Forum: GA3 Sociale Humanitaire et Culturel

Sujet: Consolider la coopération internationale afin de combattre la cybercriminalité.

Membre de l'Etat Major: Maria Mendonça

Position: Vice Présidente

Introduction

Depuis le début du 20ème siècle, le monde connait des avancées considérables dans le domaine des nouvelles technologies, avec l'apparition d'Internet, et des nouveaux systèmes de communication, mais cette évolution incontestable et révolutionnaire a néanmoins ses travers.

Aujourd'hui, 63% de la population mondiale a accès à ces nouvelles technologies et particulièrement à Internet. Internet est une plate-forme relativement anonyme où des milliers de personnes venant des quatre coins du globe peuvent se connecter. Cet accès facile et à portée de clics, rend la plate-forme dangereuse car tout le monde l'utilise à des fins différentes que ce soit pour communiquer avec sa famille ou pour effectuer des transactions illégales. Ces actes criminels font partie d'un nouveau phénomène criminel que l'on appel cybercriminalité ou cyber délinquance, qui cible de simples utilisateurs comme vous et moi mais aussi des organisations, des états, de manières différentes (virus, rançons, phishing…). Ces actes criminels sont commis par des personnes anonyme que l'on appel plus communément des hackers, en un clic ils réussissent a brouiller les systèmes penal traditionnelles qui sont de manière générale inadaptée et inapproprié face a cette nouvelle réalité de l'ère numérique. La cybercriminalité est aussi un outil de plus en plus utilisé par les gouvernements ou les organisations privées comme le FBI et la CIA qui va leur permettre d'infiltrer plus rapidement des ordinateurs d'autres états pour en soutirer des informations confidentielles. En 2017, le parquet Russe, mais aussi Vladimir Poutine sont accusés d'avoir pirater les ordinateurs du parti démocrate (partie opposé aux républicains) dans le but de perturber la campagne électorale américaines et de pousser les américains a voter pour Donald Trump l'actuel president des Etats Unis d'Amérique.

Le fait que la cybercriminalité prend différentes formes de plus en plus complexes et se déploie à une vitesse instantanée est un problème extrêmement difficile à définir et donc à résoudre. Il est donc nécessaire et urgent de trouver des moyens pour réduire ou éradiquer toutes

formes de criminalité sur le cyberespace, qu'elle soit mineure ou majeure, par la coopération des pays ici présents.

Définition des Termes Clefs

Cyberespace

Le cyberespace est un réseau virtuel constitué de milliers d'ordinateurs connectés entre eux. Ce réseaux est utilisé par des "cybernautes" à l'aide d'un objet électronique quelconque ayant la capacité à se connecter à un réseau. Les réseaux les plus utilisés et les plus connus dans le monde sont Internet et les réseaux téléphoniques.

Cybercriminalité

La cybercriminalité, ou encore cyber délinquance, est définie comme un ou plusieurs ensembles d'infractions, de crimes, sur ou bien à l'aide d'un réseau du cyberespace : Internet, les réseaux sociaux ou les réseaux de téléphoniques qui fonctionnent sans contact réel entre le criminel et la victime.

Hacker

Un hacker est une personne ou un groupe de personnes "hackivistes" qui tentent de pénétrer illégalement un objet électronique ou un système informatique pour y voler des informations ou y introduire les leurs.

Un Virus

Un virus est un programme informatique ayant pour but d'infecter des ordinateurs, de se propager sournoisement à une vitesse foudroyante et de se répandre à travers des moyens d'échanges sur les plateformes électroniques, les pièces jointes ou bien par messages virtuels.

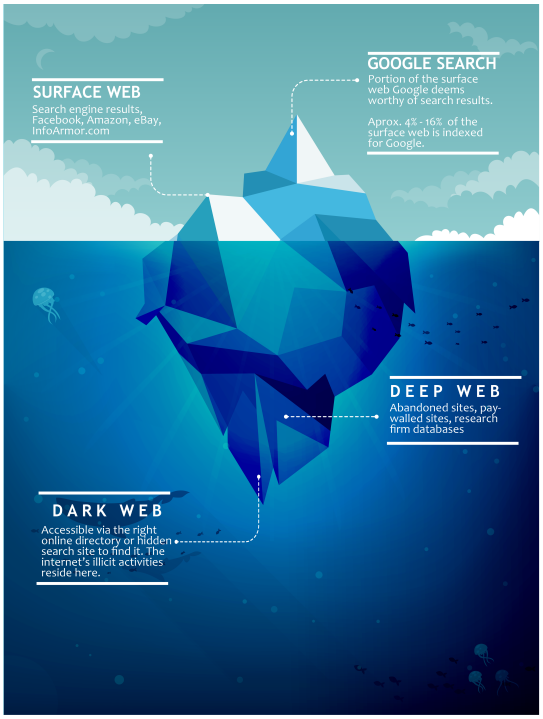
Phishing

Le phishing est une technique utilisée par les cybercriminels et les fraudeurs pour obtenir des données confidentielles et secrètes en donnant une illusion de fiabilité. Dans la plupart des cas les fraudeurs créent de fausses copies de sites sur le net que l'on utilise tous les jours, comme par exemple Google, et récoltent nos données personnelles lorsque nous tentons de nous y connecter.

L'attaque DoS est une attaque informatique ayant pour but de rendre inaccessible et indisponible un système informatique aux utilisateurs et aux modérateurs pendant un laps de temps. Pendant la durée de l'attaque, le malfaiteur soutire des informations qui sont censés lui être inconnues.

Dark and Deep Web

Le Dark et le Deep web sont les parties invisibles du réseaux Internet; un endroit où se retrouvent des associations de malfaiteurs et de criminels pour effectuer des trafics et des échanges de tout types: drogues, personnes, médicaments, organes … Le Deep Web est l'Internet de tous les contenus qui ne sont pas indexés par les moteurs de recherche. Le Dark web est, quant à lui, quasiment inaccessible à l'utilisateur lambda; il faut utiliser des protocoles, des configurations spécifiques, ainsi que des identifiants. Ces deux types de web sont souvent représentés par un iceberg:

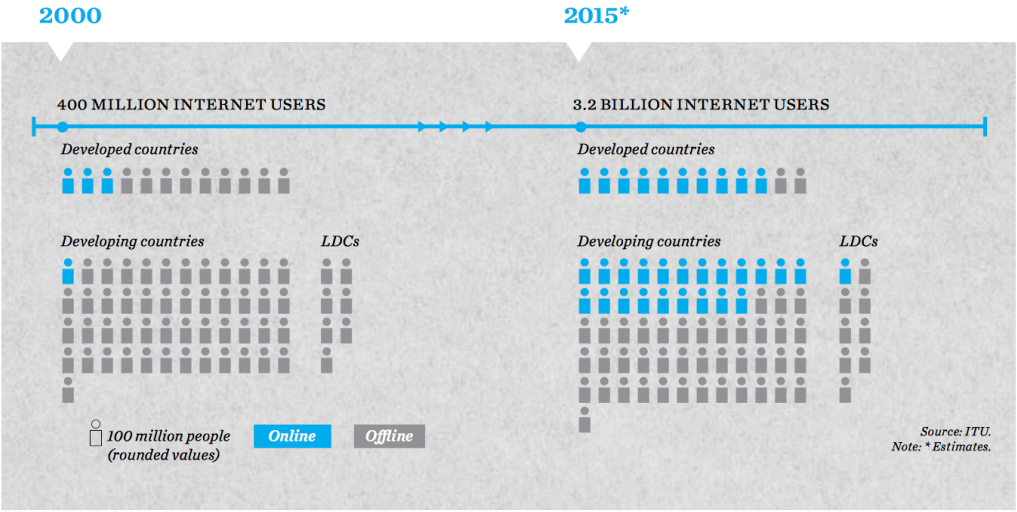


Dans le document ci-dessus, nous pouvons voir un iceberg qui représente les différentes parties du réseaux Internet. Dans celui-ci nous remarquons que la partie visible du iceberg qui est l'Internet que nous utilisons tout les jours n'est en réalité qu'une infime partie de celui ci, il ne représente que 2%. La partie submergée de l'iceberg qui représente la partie cachée, dangereuse

du réseaux , quant a elle représente 98% de celui-ci. L'iceberg est le meilleur moyen de representation pour monter l'écart et la disproportion qu'il ya entre l'internet, et sa partie "cachée".

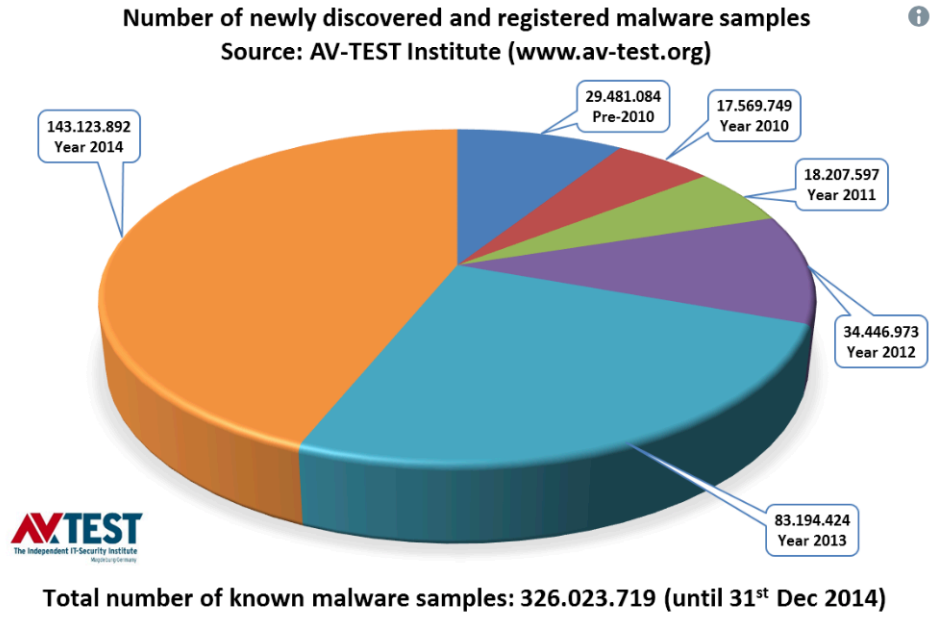
Aperçu général

Trois milliards sept cent cinquante millions; c'est le nombre de personnes qui ont accès à Internet chaque jour. Des millions d'internautes se connectent sur la toile, chacun à des fins différentes. En 15 ans, le nombre d'utilisateur a triplé.



Avec la montée fulgurante du nombre d'internautes, la quantité ainsi que la puissance des cyber attaques ont fortement augmentés. Plus de 117 000 attaques sont recensées chaque jour. Désormais, les attaques deviennent de plus en plus globales et tout les pays ayant accès à Internet peuvent être pris pour cible par les cybercriminels; les cyber attaques se diversifient dans plusieurs domaines et s'intensifient dans d'autres, la forme la plus courante étant l'installation de virus.

Le 12 mai 2017, plus de 200 000 ordinateurs distribués dans environ 150 pays ont été touchés par une cyberattaque baptisé "WannaCry". Cette attaque a déstabilisé des gouvernements entiers. Wannacry est un virus du type "ransomware ": un virus qui demande à l'utilisateur de payer une rançon. Il a réussi à infecter en seulement quelques heures la compagnie aérienne British Airways, le constructeur automobile français Renaud , le système bancaire russe, le groupe américain FedEx et plusieurs grandes entreprises.



Les virus ne sont qu'un aspect des attaques perpétrées par les cybercriminels, il en existe des milliers d'autres. Un outil d'attaque est le DoS. Ce dernier vise principalement les marchés financiers, il ralenti considérablement les services en ligne tout en modifiant les statistiques des actions en cours et des transactions. La plupart des bourses et des grands marchés financiers sont bien équipés contre ce type d'attaque, mais les bourses moins développées comme celle d'Afrique ou d'Amérique du sud en sont souvent victimes. Lorsqu'un virus s'attaque à une bourse, quelque soit son emplacement géographique, il a des effets non négligeables sur le marché mondial.

Le souci majeur du cyberespace est l'anonymat. Sur le net, nous avons tous l'impression d'être en sécurité alors qu'en réalité l'utilisateur est très vulnérable. Stéphane Bortzmeyer, spécialiste de l'Internet, a déclaré en 2014: "Il y a 20 ans, on pouvait acheter un livre ou lire un journal anonymement. Aujourd'hui, sur internet, ce n'est plus possible. Quoi que l'on fasse, on laisse toujours des traces numériques." Malgré ces problèmes de plus en plus fréquents, la plupart des gouvernements tentent tant bien que mal d'assurer à leur population un anonymat total en empêchant les sites de préserver les informations des usagers pendant une période d'environ six mois, mais aussi en bloquant des sites qui sont susceptibles d'infiltrer leurs ordinateurs.

Le cyberespace est un lieu où se développe de plus en plus de trafics illégaux comme le trafic de drogues, d'organes, d'armes, de documents confidentiels et bien plus. Ces trafics se développent dans une partie que l'on appelle le Deep Web, invisible et quasiment impossible à accéder, qui occupe aujourd'hui 97% du cyberespace. Les groupes terroristes utilisent le Deep

Web pour soutirer des informations d'état, pour recruter des personnes dans le but de commettre des attentats ou des actes de violences, pour acheter des armes ou d'objets illégaux et dangereux.

Organisation et pays concernés

Chine

La Chine, pourtant connue pour la censure qu'elle exerce sur Internet, est un pays très touché par la cybercriminalité. Plus de 83% de la population utilisant internet dit avoir été la cible d'une cyberattaque. Il y 2 ans, un logiciel malveillant nommé xxShenqi, a réussi à infecter le téléphone de 110 000 utilisateurs à travers le pays. En accédant au pouvoir en 2013, le président Xi Jinping a fait de la "cybersouveraineté" une priorité de ses efforts pour renforcer la sécurité. Il envisage par ailleurs de construire un centre national de méga données dans le but d'exploiter toutes les données de leurs réseaux. En renforçant sa censure et après avoir mené des actions pour traquer les malfaiteurs, en 2015 la Chine a arrêté un réseau de 15000 cybercriminels.

Sénégal

Le Sénégal est l'un des pays ayant le meilleur accès à Internet et aux aux technologies de l'information et de la communication (TIC) en Afrique de l'Ouest, mais depuis huit ans le pays est touché par la cybercriminalité. Pour cela, le gouvernement a mis en place une plateforme de surveillance permettant de contrôler et d'arrêter les malfaiteurs et les programmes ayant pour but de nuire aux utilisateurs avant même qu'ils atteignent le réseau du pays. De plus, des lois comme la Loi n° 2008 – 11 portant sur la Cybercriminalité condamnant avec fermeté les malfaiteurs ont également été instaurées. Par exemple, dans l'article 431-8 section première il est stipulé que :" Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement."

France

La France fait partie depuis quelques années des pays les plus touchés par la cybercriminalité. Le pays est plus particulièrement touché par le "rançongiciel" et le "Phishing" ainsi que par des vols de codes bancaires. Pour cela, le gouvernement français a crée des départements spécialisés au sein de la gendarmerie nationale afin de prévenir ce type d'attaques. Par ailleurs, la France s'est allié à l'Allemagne pour la mise en place d'un contrôle direct chez les fournisseurs d'accès à Internet (FAI).

Les Etats-Unis d'Amérique

Les Etats-Unis, regroupant le plus grand nombre d'internautes (300 millions environs), est le pays le plus touché par la cybercriminalité avec plus de 4000 attaques recensées par seconde. Le pays étant le siège des plus grandes compagnies mondiales, faisant parties des nouvelles technologies de l'information et de la communication (NTIC) dont Google, Spotify et Microsoft, la moindre cyberattaque visant ces entreprises aura des répercussions à l'échelle internationale. Afin de lutter contre la cybercriminalité, l'Etat fédéral américain a installé le Cybersecurity Information Sharing Act (CISA) permettant aux entreprises de mettre en commun et de soumettre au gouvernement américain toutes informations et traces de cyberattaques dans le but de tracker et remonter les branches d'organisations de malfaiteurs qui terrorisent le territoire.

Canada

En 2015, le Canada est devenu le second pays le plus vulnérable aux cyberattaques (derrière les USA). Avec plus de 78% de la population utilisant le cyberespace, il est important que le pays soit bien équipé en matière de protection. C'est pourquoi le gouvernement canadien a établit le Centre Canadien De Réponses Aux Incidents Cybernétiques afin de surveiller les cyber menaces et de fournir des conseils de prévention. Pour lutter contre les menaces de plus en plus violentes, le Canada et ses alliés au sein de l'organisation trans atlantique (l'OTAN), ont adopté plusieurs documents stratégiques sur la cyberdéfense. Le ministère de la Défense nationale et les Forces canadiennes étudient les différentes mesures à instaurer pour une meilleure réactivité face aux cyberattaques futures.

Office des Nations Unies Contre la Drogue et le Crime

Office des Nations Unies contre la Drogue et le Crime (ONUDC) est une organisation qui a pour mission d'assister les États-Membres dans la réalisation de l'objectif de sécurité et de justice pour tous en rendant le monde plus sûr face à la criminalité, à la drogue et au terrorisme. Le 17 avril 2015, alors que la cybercriminalité est en plein essor, l'organisation des nations unis et ses partenariats ont porté l'accent sur le sujet de la cybercriminalité durant le Congrès des Nations Unies contre le crime à Doha, au Qatar. D'ailleurs, au cours des deux dernières années, l'ONUDC, à travers son programme contre la cybercriminalité, a pu fournir une assistance technique mais aussi judiciaire dans trois régions du monde: en Afrique de l'Est, en Asie du Sud-Est et en Amérique centrale, des régions où la cybercriminalité est en hausse constante.

Développements récents

Dates	Évènements
23 novembre 2001	Convention sur la cybercriminalité qui a mené à l'harmonisation des législations contre la cybercriminalité.
Octobre 2011	Opération Dark-Net et attaque DoS sur des sites pédophiles perpétrées par l'organisation Anonymous
17 au 21 janvier 2011	Délibérations de la première réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne.
Juin 2012	Plus de 80 millions de dollars sont détournés dans une vague de cyberattaques visant des banques américaines, européennes et latino-américaines.
Avril 2014	Operation HeartBleed est un bug dans le code d'OpenSSl (encryptage utilisé par des milliers de sites internet) qui permet à des personnes malintentionnées de soutirer les données personnels des connexions utilisant OpenSSL, ils peuvent obtenir des mots de passe, des numéros de carte bancaires et des identifiants secrets. Il aura fallut deux ans pour rectifier ce bug.
Novembre 2014	Des milliers de serveurs de Sony Pictures Entertainment ont été piratés par une organisation travaillant pour le gouvernement de la République de Corée en raison de la production du film The Interview mettant en scène un acteur ressemblant au chef d'état Coréen.
8 Avril 2015	La chaîne TV5 Monde a été victime d'un piratage de grande ampleur par des individus du groupe Etat Islamique (ISIS).
16 et 17 Avril 2015	Conférence mondiale sur le Cyberespace à La Haye, les États ont envisagé d'embaucher des hackers éthiques qui auraient pour mission d'étudier les failles du cyberespace et de les signaler pour qu'elles soient corrigées.

Mai 2017	Une Attaque de type ransomware touche plus de 150 pays et 200000 utilisateurs à travers le monde. Cette attaque du nom “Wannacry” a touché plus particulièrement des compagnies importantes comme Renault mais aussi des entreprises gouvernementales comme British Airways.
13 mai 2017	Lors du sommet du G7 à Bari, les états ont reconnu la menace croissante des cyberattaques.
24 mai 2017	Le compte tweeter du gouvernement Qatari (QNA) a été hacker par des hackers provenant de l’Arabie Saoudite. Les hackers ont diffusés des propos mensongers qui ont été attribués à l'émir Cheikh Tamim Ben Hamad Al-Thani et qui traitant de questions régionales hautement sensibles. Ces messages, mensongeurs sont en partis à l’origine de l’assiégemant du Qatar à ce jour.

Tentatives précédentes de résoudre la question

A ce jour, aucune tentative concrète de résolution de la question n’a été réalisée par l’organisation des nations unies. Seul deux organisations, l’Office des Nations Unies contre la Drogue et le Crime (ONUDC) et le conseil européen CE, se sont intéressés à la question. La cybercriminalité est un problème mondiale et global, il est donc grand temps que les organisations mondiales ainsi que les populations se mobilisent pour y accorder l'attention et l'action que cette cause mérite.

Solutions Possibles

Les solutions pour combattre la cybercriminalité résident dans le renforcement des coopérations internationales. Ces solutions sont difficiles à mettre en oeuvre en raison des différentes politiques gouvernementales sur le fonctionnement du cyberespace. En effet, les mesures prises risquent de limiter l’anonymat et les libertés des utilisateurs. Par exemple, un pays comme les Etats-Unis, où la liberté est une valeur fondamentale, conçoit la censure comme une infraction aux Droits de l’Homme. La République de la Corée et la Chine, quant à elles, ne voient pas d’inconvénient à cela.

La lutte contre la cybercriminalité serait peut-être plus efficace si l’on prenait en considération l’ensemble de ces points de vues et que l’on mettait en oeuvre les lois qui ont été votées par les communautés internationales. Ce problème est un enjeu important de notre siècle, il est donc primordial que l’organisation des nations unis y apporte des solutions plus durables.

Bibliographie

Eschapasse, Baudouin. “Les États... Unis Contre La Cybercriminalité.” *Le Point*, 18 Nov. 2016, www.lepoint.fr/high-tech-internet/les-etats-unis-contre-la-cybercriminalite-18-11-2016-2083985_47.php.

“PressReader.” *PressReader.com - Connecting People Through News*, 28 Oct. 2017, www.pressreader.com/france/la-tribune-hebdomadaire/20150619/282106340275388.

Nathalie Guibert, Damien Leloup et Philippe Bernard. “Une Cyberattaque Massive Bloque Des Ordinateurs Dans Des Dizaines De Pays.” *Le Monde.fr*, Le Monde, 19 May 2017, www.lemonde.fr/international/article/2017/05/13/une-cyberattaque-massive-bloque-des-ordinateurs-dans-des-dizaines-de-pays_5127158_3210.html.

FigaroTech. “La Lutte Contre La Cybercriminalité Est Un Marché D'avenir.” *FIGARO*, 6 Aug. 2014, www.lefigaro.fr/secteur/high-tech/2014/08/06/32001-20140806ARTFIG00271-la-lutte-contre-la-cybercriminalite-est-un-marche-d-avenir.php.

“DOHA : L'ONU Et Ses Partenaires Mettent L'accent Sur Leurs Efforts Pour Combattre La Cybercriminalité.” *UN News Center*, United Nations, www.un.org/apps/newsFr/storyF.asp?NewsID=34619#.WeIXSMaB3AI.

Nadir, Karima. “Cybercriminalité, L'autre Menace Terroriste.” *Libération*, www.libe.ma/Cybercriminalite-l-autre-menace-terroriste_a69233.html.

Aigrain, Philippe. “Le Droit à L'anonymat Et Au Chiffrement.” *Club De Mediapart*, 5 Feb. 2015, blogs.mediapart.fr/edition/libres-enfants-du-numerique/article/050215/le-droit-lanonymat-et-au-chiffrement.

Manenti, parBoris. “Pourquoi Vous Ne Serez Jamais Anonyme Sur Internet.” *O Le Cahier Des Tendances De L'Obs*, 24 Jan. 2014, o.nouvelobs.com/high-tech/20140124.OBS3696/pourquoi-vous-ne-serez-jamais-anonyme-sur-internet.html.

Roman Unuchek, Maria Garnaeva, Anton Ivanov, Denis Makrushin, Fedor Sinitsyn - août 11, 2016. 3:06. “Évolution Des Menaces Informatiques Statistiques Du 2ème Trimestre 2016.”

Securelist - Information Sur Les Virus, Les Hackers Et Les Spams, 11 Aug. 2016, securelist.fr/it-threat-evolution-in-q2-2016-statistics/65318/.

"Press Release: ITU Releases 2016 ICT Figures ..." *ITU*, 2016, www.itu.int/en/mediacentre/Pages/2016-PR30.aspx.

l'Intérieur, Ministère de. "Que Faire En Cas D'escroquerie Ou De Cyberattaque ?" *Http://Www.interieur.gouv.fr/A-Votre-Service/Ma-Securite/Conseils-Pratiques/Sur-Internet/Que-Faire-En-Cas-d-Escroquerie-Ou-De-Cyberattaque*, 25 Aug. 2015, www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Que-faire-en-cas-d-escroquerie-ou-de-cyberattaque.

"Le Dessous Des Cartes - LE CYBERESPACE | ARTE." *Le Dessous Des Cartes | ARTE*, Apr. 2009, ddc.arte.tv/nos-cartes/le-cyberespace.

ITU. 2015, www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.

Anmonka Jeanine-Armelle Tano-Bian. 4 Jan. 2016, tel.archives-ouvertes.fr/tel-01249586/document.