Internet Society
Cameroon Chapter

WEBINAIRE

Global Volunteer Training Program 2020

Abdou MFOPA

Internet Society

THEME

Chiffrement :
Comment ça marche, pourquoi l'utiliser et pourquoi s'y engager.

05 JUIN 2020
17:00 GMT +1

SCANNEZ MOI POUR VOUS INSCRIRE 👉

Internet Society
Cameroon Chapter

WEBINAIRE

Global Volunteer Training Program 2020

Internet Society

THEME

CHIFFREMENT :

Comment ça marche, pourquoi l'utiliser et pourquoi s'y engager.

Abdou MFOPA P.
Officer at ISOC Cameroon
abdou@mfopa.com

05 JUIN 2020
17:00 GMT +1

PLAN

- Introduction
- Pourquoi chiffrer ses données?
- Le fonctionnement du chiffrement?
- Le chiffrement menacé?
- Quelques utilisations du chiffrement
- La législation camerounaise sur le chiffrement
- chiffrement pour tous : l'engagement avec ISOC Cameroun
- Ressources de l'Internet Society

QUI SUIS-JE ?

Je suis un professionnel des technologies de l'Information et de la Communication (IT) avec une double compétence en Télécommunications et en Entrepreneuriat et gestion des PMEs. Je suis fortement qualifié, motivé et passionné par la sécurité informatique avec 12 années d'expériences dans les métiers de l’informatique, plus de compétence en Management des Projets et entrepreneuriat.

Objectif

Le but de ce webinaire est de :
- partager les connaissances acquise durant la formation
- comprendre pourquoi chiffrer ses données et pour quel intérêt
- comment cela fonctionne
- quelques exemples de services et d'utilisation du chiffrement
- la législation camerounaise en vigueur sur le chiffrement
- chiffrement pour tous : l'engagement avec ISOC Cameroun

Introduction

- Le chiffrement est le processus de brouillage ou de cryptage des données afin que seule une personne disposant des moyens de les restituer à leur état d'origine puisse les consulter. Cela permet de sécuriser les données.

- Ce système est fréquemment utilisé pour protéger à la fois les données stockées sur des systèmes informatiques (**données au repos**) et les données transmises par les réseaux informatiques, notamment par Internet (**données en transit**).

Introduction

CHIFFRER VS CRYPTER

- Le terme crypter n’existe pas. En langage informatique le terme crypter n’est pas utilisé car il vient de l’anglicisme. On utilise le terme chiffrer.
- Le mot décrypter existe et est à utilisé dans l’opération de déchiffrement lorsque l’on ne possède PAS la clé de déchiffrement.
- alors que le terme déchiffrer est le mécanisme de déchiffrement en utilisant la clé de déchiffrement.

Pourquoi chiffrer ses données

Le chiffrement est **l'un des éléments constitutifs de la confiance sur Internet.**
Il empêche les données des utilisateurs d'être exposées, et vous aide également à:

- Empêcher l'altération de vos données (documents, fichiers, etc.)
- Savoir avec certitude avec qui vous communiquez
- Signer des documents numériques (pour prouver au destinataire que le document est authentique, et vient bien de vous)

Pour simplifier donc, il s’agit de cacher les informations qui ne pourront être lues par un tiers.

Pourquoi chiffrer ses données

<u>Nous utilisons le chiffrement au quotidien !</u> Un chiffrement robuste est fondamental pour la sécurité et la confidentialité des données que nous stockons ou transmettons. Il est crucial pour le fonctionnement de nombreux éléments de notre société.

- **Navigation sur Internet:** les navigateurs et les sites Internet utilisent HTTPS, un protocole chiffré, pour offrir des communications sécurisées, ce qui empêche que des criminels puissent lire vos données lorsqu'elles sont en transit.
- **E-commerce:** nous faisons confiance à des entreprises pour protéger nos informations financières lorsque nous faisons des achats ou consultons nos comptes bancaires sur Internet. Le chiffrement est également une méthode importante pour ce processus.
- **Messagerie sécurisée:** lorsque nous utilisons une application de messagerie, nous partons du principe que ces messages resteront confidentiels. Certaines applications de messagerie utilisent le chiffrement pour assurer la confidentialité et la sécurité des communications des utilisateurs lors du transit. D'autres utilisent même le chiffrement de bout en bout, afin que seuls l'expéditeur et le destinataire puissent lire les messages, notamment iMessage, WhatsApp, et Signal. 5

Pourquoi chiffrer ses données

Certaines personnes pensent à tort que le chiffrement, ainsi que la sécurité et la confidentialité qu'il offre à nos données, n'ont pas d'importance pour qui n'a rien à cacher.

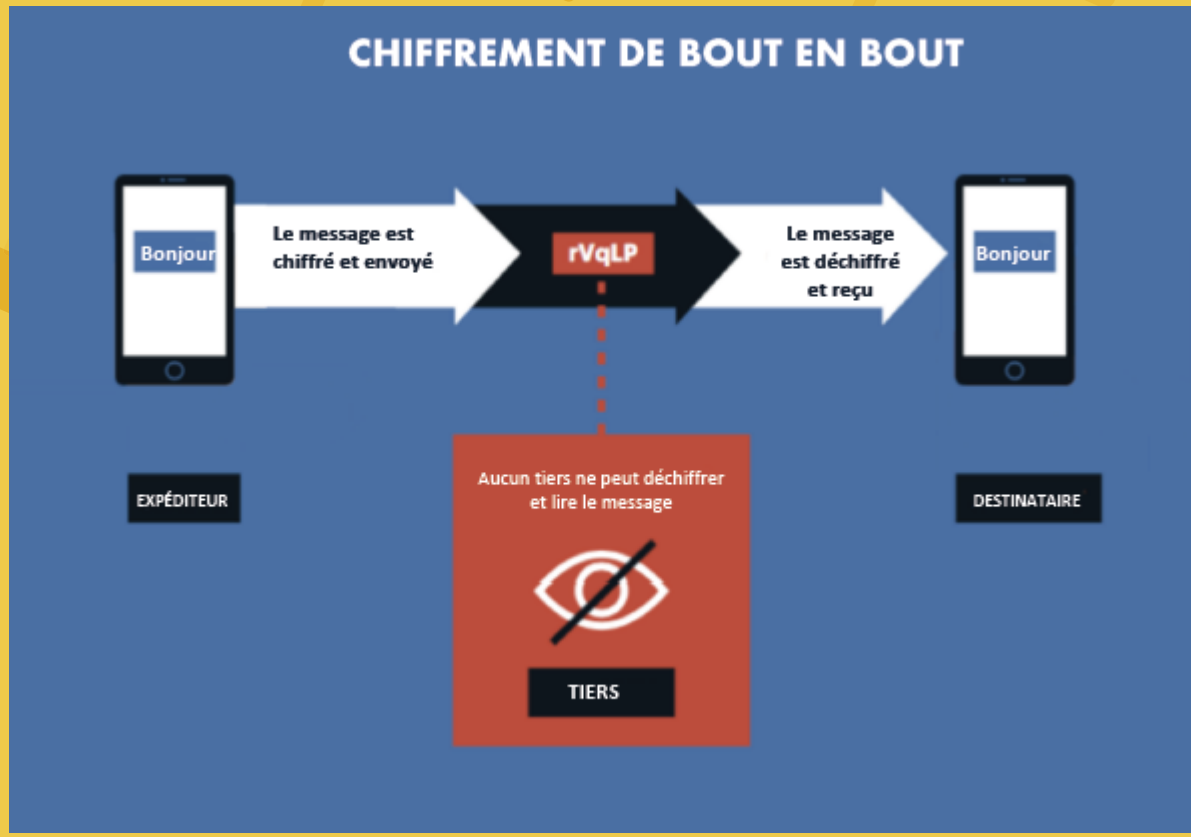
Mais si vos données tombent entre de mauvaises mains, elles peuvent servir à:

- **Nuire à votre réputation**
- **Vous nuire financièrement (ex.: usurpation d'identité)**
- **Se faire passer pour vous, rediriger un paiement, etc.**
- **Exposer à la vue de tous des éléments de votre vie privée**

Le fonctionnement du chiffrement

Le chiffrement de bout en bout (E2E) désigne toute forme de chiffrement par laquelle seuls l'expéditeur et le destinataire prévus peuvent lire le message.

- Aucun tiers, pas même le prestataire du service de communication, n'a connaissance de la clé de chiffrement.
- Le chiffrement de bout en bout est la forme de chiffrement la plus sécurisée qui soit. Ainsi, dès lors que cela est possible, utilisez le chiffrement de bout en bout pour vous protéger, vous et vos données.
- Il existe plusieurs services de communication à chiffrement de bout en bout, comme WhatsApp, Signal, Telegram et Threema.



Le chiffrement E2E et le chiffrement des données sur les appareils sont-ils le vrai problème ?

Le fonctionnement du chiffrement

Le chiffrement repose sur l'utilisation d'un algorithme de chiffrement et d'une clé vont permettre de chiffrer les données.
En retour, le destinataire utilisera une clé pour déchiffrer le message.
On distingue deux systèmes de chiffrements : **le chiffrement symétrique** et **le chiffrement asymétrique**.

- **Le chiffrement symétrique** fonctionne avec une seule clé qui permet à la fois de chiffrer et déchiffrer les données. Les algorithmes les plus connus de chiffrement symétrique sont le DES, le Triple DES et l'AES.
- **Le chiffrement asymétrique** fonctionne avec une paire de clés. Une clé publique utilisée pour chiffrer les données et une clé privée utilisée pour déchiffrer les données. L'algorithme de chiffrement asymétrique le plus connu est RSA.

Le fonctionnement du chiffrement

Chiffrement symétrique

Lors d'un chiffrement symétrique, l'expéditeur et le destinataire emploient une instance différente d'une même clé pour chiffrer et déchiffrer les messages. Le chiffrement symétrique s'appuie grandement sur le fait que les clés doivent être gardées secrètes. Distribuer la clé de manière sécurisée constitue l'une des principales difficultés du chiffrement symétrique, désignée sous le nom de « problème de distribution des clés ». Composant vital du chiffrement symétrique, la clé ne doit en aucun cas être perdue ou égarée. En cas de perte de l'une des clés, le message peut être déchiffré par des personnes malveillantes.

Le principal avantage de la cryptographie symétrique est sa rapidité par rapport à la cryptographie asymétrique.

Le fonctionnement du chiffrement

Chiffrement asymétrique

Pour le chiffrement asymétrique, voici le principe général.
Supposons qu'Alice souhaite envoyer un message secret de Bob , voici comment ils doivent procéder.

1. Bob utilise le chiffrement asymétrique et génère une clé publique et privée.
   1.La clé privée sert à déchiffrer les messages chiffrés
   2.La clé publique sert à chiffrer les messages
2. Bob envoie de manière sécurisée la clé publique à Alice.
3. Alice chiffre son message en utilisant clé publique puis envoie le message chiffré à Bob
4. Bob utilise sa clé privée pour déchiffrer le message de Alice et le tour est joué.

L'interception du message chiffré peut avoir lieu, tant que la personne a l'origine de l'interception ne possède pas la clé privée, il ne pourra pas déchiffrer le message.
Il est donc important de bien stockée sa clé privée, qui si elle est récupérée par un tiers est alors compromise. Dans ce cas, il sera nécessaire de recréer une paire de clés.

Le principal inconvénient du chiffrement asymétrique est sa lenteur par rapport au chiffrement symétrique. En effet, le chiffrement asymétrique exige une puissance de calcul bien supérieure en raison de sa complexité mathématique. Il ne convient pas aux longues sessions du fait de la puissance de traitement qu'il nécessite pour perdurer.

Le chiffrement menacé

• Certains gouvernements cherchent à faire en sorte que les entreprises créent pour eux des moyens d'accéder aux données chiffrées par leurs systèmes (une pratique connue sous le nom de « porte dérobée au chiffrement »).

• D'autres demandent un affaiblissement du chiffrement, afin de permettre le filtrage ou le blocage de données.

• Certaines entreprises veulent accéder aux données chiffrées à des fins de monétisation.

Types de menaces

- **Législative:** des lois exigent qu'une porte dérobée permette l'accès aux forces de l'ordre.
- **Juridique:** tentatives d'application de lois existantes pour créer des mandats d'accès par des portes dérobées pour les forces de l'ordre.
- **Tangentielle:** une menace qui ne cible pas le chiffrement, mais représente malgré tout un risque pour le chiffrement.

Le chiffrement menacé

- Quelle que soit la méthode employée, il est impossible de créer une porte dérobée réservée aux seules utilisations « autorisées » et qui n'affaiblisse pas la sécurité de chacun. Des criminels risquent de découvrir et d'utiliser ce moyen de s'infiltrer.
- Et les criminels utiliseront simplement un autre service chiffré pour communiquer ! Il existe de nombreuses alternatives, en dehors à la fois de la juridiction et du contrôle de tout gouvernement.

Les propositions de porte dérobée au chiffrement ne permettent pas d'empêcher efficacement les criminels de communiquer en secret et risquent d'engendrer des risques non négligeables pour les citoyens respectueux de la loi. L'accès par des portes dérobées créera de nouveaux problèmes, sans pour autant apporter de réelles solutions.

Quelques utilisations du chiffrement

A. INTERNET

Les connexions HTTPs utilisent le chiffrement symétrique et asymétrique pour permettre l'échange de données chiffrés entre le navigateur internet et le site WEB.
Le but est de pouvoir échanger avec le site WEB des données de manière sécurisé notamment dans le cas d'un échange de mot de passe ou de paiement.

Les VPN utilise aussi le chiffrement, entre le client et le serveur VPN, puisqu'un tunnel sécurisé est établi entre les deux.

SSH: Le chiffrement peut aussi être utilisé comme authentification lors d'un accès SSH,

chiffrer ses emails afin que seul le destinataire puisse lire.

ENIGMAIL SUR THUNDERBIRD

Mailvelop AVEC WEBMAIL (GMAIL, HOTMAIL ETC)

GPG4Win est un programme libre qui permet de chiffrer des fichiers et texte dans Windows.

Les Applications de Messagerie telles que **Signal** ou **Whatsapp** emploient un chiffrement de bout en bout afin de protéger la confidentialité des communications des utilisateurs ainsi que pour authentifier ces derniers.

Quelques utilisations du chiffrement

B. SUR SON ORDINATEUR

il y a beaucoup d'applications qui permettent de chiffrer ses données comme ses fichiers ou partitions de disque et autres.

Pour ce type d'usage, le chiffrement utilisé est en général du chiffrement symétrique.

Il est aussi possible de chiffrer des disques ou partitions de disques notamment pour les ordinateurs portables en cas de perte ou vol :

- VeraCrypt
- DiskCryptor
- BitLocker

C. LES LOGICIELS MALVEILLANTS

Les logiciels malveillants peuvent utiliser des communications chiffrés comme les sites HTTPs pour les échanges d'informations avec le serveur de contrôle du pirate. Mais un type de logiciel malveillant peuvent aussi utiliser le chiffrement de fichiers.

On appelle cela les ransomware ou rançongiciel ; Le but est simple rendre les fichiers inaccessibles à son propriétaire, seul le cybercriminel possède la clé de déchiffrement.

Ce dernier fait payer la clé pour que l'auteur puisse récupérer l'accès à ses données.

C'est donc une rançon qui est demandée en échange de l'accès à ses données.

La législation camerounaise sur le chiffrement

Loi N° 2010/012 DU 21 Décembre 2010 relative à la Cybersecurité et la Cybercriminalité au Cameroun.

La présente loi régit le cadre de sécurité des réseaux de communications électroniques et des systèmes d'information, définit et réprime les infractions liées à l'utilisation des technologies de l'information et de la communication au Cameroun. A ce titre, elle vise notamment à :

- Instaurer la confiance dans les réseaux de communications électroniques et les systèmes d'information ;
- Fixer le régime juridique de la preuve numérique, des activités de sécurité, de cryptographie et de certification électronique ;
- Protéger les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, ainsi que les intérêts légitimes des personnes morales.

Chiffrement : Procédé grâce auquel on transforme à l'aide d'une convention secrète appelée clé, des informations claires en informations inintelligibles par des tiers n'ayant pas la connaissance de la clé ;

La législation camerounaise sur le chiffrement

SECTION V

DE L'INTERCEPTION DES COMMUNICATIONS ELECTRONIQUES

Article 49.- Nonobstant les dispositions du Code de Procédure Pénale, en cas de crimes ou délits prévus dans la présente loi, l'Officier de Police Judiciaire peut intercepter, enregistrer ou transcrire toute communication électronique.

Article 50.- Si les opérateurs de réseaux de communications électroniques ou les fournisseurs de services de communications électroniques procèdent au codage, à la compression ou au chiffrement des données transmises, les interceptions correspondantes sont fournies en clair aux services qui les ont requis.

Article 51.- Les personnels des opérateurs des réseaux de communications électroniques ou des fournisseurs de services de communications électroniques sont astreints au secret professionnel quant aux réquisitions reçues.

La législation camerounaise sur le chiffrement

Article 55.- (1) Lorsqu'il apparaît que les données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder en clair ou sont de nature à compromettre les informations qu'elles contiennent, le Procureur de la République, le Juge d'Instruction ou la juridiction de jugement peuvent réquisitionner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair desdites données.

(2) Lorsqu'un moyen de cryptographie a été utilisé, les autorités judiciaires peuvent exiger la convention secrète de déchiffrement du cryptogramme.

La législation camerounaise sur le chiffrement

Article 58.- (1) Les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, sont tenues de remettre aux Officiers de Police Judiciaire ou aux agents habilités de l'Agence, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

(2) Les Officiers de Police Judiciaire et agents habilités de l'Agence peuvent demander aux fournisseurs des prestations visés à l'alinéa 1 ci-dessus de mettre eux-mêmes en œuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à de telles réquisitions.

Article 88.- 1) Est puni d'un emprisonnement de (01) à cinq (05) ans et d'une amende de 100.000 (cent mille) à 1.000.000 (un million) F CFA ou de l'une de ces deux peines seulement, celui qui, ayant connaissance de la convention secrète de déchiffrement, d'un moyen de cryptographie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, refuse de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités.

Chiffrement pour tous : l'engagement avec ISOC Cameroun

L'Internet Society travaille activement pour:

1. Empêcher le chiffrement d'être affaibli, que ce soit par des propositions gouvernementales visant à créer un accès pour les forces de l'ordre ou par des manœuvres du secteur privé visant à augmenter la collecte et la monétisation des données.
2. Améliorer l'adoption et la mise en œuvre d'un chiffrement robuste au sein de l'écosystème d'Internet.

ISOC-Cameroun a choisi une approche de plaidoyer en faveur du chiffrement axées sur les communautés.

Les journalistes

Nous avons travaillé le collectif des journalistes et communicateurs du Noun. Ceci nous a permis de confirmé qu'ils «**(les journalistes) dépendent du chiffrement pour réaliser leur travail et protéger la liberté de la presse »**.

- Établir une connexion sécurisée avec les sources
  - Certaines sources possèdent des informations compromettantes et sont uniquement prêtes à communiquer par le biais de plateformes sécurisées.
- Protéger l'intégrité des informations
  - Le chiffrement nous garantit que ce que nous lisons en ligne est bien le contenu publié par un journal.
- Tenir les gouvernements et les institutions responsables
  - Les journalistes ont besoin d'outils sécurisés pour tenir les gouvernements et les institutions puissantes responsables de leurs actes.
  - Sans ces outils, ces entités puissantes pourraient accéder à leurs recherches, à leurs conversations et à leurs sources et les altérer.
- Sans chiffrement, les journalistes pourraient être dissuadés de publier du contenu risqué
  - Les journalistes ont besoin de sécurité pour publier des articles risqués susceptibles de provoquer des représailles ou du harcèlement.

Parents et enfants

Les enfants sont très vulnérables et grandissent également en ligne. Le chiffrement permet de protéger les enfants et leurs informations sensibles.

- Les travaux scolaires en ligne
  - L'école se déplace de plus en plus en ligne, en particulier en raison de la pandémie du COVID-19. Le chiffrement garantit la sécurité des communications entre les élèves et les enseignants et leur permet de poursuivre leur éducation sans risque.
- Interphones intelligents pour bébés et enfants
  - De nombreux parents ont signalé que des personnes mal intentionnées piratiaient les interphones de leurs enfants et les utilisaient pour communiquer avec les enfants et leur faire peur. Un chiffrement fort permet d'empêcher ce comportement et l'interception des flux vidéo.
- Santé des enfants
  - Les parents accordent une grande importance aux informations médicales de leurs enfants. Avec l'avènement des services et informations de santé en ligne, les parents dépendent du chiffrement pour s'assurer que personne ne vole ou ne compromette les informations de leurs enfants.
- Les enfants communiquant avec des amis en ligne
  - Étant donné que les enfants passent de moins en moins de temps à l'école, ils dépendent des communications et des services de vidéo en ligne pour communiquer avec leurs amis. Le chiffrement de ces services rassure les parents qui savent que les communications privées de leurs enfants avec leurs amis ne seront pas interceptées.

Nous n'y parviendrons pas seuls.

Seule, l'Internet Society ne peut pas convaincre les gouvernements d'arrêter de créer des lois ou des politiques qui menacent le chiffrement et la sécurité numérique.

Isoc-Cameroun souhaite apporter sa contribution.

- En créant une communauté camerounaise de défenseurs du chiffrement qui portera le message d'Internet Society ;
- En formant nos alliés et en leur donnant les connaissances et compétences nécessaires à la réussite de ce projet.
- En entretenant avec des organismes gouvernementaux influents dans ce secteur comme ANTIC, ART, CAMIX, MINPOSTEL
- En développant les contenus locaux pour surmonter les obstacles à l'adoption d'un chiffrement robuste

Développer les connaissances sur le chiffrement

Comment pouvons-nous changer cette perception ?

• **En aidant les autres à comprendre ce que permet le chiffrement.** Des citoyens, des gouvernements et des secteurs d'activité entiers ne réalisent pas à quel point ils ont besoin du chiffrement. Nous pouvons changer cela avec une sensibilisation ciblée.

• **En présentant le chiffrement comme une solution.** Démontrer l'importance fondamentale d'un chiffrement robuste pour chacun de nous, notamment pour les forces de l'ordre et les agences de renseignement.

• **En apprenant aux autres à utiliser un chiffrement robuste.** Le chiffrement de bout en bout n'est pas nécessairement complexe, il suffit de savoir quels produits utiliser.

• **En rendant l'utilisation du chiffrement normale et reconnaissable.**

Les gens défendent ce qu'ils comprennent, et le chiffrement ne fait pas exception.

Ressources de l'Internet Society

- Page d'accueil sur le chiffrement: https://www.internetsociety.org/fr/issues/cryptage/
- Note de synthèse sur le chiffrement: https://www.internetsociety.org/fr/policybriefs/encryption/
- Page de ressources sur le chiffrement (uniquement disponible en anglais): https://www.internetsociety.org/encryption/internet-community-stands-up-forencryption/
- Fiche d'information sur l'accès autorisé par la loi destinée aux décideurs politiques: https://www.internetsociety.org/fr/resources/doc/2019/factsheet-for-policymakers-6-ways-lawful-access-puts-everyones-security-at-risk/

Merci.

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internetsociety.org
@internetsociety

S’impliquer.

Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internetsociety.org
@internetsociety