

Le Temps
1002 Lausanne
058 269 29 00
https://www.letemps.ch/

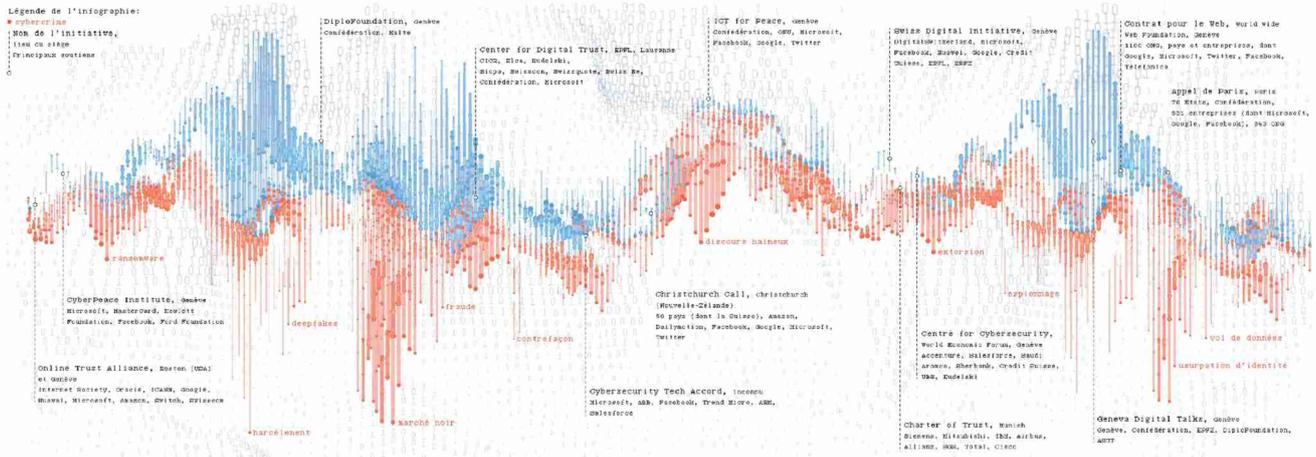
Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 33'508
Erscheinungsweise: 6x wöchentlich

Seite: 2
Fläche: 215'273 mm²

Auftrag: 3012433
Themen-Nr.: 647.011

Referenz: 76078290
Ausschnitt Seite: 1/4

Un aperçu des principales initiatives au niveau mondial



Plongée au cœur de la galaxie d'initiatives contre le cybercrime

TECHNOLOGIE Depuis Genève, Lausanne ou Paris, les organismes luttant contre la cybercriminalité, le harcèlement en ligne ou l'espionnage se multiplient à un rythme impressionnant. Chacun tente de combattre ces fléaux à sa manière. La Suisse veut se positionner en pôle mondial d'excellence, alors que Microsoft s'implique dans toutes ces organisations

ANOUCH SEYDTAGHIA

@Anouch

Combien sont-elles? Personne ne le sait. Personne, même pas les spécialistes les plus qualifiés du web. Les initiatives contre le cybercrime et pour la protection des internautes se multiplient à un rythme surréaliste et nul n'est capable de les dénombrer. De Genève à New Delhi, de Lausanne à Paris, c'est une nébuleuse d'associations, d'organisations et de fondations qui voient le jour sans discontinuer. Ce mardi soir, c'est la Swiss Digital Initiative (SDI) qui était ainsi lancée à Davos, suivant des dizaines d'autres initiatives. Leur mission? Lutter contre les criminels du web, prévenir les conflits dans le cyberspace ou encore protéger les internautes contre les dérives des géants de la technologie.

Le but de ces organismes est irréprochable. Des objectifs nobles, au service du bien mondial. Certes. Mais derrière ces bonnes intentions se cachent des tensions majeures, sur plusieurs niveaux. Il y a d'abord des tensions entre Etats, voire même entre villes, pour héberger les initiatives qui permettront de pacifier

le cyberspace. Un temps en pole position, Genève se voit désormais sérieusement menacée par d'autres cités. Il y a aussi un match entre géants du web. Microsoft dépense ainsi une énergie folle pour marquer de son empreinte ces actions, en parvenant à se placer dans quasiment toutes celles qui naissent.

Voici, en cinq questions, une plongée dans cette myriade d'organismes créés contre le cybercrime. Une lutte qui nous concerne de très près, tant la criminalité sur internet peut affecter notre vie de tous les jours, de notre smartphone à notre ordinateur, mais aussi l'économie en général et des sites aussi sensibles que les hôpitaux.

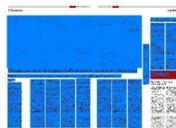
■ Pourquoi y a-t-il autant d'initiatives contre le cybercrime?

Le chiffre donne le vertige: la Geneva Internet Platform a dénombré plus de... 1000 initiatives liées à la gouvernance numérique et au combat contre la criminalité sur internet. Car les attaques se multiplient et deviennent de plus en plus perfectionnées. Il y a bien sûr les délits commis par des pirates infor-

matiques professionnels, qui paralysent de plus en plus souvent les systèmes de villes entières, d'hôpitaux ou d'entreprises pour exiger ensuite une rançon. Il y a aussi les attaques qui ciblent les particuliers – l'infection et la paralysie de centaines de milliers de PC par le virus WannaCry, en 2017, a été un choc mondial. Mais il y a aussi les cyberattaques commanditées par des Etats, jamais revendiquées et qui peuvent mettre à genoux les infrastructures vitales de certains pays.

Protéiforme, la cybercriminalité devient de plus en plus agressive. «La préoccupation est mondiale et les moyens alloués contre ce fléau ne sont pour l'heure pas à la hauteur du problème, relève Stéphane Duguin, directeur du CyberPeace Institute, basé à Genève. Il est vrai que les initiatives contre les attaques sur internet sont nombreuses, et qu'il existe encore un manque de coordination entre elles. Leur multiplicité est issue d'un accroissement constant de la menace au cours des dernières années, tant ce fléau est majeur.»

Des fléaux mondiaux, mais aussi des questions qui se multiplient: comment lutter contre l'extrémisme et



Le Temps
1002 Lausanne
058 269 29 00
https://www.letemps.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 33'508
Erscheinungsweise: 6x wöchentlich

Seite: 2
Fläche: 215'273 mm²

Auftrag: 3012433
Themen-Nr.: 647.011

Referenz: 76078290
Ausschnitt Seite: 2/4

les discours de haine en ligne? Comment protéger les enfants? Comment faire en sorte que les géants du web n'espionnent pas leurs milliards de clients? «Il y a énormément de bonne volonté, tant de la part du secteur académique que du côté des multinationales et de certains Etats», analyse Olivier Crochat, directeur exécutif du Center for Digital Trust (C4DT), basé à l'EPFL. Il poursuit: «Certaines initiatives ont une approche globale, d'autres se concentrent sur des points précis. Notre centre est une initiative académique, créant une communauté autour des thèmes de la protection des données, la transparence et la création d'outils pour restaurer la confiance dans la technologie. L'Appel de Christchurch, lancé en 2019 à la suite de l'attaque d'une mosquée dans cette ville, vise à lutter contre les discours extrémistes en ligne.»

■ Ces initiatives vont-elles vraiment résoudre des problèmes?

Tous les acteurs interrogés s'en disent certains, mais les moyens mis en œuvre semblent souvent limités. Beaucoup d'organisations, tels le CyberPeace Institute ou la Swiss Digital Initiative (SDI), regroupent à leur tête des grands noms issus du monde numérique ou de la politique. Mais le personnel opérationnel est encore limité. «Nous avons été créés en 2019 et voulons recruter d'ici à fin 2020 une vingtaine de personnes, dont des data scientists, des

«Les moyens alloués contre ce fléau ne sont pas à la hauteur»

STÉPHANE DUGUIN, DIRECTEUR DU CYBERPEACE INSTITUTE, BASÉ À GENÈVE

enquêteurs forensiques et des ingénieurs et disposons d'un budget de départ de 10 millions de francs sur trois ans, affirme Stéphane Duguin.

Mais il est clair que lorsque nous lancerons des enquêtes pour tenter de déterminer qui a lancé une cyberattaque, nous ferons aussi appel à l'expertise de sociétés externes spécialisées dans la cybersécurité.»

Avec une autre approche, le Contrat pour le web lancé en novembre 2019 par la World Wide Web Foundation de Tim Berners Lee ou l'Appel de Paris cherchent à rassembler le plus d'acteurs autour de textes fondamentaux. «A lui seul, l'Appel de Paris rassemble déjà 100 acteurs, dont 74 Etats, 500 entreprises et 300 ONG, énumère Jean-Yves Art, responsable des partenariats stratégiques chez Microsoft. Signer ce texte n'est pas anodin: il engage à respecter des principes clairs. Et en cas de manquement, il sera possible de pointer du doigt des coupables. Le but général est d'accroître les bonnes pratiques et le respect de principes éthiques. Et je pense que cela fonctionnera ainsi, d'autant que le coût du lancement des attaques, si les agresseurs sont de plus en plus facilement identifiables, va augmenter.»

Selon Blaise Lempen, auteur du livre *Guerre et paix dans le cyberspace* (Georg), «ces initiatives sont très importantes et répondent à un besoin urgent de réglementation. Mais le cyberspace est dominé par quelques grandes puissances – les Etats-Unis, la Chine, la Russie – qui ne souhaitent pas de normes contraignantes leur liant les mains afin de préserver leur suprématie technologique. De plus, toute une série de régimes autoritaires ne veulent pas entendre parler des libertés démocratiques sur internet dans un traité international. On pourrait néan-

moins trouver des accords partiels sur certains sujets comme la préservation des infrastructures critiques (télécommunications, hôpitaux) en cas de cyberguerre, car tout le monde y a intérêt.»

■ Genève et la Suisse peuvent-ils encore tenir tête à Paris?

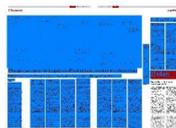
Il existe des centaines d'acteurs à

Genève, et la présence de dizaines d'ONG et de l'ONU constitue un terreau fertile. Mais ce n'est pas tout. «Le 14 février 2017, l'appel de Brad Smith, président de Microsoft, pour des Conventions numériques de Genève, a eu un écho planétaire, se souvient Pierre Maudet, conseiller d'Etat genevois chargé du Département du développement économique. Depuis, les initiatives se sont multipliées à Genève, notamment grâce à la création des Geneva Digital Talks. J'ai bon espoir que le canton puisse héberger des conventions numériques à l'avenir, vu la place mondiale qu'est en train de prendre Genève dans ce domaine.»

Depuis plus de trois ans, Pierre Maudet fait le forcing dans ce sens. Mais la partie est loin d'être gagnée. «Tant le travail effectué dans le cadre de l'ONU que l'Appel de Paris sont pour nous des points très intéressants, glisse Jean-Yves Art, de Microsoft. Quand Brad Smith a évoqué des Conventions numériques de Genève, nous savions que ce serait un très long processus semé d'embûches. Aujourd'hui, je ne peux pas vous dire où seront hébergées ces conventions numériques. Paris a effectué un travail remarquable. Il existe dans la Genève internationale un état d'esprit unique, focalisé sur la gouvernance internationale. Nous verrons pour la suite.»

La concurrence de Paris n'effraie pas Pierre Maudet. «L'engagement d'Emmanuel Macron a été remarquable. Mais lorsque vous observez l'attractivité du pays en matière numérique et l'instabilité du droit dans ce domaine, les risques sont importants. Genève, en raison de sa place unique dans l'échiquier de la gouvernance internationale, a une carte à jouer. Je suis convaincu que c'est ici que des solutions seront trouvées.»

Impossible de prédire l'avenir. Microsoft évoque beaucoup moins Genève depuis plusieurs mois. Mais en parallèle, la montée en puissance du C4DT de l'EPFL et l'énergie déployée par les responsables de DigitalSwitzerland pourraient aider la Cité de Calvin.



■ Certaines initiatives vont-elles fusionner ou disparaître?

C'est une certitude, même si tous les acteurs saluent le foisonnement de créations d'instituts, d'appels et d'associations. «Ces initiatives éparses devraient au moins se coordonner. L'ONU a un rôle déterminant à jouer sur ce plan. Le Forum global de l'internet associe des milliers d'acteurs mais il manque de pouvoir décisionnel. Il n'y a pas d'organisation internationale compétente pour le contrôle du cyberspace», souligne Blaise Lempen.

De son côté, Stéphane Duguin relève «un manque de coordination» entre les acteurs et estime que tout doit être tenté: «Combattre le cybercrime et tenter d'identifier des coupables est extraordinairement difficile, mais avec de bons partenaires et une bonne méthodologie, c'est aujourd'hui possible. Même si d'avenir nous parvenions à la conclusion que cela devait changer au regard de la mutation technologique de l'internet, il restera important d'attaquer le problème par plusieurs angles.»

Jean-Yves Art, de Microsoft, estime qu'«à un moment ou un autre, des initiatives vont converger et fusionner, c'est inévitable et salutaire. Mais tout doit être tenté, c'est une question vitale.»

L'attitude de la Chine, des Etats-Unis ou de la Russie pourrait avoir un impact important sur toutes ces bonnes volontés. Car certains de ces pays sont soupçonnés par plusieurs de nos interlocuteurs de retarder certaines initiatives, de ne pas signer certains appels ou de les vider de leur substance. Et le risque

«Tout doit être tenté, c'est une question vitale»

JEAN-YVES ART, RESPONSABLE
DES PARTENARIATS STRATÉGIQUES
CHEZ MICROSOFT

existe, bien entendu, que des attaques soient toujours menées par des Etats signataires de traités, qui n'ont toujours été les auteurs d'agressions de grande ampleur.

■ Microsoft, omniprésent, a-t-il un agenda caché?

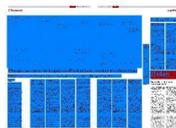
Il y a eu bien sûr l'idée lancée par Brad Smith en 2017, qui n'a cessé de sillonner le monde pour son idée de convention numérique. Et depuis, Microsoft est présent dans absolument tout ce qui se fait en matière de lutte contre la cybercriminalité et d'amélioration de la gouvernance du web. La multinationale est partout, partenaire tant du C4DT de l'EPFL que du CyberPeace Institute, signataire de l'Appel de Paris et partenaire de la Swiss Digital Initiative...

Pourquoi une telle débauche d'énergie, alors que Google ou Facebook se contentent de signer des textes généraux, sans jamais prendre d'engagements majeurs? «Ce que fait Brad Smith au nom de Microsoft, et ce que le groupe fait, est clair: nous voulons lutter contre des fléaux qui touchent des milliards d'internautes, répond Jean-Yves Art. Bien sûr, ces cybercrimes affectent Microsoft, nos

clients et nos affaires. Nous dépendons des sommes considérables pour nous protéger des attaques, mais aussi bien sûr protéger nos clients. Mais je pense qu'au-delà de cela, il y a un intérêt mondial et commun à lutter contre ces menaces.»

De son côté, Olivier Crochat estime que «Microsoft fait bouger les choses depuis plusieurs années, de façon non visible pour le grand public au début, puis maintenant avec des initiatives claires sur lesquelles le groupe communique. Une manière de répondre aux critiques, de faire preuve de transparence, et de montrer qu'il n'y a pas d'agenda caché. C'est remarquable et plutôt rare si on compare son attitude à celle des autres géants du web.» Pierre Maudet note que «la position de Microsoft est très américaine: la multinationale cible des problèmes qui affectent aussi sa marche des affaires et cherche des solutions, de manière efficace et avec pragmatisme. Bien sûr, la société aura tout à gagner d'un cyberspace avec moins de délits commis. Mais tout le monde y gagnera aussi.»

Blaise Lempen partage cet avis: «Microsoft et les multinationales ont intérêt à ce que la situation ne dégénère pas en conflit ouvert. Il y a des milliers de cyberattaques tous les jours qui sont un facteur d'insécurité et d'instabilité. La confiance dans internet est en train de décliner parmi les citoyens de nombreux pays et cela n'arrange pas les affaires des géants du numérique désormais sur la défensive.» ■



Les cyberattaques ne cessent de se multiplier

MAIS ENCORE

Les groupes étatiques, la menace la plus forte

Fin 2019, les groupes français Thales et israélien Verint publiaient un annuaire mondial des groupes de pirates informatiques les plus menaçants. Sur les 66 groupes d'attaquants de haut niveau, 49% sont considérés d'origine étatique ou soutenus par un Etat. Dans le reste des groupes, 26% sont des «hacktivistes», des militants motivés par des idéologies communautaires, religieuses, politiques. Vingt pour cent sont des cybercriminels, motivés par l'appât du gain, 5% des cyberterroristes. Parmi les groupes les plus dangereux en termes de sophistication de leurs outils, les groupes russes dominent (4 dans les 10 premiers), suivis par les groupes chinois (3 sur 10). LT

INFORMATIQUE Les «ransomwares» sont l'une des menaces qui mobilisent actuellement le plus de moyens autour de la planète

Difficile, voire impossible, d'établir un catalogue exhaustif des menaces qui planent aujourd'hui dans le cyberspace, tant elles évoluent sans cesse, changeant même souvent de forme. Chacune des initiatives lancées à Lausanne, Genève ou Paris tente de lutter contre un ou plusieurs de ces fléaux, dont voici un aperçu.

Les «ransomwares»

C'est le type d'attaque le plus virulent qui frappe particuliers, entreprises, administrations et hôpitaux. Le principe est simple: les pirates informatiques parviennent à infecter un ordinateur, par exemple via une pièce jointe glissée dans un e-mail. Ensuite, toutes les machines connectées du réseau sont à leur tour touchées. L'attaquant parvient à bloquer l'accès à ces ordinateurs, qui deviennent inutilisables. Il exige ensuite une rançon pour rendre l'accès à ces machines et parvient aussi parfois à voler des données. Il y a eu bien sûr le précédent WannaCry en 2017, qui a infecté des dizaines de milliers de PC. Ces derniers mois, de très nombreux hôpitaux et PME, voire des multinationales, ont été affectés.

Le «phishing»

Phénomène ancien, le «phishing» fait toujours des ravages. De très nombreux internautes continuent à se faire avoir par des e-mails qui semblent avoir été envoyés par Goo-

gle, Netflix ou Swisscom et qui exigent des données complètes. Des données ensuite facilement exploitées par des pirates.

Les attaques entre États

On sait très peu de choses de ces attaques, dont ni les victimes ni les agresseurs ne font la publicité. Mais régulièrement, des États, souvent cachés derrière des groupes de hackers à leur solde, tentent de paralyser en partie des États ou des infrastructures vitales de certains pays. La Russie, la Chine et la Corée du Nord sont souvent citées. Mais en parallèle, tous les États occidentaux se livrent à des activités d'espionnage.

Les vols de données

Plus une semaine ne se passe sans qu'un vol massif de données n'intervienne, que ce soit chez des géants du web, des sites de rencontre ou érotiques ou même des institutions financières. Très souvent, ces données, d'une grande valeur, se retrouvent plus tard en libre accès, permettant à leurs propriétaires de procéder à de nouvelles attaques.

Les discours extrémistes

C'est une catégorie un peu à part, qui touche tous les internautes. Les discours de haine, les contenus violents, le cyberharcèlement, les contenus terroristes sont autant de problèmes qui peuvent toucher tout le monde, et pour lesquels les géants de la tech ont une grande part de responsabilité. ■ A. S.

2,7 milliards

C'est, selon le FBI, ce qu'a coûté (en dollars) la cybercriminalité en 2018. Ce chiffre a sensiblement progressé en 2019.