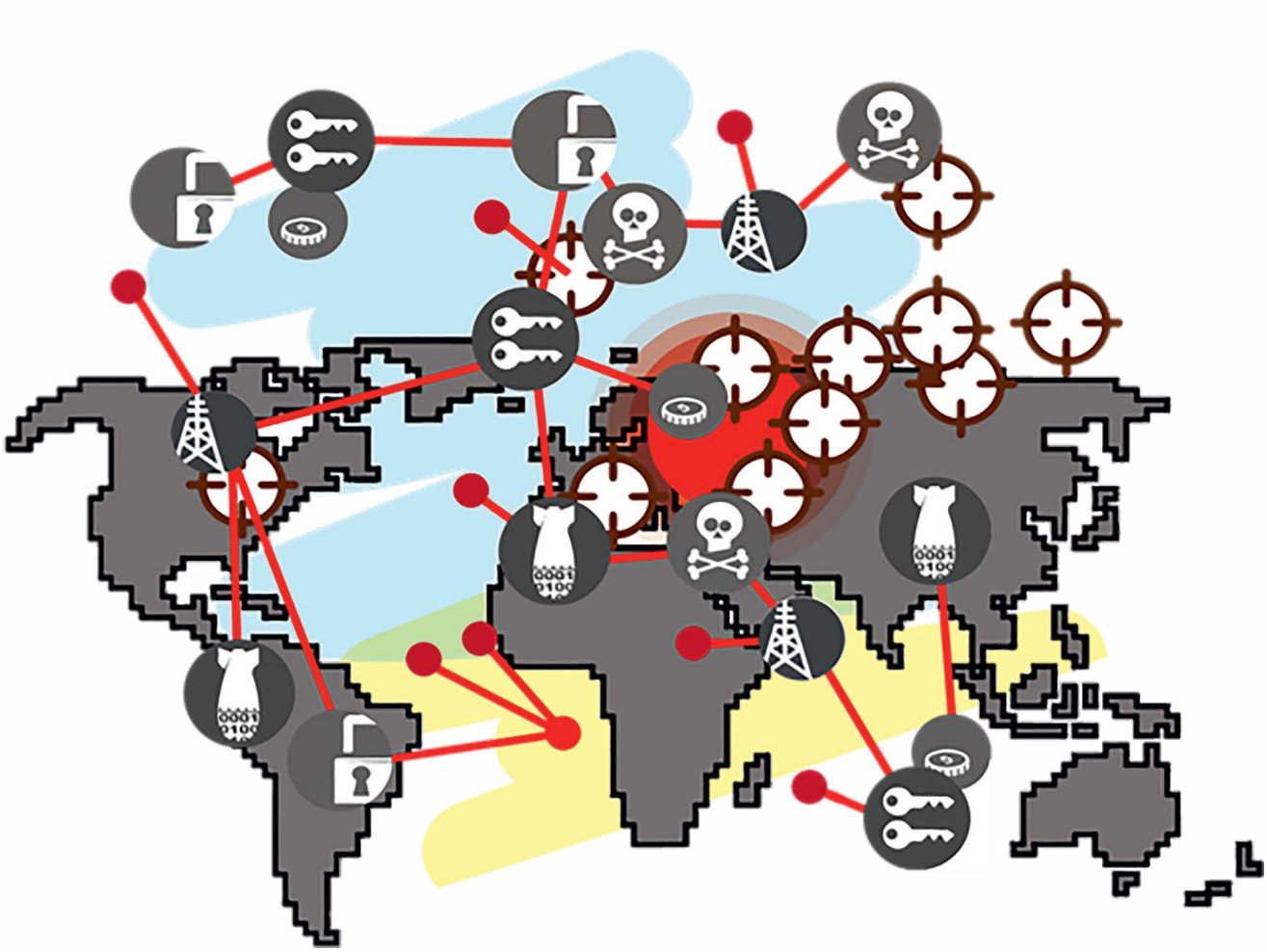
GENEVA INTERNET PLATFORM
digwatch

LETTRE D'INFORMATION

Numéro 67 – Mars 2022



NUMÉRO SPÉCIAL

Le front cyber du conflit ukrainien

Pages 2–4

ICANN

La demande de l'Ukraine à l'ICANN de couper la Russie de l'Internet a été rejetée. Plusieurs raisons expliquent cette décision.

Page 5

POLITIQUE AMÉRICAINE

Le discours sur l'état de l'Union de cette année a souligné trois priorités numériques qui ont une influence sur l'évolution des politiques mondiales et de la situation géopolitique.

Pages 6–7

BAROMÈTRE

Les récents développements en matière d'infrastructures et de développement durable ont propulsé ces questions au cœur de l'actualité.

Pages 8–9

GENÈVE

De nombreuses discussions politiques ont lieu chaque mois à Genève. Voici ce qui s'est passé au cours des dernières semaines.

Page 10–11

ORGANISATION INTERNATIONALE DE la francophonie

D-CLIC FORMEZ-VOUS AU NUMÉRIQUE !

La lettre d'information en français *Digital Watch* est publiée en collaboration et avec le soutien de l'Organisation internationale de la Francophonie dans le cadre de l'initiative D-CLIC, Formez-vous au numérique avec l'OIF.

Les cyber armes et la guerre en Ukraine

Les technologies numériques sont mobilisées de deux manières principales dans la guerre entre la Russie et l'Ukraine. La première consiste à cibler les infrastructures critiques. La seconde à utiliser la désinformation comme un pilier de l'arsenal de guerre.

Mise à mal des infrastructures critiques

Dès que la crise ukrainienne a dégénéré en attaques armées, les cyberattaques ont suivi. Les **sites Web du gouvernement** ukrainien **et des banques** ont été les premiers à être touchés. Puis sont venues les attaques contre les **organisations**, les **troupes** et les points de **contrôle frontaliers ukrainiens**.

La plupart de ces attaques **ont utilisé un logiciel malveillant appelé HermeticWiper**, permettant d'effacer les données. Ainsi les attaquants utilisent un logiciel malveillant qui détruit les données, tout comme les attaques armées détruisent des cibles physiques.

Les experts en cybersécurité qui ont analysé le logiciel malveillant ont déclaré jusqu'à présent qu'il n'y avait pas suffisamment de preuves pour attribuer HermeticWiper à la Russie, mais le moment de son déploiement était une trop grande coïncidence pour être ignoré. Les attaques par hameçonnage (*phishing* en anglais) contre les troupes ukrainiennes, en revanche, **ont été attribuées aux pirates de l'UNC1151**, des officiers de l'armée biélorusse.

En réponse, d'autres acteurs sont intervenus pour aider l'**armée informatique** ukrainienne à repousser les attaques : L'UE a déployé son **équipe de réponse rapide aux attaques informatiques (CRRT) en Ukraine** ; des entreprises (telles que **Google** et **Amazon**) ont promis de soutenir l'Ukraine en matière de cyber sécurité. Des groupes de pirates informatiques comme Anonymous ont lancé des attaques par déni de service (DDoS) contre la bourse de Moscou, le **ministère russe de la défense** et l'**agence spatiale russe Roscosmos**.

Ce que les États ne devraient pas faire, mais feront quand même

L'escalade du conflit se poursuit, tout comme les cyberattaques. Les dernières sanctions - y compris la suspension des opérations en Russie par le **réseau SWIFT**, **Paypal**, **VISA**, et **Mastercard** - ne font qu'accroître les problèmes de cybercriminalité pour les banques internationales, qui **sont en état d'alerte**.

L'histoire récente nous montre que la **cyberguerre ne s'arrêtera pas aux banques**. Même si les normes de

Un groupe de pirates informatiques affilié à Anonymous a tweeté qu'il avait « fermé le centre de contrôle » de l'agence spatiale russe Roscosmos. Mais le chef de Roscosmos a démenti ces informations. Photo : Le poste de contrôle de l'agence spatiale russe Roscosmos, mars 2018 (crédit : NASA/Joel Kowsky).

comportement des États interdisent certaines actions, elles n'ont pas empêché les attaques par rançongiciels de paralyser les réseaux électriques, l'approvisionnement en nourriture et les hôpitaux en temps de paix - et encore moins **en temps de guerre**.

La désinformation fait des ravages

Bien que les cyberattaques soient le type d'armes le plus évident en temps de guerre, la désinformation est tout aussi dangereuse et plus insidieuse. Elle peut être déployée de manière subtile, proliférer et se répandre sur de multiples canaux, et toucher les gens en masse.

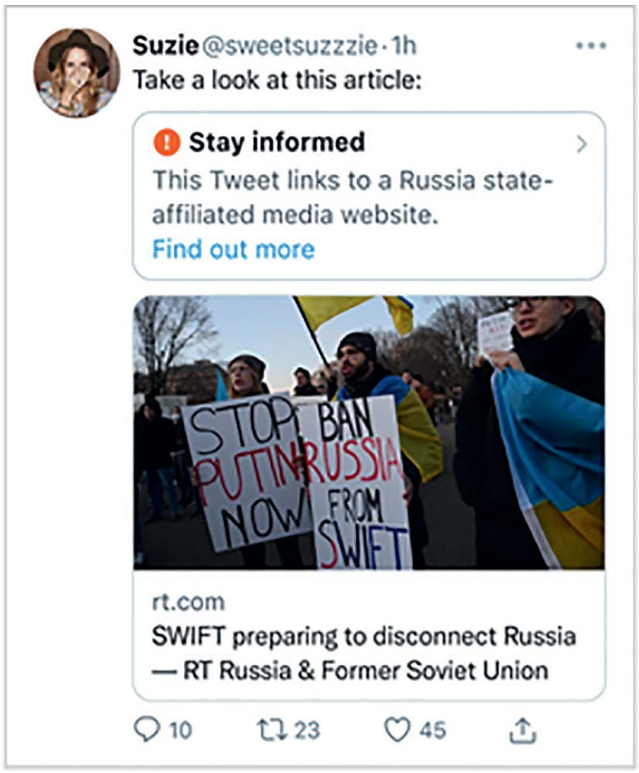
Trois éléments interviennent dans la diffusion de la désinformation :

- Le message
- Le messager
- Le destinataire.

Pour contrer la propagation de la désinformation, il est nécessaire de prendre en compte ces trois éléments.

En ce qui concerne le « message », les deux parties se sont accusées mutuellement de diffuser de la désinformation.

L'Ukraine et ses partisans affirment que les médias d'État russes **produisent des fausses nouvelles**. La Russie affirme que les informations sur le conflit ukrainien destinées au public russe sont **fausses** et **inappropriées**.



Un tweet avec une étiquette

Cependant, les médias d'État russes ont été de loin les plus critiqués, ce qui leur a valu, par exemple, une **interdiction de diffusion en Europe**.

Le « *messager* » comprend les médias traditionnels (principalement la télévision) et les canaux numériques (principalement les réseaux sociaux, qui sont également utilisés pour rester en contact avec les familles et les amis).

Contrairement aux médias grand public, les canaux numériques ont la capacité de diffuser des messages avec une portée et une rapidité étonnantes, mais pour de nombreuses personnes, la télévision reste le seul média de masse auquel elles ont accès.

L'interdiction par l'UE des médias d'État russes a affecté les deux ; les actions du secteur privé ont également concerné les deux.

Lorsqu'il s'agit du « *destinataire* », la désinformation n'a que peu de limites. Cela signifie que tout le monde peut être exposé à un contenu erroné et que chacun devrait donc avoir les moyens de vérifier les faits et de trouver d'autres sources d'information.

Alors que l'Ukraine (et de nombreux autres pays) a accès à tous les types d'informations qu'ils souhaitent, les Russes ne peuvent accéder qu'aux médias d'État, les autres canaux médiatiques étant bloqués. L'impossibilité de vérifier les informations a pour conséquence que la désinformation continue de proliférer sans limite.

Séparer le message des canaux qui le transportent

La semaine dernière, Cogent Communications, l'un des plus grands gestionnaires de trafic Internet au monde, a informé certains de ses clients russes qu'**il allait interrompre son service**. Le PDG de Cogent a expliqué : « Je ne peux pas distinguer le bon trafic russe du mauvais... C'est juste un gros tuyau ».

Si cela peut s'avérer vrai pour les opérateurs de réseaux, les plateformes de réseaux sociaux ont une meilleure visibilité (et plus de possibilités) concernant les communications de messages circulant sur leurs services. Elles sont capables de discerner qui voit un message en ligne et comment tous les autres y ont réagi.

Cela signifie qu'en pratique, les plateformes de réseaux sociaux pourraient décider de cibler leurs interdictions de manière encore plus précise (leur conformité avec l'interdiction de l'UE confirme qu'elles le peuvent) - si elles le souhaitent.

Pour les plateformes de réseaux sociaux, il s'agit d'une arme à double tranchant : tolérer la propagation de la désinformation, tout en aidant les gens à rester en contact.

Ou bloquer le contenu à sa source, et risquer une interdiction gouvernementale de toute la plateforme. Jusqu'à présent, les entreprises sont dans cet entre-deux : Elles apposent des étiquettes de mise en garde sur des messages spécifiques et espèrent que l'accès à leur plateforme reste inchangé.

Cela importe peu pour Facebook et Twitter. Le régulateur russe des communications, Roskomnadzor, a annoncé que le **pays les bloquait désormais**.

Mais cela n'en reste pas moins important pour les autres plateformes de réseaux sociaux populaires dans la région (surtout si elles aident aussi les gens à rester en contact) et les autres plateformes d'information. Elles aussi sont confrontées à cette arme à double tranchant, et jusqu'à ce que l'autorité Roskomnadzor arbitre, quel serait pour elles le moindre mal ?

Actions affectant les médias d'État russes, notamment RT et Sputnik

	EN RUSSIE	DANS L'UE	MONDIAL
Google (YouTube)		Blocage des chaînes RT et Sputnik dans toute l'Europe	
	Interdire aux médias publics de faire de la publicité		
	Limiter les recommandations des articles des médias d'Etat au niveau mondial		
	Suppression de chaînes/vidéos pour violation des règles de la communauté		
Meta (Facebook, Instagram)	Mise en pause de toutes les publicités ciblant la population russe		
		Blocage de l'accès à RT et Sputnik	
	Bloquer toutes les publicités des annonceurs russes		
Twitter	Ajout d'étiquettes sur les tweets liés aux médias d'État russes		
	Réduire la circulation des contenus de l'État russe sur Twitter		

Russie : Bloquer ou ne pas bloquer

Il est facile de se laisser emporter par des pensées bellicistes à la lecture des rapports faisant état des victimes civiles et les bombardements sur les couloirs humanitaires. Mais une demande de suppression d'un pays de l'Internet nécessite un raisonnement mesuré.

Si cela est possible...

Lorsque le vice-premier ministre ukrainien a **demandé à l'ICANN** (l'organisation qui gère le DNS ou carnet d'adresses de l'internet) de couper la Russie de l'Internet, rares étaient ceux qui doutaient de **la capacité de l'ICANN à s'exécuter**, si elle le décidait.

En termes techniques, elle pourrait déclencher un arrêt total (ou « kill-switch » en anglais) par une action unilatérale de l'Internet Assigned Numbers Authority (IANA). Sur le plan juridique, la Californie ayant compétence sur l'ICANN, les États-Unis pourraient théoriquement ordonner à l'ICANN de prendre des mesures. Et si cela n'impliquait pas la Russie, l'un des cinq membres permanents du Conseil de sécurité des Nations unies disposant d'un droit de veto, la **Charte des Nations unies (article 41)** pourrait être invoquée pour sanctionner les mesures prises par « d'autres moyens de communication ».

Ce n'est pas forcément nécessaire...

Il y a plusieurs raisons pour lesquelles **la demande de l'Ukraine a été rejetée**. La première est qu'une action unilatérale aurait détruit tout le modèle qui a mis des décennies à se construire. Il existe toute une structure de responsabilité, renforcée en 2016, qui permet de s'assurer que les fonctions de l'ICANN et de l'IANA ne sont pas utilisées à mauvais escient.

La seconde est que la demande de l'Ukraine n'aurait pas garanti que la Russie soit entièrement coupée du monde. Certaines parties du système échappent au contrôle de l'ICANN et pourraient entraîner une fragmentation de l'Internet.

La troisième est que la déconnexion d'un pays de l'Internet n'est pas la solution pour contrer les actes répréhensibles de ce pays, quelle que soit leur gravité.

Une telle action marquerait le début de la fin de l'Internet que nous connaissons aujourd'hui, qui, malgré tous ses problèmes, **reste un bien public mondial intégré**.

Les intentions de la Russie avec le RuNet

Et si c'était la Russie elle-même qui voulait se couper de l'internet ? Aussi invraisemblable que cela puisse paraître, il est possible que le pays soit déjà prêt et capable de faire cavalier seul.

Un test réalisé en 2019 a permis de conclure que l'infrastructure Internet nationale russe, connue sous le nom de RuNet, **pouvait fonctionner sans accéder au système DNS mondial et à l'internet externe**. Selon les rapports, le test a été effectué **à nouveau en 2021**. Un **tweet non vérifié** de Nexta, basé en Biélorussie, affirme maintenant que la Russie pourrait se déconnecter le 11 mars.

Quelle que soit la personne qui en donne l'ordre, les effets d'une Russie déconnectée seront les mêmes : un Internet fragmenté et un peuple encore plus isolé. Cela signifie que les Russes seront incapables d'entrer en contact avec d'autres personnes au-delà de leurs propres frontières et qu'ils ne pourront pas accéder à des informations autres que celles que l'État veut leur montrer. Si cela se produit, cela signifierait également une perte pour le reste du monde.

Approfondissez l'analyse et consultez notre chronologie des développements.

Discours sur l'état de l'Union aux Etats-Unis : Politique nationale, impact mondial

Le discours du président américain sur l'état de l'Union, prononcé (presque) chaque année, donne une bonne idée des priorités et des projets du pays pour le reste de l'année. Dans quelle mesure les trois questions numériques mentionnées dans le discours de cette année - semi-conducteurs, taxes numériques et bien-être des enfants en ligne - affecteront-elles la politique numérique et la géopolitique mondiale ?

Nationalisme économique, compétitivité mondiale

Le discours du président américain Joe Biden a souligné la volonté des États-Unis de réduire la dépendance de leur chaîne d'approvisionnement à l'égard des autres pays, notamment dans le secteur des semi-conducteurs. Les semi-conducteurs sont un composant clé de pratiquement tous les appareils électroniques que nous possédons.

Le secteur est particulièrement fragile : l'augmentation de la demande de produits de consommation) et les perturbations dans la fabrication des puces (à mettre sur le compte de COVID-19) ont entraîné d'énormes pénuries de produits électroniques et une hausse des prix.

L'industrie des puces est également l'un des secteurs qui dépendent fortement de la recherche et du développement (R&D). Si une entreprise se relâche, elle peut facilement et très rapidement être dépassée par d'autres entreprises utilisant des technologies plus avancées.

L'ambition des États-Unis s'explique par une équation simple : Si le gouvernement est en mesure de construire davantage d'usines de puces sur son propre territoire en subventionnant leurs coûts, il peut réduire les pénuries dans la chaîne d'approvisionnement et diminuer sa dépendance à l'égard des autres pays.

La partie du discours de M. Biden consacrée aux infrastructures décrit ce que fait le gouvernement américain pour réaliser cette ambition. Le fabricant de puces Intel, par exemple, **vient de lancer la construction de deux fonderies dans l'Ohio, pour un montant de 10 milliards de dollars chacune**. « ...Cela signifie, fabriquer plus de voitures et de semi-conducteurs en Amérique, plus d'infrastructures et d'innovations en Amérique, plus de marchandises circulant plus rapidement et moins cher en Amérique, plus d'emplois où l'on peut bien gagner sa vie en Amérique. Au lieu de dépendre des chaînes d'approvisionnement étrangères, fabriquons-les en Amérique. »

Mais même si le discours du président sur le « made in America » est aussi un appel aux entreprises et aux

Premier pilier	Deuxième pilier
Début 2022 - Texte de la Convention multilatérale (MLC) et exposé des motifs pour la mise en œuvre du montant A du premier pilier.	Novembre 2021 - Règles modèles pour définir le champ d'application et les mécanismes des règles GloBE.
Début 2022 - Modèle de règles pour la législation nationale nécessaire à la mise en œuvre du premier pilier.	Novembre 2021 - Modèle de disposition conventionnelle pour donner effet à la règle de l'*assujettissement à l'impôt*
Mi-2022 - Cérémonie de signature à haut niveau pour la MLC	Mi-2022 - Instrument multilatéral (MLI) pour la mise en œuvre du STTR dans les traités bilatéraux pertinents
Fin 2022 - Finalisation des travaux sur le montant B du premier pilier.	Fin 2022 - Cadre de mise en œuvre pour faciliter la mise en œuvre coordonnée des règles GloBE
2023 - Mise en œuvre de la solution à deux piliers	

Les échéances des objectifs de l'OCDE

consommateurs américains pour qu'ils contribuent à la réalisation de cette ambition, l'équation ne s'arrête pas là.

Par exemple, les principaux fabricants de semi-conducteurs du monde se livrent une concurrence acharnée pour fabriquer des produits technologiquement plus avancés. Étant donné que la technologie utilisée par TSMC (société taïwanaise) et Samsung (société sud-coréenne) est sans doute la plus avancée qui soit, les paris du gouvernement américain sur Intel doivent être assortis de mises à niveau opportunes de la technologie sur laquelle Intel travaille.

L'UE veut produire au moins 20 % des puces de nouvelle génération dans le monde d'ici à 2030.

La Chine investit également massivement dans sa propre production. Si la Chine est en mesure d'accroître l'utilisation des puces fabriquées dans le pays, elle réduira non seulement la part de marché des autres, mais aussi sa propre exposition aux retards de la chaîne d'approvisionnement. Le temps ne joue pas en faveur des États-Unis.

Taxez-les tous, mais faites-le rapidement

La plus grande bataille pour réformer les règles fiscales mondiales, afin de les adapter aux temps modernes, s'est achevée l'année dernière lorsque **près de 140 pays ont accepté les nouvelles règles de l'OCDE** (il s'agit désormais de régler les détails techniques et de les mettre en œuvre au niveau national).

Les nouvelles règles reposent sur deux piliers. Le premier pilier définit une manière de décider quelle(s) juridiction(s) doit(vent) collecter les impôts des grandes multinationales.

Les impôts (plutôt que la juridiction où elles sont constituées en société : Ce seront les pays où elles sont le plus actives économiquement). Le deuxième pilier obligera les pays à imposer un taux d'imposition minimal de 15 % pour les entreprises réalisant plus de 750 millions d'euros de recettes.

Le Congrès américain est en train de codifier les règles. En raison de complications techniques (notamment autour des **calculs**), le processus est au point mort. Une fois encore, le temps ne joue pas en faveur des États-Unis.

L'une des variables à prendre en compte est l'élection de mi-mandat en novembre : si le parti du président Biden perd l'une ou les deux chambres du Congrès, les **négociations seront encore plus bloquées**.

Si les choses continuent à stagner à Washington (**le premier pilier est plus délicat pour les États-Unis**), elles stagneront également au niveau de l'UE, malgré les progrès de cette dernière (l'Estonie, la Hongrie et la Pologne souhaitent que les deux piliers soient mis en œuvre en parallèle). Ce qui se passe - ou ne se passe pas - à Washington aura donc une incidence sur la date d'entrée en vigueur des nouvelles règles.

L'expérience autour des plateformes médiatiques

Le président Biden a émis une des critiques les plus sévères jamais formulées à l'encontre des réseaux sociaux : « Comme Frances Haugen, qui est ici ce soir avec nous, l'a montré, nous devons tenir les plateformes de réseaux sociaux responsables de l'expérience qu'elles mènent sur nos enfants à des fins lucratives ». Les **révélations** de Frances Haugen, **en octobre 2021, ont ébranlé la réputation de Facebook**, principalement en raison de leurs implications pour le bien-être des enfants.

Les milliers de documents que la lanceuse d'alerte a transmis au *Wall Street Journal* ont révélé comment l'entreprise a intentionnellement caché ce qu'elle savait sur les effets des médias sociaux sur la santé mentale des enfants.

Dans son **témoignage écrit**, l'ancienne employée de la société a prévenu que « Facebook choisit les informations que des milliards de personnes voient… avec un contrôle sur nos pensées, nos sentiments et nos comportements les plus profonds », ce qui nécessite une intervention urgente.

Le choix des mots du président américain est à la fois frappant et décevant. Frappant en raison de la pression qu'il a imposée aux décideurs politiques pour qu'ils adoptent des positions fermes à l'égard de toute personne menant des « expériences » sur des enfants (et c'est pire, selon lui, lorsque c'est motivé par le profit). Décevant en raison de la suggestion que cette expérience était « nationale », plutôt que mondiale.

Dans tous les cas, cela appuie les processus politiques en cours en matière de sécurité des enfants. Les cadres nationaux et mondiaux concernant les enfants offrent de solides protections et d'autres réformes sont à venir, notamment en Europe, avec la nouvelle loi sur les services numériques **qui devrait entrer en vigueur dès l'été**.

Les développements en matière de politiques numériques qui ont fait la « une »

Le paysage des politiques numériques évolue quotidiennement ; voici les principaux développements de février. Nous les avons décodés en petites mises à jour faisant autorité. Vous trouverez plus de détails dans chaque mise à jour sur l'Observatoire Digital Watch.

en progression

Architecture globale

Tous les regards sont tournés vers l'escalade tragique du conflit en Ukraine. Parallèlement aux assauts militaires et aux cyberattaques (voir ci-dessous), les médias russes affiliés à l'État ont été interdits en Europe, et certaines banques russes exclues des systèmes de paiement internationaux. *Plus d'informations en pages 2-5 et sur notre espace dédié : Ukraine conflict: Digital and cyber aspects.*

en progression

Développement durable

Une partie des 150 milliards d'euros d'investissements de l'UE sera **consacrée au renforcement de la connectivité numérique en Afrique**, sous la forme de câbles sous-marins (câble EurAfrica Gateway) et terrestres (à travers l'Afrique subsaharienne), ainsi que de connectivité par satellite.

en progression

Sécurité

L'Ukraine a été frappée par **plusieurs cyberattaques**, provenant a priori de la Russie ; en réponse, les pirates informatiques ont lancé des attaques contre les infrastructures russes.

Juste avant l'escalade du conflit ukrainien, la Russie et la Chine ont réaffirmé leur volonté **de coopérer en matière de « sécurité internationale de l'information »**.

Revenant sur une **récente cyberattaque** ayant affecté les données de plus de 50 000 personnes vulnérables, le Comité international de la Croix-Rouge (CICR) a expliqué comment « les pirates ont pu pénétrer dans notre réseau et accéder à nos systèmes en exploitant une vulnérabilité critique non corrigée... Malheureusement, nous n'avons pas appliqué ce correctif à temps avant que l'attaque n'ait lieu ».

en progression

Commerce électronique et économie de l'Internet

Les tensions commerciales entre l'Inde et la Chine se multiplient : L'Inde a **bloqué 54 applications mobiles, principalement chinoises**, ce qui porte à 321 le nombre d'applications chinoises bloquées. La Chine souhaite que l'Inde **utilise les mêmes critères de mesure pour tous les investisseurs étrangers dans le domaine des technologies** que ceux appliqués aux entreprises chinoises.

Les déboires antitrust de la « Big Tech » continuent. PriceRunner, un fournisseur suédois de services de comparaison de prix, a **poursuivi Google** pour avoir prétendument donné la préférence à ses propres services de comparaison de prix sur son moteur de recherche. Google a également été jugé **en infraction avec les lois antitrust de la Russie**.

en progression

Infrastructure

Les PDG de Telefónica, Deutsche Telekom, Vodafone et Orange **ont demandé à la Commission européenne d'introduire rapidement des lois** qui obligeraient les fournisseurs de contenu (tels que les entreprises impliquées dans le streaming vidéo, les jeux et les médias sociaux) à contribuer au coût de l'infrastructure numérique européenne.

L'UE a lancé un paquet de mesures de 6 milliards d'euros autour des communications. Ce paquet comprend une **proposition de règlement** visant à étendre la couverture des satellites et à rendre les communications par satellite plus sûres, ainsi qu'une **communication** sur la gestion de l'espace satellitaire, de plus en plus encombré, en fixant des règles de conduite.

neutre

Droits numériques

Les nouvelles règles proposées par la Commission européenne permettront aux utilisateurs d'appareils connectés d'avoir accès aux données qu'ils génèrent, qui sont jusqu'à présent largement conservées entre les mains d'entreprises privées.

Une **nouvelle action en justice** au Texas allègue que Meta (anciennement Facebook) a traité les données biométriques d'utilisateurs à leur insu. En parallèle, l'entreprise a décidé de régler à l'amiable une plainte pour atteinte à la vie privée de 90 millions de dollars américains datant de 2012, selon un accord transactionnel déposé en Californie.

en baisse

Politique autour des contenus

Le gouvernement britannique propose de **nouvelles mesures** dans le cadre de son projet de loi sur la sécurité en ligne pour protéger les enfants, notamment l'obligation pour les sites pour adultes d'introduire des mesures de vérification de l'âge plus strictes.

en baisse

Juridiction et questions juridiques

Selon la Commission nationale de l'informatique et des libertés (CNIL), les données des utilisateurs qui sont collectées par Google Analytics puis transférées aux États-Unis constituent une **violation du RGPD**. La CNIL a déclaré que les mesures prises par Google ne pouvaient pas garantir que les données soient à l'abri des services de renseignement américains. Une **décision similaire** a été rendue il y a quelques semaines par l'autorité autrichienne de protection des données.

en progression

Nouvelles technologies

L'OCDE a **lancé un nouveau cadre de** classification des systèmes d'IA, principalement pour promouvoir une compréhension commune de ce qu'incluent ces systèmes. La nouvelle classification permettra d'expliquer quels sont les éléments constitutifs des systèmes d'IA et ce qu'ils font en pratique.

L'ambition des États-Unis de s'appuyer sur des chaînes d'approvisionnement locales, y compris pour les semi-conducteurs, était l'une des principales priorités du **discours annuel** du président Joe Biden sur **l'état de l'Union**. La Commission européenne **a également proposé un ensemble de mesures** dans le cadre de sa nouvelle **loi sur les puces européennes**. L'objectif ? L'UE veut doubler sa part de marché dans les puces mondiales pour la porter à 20 %.

Mises à jour depuis la Genève internationale

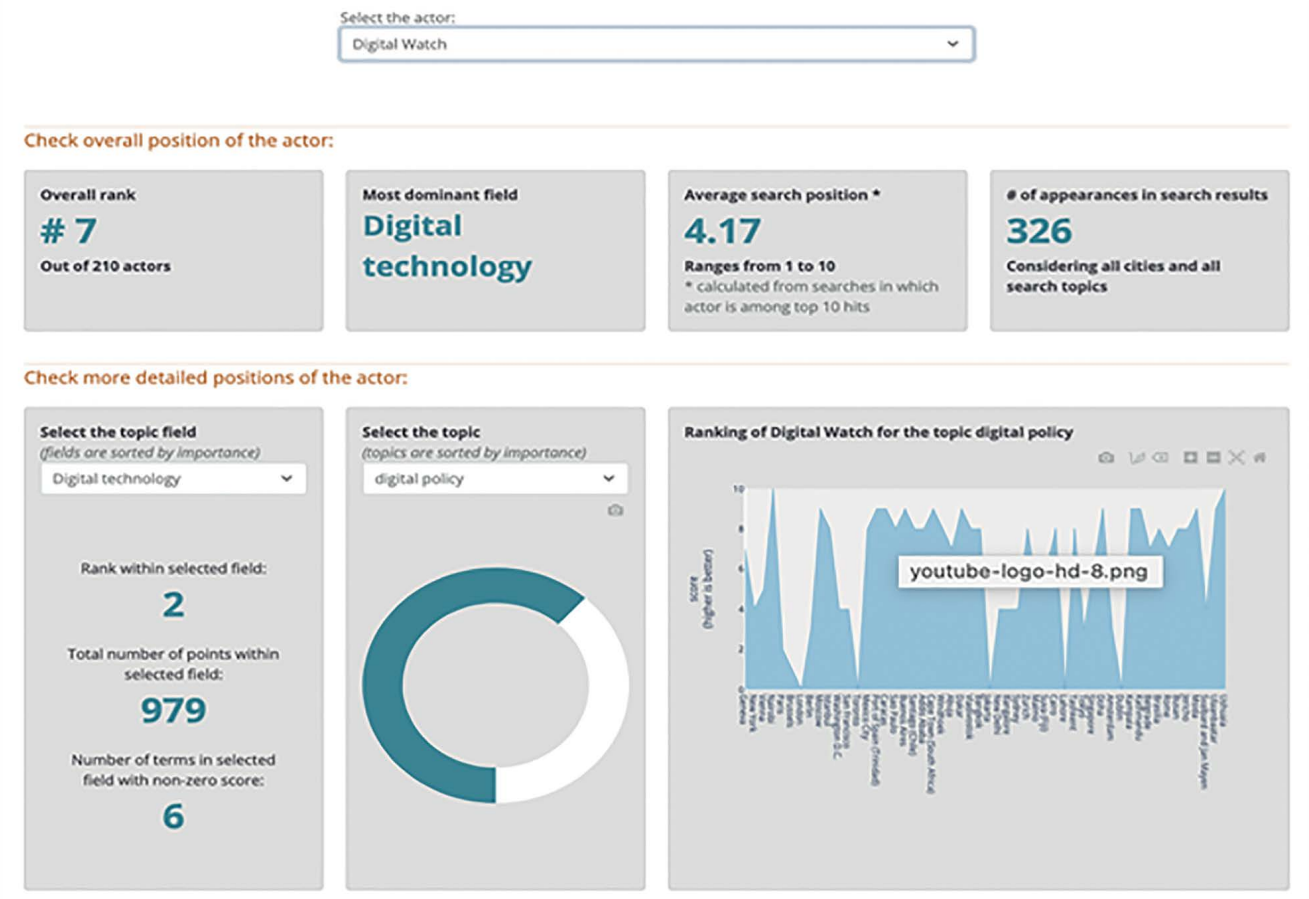
De nombreuses discussions politiques ont lieu chaque mois à Genève. Dans cet espace, nous vous informons de tout ce qui s'est passé ces dernières semaines.

1er février 2022 : 7e édition des Geneva Engage Awards

Chaque année, les **Geneva Engage Awards** récompensent les acteurs de la Genève internationale dont les actions sur les réseaux sociaux contribuent à une plus grande empreinte de Genève en ligne. En quoi cela est-il important ? Parce que les politiques discutées et négociées à Genève, dans des domaines tels que le développement, les droits de l'Homme et les questions numériques, ont un impact pour des millions de personnes dans le monde.

Les gagnants des prix de cette année pour chacune des trois catégories (organisations internationales, ONG et missions permanentes) sont : L'Office des Nations Unies à Genève, GAVI - l'Alliance du Vaccin, et la Mission permanente des Etats-Unis auprès des Nations Unies.

Cette année, la Geneva Internet Platform -l'organisateur annuel des Geneva Engage Awards - a également dévoilé un nouvel outil : Un kit électronique sur **l'empreinte mondiale de Genève**, qui analyse la portée de « l'empreinte » de Genève dans le monde, dans les domaines de la diplomatie et de la politique technologique. **Explorez cet outil**.



Capture d'écran : L'empreinte de Digital Watch dans le monde

9 février 2022 | La voie à suivre pour la coopération numérique et la réalisation des ODD

La discussion, à laquelle a participé l'invitée spéciale Marina Kaljurand, candidate estonienne au poste d'envoyée du Secrétaire général des Nations unies pour les technologies, a porté sur la création de progrès économiques et sociaux, la réduction de la fracture numérique et l'égalité des chances pour les groupes marginalisés. Le rôle de l'envoyé des Nations unies est essentiel pour concrétiser la vision du Secrétaire général des Nations unies en matière de coopération numérique, conformément à la **feuille de route pour la coopération numérique** et au rapport « **Notre programme commun** ».

La discussion, organisée par la Mission permanente de l'Estonie à Genève, s'est penchée sur le rôle unique que jouent l'ONU et le Forum sur la gouvernance de l'Internet (FGI) dans la discussion et le traitement des sujets numériques à l'échelle mondiale. Alors que la pandémie de COVID-19 a eu un impact négatif sur la réalisation des objectifs du Millénaire pour le développement dans certaines régions du monde, la réponse doit se concentrer sur le renforcement des capacités des pays en développement, en particulier dans le domaine du cyber.

Mme Kaljurand, actuellement membre du Parlement européen, a appelé à un retour à la réalité, affirmant que les clivages idéologiques peuvent bloquer le progrès, mais que la connectivité et l'inclusion sont des questions sur lesquelles tout le monde peut coopérer.

L'Ambassadeur Benedict Wechsler, responsable de la numérisation au Département fédéral suisse des affaires étrangères, a souligné que la finance durable est un domaine prioritaire pour la Direction du développement et de la coopération (DDC), l'organe du pays chargé de la coopération internationale.

Chengetai Masango, responsable du secrétariat du FGI à Genève, a déclaré que le FGI de cette année se déroulera en Afrique, la région qui compte le plus fort pourcentage de jeunes internautes.

Jovan Kurbalija, directeur exécutif de la DiploFoundation et responsable de la Geneva Internet Platform, a évoqué le modèle IGF+ comme une « maison numérique » potentielle - un lieu et un espace où les gens, en particulier ceux des pays en développement, pourraient soulever leurs préoccupations en matière de politique numérique (commerce électronique, cyber sécurité, etc.). Il a également déclaré que la gouvernance numérique inclusive et efficace dépend d'une participation plus substantielle des petits États et des États en développement.

9 février 2022 | Le risque numérique dans la médiation des conflits

Cet événement, organisé par le CyberPeace Institute (CPI), a **marqué le lancement de la plateforme d'apprentissage en ligne sur la gestion des risques numériques pour les médiateurs**.

La plateforme a été développée par le CPI, le CMI - Martti Ahtisaari Peace Foundation, et l'Unité de soutien à la médiation du Département des affaires politiques et de la consolidation de la paix des Nations Unies (UNDPPA). Elle aidera les médiateurs à évaluer les risques liés aux technologies numériques et à comprendre le paysage des menaces.

Lors du lancement, les panélistes ont souligné que la pandémie de COVID-19 a accru l'utilisation des technologies numériques et des modèles hybrides dans le processus de médiation, et que cette tendance devrait se poursuivre à l'avenir.

Ce qu'il faut surveiller : Événements mondiaux des politiques numériques en mars

Jetons un coup d'œil au calendrier mondial des politiques numériques. Voici ce qui se déroulera dans le monde entier. Pour plus d'événements, visitez la section Events de l'Observatoire Digital Watch.

1–9 mars
AMNT-20

Se tenant tous les quatre ans, l'Assemblée mondiale mondiale de normalisation des télécommunications (AMNT) décide du programme de travail du Secteur de la normalisation des télécommunications de l'Union internationale des télécommunications (UIT-T) pour la période suivante, y compris la structure et la direction des commissions d'études. Les recommandations et résolutions approuvées, bien que volontaires, déterminent l'orientation future de l'UIT-T. L'AMNT-20 se déroule physiquement à Genève, avec une participation en ligne.

7–10 mars
ICANN73

Tenu en ligne, le forum communautaire ICANN73 donne l'occasion aux organisations de soutien et à la communauté de discuter de différentes questions concernant l'activité de l'ICANN, la gestion du système de noms de domaine (DNS), les nouveaux domaines génériques de premier niveau (gTLD), les services de données des registres et la protection des données, ainsi que l'acceptation universelle.

15 mars–3 juin
SMSI 2022

L'édition 2022 du Forum du Sommet mondial sur la société de l'information (SMSI), qui se tiendra en ligne, aura pour thème « Les TIC pour le bien-être, l'inclusion et la résilience : La coopération du SMSI pour accélérer les progrès vers la réalisation des ODD ». La dernière semaine se tiendra en ligne du 30 mai au 3 juin, lorsque des tables rondes ministérielles et des déclarations de politique générale clôtureront l'événement.

17–18 mars
Blockchain Africa

Le thème de la 8e édition de la conférence Blockchain Africa sera « Ready for Business ? ». Cet événement annuel se tiendra entièrement en ligne et rassemblera des praticiens d'Afrique et d'ailleurs qui cherchent à exploiter les opportunités et les cas d'utilisation des bonnes pratiques de la technologie *blockchain* dans la région.

28 mars–1 avril
25ème session de la CSTD

La Commission de la science et de la technique au service du développement (CSTD) est un organe subsidiaire du Conseil économique et social et le point focal des Nations unies pour la science, la technologie et l'innovation. La 25ème session de la CSTD se tiendra à Genève. Les principaux thèmes de la session de cette année sont « L'industrie 4.0 pour le développement inclusif et la science, la technologie » et « L'innovation pour le développement urbain durable dans un monde post-pandémique ».

A propos de ce numéro

Numéro 67 du bulletin Digital Watch, publié le 9 mars 2022 par la Geneva Internet Platform et la DiploFoundation, sous une licence CC BY-NC-ND 4.0 | Contributeurs : Stephanie Borg Psaila (éditrice), Kristina Hojstricova, Jana Misić, Virginia (Ginger) Paque | Conception : Viktor Mijatović | Contact : digitalwatch@diplomacy.edu

En couverture :

Le front cyber de la crise ukrainienne. Credit: Vladimir Veljasević

La Geneva Internet Platform est une initiative de :

GENEVA INTERNET PLATFORM digwatch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO
www.diplomacy.edu