cette dimension de la fracture numérique est possible et présente des risques pour l'interopérabilité globale des réseaux et des dispositifs entre les pays et les régions.

Le deuxième aspect de la fragmentation IP concerne la gestion des numéros IP utilisés pour les adresses IP. Dans l'état actuel de l'Internet, cette tâche est gérée par l'IANA (Internet Assigned Number Authority), une filiale de l'ICANN (Internet Corporation for Assigned Names and Numbers), ainsi que par les registres Internet régionaux (RIR), et elle est mise en œuvre dans de vastes régions, car les structures de l'Internet ne sont pas contenues dans

[17] William J. Drake, Vinton G. Cerf et Wolfgang Kleinwächter, 2016, « Internet Fragmentation: An Overview » (Fragmentation de l'Internet : aperçu), Future of the Internet Initiative White Paper, Forum économique mondial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[18] Erik Bais, « IPv4 vs IPv6: What Security Professionals Should Know » (IPv4 ou IPv6 : ce que les professionnels de la sécurité doivent savoir), Prefix Broker, https://www.prefixbroker.com/news/ipv4-vs-ipv6-what-security-professionals-should-know/.

[19] Au moment de la publication du livre blanc du FEM, la connectivité IPv6 ne représentait que 4 % de l'Internet, alors qu'en octobre 2023, elle en couvre environ 40 % (source https://www.google.com/intl/en/ipv6/statistics.html).

les frontières nationales. Il est essentiel de disposer d'un système responsable du caractère unique des adresses IP au niveau mondial ; dans le cas contraire, il existerait un risque de création d'adresses IP alternatives et non coordonnées qui compliqueraient, voire rendraient impossible, la compatibilité avec l'infrastructure IPv4 ou IPv6 déjà déployée.[20]

Nommage

Le nommage fait référence au système de noms de domaine (DNS), qui traduit les noms en adresses IP (par exemple, pour le site web de l'UNIDIR, le DNS est https://unidir.org et l'adresse IP correspondante est 34.107.109.130). Pour garantir cette fonctionnalité, il est essentiel que la gestion de cette tâche unique de cartographie et d'appariement (effectuée par l'ICANN) reste stable, cohérente et légitime. Les tentatives de mise en place de systèmes de noms alternatifs (y compris la gestion de la zone racine[21]) constitueraient l'une des pires formes possibles de fragmentation[22], car les correspondances DNS uniques seraient perdues. Il en résulterait des incohérences et des erreurs potentielles de recherche DNS ; par exemple, différents utilisateurs tapant https://unidir.org pourraient ouvrir d'autres pages que celle prévue.

Routage

Le routage fait référence aux protocoles utilisés pour s'assurer que les informations suivent le chemin correct et optimal lorsqu'elles transitent par un réseau. Lorsque des informations doivent circuler d'un réseau à l'autre (l'Internet est composé de nombreux réseaux différents, souvent gérés individuellement par un seul fournisseur de services), les protocoles BGP (Border Gateway Protocols) servent à les connecter, permettant ainsi le système de routage global de l'Internet. Comme le souligne le livre blanc du FEM, « il est encore techniquement possible de corrompre délibérément ou accidentellement les données de routage ».[23] La sécurité du système de routage doit encore être améliorée, par exemple en mettant en œuvre ce que l'on appelle la Resource Public Key Infrastructure (RPKI), un cadre d'infrastructure à clés publiques conçu pour sécuriser le Border Gateway Protocol.[24] Globalement, si le BGP n'est pas convenablement protégé, une fragmentation peut survenir en raison de l'incapacité du réseau à garantir la confidentialité, l'intégrité et la disponibilité des données.

Domaines de préoccupation concernant la cybersécurité

L'objectif de cette introduction est non seulement de comprendre la fragmentation de l'Internet et son état actuel, mais aussi d'en identifier les implications possibles en matière de cybersécurité. La présente introduction aborde la cybersécurité d'un point de vue très général, en s'appuyant sur ce que l'on appelle la triade de la cybersécurité[25] et l'authenticité. D'une manière générale, la fragmentation de l'Internet peut entraîner des risques multiples pour la

[20] Voir, par exemple, le débat autour de la proposition de « nouvelles IP » : Alain Durand, 2020, « New IP » (Nouvelles IP), ICANN Office of the Chief Technology Officer, https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf.

[21] La zone racine désigne le premier niveau de la hiérarchie DNS (par exemple, dans https://unidir.org, le premier niveau est « .org »).

[22] Dialogue multipartite sur la fragmentation de l'Internet et la cybersécurité, 17 octobre 2023 ; William J. Drake, Vinton G. Cerf, et Wolfgang Kleinwächter, 2016, « Internet Fragmentation: An Overview » (Fragmentation de l'Internet : aperçu), Future of the Internet Initiative White Paper, Forum économique mondial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[23] Ibid., p. 23.

[24] Entretien de l'auteur avec M. Vinton G. Cerf, l'un des auteurs du Livre blanc, 26 octobre 2023.

[25] La triade se concentre sur la sécurité des données et fait référence à leur confidentialité, leur disponibilité et leur intégrité. La disponibilité fait référence au fait que les données doivent être disponibles pour les utilisateurs autorisés chaque fois qu'ils en ont besoin ; tout événement susceptible de retarder leur accès affecte la disponibilité des données. La confidentialité concerne l'accessibilité des données ; seuls les utilisateurs autorisés doivent avoir accès à des données spécifiques, qui doivent par ailleurs rester secrètes ou privées. L'intégrité concerne l'authenticité, la fiabilité et la crédibilité des données ; cela signifie que les données ne doivent pas être altérées. Voir Samuele Dominioni et Giacomo Persi Paoli, 2022, « A Taxonomy of Malicious ICT Incidents » (Taxonomie des incidents malveillants touchant les TIC), UNIDIR, https://unidir.org/publication/a-taxonomy-of-malicious-ict-incidents/.

cybersécurité, qui peuvent englober ce que l'on appelle les « problèmes pernicieux ». Ces problèmes se posent en particulier dans les domaines composites, interconnectés et multipartites (par exemple, l'Internet) et peuvent être extrêmement complexes et multiformes.[26] Une approche multipartite, qui inclut une collaboration entre différents acteurs, secteurs et pays, est souvent nécessaire pour faire face à des problèmes pernicieux (voir tableau 1).[27] Par conséquent, « un Internet fragmenté empêche toute possibilité de s'attaquer à la cybersécurité parce qu'il fait abstraction des nombreux facteurs interdépendants et ferme les portes à toute collaboration potentielle ».[28] En outre, la fragmentation de l'Internet en réseaux plus petits peut entraîner une réduction de la résilience globale des réseaux. En effet, la force de l'Internet réside dans le fait qu'il est décentralisé et qu'il repose sur des composants interopérables (normes et protocoles, dispositifs, etc.), ce qui permet à la communauté technique, en cas de besoin, de résoudre les problèmes sans compromettre l'ensemble du réseau.[29]

Type	Caractéristiques	Piste de solution
Simple	Les solutions, ou les approches de conception des solutions, sont connues	*Coopération* : sensibilisation et partage d'informations, généralement par l'intermédiaire de groupes d'opérateurs de réseaux
Complexe	Il n'existe pas de solution connue ; le problème s'étend à plusieurs parties de l'Internet	*Consensus* : élaboration de normes ouvertes et consensuelles
Pernicieux	Aucune solution n'existe dans aucun domaine ; absence générale d'accord sur l'existence ou la caractérisation du problème	*Collaboration* : dépasser les limites des domaines et des organisations existants et mettre en place des processus pour déterminer les problèmes et les solutions

Tableau 1 : Types de problèmes [source Leslie Daigle, Konstantinos Komaitis et Phil Roberts « Keys to Successful Collaboration and Solving Wicked Problems » (Les clés d'une collaboration réussie et de la résolution des problèmes pernicieux), Internet Society, 2016]

Les rubriques suivantes mettent en évidence les problèmes de sécurité liés à chacun des domaines de fragmentation identifiés.

Adressage

La fragmentation de l'adressage a deux conséquences principales sur la cybersécurité. Premièrement, l'adoption dispersée d'IPv6 dans le monde peut non seulement favoriser la fragmentation en raison de l'incompatibilité directe des deux modèles IP, mais aussi des incohérences dans les différents niveaux d'exposition aux menaces liées aux TIC. L'IPv6 présente des caractéristiques clés, notamment l'intégration du protocole IPsec (Internet Protocol Security),[30], qui offrirait une sécurité accrue.[31] Toutefois, la mise en œuvre et la configuration d'IPv6

[26] La plupart des incidents malveillants touchant les TIC ont un caractère transfrontalier et impliquent de multiples actifs et acteurs de différents secteurs et de différentes provenances géographiques.

[27] Leslie Daigle, Konstantinos Komaitis et Phil Roberts, 2016, « Keys to Successful Collaboration and Solving Wicked Internet Problems » (Les clés d'une collaboration réussie et de la résolution des problèmes pernicieux touchant l'Internet), Internet Society, https://www.internetsociety.org/resources/doc/2017/keys-to-successful-collaboration-and-solving-wicked-internet-problems/.

[28] Konstantinos Komaitis, 2023, « Internet Fragmentation: Why It Matters for Europe » (Fragmentation de l'Internet : ses enjeux pour l'Europe), Research in Focus, EU Cyber Direct – EU Cyber Diplomacy Initiative, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/ioyLip9O/internet-fragmentation-why-it-matters-for-europe.pdf, p. 8.

[29] Entretien de l'auteur avec Konstantinos Komaitis, 9 novembre 2023.

[30] IPSec est une norme qui assure la sécurité des canaux au niveau de la couche Internet. IPSec est obligatoire pour IPv6, alors qu'il était facultatif pour IPv4. Voir Internet Engineering Task Force (IETF), 2011, « IPv6 Node Requirements, Request for Comment 6434 » (Exigences relatives aux nœuds IPv6, appel à commentaires 6434), https://www.rfc-editor.org/rfc/pdfrfc/rfc6434.txt.pdf.

peuvent être plus difficiles que celles d'IPv4 et requièrent des connaissances et des compétences techniques spécifiques. Les erreurs de configuration des dispositifs compatibles avec IPv6 peuvent introduire des vulnérabilités et, par conséquent, les rendre plus vulnérables à la compromission.[32] En outre, les dispositifs et les réseaux à double pile (c'est-à-dire qui utilisent simultanément les protocoles IPv4 et IPv6) peuvent poser des problèmes de sécurité supplémentaires en raison de l'augmentation de la surface d'attaque.[33]

Deuxièmement, le développement improbable, mais possible, d'IP nationales sans coordination ou en opposition avec le système existant perturberait gravement à la fois l'accessibilité mondiale et la sécurité des réseaux nationaux. En effet, dans ce cas, les États devraient s'efforcer d'établir des accords bilatéraux avec les fournisseurs de services Internet et de garantir des normes et des protocoles de sécurité pour leurs propres réseaux. Tous les États ne disposent pas des mêmes capacités pour atteindre le même niveau de sécurité. Actuellement, chaque État peut compter sur une communauté multipartite ouverte dédiée à l'élaboration, à la discussion et à la mise à jour de normes et de protocoles pour tous.

Nommage

La fragmentation au niveau du nommage, qui intervient principalement à travers le développement de systèmes de nommage alternatifs, entraînerait d'énormes défaillances au niveau de la cybersécurité. Dans ce scénario, par exemple, lorsque l'utilisateur taperait le nom d'un site web, il pourrait ne pas réussir à atteindre le site voulu ou se retrouver sur un site différent. De manière générale, dans le cas de systèmes de noms alternatifs, les utilisateurs ne seraient pas en mesure d'accéder aux données, qui, à leur tour, deviendraient indisponibles. En outre, les efforts entrepris par la communauté des parties prenantes pour relier le DNS à des systèmes de noms alternatifs peuvent conduire à « des résultats imprévisibles, à la frustration des utilisateurs, à l'augmentation des coûts d'assistance et, finalement, à un Internet moins sûr et moins stable ».[34]

Routage

Les protocoles frontaliers sont vulnérables aux piratages qui peuvent altérer les flux de données. En effet, le protocole BGP dispose de mécanismes internes limités pour se protéger contre les actes malveillants qui modifient ou même suppriment des données et, par conséquent, perturbent le comportement global du réseau en matière de routage.[35] En effet, le BGP est susceptible de faire l'objet de menaces graves et diverses concernant les TIC, notamment le détournement de routage,[36] qui peut entraîner une fragmentation de l'internet et des effets perturbateurs ou d'exploitation.[37] La plupart du temps, ces effets ont un impact et une portée limités ; cependant,

---

[31] Emre Durda et Ali Buldu, 2010, « IPV4/IPV6 Security and Threat Comparisons » (Comparaison des menaces et de la sécurité des protocoles IPV4/IPV6), *Procedia—Social and Behavioral Sciences* 2, www.sciencedirect.com/science/article/pii/S187704281000902X, p. 5 285-5 291.

[32] National Security Agency, 2023, « IPV6 Security Guidance » (Lignes directrices sur la sécurité du protocole IPV6), U/OO/105622-23 | PP-22-1805 , v. 1.0, https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF.

[33] Ibid.

[34] Alain Durand, 2022, « Challenges with Alternative Name Systems » (Défis posés par les systèmes de noms alternatifs), OCTO-034, ICANN, https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf.

[35] IETF, 2006, RFC#4272, « BGP Security Vulnerabilities Analysis » (Analyse des vulnérabilités de la sécurité BGP), https://datatracker.ietf.org/doc/html/rfc4272.

[36] Ce scénario se produit lorsque les pirates détournent délibérément le trafic Internet en annonçant faussement une adresse IP, ce qui conduit en fait le trafic vers une autre adresse. En d'autres termes, « le détournement BGP est un peu comme si quelqu'un changeait tous les panneaux sur un tronçon d'autoroute et redirigeait le trafic automobile vers des sorties incorrectes » ; Cloudflare, « What is BGP Hijacking » (Qu'est-ce que le détournement BGP), https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/.

[37] Chaque cyberincident produit un effet sur une cible, et il existe deux grands types d'effets principaux : l'effet perturbateur, qui consiste à interférer avec le fonctionnement des TIC, et l'effet d'exploitation, qui consiste à voler des informations. Voir Samuele Dominioni et Giacomo Persi Paoli, 2022, « A Taxonomy of Malicious ICT Incidents » (Taxonomie des incidents malveillants touchant les TIC), UNIDIR, https://unidir.org/files/2022-08/UNIDIR_Taxonomy_of_Malicious_ICT_Incidents.pdf ;

dans d'autres cas, ils peuvent entraîner une défaillance dévastatrice des communications.[38] La mise en œuvre de la RPKI peut constituer une mesure de cybersécurité efficace.

Conclusion et prochaines étapes

L'Internet reste stable, généralement ouvert et sûr dans ses fondements. Cependant, les fragilités et les risques s'accroissent à tous les niveaux. La fragmentation technique de l'Internet pourrait briser un environnement des TIC ouvert, sûr, stable, accessible et pacifique, ce qui aurait des répercussions considérables sur la cybersécurité.

Des tendances inquiétantes se dessinent et mettent en évidence une augmentation possible des pratiques et des politiques visant à s'opposer aux normes et aux protocoles internationaux essentiellement techniques, ce qui pose plusieurs défis en matière de cybersécurité. Par conséquent, toute tentative arbitraire et unilatérale d'altération des composants critiques de l'Internet risque d'aggraver la fragmentation déjà en cours et d'appauvrir la sécurité globale du réseau des réseaux et au-delà. En effet, la fragmentation de l'Internet pourrait avoir des implications non seulement pour la cybersécurité, mais aussi pour la sécurité internationale. Les recherches futures porteront sur la manière dont les risques et les tendances identifiés dans cette introduction pourraient avoir un impact sur la mise en œuvre du cadre, et donc sur la paix et la sécurité internationales.

Enfin, pour garantir un environnement des TIC ouvert, sûr, stable, accessible et pacifique, la communauté multipartite, y compris les États Membres de l'ONU, devrait envisager de protéger l'intégrité, la disponibilité et l'interconnexion des composants essentiels de l'Internet. Pour ce faire, il est essentiel d'évaluer les interdépendances de ces composants et les effets d'entraînement qu'une altération de ces systèmes complexes et interconnectés entraînerait pour ce bien commun mondial créé par l'être humain. Cette introduction est un effort dans ce sens.

Charles Harry et Nancy Gallagher, 2018, « Classifying Cyber Events » (Classification des cyberévénements), *Journal of Information Warfare*, vol. 17, no. 3, https://www.jstor.org/stable/26633163, p. 17-31.

[38] « Par exemple, des applications critiques telles que les services bancaires en ligne, les transactions boursières et la télémédecine fonctionnent sur Internet » ; Kevin Butler et al. 2010, « A Survey of BGP Security Issues and Solutions » (Enquête sur les problèmes de sécurité BGP et leurs solutions), *Proceedings of the IEEE*, Vol. 98, No. 1, https://ieeexplore.ieee.org/abstract/document/5357585, p. 100-122.

Remerciements

L'ensemble des activités de l'UNIDIR reposent sur le soutien apporté par les principaux bailleurs de fonds de l'Institut. Cette publication a été financée par l'Union européenne dans le cadre du programme Sécurité et technologie de l'UNIDIR, soutenu par les gouvernements de l'Allemagne, de l'Italie, des Pays-Bas, de la République tchèque et de la Suisse, ainsi que par Microsoft. L'auteur tient à remercier les divers experts issus de l'industrie, des administrations publiques et du monde universitaire qui ont fourni un retour d'information important sur les différentes versions et sections du présent document et qui ont participé à l'atelier multipartite, notamment Ang Benjamin, Jaya Baloo, Vinton Cerf, Alain Durand, Marie Humeau, Konstantinos Komaitis, Allison Mankin, Kevin Reifsteck, Rob Spiger, Bill Woodcock et Michael Zappa. Elia Smith, professionnelle diplômée du programme « Sécurité et technologie », a contribué au projet de recherche.

À propos de l'UNIDIR

L'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) est un institut autonome financé par des contributions volontaires, au sein des Nations Unies. L'UNIDIR est l'un des rares instituts politiques du monde à se concentrer sur le désarmement. Il génère des connaissances et encourage le dialogue et l'action en matière de désarmement et de sécurité. Basé à Genève, l'UNIDIR aide la communauté internationale à développer les idées pratiques et innovantes nécessaires pour trouver des solutions aux problèmes de sécurité les plus graves.

Pour citer cette publication

S. Dominioni. Fragmentation de l'Internet et sécurité internationale. Explorer les implications en matière de cybersécurité. Genève, Suisse : UNIDIR, 2023.

Remarque

Les désignations employées dans la présente publication et la présentation des données qui y figurent n'impliquent, de la part du Secrétariat de l'Organisation des Nations Unies, aucune prise de position quant au statut juridique de tel ou tel pays, territoire, ville ou zone, ou de ses autorités, ni quant au tracé de ses frontières ou limites. Les points de vue exprimés dans la présente publication n'engagent que leur auteur. Ils ne reflètent pas nécessairement ceux de l'Organisation des Nations Unies ni ceux de l'UNIDIR, de l'Union européenne, de leur personnel ou des organismes qui lui apportent leur concours.