Comprendre la sécurité et la résilience de l'Internet

La cybersécurité est un terme général plutôt vague, utilisé dans différents contextes pour signifier différentes choses tel que « sécurité des systèmes d'information et des systèmes informatiques » ; sécurité de l'infrastructure de l'Internet ; sécurité de tout ce qui touche à l'Internet (y compris les « services essentiels » tels que la distribution d'électricité) ; sécurité des données ; applications et communications ; sécurité des utilisateurs de l'Internet (en particulier les enfants), qui englobe souvent les notions de sécurité « nationale » ainsi que sécurité « privée ». En fait, il n'existe pas de consensus sur ce que signifie le terme.

Sans chercher à mieux définir le terme « cybersécurité » ni à proposer de solutions pour tous les aspects que pourrait englober son champ d'application, cet article explore les éléments essentiels à la sécurité et la résilience de l'écosystème de l'Internet (fondement de toute stratégie de cybersécurité saine). Ces éléments sont les suivants : des solutions techniques et politiques alignées avec les invariants de l'Internet ; la responsabilité individuelle et collective pour le risque ; et la collaboration.

Les invariants de l'Internet

> *L'Internet a connu d'immenses changements depuis sa création et continue d'évoluer. Il est important de comprendre ce qui est réellement immuable concernant l'Internet – les principales propriétés, ou invariants, « qui ont permis à Internet de servir de plate-forme à une innovation qui paraît sans limite, décrivent non seulement sa technologie, mais aussi sa forme en termes d'impact mondial et de structures sociales »1."*

Toute stratégie pour aborder la cybersécurité doit commencer par une compréhension des propriétés fondamentales de l'Internet qui font vraiment de ce moyen de communication mondial ce qu'il est - un outil pour la créativité, la collaboration, l'ingéniosité, l'expression des idées, l'identité culturelle et sociale, l'activité commerciale, etc. Nous décrivons ces propriétés fondamentales comme les « **invariants de l'Internet** » car le succès continu et généralisé de l'Internet dépend de la durabilité de ces propriétés.

Les deux premières propriétés sont **la portée mondiale et l'intégrité**.

L'Internet est mondial car n'importe quel point de terminaison qui y est connecté peut communiquer avec n'importe quel autre point de terminaison. Un point de terminaison peut

être un ordinateur portable, un smartphone, un système de navigation automobile avec accès Internet, etc.

L'intégrité de l'Internet signifie qu'un point de terminaison reçoit l'information qui lui était destinée par l'expéditeur, quel que soit l'endroit où le destinataire se connecte à Internet. Peu importe la localisation d'un utilisateur, il doit recevoir le même contenu Web en accédant à la page d'accueil de l'Internet Society **www.internetsociety.org**. Bien sûr, un utilisateur peut décider de limiter le contenu qu'il reçoit sur son appareil (par exemple, en utilisant un plug-in de navigateur (Ghostery, par ex.) pour bloquer des éléments de suivi tels que des étiquettes, web bugs, pixels et balises qui sont inclus dans les pages web pour observer le comportement des utilisateurs en ligne ainsi que les sites Web qu'ils visitent). Cela n'affecte pas l'intégrité de la communication. Toutefois, si un Fournisseur d'accès Internet (FAI) devait bloquer l'accès d'un utilisateur au site **www.internetsociety.org**, ceci porterait atteinte à l'intégrité de l'Internet parce que l'information est détournée ou abandonnée par le FAI avant d'atteindre le point de terminaison. Concrètement, cette mesure n'est pas prise par un point de terminaison, mais plutôt par un intermédiaire dans le réseau.

La troisième propriété clé est le **soutien à l'innovation sans besoin d'autorisation**. Autrement dit, c'est la possibilité pour quiconque de créer une nouvelle application sur Internet sans avoir à obtenir une autorisation spéciale de quiconque. L'histoire de l'Internet contient de nombreux exemples de technologies et services extraordinaires rendus possibles grâce à la possibilité de pouvoir introduire librement une nouvelle application ou un service sans demander l'autorisation du gouvernement, du FAI ou de qui que ce soit. L'exemple le plus connu est peut-être le langage HTML (HyperText Markup Language), qui a donné naissance au World Wide Web. Il a été développé par un chercheur au CERN, en Suisse, et mis à la disposition d'autres personnes. Si Tim Berners-Lee avait dû demander une autorisation, le World Wide Web existerait-il ? L'idée de fournir des liens vers des données aurait-elle été rejetée, interrompant le développement de services de recherche sur Internet tels que Google ? Est-ce que Facebook aurait un milliard d'utilisateurs actifs par mois2 ? Les services de visualisation et de collecte de données à externalisation ouverte tels que Ushahidi3 existeraient-ils ? Que dire de Wikipedia, Twitter, YouTube, des applications, des logiciels de cartographie, de la musique en continu et des centaines d'autres choses que nous tenons pour acquises dans notre vie quotidienne ?

La quatrième propriété est **l'ouverture** – développé librement et accessible à tous. L'Internet repose sur des normes techniques qui sont développées ouvertement par consensus et ensuite libérées aux fins de leur utilisation dans le monde entier. Parmi ces normes, nous pouvons citer HTTP (pour accéder à du contenu Web), SMTP (pour le courriel), SIP et RTP (pour les communications vocales et audio).

Une cinquième propriété que nous devons préserver est l'**accessibilité de l'Internet**. Cela va au-delà de la possibilité d'accéder à des informations et des services en ligne. Cela s'étend à la capacité à : contribuer au contenu ; interagir avec les autres dans le monde entier ; ajouter une « app » ou un service ; rattacher un serveur ou un nouveau réseau tout en respectant les normes techniques de l'Internet.

La sixième propriété essentielle que nous devons sauvegarder est l'**esprit de collaboration** de l'Internet. En abordant les problèmes de sécurité sur Internet, nous devons trouver un moyen d'obtenir l'implication de toutes les parties prenantes - les utilisateurs, la communauté de chercheurs concernant l'Internet, les sociétés commerciales, les décideurs et au-delà. Les solutions développées isolément soit ne permettent pas de résoudre le problème ou causent plus de mal que de bien. Dans certains cas, elles peuvent même créer des problèmes importants nuisant à la stabilité de l'Internet.

La complexité du paysage sécuritaire

> *Atteindre les objectifs de sécurité, tout en préservant les propriétés clés de l'Internet, est un équilibre délicat et le vrai défi d'une stratégie de cybersécurité. Il est essentiel que les solutions soient compatibles avec les invariants de l'Internet.*

Satisfaire aux exigences de sécurité au sein d'un système d'exploitation fermé dans un contexte de contraintes est relativement facile et, dans de nombreux cas, une simple stratégie de « sécurité par l'obscurité » (qui repose sur la non-divulgation d'information relative à la conception du système) peut bien fonctionner. En revanche, sécuriser un système ouvert, comme l'Internet, présente plusieurs défis différents.

Premièrement, les mêmes propriétés de l'Internet qui sous-tendent son succès et sa valeur pour les utilisateurs, ouvrent de nouvelles possibilités pour différents types d'activités malveillantes. Par exemple :

- L'Internet est accessible.
    - Mais, cela signifie qu'il est également accessible pour les attaques et intrusions.
- L'Internet est en plein essor en raison de l'innovation sans besoin d'autorisation.
    - Mais, cela permet également le développement et le déploiement de logiciels malveillants de différents types.
- Nous apprécions la portée mondiale de l'Internet.
    - Mais, en termes de cybersécurité, cela signifie que la cybercriminalité transfrontalière peut être plus facile à commettre et que les attaques pourraient avoir des effets de grande portée.
- Les normes de l'Internet sont délibérées, tout comme leur adoption. Elles sont le fruit de la collaboration - la collaboration qui fait partie intégrante du fonctionnement de l'Internet.
- Mais, en même temps, il est difficile d'attribuer la responsabilité et prescrire des solutions.

En abordant les questions de cybersécurité, il est important de noter que tandis que les acteurs malveillants exploitent la moindre occasion, les invariants d'Internet eux-mêmes ne sont ni l'origine ni la cause de l'activité malveillante. L'atteinte des objectifs de sécurité, tout en préservant ces propriétés, est un équilibre délicat et le vrai défi de la stratégie de cybersécurité. Cela signifie que la conception et la mise en œuvre de solutions de sécurité devraient être entreprises en tenant compte de l'effet potentiel

qu'elles pourraient avoir sur les propriétés fondamentales de l'Internet. Comme indiqué plus haut, il est important que les solutions de sécurité soient basées sur, ou au moins compatibles avec, les invariants de l'Internet pour assurer le succès continu de l'Internet comme moteur de prospérité économique et sociale.

Éléments constitutifs de la technologie en matière de sécurité

En matière de technologie, la communauté technique de l'Internet a la réputation de développer de telles solutions (parmi lesquelles les protocoles techniques et les technologies, ainsi que les meilleures pratiques opérationnelles) et de les mettre à la disposition du monde entier pour aider à construire un Internet plus fiable et sécurisé. Ces solutions sont développées dans différents organismes de normalisation et des forums, de manière ouverte, en collaboration et par consensus.

Parmi quelques exemples de normes techniques développées par l'Internet Engineering Task Force (IETF) pour améliorer la sécurité de l'infrastructure de l'Internet, on peut citer :

- IPsec (Internet Protocol Security) - assure à la couche Internet la sécurité de bout en bout
- TLS (Transport Layer Security) - assure la sécurité des communications sur Internet et est largement utilisé, par exemple, pour sécuriser des communications Web
- Système d'authentification réseau Kerberos - fournit un moyen de vérifier l'identité des entités sur un réseau ouvert (non protégé)
- DNSSEC (extensions de sécurité du système de noms de domaine) - assurer l'intégrité et l'authenticité des réponses DNS
- DANE (authentification d'entités nommées basée sur les DNS) - tirer profit du DNSSEC pour permettre aux administrateurs d'un nom de domaine de spécifier les clés utilisées afin d'établir une connexion sécurisée cryptographiquement à un serveur portant ce nom.

Parmi quelques exemples de travaux portant sur les normes techniques en cours de développement et examen au World Wide Web Consortium (W3C) pour améliorer la sécurité du Web et de l'Internet, on peut citer :

- Politique de sécurité de contenu
- Partage des ressources cross-origin
- Signature XML, chiffrement XML et spécifications connexes
- API cryptographiques pour JavaScript

Parmi les exemples de normes de sécurité des données de l'OASIS (Organization for the Advancement of Structured Information Standards) figurent :

- Services de signature numérique (DSS) - normes de services de signature numérique pour XML
- Protocole d'interopérabilité de gestion des clés de cryptographie (KMIP) - fournit des fonctionnalités étendues aux technologies de clés cryptées asymétriques
- Security Assertion Markup Language (SAML) - structure basée sur XML pour la création et l'échange d'informations en matière de sécurité entre partenaires en ligne
- eXtensible Access Control Markup Language (XACML) - représenter et évaluer les politiques de contrôle d'accès

Deuxièmement, il n'y a pas de sécurité absolue. Il y aura toujours des menaces et des vulnérabilités, donc le terme « sécurisé » signifie simplement que les risques résiduels sont acceptables dans un contexte spécifique. Voilà pourquoi la « résilience » est un indicateur important lors de la définition de l'objectif des efforts en matière de cybersécurité. Comme un corps humain qui peut souffrir de virus, mais devient plus fort et plus résistant par la suite, les nouvelles technologies, solutions et efforts de collaboration rendent l'Internet plus résistant aux activités malveillantes.

Culture de responsabilité partagée et collective en matière de risque

> *Un degré élevé d'interconnexion et d'interdépendance dans l'écosystème de l'Internet crée une nouvelle condition importante pour assurer la sécurité effective : gérer les risques « intérieurs » et « extérieurs » en collaboration.*

Les approches traditionnelles de sécurité traitaient principalement des menaces internes et externes, et de leur éventuel impact sur les actifs. Il y a, cependant, une reconnaissance croissante qu'un paradigme de sécurité pour l'écosystème de l'Internet doit être fondé sur la protection des opportunités de prospérité économique et sociale, par opposition à un modèle basé simplement sur la prévention des dommages perçus. En outre, la sécurité doit être abordée sous l'angle de la gestion des risques - une approche qui tient compte des menaces et des vulnérabilités ainsi que de leur probabilité et impact.

L'Internet, avec son haut degré d'interconnexion et de dépendances, apporte une autre dimension à l'évaluation des risques. La sécurité et la résilience de l'Internet dépendent non seulement de la façon dont les risques pour une organisation et ses actifs sont gérés, mais aussi et surtout, de la reconnaissance et la gestion des risques que l'organisation elle-même (par son action ou son inaction) présente à l'écosystème de l'Internet - les risques « extérieurs ». Par exemple : l'existence et le mauvais entretien des soi- disant « résolveurs DNS ouverts » qui sont couramment utilisés comme réflecteurs pour les attaques DDoS 4 ; les politiques et pratiques de sécurité médiocres qui permettent à des ordinateurs compromis de rejoindre les réseaux zombies à long terme ; une autorité de certification (CA) PKI avec une protection insuffisante et une capacité de détection de violation de la sécurité inappropriée conduisant à un compromis et une annonce tardive d'un incident de sécurité 5.

Cet aspect particulier de la gestion des risques n'est pas forcément évident, surtout étant donné qu'il n'y a souvent aucun préjudice immédiat à l'organisation ou à ses actifs clairement identifiable et, par conséquent, aucune analyse de rentabilisation directe pouvant être immédiatement associée à la réduction des risques « extérieurs ». En même temps, la négliger conduit à une diminution de la sécurité globale de l'écosystème.

En outre, certains risques doivent être gérés par plus d'un acteur. Il s'agit de la notion de gestion partagée des risques. Cela est particulièrement important lorsque la sécurité de l'infrastructure mondiale de l'Internet est concernée. Étant donné que les réseaux sont

interconnectés et interdépendants, un réseau agissant seul ne peut pas faire une grande différence, même pour protéger ses propres ressources. La responsabilité collective joue donc un rôle particulièrement crucial dans la sécurité et la résilience du système de routage mondial de l'Internet. Par exemple, atténuer le risque des attaques DDoS par réflexion requiert une vaste adoption des pratiques de filtrage d'entrée pour empêcher l'usurpation des adresses IP6. Alors qu'une ressource (par exemple, un serveur web) peut encore être attaquée même si le réseau d'hébergement utilise le filtrage d'entrée, si d'autres réseaux connectés ne déploient pas le filtrage d'entrée, l'action de ce réseau profite à l'Internet dans son ensemble parce que ce réseau ne serait pas une rampe de lancement pour de telles attaques.

La culture de la responsabilité partagée et collective est bien alignée avec la nature «d'intérêt public » de l'Internet. Dans le contexte de la cybersécurité, cela signifie que la mise en œuvre de solutions de sécurité est un investissement à long terme dans l'écosystème de l'Internet dont tout le monde profite, et que toutes les parties prenantes ont un intérêt commun dans la gestion de ces ressources.

La collaboration en tant que composante essentielle d'une sécurité efficace

> *En fin de compte, ce sont les gens qui assurent le maintien de l'Internet. Le développement de l'Internet a été fondé sur la coopération et la collaboration volontaires, et nous pensons que c'est l'un des facteurs essentiels à sa prospérité et son potentiel.*

La sécurité, en général, est un domaine ardu quand il s'agit d'identifier des mesures incitatives. La sécurité de l'infrastructure mondiale de l'Internet, qu'il s'agisse de DNS ou de routage, pose des défis supplémentaires : l'utilité des mesures de sécurité est fortement dépendante de l'action de nombreuses autres parties.

En outre, si les participants à l'écosystème de l'Internet agissent de manière indépendante et exclusivement dans leur propre intérêt, non seulement cela influera sur la sécurité de l'écosystème, mais cela diminuera aussi l'enveloppe globale du potentiel social et économique offert par l'Internet. Une telle situation est souvent décrite comme la « tragédie des biens communs » - expression inventée par Garrett Hardin 7 dans son article portant le même titre. En effet, l'analogie des biens communs peut être appliquée à l'écosystème de l'Internet, mettant l'accent sur certains des défis, en particulier dans le domaine de la cybersécurité.

Il n'est pas facile de surmonter la « tragédie des biens communs » dans le domaine de la sécurité et de la résilience de l'Internet parce que la recherche de résultats qui soient dans notre intérêt individuel fait partie de la nature humaine. Cependant, cette approche est contre-productive et, à long terme, préjudiciable aux intérêts de chacun.

Les solutions technologiques sont un élément essentiel ici, mais la technologie seule n'est pas suffisante. Pour réaliser des améliorations visibles dans ce domaine, il faut d'abord une

meilleure articulation du problème en termes de risques, en fonction des indicateurs et des tendances, et, plus important encore, un changement culturel encourageant la responsabilité collective dans tous les domaines d'activité : politique, juridique, technique, économique, social.

Le développement de l'Internet a été fondé sur la coopération et la collaboration volontaires. L'histoire de l'Internet contient de nombreux exemples de cette coopération et son efficacité. Un excellent exemple est le groupe de travail Conficker 8, créé pour lutter contre l'attaque propagée sur Internet et menée par un logiciel malveillant connu sous le nom de Conficker. Les groupes d'opérateurs de réseau (NOG) régionaux et nationaux, et leur rôle dans la résolution des problèmes opérationnels (couvrant souvent plusieurs réseaux), est un autre exemple.

Les enjeux, les défis et les opportunités associés à la collaboration, ainsi que le changement culturel qui est nécessaire peuvent être regroupés en quatre grands domaines. À notre avis, faire des progrès dans chacun de ces domaines est une condition préalable pour un impact positif sur la sécurité et la résilience de l'Internet :

1. **Compréhension commune du problème.** Plus les parties prenantes sont alignées à l'égard des problèmes, leur gravité et la priorité de leur résolution, plus le dialogue sera ciblé, et plus les différents efforts visant à améliorer la sécurité et la résilience seront cohérents.
2. **Compréhension commune des solutions.** Le défi ici est qu'il y a tout un éventail de solutions possibles (techniques, politiques, économiques, sociales) et que chacune d'elles ne résout qu'une partie ou un ensemble de problèmes à un moment donné dans le temps. Il est important de comprendre qu'il n'y a pas de « solution miracle », mais plutôt, l'évolution d'éléments constitutifs pouvant être utilisés dans la construction d'une solution de sécurité.
3. **Compréhension des coûts/bénéfices communs et individuels.** Les éléments constitutifs technologiques varient en termes de coûts et bénéfices qu'ils apportent à un participant individuel et au bien commun de l'infrastructure globale. La compréhension de ces facteurs et comment ils sont alignés avec les objectifs commerciaux des opérateurs de réseaux et autres est cruciale pour l'amélioration durable de la sécurité et de la résilience.
4. **Capacité à évaluer les risques.** La sélection adéquate des outils et des approches dépend de la capacité à évaluer correctement les risques, à la fois « intérieurs » ainsi que « extérieurs ». Cela nécessite un accord sur les indicateurs et les données factuelles, et sur les tendances qui leur sont associées. Ces données sont également importantes pour mesurer l'efficacité et l'impact de ces outils une fois qu'ils sont déployés, et pour suivre l'évolution dynamique de l'environnement.

Il n'est pas réaliste de supposer qu'il y aura un accord universel sur les questions sous-jacentes, ou qu'un plan cohérent d'action sera adopté au niveau mondial dans un avenir prévisible. La concurrence commerciale, la politique et la motivation personnelle jouent également un rôle dans la façon dont la collaboration se passe. Mais, comme

plusieurs efforts de collaboration l'ont démontré, les différences peuvent être surmontées pour coopérer contre une menace. Une telle collaboration volontaire et selon les besoins en termes de « travailler au bénéfice de tous » est remarquable par son évolutivité et sa capacité à s'adapter aux conditions changeantes et à l'évolution des menaces, générant une efficacité sans précédent.

End Notes

1 « Invariants d'Internet : ce qui compte vraiment »,http://www.internetsociety.org/internet-invariants-what-really-matters

2 http://news.cnet.com/8301-1023_3-57525797-93/facebook-hits-1-billion-active-user-milestone/

3 Ushahidi est un projet open source qui permet aux utilisateurs de crowdsourcer les informations de crise à envoyer via mobile, www.ushahidi.com/

4 Par exemple, une technique utilisée dans l'attaque contre www.spamhaus.org en mars 2013.

5 Par exemple, un compromis de l'autorité de certification néerlandaise DigiNotar, le rapport complet http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip- update.pdf

6 Pour plus d'informations, consultez le RFC 2827 Filtrage d'entrée de réseau : vaincre les attaques par déni de service qui emploient l'usurpation d'adresse IP source(http://tools.ietf.org/html/rfc2827)

7 Hardin, G. « La tragédie des biens communs ». Science 162 (3859): 1243–1248, 1968.

8 Groupe de travail Conficker, http://www.confickerworkinggroup.org/wiki/

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org

Internet Society™