

Geneva Internet Platform

DigitalWatch

NEWSLETTER
EN FRANÇAIS

Vous recevez des centaines d'informations
sur les politiques numériques.

Nous les recevons aussi.

Nous les décodons, contextualisons, et analysons.
Ensuite, nous les résumons pour vous.

TENDANCES DES POLITIQUES NUMÉRIQUES EN NOVEMBRE

1. La recherche de cyber-normes continue

Suite à une cinquième réunion du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (UN GGE) marquée par l'absence de consensus, la recherche de solutions et moyens pour résoudre les problèmes de cybersécurité au niveau mondial se poursuit.

À Genève, le Président de Microsoft a renouvelé son appel en faveur d'une Convention de Genève numérique afin de rendre les gouvernements responsables de la cybersécurité. En parallèle, le Geneva Digital Talks a abordé les solutions techniques aux défis croissants en matière de cybersécurité. Bien que le débat sur la cybersécurité comporte de nombreux volets politiques, des solutions techniques pourraient résoudre certains des principaux problèmes. *Plus d'informations à la page 2.*

À New Delhi, la Conférence mondiale sur le cyberspace a abordé certains aspects de la coopération mondiale en matière de cybersécurité, et notamment concernant le renforcement des capacités. Lors de la même réunion, la Commission mondiale sur la stabilité du cyberspace a lancé un Appel pour protéger le noyau public d'Internet, exhortant les acteurs étatiques et non étatiques à éviter toute activité qui endommagerait

intentionnellement et substantiellement la disponibilité ou l'intégrité du «noyau public» d'Internet. Reste à voir comment les acteurs majeurs du cyberspace réagiront à cet appel.

La question principale est de savoir où et comment les gouvernements vont de nouveau converger vers l'adoption de solutions globales pour la cybersécurité.

2. Débat sur les armes autonomes létales

Le débat sur les systèmes d'armes létales autonomes (SALA) s'est poursuivi ce mois-ci à Genève lors d'une discussion de haut niveau d'une semaine. Le Groupe d'experts gouvernementaux (GGE) nouvellement créé dans le cadre de la Convention sur certaines armes classiques, a adopté diverses conclusions après une discussion réunissant des experts de premier plan.

Le groupe a suivi une approche réaliste concernant le développement des systèmes d'armes létales autonomes, concluant que l'usage de cette technologie ne devrait être ni exagérée, ni sous-estimée. Bien que des systèmes d'armes entièrement autonomes n'ont pas encore été mis au point, comment les risques associés aux systèmes d'armes létales autonomes pourraient-ils être minimisés? Les discussions du GGE ont mis en évidence plusieurs solutions.

La suite en page 3



Le Bitcoin a atteint les 11.000 dollars par unité le mercredi 29 novembre, quelques heures après avoir franchi les 10.000 dollars. *Plus de développements sur les politiques numériques aux pages 4-5.*

DANS CE NUMERO

DISCUSSIONS A GENEVE



Des Geneva Digital Talks aux discussions de haut niveau sur la politique numérique, nous résumons les principaux résultats des réunions tenues à Genève.

Plus à la page 2

NEUTRALITE DU NET



Les règles de neutralité du net devraient être renversées aux États-Unis. Nous examinons les réactions et ce qui risque de se produire après le vote.

Plus à la page 6

ARMES LETALES AUTONOMES



Les experts ont récemment exploré les implications technologiques, militaires, juridiques et éthiques liées à de tels systèmes. Cinq problèmes clés apparaissent.

Plus à la page 7

FORUM SUR LA GOUVERNANCE DE L'INTERNET



Le GIP participera activement au 12ème Forum sur la Gouvernance de l'Internet du 18 au 21 Décembre à Genève.

Plus à la page 8

Le numéro 26 de la revue *Digital Watch*, publié le 30 novembre 2017 par la Geneva Internet Platform (GIP) et la DiploFoundation | Traducteurs de l'édition française: Mamadou Lo, Clément Perarnaud, Sorina Teleanu | Collaborateurs: Stephanie Borg Psaila, Jovan Kurbalija, Virginie Paque, Roxana Radu, Barbara Rosen Jacobson, Sorina Teleanu | Conçu et réalisé par Viktor Mijatović, mise en page par Aleksandar Nedeljkov, CreativeLab de Diplo | En plus de la revue, vous pouvez trouver un traitement en profondeur des développements sur l'observatoire *GIP Digital Watch* (<http://dig.watch>) et rejoindre les discussions le dernier mardi de chaque mois, en ligne, ou au Geneva Internet Platform (<http://dig.watch/briefings>) | Envoyez vos commentaires à digitalwatch@diplomacy.edu

Comment les solutions technologiques peuvent-elles faire progresser la cybersécurité?

La deuxième session [des Geneva Digital Talks](#), tenue le 3 novembre, portait sur la cybersécurité et ses interactions avec les changements technologiques récents ou à venir. Le débat a mis en évidence la dichotomie entre les volets technologiques et politiques en matière de cybersécurité et la nécessité de renforcer la confiance et la collaboration entre ces deux champs. Sur le plan technologique, une solution pratique a été présentée: l'architecture «Scalability, Control and Isolation on Next-Generation Networks» (SCION), développée par une équipe de l'ETH Zurich et permettant aux individus de suivre leurs données à travers leur cheminement dans les réseaux, tout en assurant un contrôle plus complet des réseaux.

Semaine de la Paix de Genève 2017

Lors de l'édition 2017 de la Semaine de la Paix à Genève, tenue du 6 au 10 novembre, il a été mis en évidence que la technologie numérique avait d'importantes implications pour la prévention des conflits, notamment à travers deux angles distincts et contradictoires. Plusieurs sessions ont identifié comment la technologie numérique peut aider à prévenir les conflits. Ont été mis en évidence le potentiel du commerce électronique, des métadonnées, de l'intelligence artificielle (IA) et des systèmes d'information géographique. D'autre part, l'accent a également été mis sur les situations dans lesquelles les technologies numériques peuvent donner lieu à des menaces accrues.

Prévenir les cyber-conflits: Avons-nous besoin d'un cyber-traité?

La troisième session des Geneva Digital Talks, le 9 novembre dernier, a porté sur l'appel du président de Microsoft, Brad Smith, en faveur d'une Convention de Genève numérique, et s'est développée autour de trois considérations principales. Tout d'abord, il a été considéré que relever les défis de la cybersécurité nécessitait un changement de mentalité: «La paix ne peut pas être endoctrinée mais elle doit être discutée, en tant que mentalité, en tant que climat ». Deuxièmement, des intervenants ont souligné l'importance d'une approche multipartite pour la rédaction d'un éventuel cyber-traité (par exemple, le processus de Montreux). Enfin, il a été noté que la proposition de Microsoft est une invitation bienvenue aux gouvernements à prendre des mesures pour remédier aux vulnérabilités dans le cyberspace.

Big Data pour la prévention: Equilibrer les opportunités et les défis

Organisée dans le cadre de la Semaine de la Paix de Genève 2017, cette session a exploré le potentiel du Big Data pour la prévention des conflits. Ces discussions ont souligné que la technologie peut constituer à la fois un risque de déclencheur de conflit mais également un facteur d'atténuation, et que les données peuvent être interprétées de façon diverse. Les visualisations (telles que l'outil développé par l'Institut interrégional de recherche des Nations-Unies sur la criminalité et la justice (UNICRI) et le CERN) jouent un rôle clé dans l'analyse et la fourniture de données basées sur les connaissances. Les données satellitaires ont été présentées comme un exemple à travers lequel le Big Data peut contribuer à la prévention des conflits, en rendant compte de la situation et en permettant le développement d'indicateurs rapides d'alerte, tout en fournissant des informations exploitables pour les communautés nationales et internationales.

Les défis actuels de la gouvernance de l'Internet: Quelle est la prochaine étape?

Cet événement, tenu le 9 novembre, portait sur les défis actuels de la gouvernance de l'Internet et les moyens possibles pour les résoudre. Malgré les avantages apportés par Internet, plus de 3,5 milliards de personnes ne sont toujours pas connectés. Le risque de conflit et la nouvelle course aux armes cybernétiques, la propagande terroriste en ligne et la violence extrémiste ont été identifiés comme des défis croissants, qui nécessitent une volonté politique afin d'identifier des solutions. Les discussions ont porté sur la cybersécurité et la nécessité de l'envisager comme une responsabilité partagée. À cet égard, le président de Microsoft, Brad Smith, a réitéré la proposition d'un accord sectoriel technologique dans le domaine de la cybersécurité, et une Convention de Genève numérique pour guider le comportement des gouvernements dans le cyberspace.

Économie de partage et défis sociaux

Cette discussion de haut niveau, le 21 novembre, a porté sur le fonctionnement des plateformes numériques et sur la manière de déterminer si elles autonomisent ou exploitent leurs travailleurs. Les nouveaux modèles économiques de l'économie du partage reposent sur l'effet de réseau: une entreprise ne crée plus le produit ou le service final; il fournit une infrastructure commune et met en relation les consommateurs et les producteurs en utilisant sa connaissance du marché. Les intervenants ont convenu que la fonction sociale du travail devrait être au centre des préoccupations et que les solutions doivent être centrées sur les personnes.

6e Forum des Nations Unies sur les entreprises et les droits de l'homme

Tenu du 27 au 29 novembre sous le thème «Réaliser l'accès pour une remède effective», le Forum a présenté plus de 60 sessions traitant des questions relatives aux droits de l'homme liées aux entreprises. Les discussions ont souligné que si la technologie est vitale pour la société moderne, les développements technologiques ont accru les préoccupations concernant la protection des droits de l'homme, tels que la vie privée et la liberté d'expression. De nouvelles formes de violation des droits de l'homme à l'ère du numérique pourraient être évitées si les parties prenantes – entreprises, gouvernements et société civile – travaillaient ensemble pour identifier et mettre en œuvre des outils de protection et d'application des droits de l'homme.

Où et comment protéger les intérêts juridiques à l'ère du numérique

Lors de cette session, tenue le 28 novembre, dans le cadre des Geneva Digital Talks, trois panélistes ont offert des réponses avec des points de vue différents, à la question du rôle des tribunaux dans la gouvernance de l'Internet et sur comment l'accès à la justice peut être assurée dans le cyberspace. La discussion a porté sur la réglementation des questions traditionnelles de gouvernance de l'Internet, en les opposant aux problèmes technologiques actuels. La politique numérique et la pratique de l'arbitrage soutiennent la position de Genève en tant que centre mondial de solutions.

TENDANCES DES POLITIQUES NUMÉRIQUES EN NOVEMBRE

Suite page 1

La conduite d'examen juridiques sur les armes au niveau national est requise en vertu du Protocole additionnel I aux Conventions de Genève. Ceci est considéré comme une garantie pour assurer la conformité des armes nouvellement développées avec le droit international humanitaire. Pourtant, certains états soutiennent que les examens au niveau national ne sont pas suffisants.

La réflexion sur de nouveaux dispositifs politiques pourrait inclure un instrument légal tel qu'un protocole additionnel, interdisant les SALA; une déclaration politiquement contraignante; ou un futur code de conduite. Les experts ont également mentionné la nécessité d'un moratoire immédiat sur le déploiement des systèmes d'armes létales autonomes. Certains ont toutefois soutenu qu'une interdiction serait prématurée, car de telles armes n'ont pas encore été développées.

La minimisation des risques pourrait également être davantage intégrée dans la conception de ces technologies. L'industrie tente de répondre à la question des risques, «notamment à travers un processus de validation et vérification rigoureux, ainsi qu'à des méthodes de test et d'évaluation. Certaines entreprises intègrent l'éthique dans la conception et le développement et examinent les meilleures pratiques dans le monde entier.» Les états pourraient davantage encourager de telles pratiques.

Des analyses supplémentaires sur les questions clés survenues au cours des discussions se trouvent à la page 7.

3. Rétention d'informations: Plus de fuites et vulnérabilités

Uber est à nouveau dans la tourmente, suite à 'un piratage de données que l'entreprise n'avait pas communiquée. Après que les serveurs de l'entreprise aient été pénétrés en 2016, Uber a payé 100.000 \$ aux hackers pour qu'ils suppriment les données et gardent le silence, a révélé Bloomberg. Les criminels ont eu accès aux noms, adresses e-mail et numéros de téléphone de plus de 50 millions d'utilisateurs, ainsi qu'aux informations personnelles d'environ 7 millions de conducteurs.

La question qui se pose est donc: les entreprises sont-elles obligées d'informer sur les fuites de leurs données? La réglementation aux États-Unis oblige les entreprises à alerter le public et les agences gouvernementales. En ce qui concerne les données des citoyens européens, le Règlement général sur la protection des données de l'UE, qui doit entrer en vigueur en mai 2018, obligera également les entreprises à signaler rapidement les attaques et vols.

Réciproquement, les vulnérabilités découvertes par les gouvernements doivent également être divulguées. En novembre, la Maison Blanche a publié une version mise à jour de son Vulnerability Equity Process (VEP) à partir duquel les agences de sécurité américaines décident quelles vulnérabilités, parmi celles découvertes, seront révélées au développeur du logiciel. Le gouvernement révèle plus de 90% des vulnérabilités qu'il trouve.

Qu'en est-il du reste? Des vulnérabilités non publiées pourraient fuiter et auraient de terribles conséquences, comme en témoigne le cas du ransomware WannaCry. Le lanceur d'alerte Edward Snowden a également mis en garde sur le fait que la non-divulgaration de 10 failles de sécurité importantes annulait les bénéfices de divulgation de 90 failles d'importance moindre.

4. Les tribunaux façonnant les politiques numériques, les complications apparaissent

Une nouvelle fois, les tribunaux continuent d'influencer l'application des politiques en matière de numérique au sein de diverses juridictions, ajoutant de la complexité à ces processus.

Ce mois-ci, un juge américain a empêché une décision de la Cour suprême du Canada de s'appliquer aux États-Unis. En juin, la Cour suprême du Canada avait ordonné à Google de retirer les résultats de recherche violant les droits en matière de propriété intellectuelle au niveau global, et non seulement au Canada.

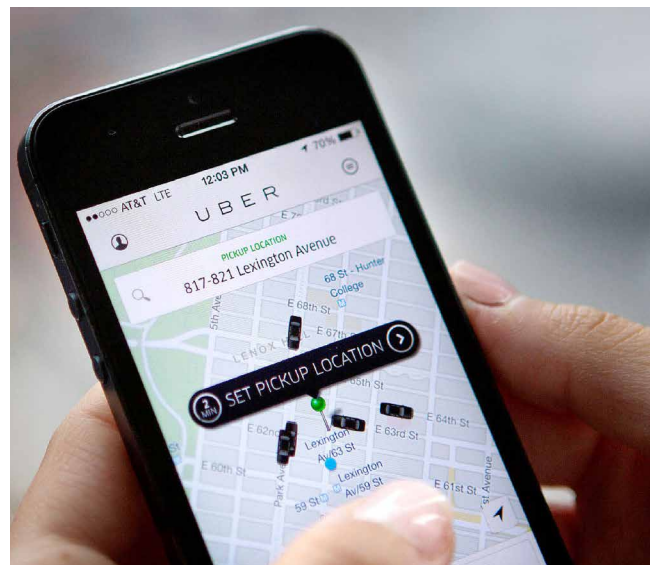
Ce n'est pas la première fois que les tribunaux rendent des décisions contradictoires. Une cour d'appel a statué que le gouvernement ne pouvait pas utiliser un mandat de perquisition pour forcer Microsoft à transmettre des données stockées à Dublin, alors qu'un tribunal de Philadelphie a jugé que Google devait se conformer aux mandats de perquisition du FBI. Les affaires liées à Uber offrent un autre exemple: bien que certains tribunaux aient statué que les conducteurs d'Uber soient des entrepreneurs indépendants, d'autres tribunaux ont statué que les chauffeurs sont des employés. Comme le note un expert, les décisions de justice peuvent parfois donner lieu à sentences conflictuelles.

5. De grandes divergences dans les négociations sur le commerce électronique en amont de la MC11

En prévision de la Conférence ministérielle (MC11) de l'Organisation mondiale du commerce (OMC), des divisions apparaissent déjà entre pays en développement et pays développés. Comme nous l'avons noté le mois dernier, les questions de politiques numériques sont de plus en plus considérées comme des questions commerciales. Si certains pays sont en faveur de la négociation de nouvelles règles en matière de commerce électronique lors de MC11, d'autres s'y opposent.

Au cours de ces discussions, une grande majorité des pays en développement, y compris l'Inde et l'Afrique du Sud, ont clairement fait savoir qu'ils s'opposeraient à de telles négociations. Lors d'une réunion, organisée par le Président du Conseil général le 21 novembre, ces pays ont indiqué qu'ils n'adhéreraient qu'au programme de travail non contraignant de 1998. L'Union européenne, avec le Japon et d'autres pays développés, plaident eux en faveur de la promotion d'un programme sur le commerce électronique. Prendre en compte les nouveaux aspects liés au commerce augmenterait leur adoption en ligne, estime l'UE.

Le MC11 se tiendra du 10 au 13 Décembre à Buenos Aires. Suivez l'observatoire GIP Digital Watch pour les mises à jour.



Après un vol de données sur les serveurs d'Uber en 2016, la société a payé les pirates pour qu'ils suppriment ces données et gardent le silence.

POLITIQUES NUMERIQUES: EVOLUTIONS EN NOVEMBRE

Architecture globale de la gouvernance de l'Internet



Evolution en hausse

Après que la réunion du Groupe d'experts gouvernementaux des Nations Unies se soit terminée sans consensus, la quête d'espaces politiques appropriés pour répondre aux principaux défis en matière de cybersécurité se poursuit. [Plus d'informations sur la page 1.](#)

Développement durable



En stagnation

L'UIT a annoncé l'augmentation du nombre de ses indicateurs utilisés pour évaluer et classer le développement des TIC dans différents pays. La nouvelle méthodologie de 14 indicateurs, au lieu de 11, est conçue pour prendre en compte les développements récents dans les marchés des TIC, et notamment l'introduction de technologies émergentes. L'Index de développement des TIC [est](#) une composante essentielle du Rapport annuel de l'UIT *Mesurer la société de l'information*.

Sécurité



Evolution en hausse

Le nombre d'attaques DDoS continue d'augmenter; les criminels profitant des périphériques non sécurisés de l'Internet des objets. Un rapport de Corero Network Security [révèle](#) une augmentation de 35% des tentatives d'attaques par mois par rapport au trimestre précédent et une augmentation de 91% des tentatives d'attaques mensuelles par rapport au premier trimestre de 2017.

Une vulnérabilité en terme de sécurité dans les portefeuilles Ethereum a conduit au blocage de 500 000 unités de la cryptomonnaie d'Ether. Cela s'est produit pour les portefeuilles à signatures multiples, c'est-à-dire les portefeuilles qui requièrent plus d'un propriétaire pour «signer» une transaction. Parity Technologies, la société responsable de ces portefeuilles, a déclaré que cela s'est produit en raison d'une exploitation accidentelle au niveau global d'une vulnérabilité qui a bloqué de façon permanente plus de 150 millions de dollars en crypto-monnaie.

Bitcoin a dépassé 11.000 dollars par unité, quelques heures après avoir franchi les 10.000 dollars. [SegWit2X](#) la mise à jour proposée du système de paiement Bitcoin, connu sous le nom de New York Agreement, a été reportée. La mise à niveau n'est pas parvenue à obtenir un large soutien nécessaire parmi les utilisateurs du Bitcoin. Au niveau mondial, il est peu probable que la Conférence ministérielle de l'OMC parvienne à un consensus en ce qui concerne l'avancement de l'agenda du programme de commerce électronique. [Plus à la page 3.](#)

Commerce en ligne et économie de l'Internet



Evolution en hausse

Au niveau régional, des changements dans la dynamique du commerce électronique ont été notés. Les ministres du commerce des 11 pays du Partenariat transpacifique (PTP) ont annoncé qu'ils étaient d'accord sur les éléments clés de l'accord. Néanmoins, une réunion prévue pour annoncer l'accord a été annulée après que le Premier ministre canadien ait décidé de ne pas y assister en raison de certaines questions encore indéterminées. Les négociateurs du Canada, du Mexique et des États-Unis ont conclu leur cinquième ronde de négociations pour moderniser l'Accord de libre-échange nord-américain (ALENA). Les négociations ont considérablement progressé dans des secteurs tels que les télécommunications, la facilitation des échanges, le commerce électronique et les obstacles techniques au commerce.

Le Trésor britannique se prépare à mener des actions unilatérales en matière de taxation de l'économie numérique. Il appuiera les réformes fiscales internationales, tout en explorant des solutions provisoires pour augmenter les revenus des entreprises numériques. Uber fait face à de nouvelles questions concernant la légalité de ses opérations. Au Royaume-Uni, l'entreprise de covoiturage a perdu son appel suite à une décision de justice rendue l'année dernière par un tribunal du travail, qui a statué que les employés d'Uber sont des travailleurs ayant droit à un salaire minimum. L'entreprise entend continuer à contester la décision. Les chauffeurs d'Uber au Nigeria ont intenté une action similaire devant un tribunal de Lagos.

Uber a dissimulé la fuite des données de 57 millions d'utilisateurs, rapporte Bloomberg. [Plus en page 3.](#) Au Royaume-Uni, Google est poursuivi en justice pour des allégations de collecte illégale de données personnelles de plus de 5 millions d'utilisateurs en contournant les paramètres de confidentialité de leurs iPhones.

Droits numériques



Evolution en hausse

L'Assemblée constituante du Venezuela a adopté une loi dont les auteurs disent qu'elle «punira les messages de haine dans les médias sociaux et les médias avec des peines pouvant aller jusqu'à 20 ans de prison».

Le Conseil de l'Europe et le développeur d'antivirus russe Kaspersky Lab, ainsi que d'autres sociétés informatiques et Internet, se sont engagés à protéger les droits de l'homme et de contribuer au maintien d'un Internet sécurisé. Ils coopéreront pour lutter contre l'exploitation et les abus sexuels en ligne des enfants; lutter contre la cybercriminalité et le terrorisme; et promouvoir les droits de l'homme en ligne.

La liberté sur Internet a décliné pour la septième année consécutive, révèle le *Freedom on the Net 2017*, le rapport de Freedom House. L'utilisation des médias sociaux pour «faire avancer un agenda antidémocratique» a apporté de nouveaux défis, car il est «plus difficile à combattre que d'autres types de censure», a expliqué le directeur du projet.

Juridiction et questions juridiques



Evolution en hausse

Un juge de la Californie a bloqué l'effet aux États-Unis d'une décision de la Cour suprême du Canada sur le droit à l'oubli numérique. [Plus de détails à la page 1.](#)

La Commission européenne a mis en place un groupe d'experts de haut niveau sur les fausses informations et la désinformation en ligne, avec des représentants du monde universitaire, de l'industrie des technologies, des médias et de la société civile. Il a lancé une consultation publique pour nourrir une stratégie de l'UE pour lutter contre la diffusion de fausses informations.

Infrastructures



En stagnation

Une nouvelle loi en Russie limitant l'utilisation d'outils de proxy tels que les réseaux privés virtuels (VPN) et services d'anonymisation est entrée en vigueur le 1er Novembre.

Le Conseil de sécurité de la Russie aurait demandé au gouvernement d'entamer des pourparlers avec les pays du BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) sur la possibilité de construire un système de serveur racine DNS alternatif.

Skype, appartenant à Microsoft, a été retiré de plusieurs boutiques d'applications informatiques chinoises, y compris celles exploitées par Apple et Android. Apple a été informé par le Ministère de la sécurité publique qu'un «certain nombre d'applications de voix sur protocole Internet ne respectaient pas la législation locale».

Neutralité du net



Evolution en hausse

La Commission fédérale des communications (CFC) des États-Unis se prépare à voter sur le retrait des règles de neutralité du net de 2015. [Plus d'informations à la page 6.](#)

L'Autorité de régulation des télécommunications de l'Inde a publié une série de recommandations en faveur de la neutralité du net, indiquant que les conditions de licence applicables aux fournisseurs d'accès Internet devaient inclure des restrictions explicites sur toute forme de discrimination dans l'accès à Internet basé sur les contenus, les protocoles utilisés et l'équipement déployé.

Nouvelles technologies: Intelligence artificielle, Internet des objets, etc.



Evolution en hausse

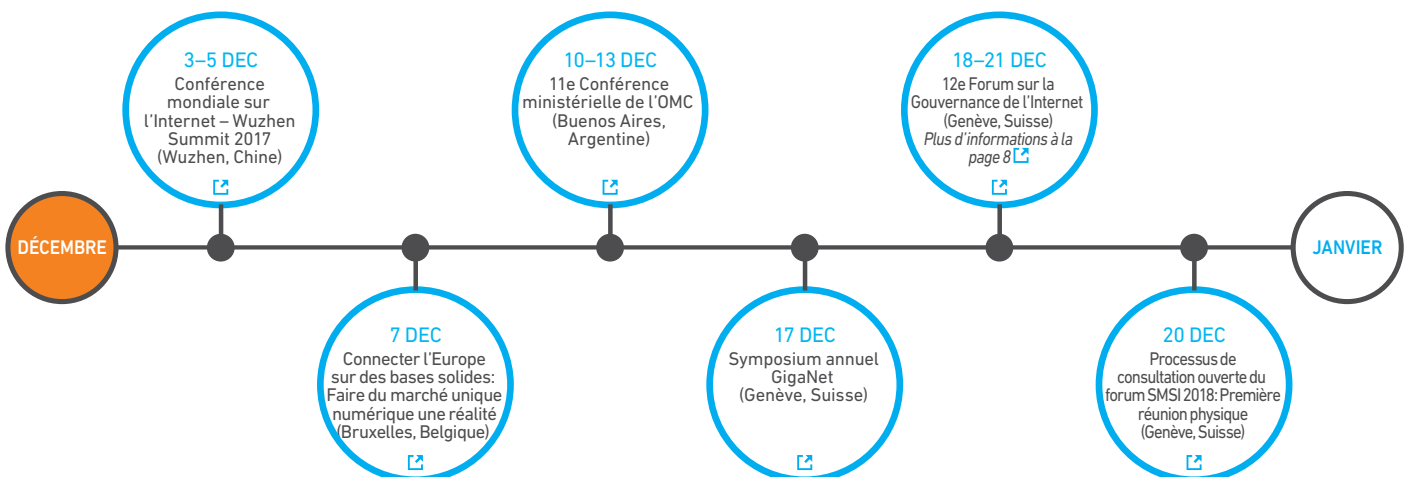
Le Groupe d'experts gouvernementaux sur les systèmes d'armes létales autonomes s'est réuni pour la première fois à Genève, pour discuter des questions technologiques, militaires, juridiques et éthiques relatives à ce type d'armes. [Plus aux pages 1 et 7.](#)

À Tokyo, le chatbot Shibuya Mirai – programmé pour ressembler à un garçon de 7 ans – bénéficie d'une résidence officielle. Le chatbot vise à rendre le gouvernement local plus familial et accessible aux résidents, permettant aux fonctionnaires de mieux prendre en compte leurs opinions.

En Arizona, aux États-Unis, la société Waymo, appartenant à Alphabet, a commencé à tester des voitures autonomes sur les routes publiques, sans un pilote humain à bord. Le Royaume-Uni a annoncé des plans pour des voitures entièrement autonomes, sans opérateur humain d'ici 2021. Singapour vise à avoir des bus sans conducteur d'ici 2022.

Un rapport publié par le Center for Policy Studies au Royaume-Uni soutient que taxer les robots ne protégera pas les emplois, et que les appels à un revenu de base universel sont prématurés car cela impactera de manière négative le marché du travail.

ÉVÉNEMENTS EN DÉCEMBRE



Pour plus d'informations sur les événements à venir, visitez <http://dig.watch/events>

NEUTRALITE DU NET DANS TURMOIL

La Commission fédérale des communications (CFC) des États-Unis devrait revenir sur les règles en faveur de la neutralité du net en décembre. Les règles adoptées en 2015 soutenaient fortement la neutralité du net. Les nouvelles règles vont-elles compromettre la protection du principe de neutralité de l'internet?

Plus tôt cette année, la CFC a annoncé son intention d'annuler ces règles. Cette campagne a été menée par son président Ajit Pai. La CFC, à majorité républicaine, devrait voter en décembre pour remplacer l'*Open Internet Order* de 2015 par le nouveau *Restoring Internet Freedom Order*.

Les règles de 2015 soutenaient fortement la neutralité du net. Elles ont reclassé les fournisseurs de services d'accès Internet à large bande en fournisseurs de services publics, ce qui signifie qu'ils sont soumis à l'autorité et à la surveillance de la CFC pour s'assurer qu'ils n'interfèrent pas avec la vitesse ou la sélection du contenu par l'accès à Internet qu'ils fournissent à leurs utilisateurs.

Le projet des nouvelles règles, diffusé en novembre, rétablirait la classification des fournisseurs de services à large bande en tant que fournisseurs de «services d'information», limitant ainsi l'autorité de la CFC et leur permettant de développer des modèles allant à l'encontre des principes de neutralité du net. Les nouvelles règles exigeront seulement que les fournisseurs de services Internet soient transparents et divulguent des informations sur leurs pratiques aux consommateurs, aux entrepreneurs et à la commission.

Des réactions diverses

Le projet de règles a trouvé le soutien d'entreprises telles que Verizon et Comcast, qui ont également demandé à la CFC d'adopter une décision confirmant la primauté de la loi fédérale et empêchant les états d'adopter leurs propres règlements de neutralité du net.

Cependant, d'autres entreprises de l'Internet s'opposent à ces nouveaux plans. Parmi celles-ci, on note Google, Facebook et Netflix qui estiment que les règles actuelles fonctionnent bien. Deux cent autres entreprises de technologie, parmi lesquelles AirBnB, Reddit et Twitter, partagent ce point de vue et ont envoyé une lettre à la CFC demandant à la commission de voter contre la nouvelle réglementation.

Au-delà des États-Unis, le Premier ministre canadien Justin Trudeau a exprimé une inquiétude quant à la possible révision des règles de neutralité du net aux États-Unis, notant que la neutralité du réseau «est essentielle pour les petites entreprises et les consommateurs, et qu'il est essentiel de préserver la liberté associée à Internet».

Alors que la plupart des regards se tournent vers les États-Unis, l'Inde a également attiré l'attention récemment, par le biais de

son Autorité de régulation des télécommunications a publié une série de recommandations en faveur de la neutralité du net.

Que va-t-il se passer ensuite?

A quelques semaines seulement du vote de la CFC, il y a plusieurs scénarios possibles:

1. **Activisme.** En juillet dernier, de grandes entreprises de l'Internet et des organisations de la société civile ont participé à une «journée d'action» en ligne en faveur des règles de neutralité du net, dans le cadre de la campagne *Battle for the Net*. La campagne a été relancée et des militants à travers les États-Unis organisent une manifestation le 7 décembre. Il reste à voir si de telles actions auront l'impact souhaité.

2. **Congrès.** Lors d'une interview en septembre, le président de la CFC, Pai, a plaidé pour que la question de la neutralité du net soit abordée par le Congrès américain, qui «serait bien placé pour se saisir de cette question et déterminer quelles seraient les règles ou la feuille de route à long terme».

Cela pourrait en être le cas, alors que plusieurs voix appellent le Congrès à intervenir et à commencer à travailler sur la législation en faveur de la neutralité du net. Mais il y existe aussi la possibilité – du moins en théorie – pour le Congrès d'adopter une résolution de désapprobation et rejeter l'abrogation de l'*Open Internet Order* de 2015. La probabilité que l'une de ces deux options devienne une réalité demeure incertaine.

3. **Action en justice.** Si la CFC adopte l'acte proposé par le président Pai, il est possible qu'il soit attaqué en justice, au motif qu'il n'est pas dûment justifié. Conformément à la jurisprudence américaine, les agences ne peuvent pas renverser les règles existantes sans faire valoir une argumentation solide:

Une décision de la Cour suprême rendue en 1983 stipulait qu'«une agence qui change de cap en annulant une règle est obligée de fournir une analyse en profondeur du changement au-delà de ce qui peut être requis lorsqu'une agence n'agit pas en première instance». Certains commentateurs soutiennent que ce n'est pas le cas avec le projet d'ordonnance, qui semble reposer sur l'argument selon lequel les investissements dans les infrastructures à haut débit ont diminué au cours des deux dernières années.

Suivez l'observatoire GIP Digital Watch pour les mises à jour.



SYSTEMES D'ARMES LÉTALES AUTONOMES: LES EXPERTS IDENTIFIENT LES PRINCIPAUX PROBLÈMES

La technologie a toujours révolutionné les conflits. Aujourd'hui pourtant, la société pourrait être à l'aube d'un développement technologique fondamentalement différent: la perte du contrôle humain dans la guerre. En novembre, le Groupe d'experts gouvernementaux (GGE) a exploré les implications technologiques, militaires, juridiques et éthiques liées à de tels systèmes.

Pour éviter les scénarios dans lesquels les systèmes d'armes létales autonomes (SALA) causeraient des préjudices inutiles, les Hautes parties contractantes à la Convention sur certaines armes classiques (CCAC) ont établi le Groupe d'experts gouvernementaux pour examiner les questions liées aux technologies émergentes dans le domaine des SALA, avec la participation des différentes parties prenantes. Au cours des discussions du groupe, les 13 et 17 novembre, cinq questions clés ont émergé.

1. Prévisibilité et fiabilité: peut-on faire confiance à un robot tueur?

Alors que les systèmes d'armes parfaitement autonomes peuvent être source d'inquiétude, un des défis majeurs concernent l'imperfection potentielle de ces systèmes. Comme elles sont guidées par des technologies telles que l'apprentissage automatique, l'action des SALA peuvent être difficile à prévoir, et les résultats attendus pourraient ne pas être garantis. Ces systèmes soulèvent également la question de savoir si et dans quelle mesure les normes éthiques et le droit international pourraient être incorporés dans les algorithmes dirigeant ces systèmes d'armes.

L'imprévisibilité potentielle des SALA pourrait également signifier qu'elles ne seront pas largement utilisées. Un certain niveau de confiance dans la technologie est nécessaire avant qu'elle puisse être utilisée à des fins militaires.

2. La prolifération et la course aux armements: Vers une destruction mutuelle ou une dissuasion?

Beaucoup craignent que les états qui fabriquent des SALA ne soient pas en mesure d'empêcher leur prolifération au fil du temps, ce qui pourrait aboutir à une course mondiale aux armements. Des inquiétudes concernent aussi l'utilisation de tels systèmes par des acteurs nationaux contre leur propre population, ainsi que par des groupes terroristes et des acteurs non étatiques. À cet égard, certains ont soulevé la question de savoir dans quelle mesure le développement de telles technologies par des entreprises privées pourrait être réglementé.

La prolifération des SALA pourrait avoir des implications importantes pour la paix et la sécurité internationale, même si nous ne pouvons que spéculer sur leurs possibles retombés. Par exemple, une relation de dissuasion mutuelle entre les pays possédant des SALA pourrait se développer, mais il y a également des inquiétudes quant à une possible destruction mutuelle.

3. L'humanité en conflit: Devons-nous externaliser les décisions de vie et de mort?

Beaucoup affirment que les machines sont incapables de remplacer les humains dans les jugements qualitatifs sur lesquels repose la décision de cibler mortellement un individu. Prendre de telles décisions exige de la compassion et de l'intuition, attributs que nous ne pouvons pas attendre des robots. Bien que les SALA soient capables de prendre des décisions rapides et précises, ils ne seront pas en mesure d'évaluer les contextes.

L'externalisation des décisions de vie ou de mort à des machines non seulement risquerait de leur permettre de choisir la mauvaise option, mais rendrait également la guerre plus inhumaine et pourrait abaisser le seuil d'utilisation de la force.

Cependant, certains estiment que les systèmes d'armes automatisés offrent en réalité des avantages humanitaires potentiels et génèreraient moins de dommages collatéraux. Les machines pourraient être en mesure de prendre des décisions plus rapidement et de meilleure qualité, ce qui contribuerait ainsi à la protection des civils et à la proportionnalité de l'attaque. En outre, certains soulignent aussi que les êtres humains ne sont pas toujours éthiques eux-mêmes.

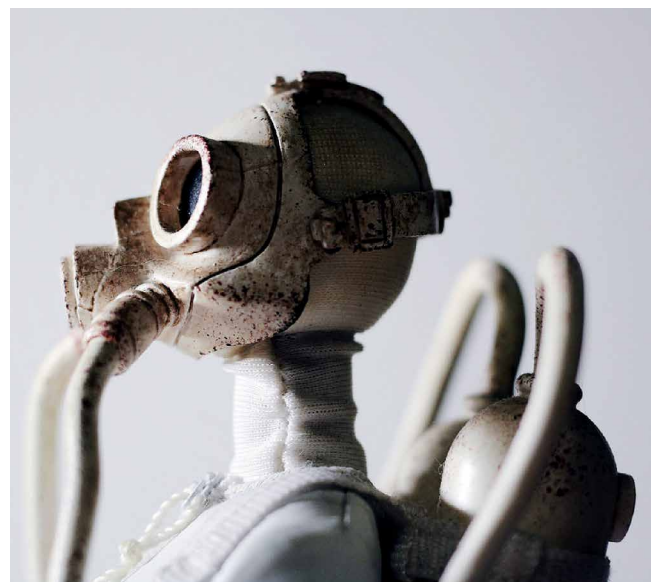
4. Responsabilité: Comment pouvons-nous tenir un robot responsable?

L'une des principales préoccupations concerne la responsabilité légale. Si une arme autonome mène une attaque mortelle, qui est responsable? Comme les SALA couvrent de nombreux échelons dans la chaîne de responsabilité militaire, il peut être difficile de déterminer qui est responsable. Il existe des craintes qu'une responsabilité imprécise, non déterminée, puisse donner lieu à de l'impunité. Cependant les lois s'appliquent aux humains, et la responsabilité légale incombe à ceux qui planifient, décident et mènent des attaques. Cette responsabilité légale ne peut être transférée à une machine. Dans ce contexte, certains états ont également mis en garde contre la mise en place de systèmes autonomes dotés d'une personnalité juridique.

5. Double usage: Et si la force du mal est simultanément une force pour le bien?

L'application future de l'intelligence artificielle et de la robotique dans de nombreux aspects de la vie civile et économique, au profit de l'humanité, a amené certains négociateurs à demander instamment la mise en garde contre d'autres actes législatifs ou une interdiction concernant les SALA. Pour autant, la nature à double usage de ces technologies signifie également que les armes autonomes conçues pour un usage civil pourraient être transformées en armes létales, ajoutant plus de complexité à la question.

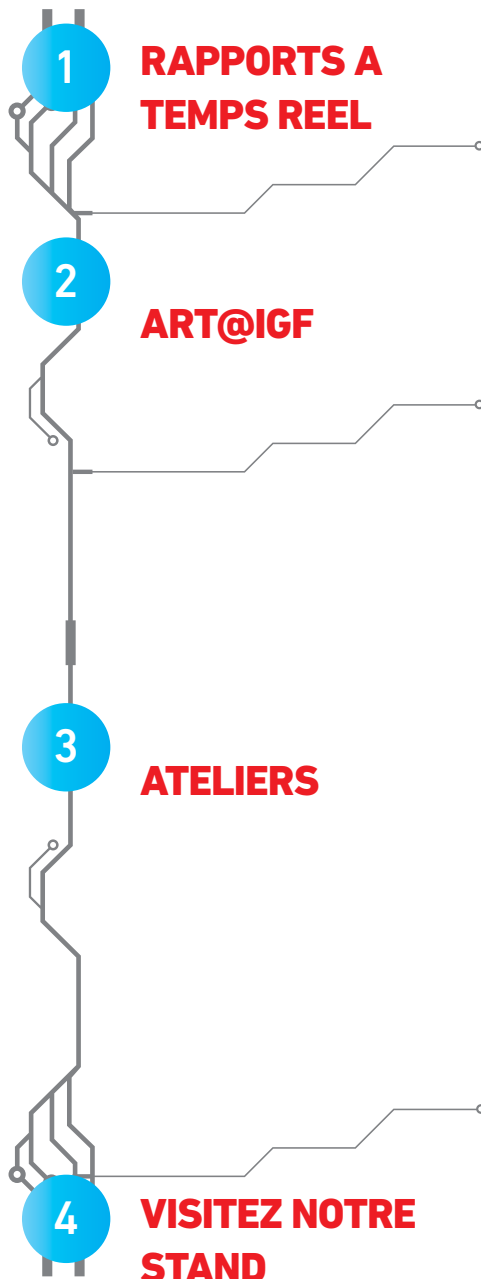
Lire le document d'orientation complet sur les résultats de la réunion du Groupe d'experts gouvernementaux sur les SALA. [↗](#)



Crédit: Siyan Ren on Unsplash

LA GIP AU 12^{ème} FORUM SUR LA GOUVERNANCE DE L'INTERNET

La Geneva Internet Platform sera activement présente au 12^e Forum sur la Gouvernance de l'Internet (FGI), à Genève et en ligne. Rejoignez-nous pour les activités suivantes et suivez les rapports des sessions en temps réel et les bulletins d'information quotidiens sur le FGI.



L'observatoire *GIP Digital Watch* fournira des rapports de sessions en temps réel sur le FGI et des bulletins d'information quotidiens, qui seront disponibles sur une page Web dédiée, à l'adresse dig.watch/igf2017. Un rapport final, publié après la réunion du FGI, résumera les principaux sujets. Ceux-ci compléteront les mises à jour continues offertes par l'observatoire.

Ce projet reliera la politique numérique à l'art dans une exposition interactive et interdisciplinaire sur les questions numériques. L'exposition utilisera une carte de métro comme métaphore d'un voyage pour explorer différentes questions de gouvernance de l'Internet (infrastructure, sécurité, droits de l'homme, etc.), chacune représentée comme une ligne de métro d'une couleur différente sur le sol de l'exposition. Au fur et à mesure que les participants suivront les différentes lignes, ils arriveront dans les stations de métro où des artistes numériques présentent leurs perceptions sur des questions importantes et actuelles de politique numérique.

Le GIP co-organise les ateliers suivants au FGI:

Gouvernance et politique des données: Elaboration d'un curriculum (WS186) – Lundi 18 Décembre, 09h00-10h30, Salle XI – A

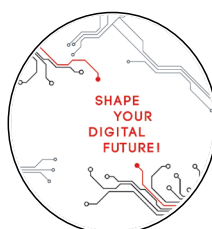
Les données sont au cœur de la société moderne, de notre empreinte digitale via le courrier électronique et les médias sociaux, à l'analyse des Big Data. Bien que la gouvernance et la politique des données requièrent de nouvelles compétences et techniques, la demande d'experts en politiques de données n'est pas satisfaite par l'offre. Cet atelier discutera d'un programme qui devrait être utilisé pour le renforcement des capacités, la formation et les activités académiques pour améliorer l'élaboration des politiques.

Une Convention de Genève numérique pour la protection du cyberspace (WS34) – Mardi 19 Décembre, 10h40-12h10, Salle XXI – E

Une cybersécurité efficace étant essentielle à la paix internationale et à la stabilité économique, la création d'une Convention de Genève numérique pourrait jouer un rôle central dans la protection des citoyens, des infrastructures et des entreprises privées du monde entier contre les cyberattaques dirigées par des états. Cet atelier réunira des experts en matière de cybersécurité et de politique technologique de différents groupes de parties prenantes afin de les sensibiliser aux questions cruciales des normes de cybersécurité, au fossé entre les efforts internationaux et la réalité, et de discuter de la marche à suivre.

En outre, l'équipe GIP et Diplo seront impliqués dans un certain nombre d'autres sessions, en tant qu'intervenants, modérateurs in situ et en ligne, et rapporteurs.

Le GIP et Diplo auront un stand dédié au Village FGI. Rendez-nous visite toute la semaine pour obtenir vos exemplaires des bulletins quotidiens du FGI et autres publications sur la gouvernance de l'Internet (y compris le dernier numéro du bulletin *Geneva Digital Watch*, le livre *Introduction à la Gouvernance de l'Internet* et le livret des acronymes sur la gouvernance de l'Internet).



Abonnez-vous aux mises à jour de GIP Digital Watch à <http://dig.watch>