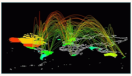
Accueil / Transcriptions / Cyberguerre - Big Techs et géopolitique avec Asma (...)

Cyberguerre - Big Techs et géopolitique avec Asma Mhalla



D'après un média publié le 04/11/2022 **Source Avertissement**

Personne·s Asma Mhalla Fabrice Epelboin Damien Douani Bertrand Lenotre
Thèmes Partage du savoir Internet Cyberattaques - Cybersécurité
Type d'action Conférence
Type de publication Audio

Comment les grandes puissances de la tech sont-elles devenues des alliés objectifs de leur États dans la conduite d'une politique internationale ?

Asma Mhalla - Voix off : « Les Big Tech en général, américains en l'occurrence, chinois de la même façon, n'importe quel Big Tech, sont, de mon point de vue, rien d'autre que les bras armés technologiques de leur État, de leur État référent. »

Voix off : Les Éclaireurs du Numérique. Le podcast qui décrypte les enjeux cachés d'internet.

Bertrand Lenotre : Salut tout le monde, bienvenue dans un nouvel épisode des Éclaireurs du Numérique. Nous sommes contents de revenir, d'autant que nous avions été absents pendant quelques semaines pour cause de petite parenthèse au Sénat, pour une journée spéciale blockchain et crypto, qui a connu un joli succès. D'ailleurs on va remettre ça dans quelques temps, cette fois-ci du côté de l'Assemblée nationale. Il faut croire que les Éclaireurs du Numérique deviennent *bankables* du côté de la classe politique, aujourd'hui. Et c'est toujours avec Fabrice Epelboin, salut Fabrice.

Fabrice Epelboin : Salut.

Bertrand Lenotre : Avec Damien Douani, salut, Damien.

Damien Douani : Bonjour.

Bertrand Lenotre : Et c'est avec Asma Mhalla que nous sommes vraiment contents de recevoir dans ce podcast. Bonjour Asma Mhalla.

Asma Mhalla : Salut.

Bertrand Lenotre : Asma Mhalla, experte en *tech policy*, ça ne veut rien dire en français, ça veut dire un peu « enjeux géopolitiques du numérique », c'est un petit peu ça l'histoire. Professeure à Sciences Po et à Polytechnique.

Asma Mhalla : Enseignante. Attention au titre !

Bertrand Lenotre : Pardon, enseignante à Sciences Po et Polytechnique. C'est vrai que la différenciation est assez notable, il faut faire attention, Fabrice est assez sensible !

Fabrice Epelboin : Après tu te fais défoncer en interne.

Asma Mhalla : Et puis je n'ai aucune prétention ni à faire de la recherche de laboratoire, ni à faire de la grande théorie sur le sujet.

Bertrand Lenotre : On t'a fait venir parce qu'un article a fait un peu parler de lui dans *Figaro Vox*, le 13 octobre : « Il est temps de nous préparer à la cyberguerre » [1]. Tu n'es pas une spécialiste de la cyberguerre ; en fait, ton champ d'analyse, c'est l'analyse de ce que font les Big Tech, au niveau international notamment, et ça ouvre plein de champs dont on va pouvoir discuter. D'abord sur cet article dont on a un petit peu parlé : est ce qu'il est temps de nous préparer à la cyberguerre ou est-ce qu'elle n'a pas déjà lieu ? Moi j'ai l'impression que c'est déjà parti depuis un petit moment.

Asma Mhalla : Tu as absolument raison, Bertrand. En fait c'était un titre, mais il faut toujours se demander à qui on s'adresse. Et là, en l'occurrence, c'était un article très court, très vulgarisateur, pour des gens qui n'ont pas forcément accès à ce type de sophistication de pensée, on va dire, ou, en tout cas, conceptuel. L'idée c'était de donner quelques premières briques, quelques premiers axes de réflexion à ce qui est en jeu. Tu as raison, depuis de nombreuses années déjà, les cyberattaques en l'occurrence, mais pas que, sont des phénomènes qui ne sont pas nouveaux, qui sont émergents, parce qu'en termes de doctrine, en termes de maîtrise, en termes de recul on en est encore à documenter, parce que la guerre d'Ukraine de cette année 2022 est un laboratoire à ciel ouvert et vraiment à échelle. Mais, dans le champ des cyberattaques, ce qui s'est passé en 2014 au moment de l'annexion de la Crimée, etc., était aussi un champ d'étude et de première documentation sur le champ de la guerre informationnelle. Ce qui se passe en Afrique depuis de nombreuses années en est un aussi, etc.

Il est vrai que tout d'un coup, dans le débat public, le sujet commence à émerger, commence à apparaître et il est heureux qu'il apparaisse et qu'il émerge pour le plus grand nombre, parce qu'il est temps, vraiment, que tout le monde puisse s'en emparer et ait les moyens de s'en emparer.

Bertrand Lenotre : Le tournant dans le cyberespace dont tu parles, en 2022 en fait, c'est la prise de conscience un peu majoritaire de l'existence de ce danger-là, du fait qu'on va vers une autre forme de conquête de pouvoir ?

Asma Mhalla : Exactement. Le risque qu'on a, comme sur à peu près tous les sujets, c'est que ce soit toujours des experts entre eux qui travaillent, que ça n'essaime pas, que ça reste un débat dans un entre-soi qui est absolument utile et fondamental, et que la majorité n'ait pas les moyens de s'emparer. Je le vois avec mes étudiants ou lors de tables rondes : les gens sont curieux, les gens ont besoin de comprendre, les gens ont besoin de trouver du sens à ce qui se passe ; il y a une curiosité, réellement, voire parfois une fascination par rapport à ça, mais ce sont des champs qui, aujourd'hui, sont toujours parés d'une appréhension de technicité, d'intangibilité, qu'on ne sait pas matérialiser. Il est donc temps que tous, collectivement, chacun à sa place, puissions justement aider le plus grand nombre à comprendre ce qui se joue — et tu as raison encore une fois —, ce qui se joue en réalité depuis quelques années déjà, en fait.

Tout à l'heure on en parlait hors micro, il y a deux choses que j'aimerais souligner en préambule, pardon de faire les questions et les réponses.

Un, c'est le terme, la terminologie, la bataille sémantique sur « cyberguerre ». Je ne sais pas si tout le monde le sait, mais le terme n'est pas fixé. C'est un terme qui permet, si vous voulez, d'attirer ou d'accrocher une attention. C'est le terme qui est utilisé par les médias, souvent, mais disons que dans la sphère des experts et des géo-politologues chevronnés, on n'utilise pas le mot guerre à tort et à travers. Le mot guerre est un mot très spécifique qui renvoie à une réalité de terrain très spécifique. Du coup, simplement pour éclairer le plus grand nombre de personnes possible sur ça, il existe aujourd'hui, en effet, une bataille sémantique : quel est le mot ? Est-ce que c'est une guerre hybride ? Est-ce que c'est le mot cyberguerre ? Est-ce que c'est encore autre chose ? Ou tout simplement est-ce que — et ça serait d'ailleurs peut-être aussi paradoxalement mon approche —, en fait le cyber, c'est-à-dire le cyberespace, et on reviendra peut-être sur ce qu'est le cyberespace, c'est une cinquième dimension, ni plus ni moins, de la guerre, au même titre que l'air, la terre, la mer, l'espace, etc., donc c'est un champ nouveau.

Il est hybride parce qu'il est à la fois artificiel, c'est une construction. Quand on regarde le socle technologique, physique, la première couche du cyberespace, l'ensemble de nos usages, c'est bien une construction artificielle de l'homme. Il n'en reste pas moins qu'aujourd'hui, par l'ensemble du réseau, c'est bien une cinquième dimension à part entière et en tant que telle, de la guerre dite conventionnelle.

Damien Douani : Tu disais qu'on n'utilise pas le terme guerre à tort et à travers, alors que peut-on utiliser comme terme ? Parce que, quelque part, ça prend les atours de ce qu'est qu'une guerre qui, peut-être, n'a pas la violence ou l'immédiateté que l'on peut avoir, mais c'est quelque chose qui est beaucoup plus larvé, qui dure beaucoup plus longtemps, qui peut être éventuellement masqué ?

Asma Mhalla : Non, ce n'est pas larvé. Quand on a des cyberattaques ou quand on a des vraies opérations d'ingérence étrangère, ce n'est pas larvé, ce sont de vraies actions, de vraies opérations, qui sont d'ailleurs organisées, souvent depuis très longtemps, aussi bien dans le champ informationnel ou sémantique — on y reviendra peut-être — que dans le champ des cyberattaques. Une vraie cyberattaque qui fonctionne, reprenez l'exemple de Stuxnet [**2**], ce sont des opérations qui ont duré des années en termes de préparation de l'opération elle-même. Donc non, il n'y a rien d'éphémère ou de soudain. Ce sont souvent des stratégies qui se construisent sur le temps long et à bas bruit dans le cyber. C'est la première chose.

Maintenant, pour revenir sur le terme. C'est une dimension de la guerre à part entière, un champ d'opérations qui n'est pas kinésique mais qui a des conséquences réelles. Là où il y a eu aussi tout un débat, un des problèmes qu'il y a eu, c'est de dire que la guerre fait des morts, elle est létale, là où la guerre cyber ne l'est pas. Alors oui et non ! Elle ne l'est peut-être pas directement, mais quand vous empêchez une armée d'avoir accès à sa chaîne d'approvisionnement, quant vous tapez des hôpitaux comme récemment sur un autre champ qui était la série de cyberattaques des hôpitaux en France, etc., de façon indirecte, elle peut avoir des conséquences dramatiques et énormes.

Donc, attention aussi à ne pas trop sous-estimer ou à dire « bah ! ce n'est une cyberguerre, etc. » Et puis, au bout d'un moment, il faut dépasser cette espèce de bataille sémantique et voir les choses comme elles sont sur le terrain. En anglais — paradoxalement et pour une fois, l'anglais est peut-être un tout petit peu plus précis que le français — on a le terme *cyberwar* et après il y a la *cyberwarfare* [**3**] et ce n'est pas exactement la même chose : c'est-à-dire que vous avez les techniques militaires du cyber — et c'est davantage de ça dont on parle — qu'une cyberguerre, au sens où vous avez une guerre qui est circonscrite, simplement, en tout cas une surestimation, une surévaluation de la dimension cyber dans la guerre.

De ce point de vue-là, c'est bien le champ cyber de la guerre qui est aujourd'hui très investi et qui va aller croissant.

Fabrice Epelboin : Une petite remarque sur les hôpitaux : on est plutôt dans la délinquance que dans un acte de guerre. On n'est pas dans une volonté de la part d'un État étranger d'infliger un dommage à un autre État.

Asma Mhalla : Oui, ta remarque est très intéressante. Je prenais l'exemple des hôpitaux d'abord parce qu'on en a eu un récemment, et j'expliquais simplement que la question du critère létal ou non létal, était, pour moi, un faux critère puisque, indirectement, tu peux avoir une létalité ou, en tout cas, une très grande difficulté sur le terrain qui peut mener à des conséquences tout aussi dramatiques et tout aussi graves que des morts directs de guerre conventionnelle.

Fabrice Epelboin : D'autant plus que, au final, tuer des gens n'est pas non plus le but ultime de la guerre, c'est juste un moyen. Le but ultime c'est quand même de plier l'adversaire et de l'asservir. S'il y a moyen de faire ça sans tuer, *why not ?*.

Asma Mhalla : Tu as raison. Et puis le deuxième sujet, ta remarque très juste de dire que ce sont des groupes de cybercriminels qui ont organisé les dernières attaques, Corbeil-Essonnes en l'occurrence, etc., oui, mais ça touche un autre sujet qui, lui, est fondamental, c'est l'hybridité de ces nouveaux acteurs paramilitaires. On a vu en Ukraine et en Russie, souvent, en tout cas dans cette guerre-là mais qui était vrai par ailleurs et depuis bien avant cette guerre-là, des groupes qui sont des groupes cybercriminels purs et parfaits, qui fonctionnent avec des rançongiciels, qui gagnent leur vie très bien comme ça, etc. Tout d'un coup, dans le cadre de la guerre, ils peuvent être mis à contribution au service de l'État et avec de très faibles coûts puisque, en fait, c'est un peu leur job ; que ce soit pour un rançongiciel ou, finalement, pour bloquer carrément toutes tes données ou bloquer ta chaîne logistique, à la fin, ils maîtrisent de la même façon. Ils sont organisés pour ça, ils ne coûtent pratiquement rien à ton État et, après, tu évites la question de l'attribution directe, c'est-à-dire qu'en fait, c'est une ramification : ils sont autour, c'est un peu le Wagner du cyber, en gros, vous voyez ; Wagner, c'est le groupe de mercenaires tenu par Prigogine en Afrique, mais aussi en Ukraine.

Fabrice Epelboin : On en avait parlé dans un épisode des Éclaireurs.

Asma Mhalla : La question de « ce ne sont que des groupes criminels », pour Corbeil-Essonnes il faudrait vraiment vérifier. Je me demande si ce n'était pas le groupe Killnet [**4**]. Ils se sont prétendus eux-mêmes comme étant le versant de la *IT Army* ukrainienne [**5**] et ont d'ailleurs fait la série de petites cyberattaques contre les sites d'un certain nombre d'aéroports, début octobre, aux États-Unis ; ils se prétendent comme étant un groupe nationaliste russe, injectant le narratif russe, etc.

Tout ça est donc assez hybride, liquide on va dire, entre ce qui est de l'ordre de la cybercriminalité et de l'ordre du militantisme ou de l'action cyber-militaire.

Bertrand Lenotre : Le terme même de cyberguerre est un peu complexe parce qu'il peut y avoir du sabotage de câbles sous-marins, de *datacenters*, de réseaux télécoms ; il peut y avoir de l'espionnage via tous les tuyaux possibles et imaginables, et puis il y a aussi la dimension de manipulation des opinions, et tout ça peut se faire soit par des entités étatiques soit par des entités privées mises au service pour les intérêts différents d'un État à un moment précis. Donc ça devient très complexe tout ça.

Asma Mhalla : Ça devient très complexe si on ne décompose pas le problème.
Ça revient à essayer de comprendre ce qu'est le cyberespace, et j'aurais peut-être dû commencer par là.

Le cyberespace est cet énorme réseau interconnecté, mondial, sur lequel repose Internet. Pour schématiser, parce qu'on pourrait entrer dans un niveau de complexité et de détail beaucoup plus profond, beaucoup plus avancé que ça, vous avez trois grandes couches qui sont interdépendantes, ce ne sont pas des couches qui sont chacune dans son coin.

La première, c'est la couche disons physique, les infrastructures solides, et c'est là où vous allez retrouver, en effet, les câbles sous-marins, les satellites, les réseaux divers et variés, les terminaux, les *datacenters*, etc., qui peuvent, eux, être l'objet de sabotages physiques. Tu coupes ton câble sous-marin, tu bombardes ton réseau, tu détruis ton *datacenter*, etc. Ça peut d'ailleurs parfaitement être l'objet des modalités des opérations, des manœuvres de guerre conventionnelle : un bombardement, par exemple.

Vous avez ensuite la deuxième couche, la couche logique sur laquelle vont avoir lieu les cyberattaques. C'est là où vous avez toute la construction du protocole d'Internet, les langages, votre système d'information, à partir duquel on va s'insérer dans ses vulnérabilités ou dans ses failles pour, typiquement, y loger des *ransomwares*, des virus divers et variés et organiser potentiellement les cyberattaques.

La troisième et dernière couche est la couche sémantique. C'est là où vous allez avoir tous vos usages directs : les applications, les réseaux sociaux, vos sites de e-commerce. C'est là où on va tous, collectivement, laisser, produire même, parce que c'est de la production, nos données, nos usages numériques, nos traces numériques. Et c'est là où se travaillent, typiquement sur les réseaux sociaux, les guerres informationnelles, en tout cas les opérations d'ingérence et de désinformation.

Les trois sont parfaitement et totalement imbriquées.

Je reprends l'exemple de Killnet sur les aéroports américains, en fait c'était de la nuisance, ils ont rétabli l'accès au site internet très rapidement, mais ça a permis quoi ? De créer une campagne de communication qui va être relayée et qui va réinjecter du narratif sur les réseaux sociaux, qui va être relayée, dont on va parler, dont les médias vont parler, etc. Et il est très intéressant d'observer qu'il n'y a pas eu de réaction directe et officielle des États-Unis, typiquement pour ne pas donner plus d'ampleur que ça et plus de caisse de résonance à ce qui s'était passé.
Killnet est symptomatique de cette articulation entre, par exemple, une cyberattaque et la guerre informationnelle, l'intimidation de l'opinion publique, faire peur aux opinions publiques occidentales, par exemple.

Damien Douani : L'autre aspect, l'autre articulation assez vicelarde c'est que, très concrètement, les compétences et l'état d'esprit qu'il faut pour mener des attaques cyber — j'ai envie de dire classiques — sur la couche logique, sont très proches des compétences qu'il faut pour mener des attaques sur la couche sémantique, parce que, à la base, un réseau social, c'est un système d'information avec des êtres humains au milieu. Donc ce n'est n'est pas fondamentalement différent d'un système d'information classique, il y a juste des êtres humains qui sont des relais et qui, en quelque sorte, peuvent être appréhendés comme des algorithmes comme les autres. C'est cette grande proximité intellectuelle entre ces deux systèmes qui fait qu'il y a une capacité du monde du hacking à adapter son approche à cette grande opération d'*astroturfing* [**6**] dans tous les sens et je ne pense pas qu'aux opérations d'ingérence d'un État contre l'autre. Ça touche aussi bien le militantisme politique local, donc quelque chose qui, à priori, n'est pas répréhensible, en tout cas pas du tout au même titre qu'un État qui s'ingère, mais ça reste le même état d'esprit. Les réseaux sociaux ne sont guère que des systèmes d'information avec des êtres humains qui ne font guère, au même titre qu'un algorithme, que récupérer de l'information, la transformer et la réinjecter dans le système.

Asma Mhalla : C'est d'autant plus similaire que ce qu'on a vu apparaître aussi dans les groupes de cybercriminels, vraiment de grande ampleur — ça existait avec les Anonymous [**7**], vous me direz, ou d'autres — c'est cette espèce de *crowdsourcing* de la guerre, c'est-à-dire que n'importe qui peut se porter volontaire, n'importe qui peut organiser une cyberattaque, avec un niveau de sophistication très léger, c'est de la nuisance, ce n'est pas vraiment quelque chose qui va mettre à plat des organisations, des infrastructures vitales ou des secteurs absolument critiques ; mettre à plat un site internet pendant deux heures, globalement on s'en remettra. Mais tout le monde peut se porter volontaire, s'organiser sur des chaînes Telegram, etc., et, de la même façon, sur des réseaux sociaux. Une bonne campagne de désinformation va aussi avoir des relais gratuits, des relais d'influence. On l'a beaucoup vu avec l'extrême droite française qui relayait tout le discours de Poutine pendant un moment donné, franchement quasiment gratuitement, les Philippot, etc. C'est assez intéressant de voir que ça fonctionne aussi, d'une certaine façon, pas quand ce sont des opérations hyper-sophistiquées, militaires, avec des agences de renseignement derrière qui sont millimétrées au cordeau, sur du *crowdsourcing* de base. On peut avoir exactement les mêmes dynamiques avec des relais dans la société civile, aussi bien sur le champ des cyberattaques que dans la guerre informationnelle ou dans des stratégies de désinformation plus large.

Bertrand Lenotre : Il y a deux choses qu'il faut qu'on dise, c'est qu'il y a la prise de conscience : tu disais qu'il y a un tournant en 2022 qui est à peu près la prise de conscience générale de l'histoire. Mais, évidemment, la prise de conscience dans les milieux autorisés a eu lieu depuis un petit moment. Il n'empêche qu'il y a un décalage entre la prise de conscience et la mise à jour des systèmes d'information, ceux qui seront attaquables demain. En France on a malheureusement ce décalage-là, comme dans plein d'autres pays, qui fait que nous sommes faibles à ce niveau-là.

Asma Mhalla : J'ai toujours habitude de dire que le grand problème qu'on a avec la technologie ou les nouvelles technos, depuis de nombreuses années maintenant, c'est le décalage de temporalité : le temps institutionnel, le temps politique et le temps technologique sont, en fait, totalement décorrélés. La technologie a compressé le temps, on va très vite. On le voit très bien dans l'éclosion des Big Tech qui trouvent des modèles économiques très rapidement avec une captation des usages, je ne vous refais pas tout le cours sur les modèles économiques des plateformes, effet de réseau, etc. Et puis vous avez la prise de conscience politique, mais il faut toujours qu'il y ait un incident, un problème pour qu'on se rende compte qu'il y a quelque chose à aller préempter d'un point de vue politique. Et puis, après, il y a le temps institutionnel. C'est-à-dire le temps que toute la machine s'adapte, que les institutions s'adaptent, se mettent en place, mettent en place les bonnes procédures, les bons réflexes, les bonnes compétences.

Dans le champ cyber, en France, il est hors de question de dire qu'on est complètement nuls ou qu'il ne se passe rien. Au contraire, vous avez aujourd'hui une réflexion, une doctrine qui est relativement poussée. Vous avez des compétences qui sont très fortes. On a une filière cyber qui est très bien organisée par ailleurs. L'ANSSI [Agence nationale de la sécurité des systèmes d'information] fait son travail et je crois qu'elle le fait bien. Au niveau du ministère des Armées c'est fait également et tout ça est organisé. Ce que tu pointes très justement, Bertrand, c'est une fois qu'on a posé la doctrine, une fois qu'on a organisé l'État, une fois qu'on a rattrapé le temps techno et le temps politique, l'autre écart qui reste, c'est la résilience des infrastructures, c'est-à-dire des hôpitaux, des entreprises ; en fait, le cheval de Troie est ta vulnérabilité. Si je reprends l'exemple des hôpitaux, ou même, il y a un an ou un an et demi, la mairie d'Angers, où on s'est retrouvé à revenir sur du fax, du papier et du stylo parce que les systèmes ne fonctionnaient plus, littéralement. Oui, on a un problème de résilience et de mise à jour des infrastructures, mais concrètement, c'est-à-dire sur le terrain. Et là, à mon avis, on a une grosse marche à franchir. Et encore, en plus, avec un décalage, c'est-à-dire une espèce de décrochage, par ailleurs, entre le public et le privé.

Damien Douani : Si on tire un peu le fil, Asma, sur ces notions de cyberguerre et de Big Tech, la situation en Ukraine a fait apparaître un acteur assez surprenant, qu'on voit débarquer d'un seul coup, qui est Elon Musk. Il rentre par le biais de Starlink [**8**] en expliquant qu'en gros, c'est bien gentil, mais maintenant il va falloir passer à la caisse parce qu'il en a marre de

subventionner l’Internet satellitaire ; soi-disant qu’il aurait discuté avec Poutine et ainsi de suite. Bref ! D’un seul coup on a l’apparition de ce personnage assez iconoclaste, mais dont on sait qu’il est assez touche-à-tout et qu’il n’est jamais là par hasard.
Sur ce champ-là, quelle lecture peut-on avoir au regard de ce que tu viens de nous expliquer, sur les différentes couches et la connexion de ces différentes couches ?, sachant que, pour finir, Elon Musk veut racheter Twitter, va l’acheter. Donc quelque part on pourrait, un peu par approximation, se dire qu’il va s’acheter un média, je fais très court et très ramassé, mais je pense qu’il y a autre chose qui se joue derrière, notamment, certainement, peut-être, au niveau des données.

Asma Mhalla : Merci Damien, je vais répondre en deux temps et merci d’ouvrir sur ça parce que, en ce moment, je me réveille avec Musk, je mange avec lui, je me couche avec lui ! Il est, en ce moment, absolument omniprésent dans ma vie. Merci de me redonner encore une occasion de parler de lui.

Musk en Ukraine c’est comme Microsoft en Ukraine, ça pose une question. Si je monte d’un cran en termes de compréhension des systèmes — c’est mon avis, c’est sujet à discussion et je serais ravie d’en discuter avec les gens que le sujet intéresse —, les Big Tech, en général, américains en l’occurrence, chinois de la même façon, n’importe quels Big Tech, ne sont, de mon point de vue, rien d’autre que les bras armés technologiques de leur État référent.
vice-Premier ministre et ministre de la Transformation numérique de l’Ukraine
Musk est aujourd’hui un Big Tech américain qui répond aux injonctions, aux demandes de l’État américain, du Pentagone, en l’occurrence du DOD [Département de la Défense des États-Unis], etc. Il n’est pas allé en Ukraine comme ça, par l’opération du Saint-Esprit. Il a d’abord été interpellé directement sur Twitter, il me semble par Fedorov, le vice-Premier ministre délégué au numérique, une espèce de titre à rallonge, ukrainien [vice-Premier ministre et ministre de la Transformation numérique de l’Ukraine]. Et puis, en effet, on a réussi, d’un point de vue logistique, ce qui était absolument extra ordinaire, en deux mots, à acheminer, en deux/trois jours, en un temps record, les terminaux qui allaient bien, les satellites, etc., et à les connecter. Et en effet, de ce point de vue-là, de l’aveu même des armées ukrainiennes, du gouvernement et de l’exécutif ukrainiens, les satellites Starlink sont absolument vitaux pour les communications militaires, pour l’organisation de la logistique militaire dans les zones qui ont été occupées, qui ont vu leurs réseaux télécoms ou leurs réseaux de connectivité détruits ou, disons, dérivés par les Russes.

De ce point de vue-là, en termes de protection et de maintien, de résilience, de redondance de la communication et de la connectivité, ça a été vital, ça a été clef. Donc, quand Musk a dit, tout d’un coup, je n’ai plus les moyens de…, c’est à prendre avec beaucoup de précautions et il est revenu, depuis, sur ses déclarations. Mais qu’est-ce que racontent Musk et Starlink en Ukraine ? Ça raconte, en fait, que les Big Tech, aujourd’hui, sont des extensions de l’État américain, ce sont des entreprises qui sont devenues hybrides, qui sont à la fois des boîtes privées et des entités géopolitiques. Et vous avez exactement la même réflexion sur les réseaux sociaux qui sont à la fois des entreprises privées, qui rendent des comptes aux marchés, qui sont en même temps des espaces publics et, en même temps aujourd’hui, parce que terrain de guerre informationnelle, des entités géopolitiques. On l’a vu, encore une fois là aussi au début de la guerre en Ukraine ou dans le contexte de la guerre informationnelle au Sahel qui, pour le coup, met en regard la France et la Russie, où vous avez du Twitter, du Facebook, à qui on demande de modérer, de supprimer des comptes, etc., liés à des armées ou à des groupes paramilitaires qui injectent des narratives et des campagnes de désinformation au sens large.

Attention, une parenthèse,la désinformation n’est pas simplement de la *fake news*, juste pour clarifier tout ça, ça peut être de la vraie information décontextualisée, manipulée, etc., et surtout à qui on va donner du boost de viralité par tout un tas de modalités inauthentiques.
Je vous invite à lire les deux rapports de l’IRSEM [Institut de Recherche Stratégique de l’École Militaire] [**9**], qui sont absolument fondamentaux, sur les campagnes de désinformation russe et chinoise qui ont été écrits et sortis ces trois dernières années, en 2017 et plus récemment. Ils sont absolument éclairants dans le détail de comment un État organise, de façon extrêmement industrielle, des campagnes de désinformation sur les réseaux sociaux et avec des résultats probants. La Chine, d’ailleurs, commence à se mettre à niveau sur le modèle russe dans sa zone d’influence directe, Singapour, Taïwan, etc. Je vous invite vraiment à lire ces rapports qui sont fondamentaux pour comprendre ce qui se joue.

Donc les Big Tech sont des bras armé technologiques. Ce ne sont certainement pas des États parallèles, pas des États « je ne sais quoi ». C’est ce qu’on a raconté pendant longtemps dans les médias. Non, ce sont des entités qui sont sur des partenariats public/privé plus ou moins confidentiels ou plus ou moins publics. En l’occurrence, sur la question de Starlink, c’était bien un PPP avec le Pentagone de l’aveu même, en tout cas de la bouche même du Pentagone et tout ça fonctionne sur un continuum qui est assez fluide, en fait.

Sur la deuxième question que tu me posais : Twitter et Musk. Il y a eu cette histoire de procès : il veut, il ne veut pas, il est capricieux. Je ne pense pas du tout que Musk soit un homme capricieux, il n’est pas assez bête pour ça. Je pense qu’il a un vrai projet avec Twitter, qui est un projet politique, qui est un projet idéologique. Tu évoquais la question de la donnée, évidemment. Je pense surtout que Twitter va être la base, le socle de sa X App. Et sa X App demain, avec les satellites, c’est en fait un énorme panoptique qu’on va mettre en place, une espèce d’énorme écosystème fermé sur lui-même. On va non seulement capter énormément de data mais, surtout, on va avoir une vision sur à peu près tout. Dans cette ambition un peu démiurgique de contrôle absolu de tout par la donnée, en fait de techno-surveillance généralisée, le projet Twitter comme socle technologique de base à cette nouvelle infrastructure qu’il a en tête et qu’il commence vraiment à formuler, sur laquelle il commence à communiquer, est une pièce maîtresse.

Damien Douani : Un dernier mot. Le fait d’intégrer la dimension sémantique à la cyberguerre, qui n’est pas quelque chose avec lequel je suis familier, mais ça a quand même a un grand mérite, c’est que ça permet de regarder différemment le conflit dans lequel on est plongé aujourd’hui et de prendre pas mal de distance avec cette façon dont la presse occidentale nous raconte une défaite russe annoncée et, si ce n’est un triomphe de l’Occident, du moins quelque chose qui fait que l’Occident n’est pas remis en question par cette guerre.

Si on intègre la dimension sémantique, c’est-à-dire, très concrètement, les opérations de manipulation, notamment en prenant en compte toute une série de trucs qui ont été démontés l’an dernier par Facebook, dans lesquels il y avait l’armée française, on aperçoit d’un territoire de conflits qui touche aussi bien l’Asie que l’Afrique que l’Occident et on s’aperçoit d’un territoire sur lequel on perd. On est en train de perdre de façon assez lamentable en Afrique. Perdre, au sens où la France était une ex-puissance coloniale qui, malgré tout, avait une assise très importante en Afrique et qu’elle est en train de se faire jeter de tout un tas de pays, ça a évidemment commencé par le Mali. Il y a des armées de trolls un peu partout dans l’Afrique francophone, évidemment au Mali mais pas que, on les a vus au Burkina Faso il n’y a pas longtemps où la France a aussi connu des déboires, il y en a au Cameroun, au Sénégal ; il y en a à peu près partout, notamment en Afrique du Nord et très vraisemblablement au Tchad, je ne sais plus, mais c’est très vraisemblable. Ce qui fait qu’au final, si on regarde le continent africain, la France est en train de perdre de façon spectaculaire et accélérée ces dernières années, et on est obligé de rattacher ça à la guerre en Ukraine, vu que ce sont les mêmes acteurs. C’est la France par proxy et la Russie à travers les différentes entreprises de Prigojine ; rappelons que le loustic a certes Wagner qui a fait sa gloire, mais il a aussi l’armée des trolls. Et l’armée des trolls, combinée à Wagner, montre qu’il y a quand même une certaine approche stratégique au-dessus et une certaine idée de l’appareil qu’ils sont en train de construire, qui est assez unique, d’autant plus unique qu’il a été construit dans la contrainte de très peu d’argent et qu’il est extrêmement efficace.

En dehors de la manipulation par les réseaux sociaux, dont on parle régulièrement ici, le fait d'intégrer ça comme une sous-division, quelque part, de la cyberguerre, c'est quelque chose qui a cet intérêt de nous permettre de voir qu'on est en train de perdre cette guerre qu'on mène à la Russie à travers l'Ukraine. C'est discutable pour les Américains. Je ne suis pas sûr qu'ils soient en train de perdre, mais pour ce qui est des Français, tout particulièrement des Français, très clairement on est en train de la perdre et dans des proportions qui sont spectaculaires. Et c'est quelque chose qui est difficile à montrer en France, difficile à être entendu et complètement contradictoire avec la doxa ambiante qui veut que Poutine est une brèle, qu'il est totalement isolé, que toutes ses opérations se traduisent par des catastrophes, qu'il est en train de mener une guerre avec une armée de branquignoles, qui ne sont absolument pas professionnels, sur un territoire ukrainien. Ce qui est en partie vrai, mais il n'y a pas que ça. Il y a un autre territoire qui est l'Afrique, probablement beaucoup plus important d'un point de vue stratégique et économique pour la France, sur lequel on perd lamentablement.

C'est un message qui reste à être entendu parce qu'il est loin d'être aussi entendu aujourd'hui, mais c'est une voix pour le porter au grand public qui est vraiment intéressante.

Asma Mhalla : Sur la question des stratégies d'influence de la France en Afrique, on pourrait même faire référence au fameux discours de septembre dernier [2021] d'Emmanuel Macron où il expliquait aux ambassadeurs qu'il fallait absolument qu'ils se saisissent des réseaux sociaux comme arme d'influence et potentiellement, et pourquoi pas, du réseau France Médias Monde. Ça avait créé une espèce de réaction absolument outrée de RFI, France 24, disant qu'ils n'étaient absolument pas des médias d'État, ce en quoi, d'ailleurs, ils ont raison, à mon avis.

Damien Douani : Ils ont raison si ce n'est que France 24 a été construit comme étant la voix de la France à l'étranger, sous le président Chirac.

Asma Mhalla : Oui, mais pas comme étant le relais systématique et immédiat de la parole de l'Élysée, on va dire.

Damien Douani : Sur ça on est d'accord.

Fabric Epelboin : Parce qu'on est dans une démocratie.

Bertrand Lenotre : Et, malgré tout, c'est une chaîne vraiment intéressante, quand on l'écoute un petit peu pas mal de choses s'y disent.

Fabrice Epelboin : C'est une très bonne chaîne. Toujours est-il que, malgré tout, elle émane de la France et elle est quand même dans une liberté d'expression qui est contingentée par la France et qui est bien supérieure aux chaînes d'info françaises qui s'adresse à des Français. C'est certainement ce qu'il y a de plus bluffant pour France 24.

Asma Mhalla : Juste pour repréciser. En effet, je suis d'accord avec toi, sinon je ne l'aurais pas écrit comme ça. Pour moi, si on parle de cyber, cinquième dimension de la guerre, il faut bien prendre en compte l'ensemble du spectre, de façon macro encore une fois, c'est-à-dire ce qui se passe sur les trois couches du cyberespace qui sont interconnectées, qui s'interpellent, d'ailleurs l'une peut alimenter l'autre, c'est ce que j'ai essayé de dire. Les cyberattaques, la guerre informationnelle, participent de logiques qui peuvent être convergentes, mais, néanmoins, différentes dans les modalités, dans la façon de faire. Et c'est là où j'aimerais juste apporter une précision.

Aujourd'hui, sur la guerre en Ukraine, la documentation est en cours. On sait qu'il y a eu un certain nombre de cyberattaques russes au début du conflit. Pourquoi est-ce que l'arme cyber n'a pas pris ou n'a pas pris dans des proportions qu'on aurait estimées ? Ou que la grande cyberguerre, au sens où on l'a tous fantasmée, avec des sites gouvernementaux complètement à plat, des pays totalement désorganisés, mis à sac, etc., n'a pas éclos ? Il y a un certain nombre d'hypothèses aujourd'hui sur la table : la résistance ukrainienne déjà, par résilience, parce qu'ils subissent des campagnes de cyberharcèlement de la part de la Russie depuis 2014 donc ils se sont aguerris ; parce qu'il y a eu le soutien très fort des Américains, d'ailleurs assumé en juin dernier par le gouvernement américain lui-même ; parce que peut-être qu'aujourd'hui il y a un certain nombre d'hypothèses sur le fait que l'arme cyber n'est pas si agile que ça, parce que de vraies opérations de cyberattaques supposent une vraie préparation en amont et que, par ailleurs, elles sont *spot* dans les résultats, c'est-à-dire que le résultat ne sera peut-être pas pérenne dans le temps ; parce que vous avez aujourd'hui des chaînes de commandement qui ne sont pas toutes agiles ou qui n'ont pas toutes une littératie cyber dans l'état-major d'un certain nombre d'armées. Donc vous avez un ensemble d'hypothèses.

Il y a une interview [**10**], si vous permettez que je donne une référence, qui est très intéressante, parue le 12 octobre dans *L'Express*, d'Eviatar Matania qui est un des grands experts cyber israéliens, qui explique très précisément une partie de ces hypothèses : pourquoi est-ce que aujourd'hui l'arme cyber est une arme parmi tant d'autres, mais qu'elle n'est pas encore au niveau de sophistication qu'on aurait pu fantasmer d'elle.

Vous avez aussi la question de la maturité technologique et de la maturité cyber de l'armée au sens général, c'est-à-dire hormis les unités dont c'est la spécialité. Aujourd'hui ça n'a pas totalement essaimé, on n'a pas encore une culture cyber qui s'est complètement généralisée dans les corps armés, par exemple. Il y a tout un tas d'autres hypothèses, je vous renverrai vers un certain nombre de lectures à la fin de l'entretien, si ça vous intéresse.

Les intentions ne sont pas exactement les mêmes.
Les guerres informationnelles, elles, ont pour objet de déstabiliser non pas des infrastructures, mais des opinions publiques, donc ça se passe sur un temps beaucoup plus long. Une campagne de désinformation qui fonctionne, c'est une campagne de désinformation qui travaille dans les failles de votre système, de votre société, de façon très longue, sur des années. Typiquement, quand on regarde les stratégies de désinformation ou désinformationnelles russes, elles n'ont pas du tout les mêmes stratégies, en tout cas les mêmes narratifs ou les mêmes mécaniques en France qu'en Afrique. Elles ne vont pas du tout travailler sur les mêmes sujets, donc elles ont une connaissance extrêmement fine de votre contexte culturel, socio-économique, etc., donc de la cible, et c'est hyper intéressant.

En fait, il y en a une qui se travaille vraiment sur un temps long, l'autre aussi se travaille sur un temps long, mais avec des effets pour l'instant et en l'état des choses visiblement beaucoup plus *spot*

Et vous avez d'une part, sur les guerres informationnelles, une porosité de l'opinion publique — encore faudrait-il que ce concept d'opinion publique existe réellement —, c'est-à-dire, en fait, de nous tous. Et là tu vas aller taper les questions de *sourcing*, d'éducation à l'information, de comment ne pas croire tout ce que tu reçois très vite, de résilience individuelle et collective, on va dire, sur le modèle finlandais ou canadien, par exemple. Au Canada, ils ont des systèmes d'éducation de la population, c'est-à-dire des enfants mais aussi des adultes — et c'est très important d'embarquer les adultes là-dedans —, qui est très intéressant, qui s'appelle le « module de 30 secondes » : prenez toujours 30 secondes avant de croire n'importe quoi, toujours 30 secondes ! Ils éduquent les gens à toujours avoir ces 30 secondes de discernement avant de croire n'importe quelle source, qu'elle soit juste ou pas juste, vraie ou pas vraie, officielle ou non, fiable ou pas, peu importe.

Ce sont des réflexes cognitifs et de discernement à réinjecter, à re-explorer, ce qu'on ne fait pas encore tout à fait bien, qu'on commence à faire en France, mais qui suppose d'être très largement musclés. Sur la sphère informationnelle il y a une porosité beaucoup plus large que dans la sphère des cyberattaques en l'état.

Bertrand Lenotre : Asma, on va terminer par ta bibliographie, puisque tu y tenais. Quels sont les bouquins que tu recommandes instamment, par exemple, à ceux que tu rencontres à Polytechnique ou à Sciences Po, sur la compréhension de ces phénomènes aujourd'hui ? Il y en a deux/trois qu'il faut lire, qui sont récents ?

Asma Mhalla : Il y a le dernier bouquin, qui vient de sortir, d'Eviatar Matania [<em<Cyberpower. Israël, la révolution cyber et le monde de demain], que j'aime beaucoup. En fait, il va encore plus loin, il explique toute la stratégie de développement cyber, on n'en a pas parlé. Comment un État s'organise en termes de stratégie d'innovation, en termes de stratégie de développement, sur des technologies qui sont duales, à la fois le civil et le militaire, etc. L'exemple israélien est, évidemment, un des premiers exemples qui nous vient tous en tête. Il a une espèce de retour d'expérience sur la stratégie israélienne, sur son expérience personnelle. Il explique aussi, d'une certaine façon, pourquoi la guerre d'Ukraine de 2022 n'a pas été à ce point le théâtre d'explosions qu'on attendait tant en termes de cyberattaques, etc. Il a eu deux grands entretiens-fleuves dans *L'Express* du 12 octobre qu'il faut absolument lire. Et puis son livre.

Sur les stratégies de désinformation, les deux rapports de l'IRSEM sont absolument incontournables sur les stratégies de désinformation russe, et puis le plus récent, sur les stratégies de désinformation chinoise, dont on ne parle pas assez, qu'on va commencer à découvrir et on va dire « tiens, c'est nouveau » et en fait, pas du tout ! Ils commencent d'ailleurs à se caler sur les stratégies russes, mais dans leur zone d'influence directe.

En premier élément, ça peut être des lectures hyper-intéressantes et puis se documenter plus généralement. Il y a un certain nombre de médias ou de revues spécialisées, comme Le Rubicon [**11**], *Le Grand Continent* [**12**] parfois, où il peut y avoir des textes assez longs et très fouillés d'experts qui expliquent un peu les grands enjeux, les grandes dynamiques sur ces questions.

Bertrand Lenotre : Asma, il faudra que tu reviennes nous voir, d'ailleurs je vais teaser pour la prochaine fois. La prochaine fois tu nous parleras, par exemple, de guerre cognitive.

Asma Mhalla : Ah, on n'en a pas parlé ! Zut…

Bertrand Lenotre : Mais justement, on le garde pour une prochaine fois. La militarisation possible des métavers, c'est absolument passionnant, parce que…

Asma Mhalla : Des cerveaux ! La militarisation des cerveaux !

Bertrand Lenotre : Des cerveaux. C'est vraiment un sujet passionnant qui pousse encore plus loin la perspective de tout ce qu'on vient de se dire depuis 40 minutes.

Asma Mhalla : Je précise juste : la guerre cognitive, pareil, c'est un concept, un terme qui existe, mais, en fait, il est réinvesti par de nouveaux outils, par de nouveaux écosystèmes technologiques qui sont de masse et très puissants et qui permettent d'avoir des échelles d'attente et de ciblage qui sont inégalées, le métavers en l'occurrence, mais pas que.

Bertrand Lenotre : Merci Asma Mhalla.

Asma Mhalla : Merci à vous.

Bertrand Lenotre : Damien, tu as dix secondes pour faire ta petite partie promo.

Damien Douani : Si, comme Asma, vous pensez que Les Éclaireurs du Numérique sont là pour essayer de rentrer dans votre cerveau et vous apprendre des choses, eh bien vous êtes au bon endroit. N'hésitez surtout pas à nous mettre cinq étoiles sur votre plateforme préférée de baladodiffusion ou à nous mettre un petit commentaire pour nous dire combien vous nous aimez, ça nous fera toujours plaisir. Si vous ne nous aimez pas, ne nous le dites pas, ce n'est pas très grave, comme ça nous resterons non amis. À très vite.

Bertrand Lenotre : C'était dix secondes, c'était bien fait comme d'habitude. Merci Damien. À bientôt. Merci Fabrice.

Damien Douani : À bientôt.

Fabric Epelboin : À bientôt.

Bertrand Lenotre : Merci beaucoup, Asma Mhalla, d'être venue dans ce podcast. À très bientôt.

Signaler une erreur, poser une question

Références

[**1**] « Il est temps de nous préparer à la cyberguerre », Asma Mhalla, 13/10/2022
[**2**] Stuxnet
[**3**] Cyberwarfare, EN
[**4**] Killnet, groupe de hackers pro-russe
[**5**] Armée informatique d'Ukraine
[**6**] *Astroturfing*
[**7**] Anonymous (collectif)
[**8**] Starlink
[**9**] Rapports IRSEM - « les opérations d'influence chinoise » et « les manipulations de l'information »
[**10**] Cyberpuissance : comment Israël est devenu un acteur redoutable
[**11**] Le Rubicon, plateforme francophone d'analyse des questions internationales
[**12**] *Le Grand Continent*,

Média d’origine

Titre : [Cyberguerre] Big Techs et géopolitique avec Asma Mhalla
Personne·s : Asma Mhalla - Bertrand Lenotre - Damien Douani - Fabrice Epelboin
Source : Podcast
Lieu : Les Eclaireurs du Numérique
Date : 04/11/2022
Durée : 40 min
Licence : Verbatim
Crédits des visuels : Cyberespace , Clio Prépas - Cyberespace et géopolitique - Licence Creative Commons CC BY NC SA

Avertissement : Transcription réalisée par nos soins, fidèle aux propos des intervenant·e·s mais rendant le discours fluide. Les positions exprimées sont celles des personnes qui interviennent et ne rejoignent pas nécessairement celles de l'April, qui ne sera en aucun cas tenue responsable de leurs propos.

Transcriptions sur les mêmes thèmes :

Mardi 14 décembre 2021
Émission *Libre à vous !* diffusée mardi 7 décembre 2021 sur radio Cause Commune
Agnès Crepet - Étienne Gonnu - Frédéric Couchet - Gaël Duval - Jean-Christophe Becquet - Laurent Costy - Lorette Costy

Samedi 25 mai 2024
Cybersécurité et cyberdéfense : un sujet géopolitique - Guillaume Poupard
Guillaume Poupard
Devoxx FR 2024

Lundi 29 août 2022
Keynote - Cloud Souverain - Quentin Adam
Quentin Adam
Conférence Cloud Nord 2021

Transcriptions avec les mêmes personnes :

Mardi 28 juillet 2020
La ligne rouge de la souveraineté numérique - Les Éclaireurs du numérique
Bertrand Lenotre - Damien Douani - Fabrice Epelboin - Tariq Krim

Mardi 5 juillet 2022
[Souveraineté numérique] Assemblée Nationale : le grand reset ?
Bertrand Lenotre - Damien Douani - Fabrice Epelboin - Philippe Latombe

Lundi 3 avril 2023
L’IA va-t-elle tuer l’école ?
Prospective
Bertrand Lenotre - Damien Douani - Fabrice Epelboin

Thèmes récents

Tri par titre ou par utilisation

- **Institutions (390)**
- **Partage du savoir (269)**
- **Internet (256)**
- **Vie privée - données personnelles (247)**
- **Administrations et collectivités (216)**
- **Éducation (189)**
- **Le Logiciel Libre (173)**
- **Associations (171)**
- **Divers (157)**
- **Économie (146)**
- **Licences (140)**
- **Libre à vous ! (137)**
- **L’April (120)**
- **Transcription (120)**
- Entreprise (98)
- Intelligence artificielle (92)
- Europe (79)
- Droit d’auteur (74)
- Conference (74)
- Sensibilisation (63)
- Innovation (61)
- Open Data / Données libres et ouvertes (61)
- Informatique (48)
- État et administrations (48)
- CHATONS (47)
- Philosophie GNU (46)
- Informatique en nuage (43)
- Informatique déloyale (41)
- RGPD (37)
- Interopérabilité (34)
- Promotion (34)
- DRM (33)
- Réseaux sociaux (33)
- Logiciels propriétaires (32)
- GAFAM (31)
- Recherche (30)
- Entreprises (28)
- Souveraineté numérique (27)
- Neutralité du Net (25)
- Place des femmes - Inclusivité (25)
- Cyberattaques - Cybersécurité (22)
- Transition écologique (22)
- Accessibilité (21)
- Standards ouverts (21)
- Surveillance (20)
- Marchés publics (19)
- Internet (19)
- Désinformation (17)
- Sciences (16)
- Vente forcée / vente liée (16)
- HADOPI (14)
- Environnement (14)
- Chapril (14)
- Musique libre (13)
- Brevets logiciels (13)
- Open Bar (13)
- Économie sociale et solidaire (13)
- Wikipédia (13)
- Framasoft - Dégooglisons Internet - Contributopia (11)
- Communs (10)
- Libre en Fête (9)
- Vote électronique (9)
- OpenStreetMap (9)
- Archive (8)
- Évènements libristes (8)
- Parlezmoid’IA (8)
- Santé (7)
- Téléphonie mobile (7)
- Aprilien (6)
- Infrastructures (6)
- Cloud computing (6)
- Libertés informatiques (6)
- Café libre (6)
- Formation aux logiciels libres (5)
- ACTA (5)
- RGI (5)
- Communs numériques (5)
- Technopolice (4)
- DADVSI (4)
- Site web (4)
- Trad-GNU (4)
- Framasoft - Collectivisons Internet / Convivialisons Internet (4)
- Parcours libriste (4)
- Rançongiciel (3)
- Software Heritage (3)
- Mastodon (3)
- Sécurité (3)
- Privacy - personal data (3)
- Espace membre (2)
- Logiciels libres de dessin et de retouche d’image (2)
- Blockchain (2)
- Pacte du Logiciel Libre (2)
- Inclusion numérique (2)
- Culture libre (2)
- TAFTA (2)
- Fédiverse (2)
- Au cœur de l’April (2)
- Ma Dada (2)
- Big Tech (1)
- Windows (1)
- Syndicalisme (1)
- Traduction (1)
- Logiciel de caisse (1)
- Candidats.fr (1)
- Aaron Swartz (1)
- Métavers (1)
- Cryptographie (1)
- Raising awareness (1)
- Technosolutionnisme (1)
- Podcasting (1)
- Graine de libriste (1)
- Actualité du Libre (1)
- Fournisseurs d’accès à Internet associatifs (1)
- Diversité (1)
- Journalisme et logiciels (1)
- Médecine (1)