INSTITUT DIDEROT

Les Carnets des Dialogues du Matin

NICOLAS ARPAGIAN

Quelles menaces numériques dans un monde hyperconnecté ?

www.institutdiderot.fr

Les Carnets des Dialogues du Matin

NICOLAS ARPAGIAN

Quelles menaces numériques dans un monde hyperconnecté ?

AVRIL 2018

Sommaire

Avant-Propos

Dans la lutte historique entre l'épée et le bouclier, la conception de la défense a toujours, par nature, un temps de retard sur la technique de l'agresseur puisqu'on ne peut se défendre contre ce qu'on ignore.

L'explosion du numérique a singulièrement aggravé le problème.

Le numérique a permis le développement d'un nombre d'images quasiment infini de la réalité : hommes, entreprises, équipements, objets dont les représentations sont autant de possibilités d'accéder au contrôle des réalités sous-jacentes en dehors des lois ordinaires qui condamneraient une opération visant au même but dans le monde physique.

Ces possibilités multiples peuvent être exploitées par des intéressés également multiples : pirates agissant pour leur compte ou celui de groupes d'intérêts et de mafias, voire corsaires agissant discrètement pour le compte d'États. Les risques qui en résultent forment une palette allant de l'équivalent du vol à l'étalage au blocage de l'économie d'un pays et à l'affaiblissement de ses capacités de défense en cas de guerre.

Nombre infini de possibilités et d'acteurs, évolution ultrarapide des techniques renforçant le retard structurel des carabiniers dans leur lutte contre les agresseurs, ignorance technique, naïveté et penchant pour la facilité des utilisateurs dessinent de sombres perspectives sur lesquelles Nicolas Arpagian nous alerte.

Il esquisse les voies d'une réponse qui ne peut être efficace que si elle se déploie simultanément sur plusieurs plans :

- de la technologie bien sûr pour lutter contre les méfaits qu'elle a elle-même rendus possibles,
- des utilisateurs et futures victimes qu'on ne peut protéger contre leur insouciance,
- des hébergeurs, en leur faisant endosser la qualité d'éditeurs pour les responsabiliser,
- politique et judiciaire, au niveau de l'Europe, pour créer un droit adapté à cette réalité nouvelle.

La bataille sera longue et incertaine. La première condition du succès est une prise de conscience de l'étendue et de la diversité du risque.

Nicolas Arpagian nous y invite.

Entendons-le.

Jean-Claude Seys
Président de l'Institut Diderot

Quelles menaces numériques dans un monde hyperconnecté ?

☛ *L'auteur s'exprime ici à titre personnel, sans engager les institutions auxquelles il collabore.*

Il y a une dizaine d'années, l'Institut Diderot m'invitait déjà à venir parler de cybersécurité [1]. À l'époque, le sujet n'intéressait que quelques technophiles ou des responsables de la sécurité nationale. Il est maintenant entré dans le débat public. Ce qu'on a vu tout récemment avec l'audition de Mark Zuckerberg devant le Sénat américain au printemps 2018. En toute rigueur, il est vrai, l'affaire Cambridge Analytica n'est pas une affaire de piratage. La question soulevée par ce scandale est celle d'une exploitation abusive des données dans un cadre contractuel. Mais l'émotion soulevée par cette affaire et les réactions qu'elle a suscitées montrent bien une sensibilité plus aiguë au problème de la protection des données.

1. *L'avenir de la cybersécurité*, décembre 2009, disponible sur : http://www.institutdiderot.fr/lavenir-de-la-cybersecurite

I. DES MENACES D'UNE NATURE INÉDITE

Quand on parle de piratage, ce qui frappe au premier abord, ce sont les chiffres. Un milliard de boîtes mail Yahoo!, peut-être même trois milliards, ont été piratées en 2013. Voilà qui est complètement inconcevable dans le monde physique.

La portée des attaques aussi est remarquable. Le pirate peut toucher la planète entière. Ses agissements sont transnationaux. Cela lui est d'ailleurs bien utile : les réponses juridiques étant, quant à elles, restées nationales, le pirate peut mettre entre lui et ses victimes un ensemble de frontières lui assurant une forme d'impunité.

Les rançongiciels illustrent bien la nature véritablement pandémique des attaques numériques. En mai 2017, WannaCry a frappé 200 000 entreprises et 150 pays. Ce type de menaces est d'autant plus inquiétant qu'après quelques temps, le pirate met sur le marché son code, si bien que d'autres personnes, qui n'ont pas nécessairement de liens personnels, idéologiques ou géographiques avec lui, vont se procurer le logiciel et le réutiliser, parfois après l'avoir modifié. Des générations successives et dégénérées du même virus apparaissent, suffisamment différentes pour nécessiter à nouveau un travail de recherche afin de les contrer.

Les rançongiciels demandent en général une somme « raisonnable ». 300 euros, par exemple. C'est ennuyeux, mais la somme est accessible. La personne ou l'entreprise

est donc tentée de payer pour se remettre au travail. Mais payer la rançon encourage les pirates à continuer, d'autant que la récupération des données n'est pas assurée. C'est ce qui s'est passé avec Petya. Les analyses ont montré que les données étaient non seulement chiffrées, avec demande de rançon, mais détruites. Tout se passe comme si vous preniez un otage en demandant une somme en échange, mais que vous tuiez l'otage. Voilà qui est extrêmement préoccupant. On sort d'un cadre où les malfaiteurs, aussi condamnables soient-ils, cherchent « seulement » à gagner de l'argent et donc, par intérêt personnel, proportionnent les nuisances qu'ils vous imposent au gain qu'ils espèrent retirer. Si vous pensez que vos données ont toutes probablement été détruites, à quoi bon payer ? La menace change de nature.

Indépendamment du changement d'échelle, le numérique pose un certain nombre de problèmes spécifiques quant à la sécurité. Le premier de ces problèmes tient à ce qu'une attaque numérique n'est pas clairement définie et repérable. Si une personne vous menace et vous vole votre portefeuille, vous n'ignorez pas que vous vous êtes fait agresser. Vous savez quand l'attaque a eu lieu et quand elle s'est achevée. Vous avez une idée assez précise de ce que vous avez perdu. Corrélativement, vous connaissez les mesures de remédiation à mettre en œuvre : porter plainte, faire opposition, refaire vos papiers. Or c'est une particularité du numérique que de laisser la cible ignorer son statut de victime. Un peu comme si le pirate s'introduisait chez vous pendant

votre absence sans rien y dérober ou abîmer, en se contentant de tout prendre en photo pour se servir ultérieurement de ces informations. Vous pouvez être complètement ignorant de cette attaque et vous croire autant en sécurité qu'avant.

La nature des données numériques rend aussi problématique la notion même de vol. Le droit pénal le définit comme « la soustraction frauduleuse de la chose d'autrui ». Le problème, avec une donnée numérique, c'est que si je la duplique, a *fortiori* à votre insu, celle-ci ne vous est pas soustraite. Vous ne vous êtes peut-être même pas rendu compte du problème. Comment évaluer le préjudice subi quand rien ne vous a été retiré, mais qu'il s'agit d'une information dont la possession exclusive fait la valeur ?

Une troisième difficulté tient à l'identification de la cible de l'attaque. Le numérique permet en effet deux grands types d'agression : les attaques en gros, comme le piratage d'un milliard de boîtes mail Yahoo!, ou des attaques très fines sur un seul individu (John Podesta, par exemple, le directeur de campagne de Hillary Clinton). Il faut ainsi distinguer les attaques globales des opérations visant une entité précise car ces dernières ont une cible bien définie, pour des raisons idéologiques ou en vue d'exploiter une faille individuelle. Les premières sont de nature différente. Dans ce cas, le pirate sait juste exploiter une faille répandue dans un nombre important de systèmes. Afin de maximiser son profit, il lance une attaque généralisée qui touchera tous les systèmes

affectés par cette faille, quels qu'ils soient. Dans ce cas, il est tentant de croire, si un grand groupe est touché, qu'il était la cible de l'attaque. C'est en effet pourtant inexact : il se trouve que ce groupe faisait partie des cibles vulnérables. Cela complique l'analyse et la recherche de l'intérêt à agir du pirate.

Nous avons ainsi connu après les attentats de Paris en 2015 une campagne où des milliers de collectivités locales ou d'institutions ont vu leur page d'accueil remplacée par un appel au jihad. En matière de terreur, l'effet est important : cela a changé depuis, mais pour toute une partie des Français, le terrorisme était quelque chose qu'on voyait à la télévision et qui touchait les grandes villes. Découvrir, du jour au lendemain, un appel au jihad sur le site d'une institution locale est assez perturbant. On s'est demandé s'il y avait une raison particulière derrière le choix des sites attaqués. Il y en avait effectivement une, mais de nature purement technique : ces collectivités avaient en commun de se servir de WordPress et n'avaient pas fait leur mise à jour. Le pirate connaissait la faille dans WordPress, et a lancé une attaque automatisée à grande échelle.

Un autre exemple de la difficulté à identifier la cible des pirates a été l'attaque contre Saint-Gobain durant l'été 2017. Le coût de cette offensive a été considérable : Saint-Gobain a déclaré 220 millions d'euros de pertes. Mais ce qui est intéressant est qu'on ne peut pas considérer que Saint-Gobain était la cible. L'entreprise a été touchée après une mise à jour de son logiciel

comptable et fiscal en Ukraine : ce n'est pas elle qui était visée, mais l'économie ukrainienne en général.

L'exemple de Saint-Gobain permet aussi de souligner une dernière particularité des menaces numériques. Elles obligent à repenser complètement la géographie de nos défenses. Car les menaces et les attaques numériques ne sont pas solubles dans les notions traditionnelles de guerre et de paix. Il n'y a plus de déclarations de guerre, de traités de paix, de droit de la guerre. Il n'y a plus de troupes officielles dont vous pouvez surveiller les déplacements d'un côté ou de l'autre de la frontière. Même les notions de front, d'avant et d'arrière sont caduques : les fronts se démultiplient et vous n'avez plus d'arrière où mettre vos ressources à l'abri. Les pirates s'affranchissent des règles géographiques et juridiques. Et s'ils travaillent pour un État, ce n'est pas comme membres d'une force officielle, mais comme supplétifs ou mercenaires numériques.

II. UN PAYSAGE MODIFIÉ

Trois forces ont profondément renouvelé le paysage de la cybersécurité.

La première est la mondialisation qui pousse les administrations et les entreprises à s'interconnecter. Dans un monde globalisé, les organisations sont invitées à créer des réseaux, à se mettre en maillage, à créer des

interdépendances technologiques. Elles sont ainsi corrélativement poussées à réfléchir aux possibilités et aux risques de cette mêlée numérique.

De ce point de vue, les « hackers » sont très utiles. Il faut les distinguer des pirates. Car un hacker a une démarche constructive. Il s'interroge sur la façon dont fonctionne une technologie donnée. Le hacker est quelqu'un qui, lorsque vous lui mettez un outil entre les mains, se demande comment il marche et comment il peut le personnaliser, l'améliorer, le modifier, lui ajouter des fonctionnalités. Sur le marché de l'emploi, ces profils sont rares et donc chers. Ils sont très demandés par l'ensemble des acteurs : entreprises, administrations civiles ou militaires, crime organisé… Évidemment, il faut que le hacker dans votre entreprise soit solide sur le plan éthique : il est tentant, quand on se rend compte qu'on peut entrer sans laisser de traces dans un service verrouillé à double tour, d'essayer d'en profiter.

La mise en réseau des entreprises et des administrations provoque un changement profond de modèle : nous passons du château fort à l'aéroport. Dans un château fort, une enceinte épaisse entoure le lieu ; il n'y a qu'un nombre très réduit d'entrées, bien identifiées, où l'accès est quantitativement limité et où il est possible de contrôler aisément les arrivées et les sorties. Un aéroport est radicalement différent : des milliers, voire des dizaines de milliers de personnes passent par-là, toute la journée, pour des raisons très différentes. Les entrées sont très nombreuses. Il y a aussi des zones de transit.

De plus, les prestataires de sécurité peuvent être étatiques ou appartenir à des sociétés de sécurité privée dont vous ne savez que peu de choses. Or il en va un peu de même avec les données. Imaginons que vous mettiez celles-ci dans le cloud. Cela, vous l'avez décidé. Mais pour le reste, où sont-elles conservées, par quelle entreprise, quels prestataires, ou avec quels appareils ? Vous ne l'avez pas choisi, comme vous n'avez pas choisi la compagnie de sécurité privée chargée de vérifier les bagages.

Une deuxième force à l'œuvre dans le monde de la cybersécurité est la progressive mise en place, dans tout un ensemble de pays, quel que soit leur régime politique, d'un cadre juridique et réglementaire permettant de demander des comptes. L'audition de Mark Zuckerberg au printemps 2018 a bien montré l'existence d'une attente de l'opinion publique dans ce domaine, bien que, dans les faits, la pratique quotidienne des citoyens ne soit pas toujours très cohérente avec la conscience d'une menace sur leur sécurité et leur vie privée.

Enfin, nous vivons dorénavant dans un monde où expertise technique et ressources importantes ne sont plus nécessaires pour attaquer. Il n'est, par exemple, pas très compliqué de faire des faux en se servant d'Internet et des réseaux sociaux. Tel chef d'entreprise a signé une déclaration ou un document relatif à une cause qui lui tient à cœur : vous pouvez trouver ce document ; reprendre l'en-tête de la présidence, voire la signature du président si elle correspond à un fichier spécifique

dans le texte ; reproduire la façon dont les documents de cette entreprise sont présentés ; enfin, regarder sur Internet l'organigramme de l'entreprise. Avec tous ces éléments, vous pouvez commencer à vous prendre pour le dirigeant de l'entreprise. C'est apparemment ce qui arrivé dans le cas du pirate qui a usurpé l'identité de Brigitte Macron pour faire des commandes frauduleuses dans des établissements prestigieux. Car une fois que vous avez les noms, les documents et l'organigramme, l'usurpation d'identité n'est pas très compliquée. Pas besoin, donc, de moyens d'investigation colossaux. On l'a aussi vu entre les deux tours de l'élection présidentielle de 2012, quand les Américains sont entrés dans l'Intranet de l'Élysée. Ceux-ci ont simplement eu à regarder qui étaient les collaborateurs du Président sur le site ou sur Legifrance.gouv.fr, puis à aller sur les réseaux sociaux pour connaître les centres d'intérêt de tel ou tel collaborateur. Ensuite, à force de lui envoyer des mails ou des notifications sur le sujet, il y a bien un moment où ce collaborateur clique sur un lien sur lequel il n'aurait pas dû cliquer. L'infection initiale n'est donc pas particulièrement complexe. Ceci implique qu'une des clefs du problème est celle de la confiance. Quand le Premier ministre David Cameron bannit les iPads dans les réunions du Cabinet, ce n'est pas parce que ces appareils ne sont pas satisfaisants sur le plan opérationnel, mais parce que la confiance n'est pas là.

Un autre phénomène, particulièrement inquiétant, illustre aussi une forme de démocratisation de la menace numérique : l'apparition d'outils simples à utiliser, faciles

d'accès et qui, pour un coût modique, permettent à son acquéreur d'espionner ou de lancer des attaques.

Ces outils sont très réussis sur le plan commercial : ils sont simples (vous pouvez par exemple vous limiter à mettre l'URL de la page que vous voulez attaquer, avec la durée de l'attaque), vous pouvez faire des tests, vous avez des services d'assistance 7j/7, 24h/24, des points de fidélité, des notes comme sur Amazon, etc. Ce n'est pas étonnant : la concurrence fait rage, et chacun essaye de proposer le meilleur service possible pour satisfaire la demande. Car celle-ci existe. Quand vous faites une recherche dans Google, Google Suggest vous propose un résultat dès les premières lettres : plusieurs millions de personnes ont déjà fait la même demande, Google sait déjà ce que vous allez lui demander. Tapez « comment pi… ». Les résultats seront : « comment pirater un iPhone, une adresse mail, un compte », etc. Vous pourrez même avoir comme suggestion « comment pirater un compte gmail ».

De cette petite expérience, on peut tirer deux conclusions. Premièrement, que le piratage ne concerne pas que les mafias ou les triades mais intéresse aussi le grand public. Les résultats sont exprimés en français, ils ont dû être tapés plusieurs millions de fois pour être suggérés. Deuxièmement, le résultat obtenu est une phrase en bon français (« comment pirater un compte Facebook », non pas « logiciel xb22-46 v.2.1 »). On met clairement en avant l'objectif, en cherchant un moyen simple de l'atteindre. Alors que cet objectif est évidemment illégal.

Vous pouvez ainsi vous procurer des applications qui, une fois installées sur l'appareil de quelqu'un (sans être visibles, bien évidemment), vous permettront d'obtenir de façon claire, avec tableaux, cartes, graphiques et service de dépannage 24h/24 tout un ensemble d'informations fort intéressantes : intégralité de ses déplacements grâce au GPS, ce que celui-ci a tapé sur son clavier, les métadonnées de ses communications, ses SMS, etc. Tout ceci est illégal. Pourtant, la vente de ce type de programmes est libre. Car on présente la chose sous un jour acceptable : un logiciel de surveillance parentale, ou un outil permettant de suivre un aîné atteint de maladie dégénérative. Jamais comme un moyen d'espionner votre conjoint ou un collègue. On se retrouve alors face au paradoxe suivant : un policier qui dans le cadre de son travail veut surveiller quelqu'un utilise, pour des raisons juridiques, des outils moins puissants que ceux auxquels il aurait accès s'il voulait surveiller son conjoint. Pour le dire autrement : des outils qui auparavant restaient l'apanage de services de renseignements sont maintenant assez facilement accessibles aux particuliers. On le voit dans un nombre croissant de contentieux, notamment dans les divorces : bien entendu, ces outils ne peuvent pas être présentés à titre de preuve, mais ils aident en amont à la constitution d'un dossier. Une fois que vous avez obtenu les informations que vous recherchez, vous pouvez désactiver l'application à distance.

III. LES RÉPONSES RÉCENTES AUX MENACES NUMÉRIQUES

La première façon de se défendre contre des attaques numériques est d'identifier les cibles vitales. En France, la loi de programmation militaire de 2013 a identifié des OIV (Opérateurs d'Importance Vitale), dont la liste est classifiée. Ces OIV sont principalement définis au moyen d'un raisonnement *a contrario* : ce n'est pas tant leur importance quand ils fonctionnent qui compte, mais le fait que leur défaillance mettrait en péril le bon fonctionnement de la Nation.

Les autorités françaises ont eu une influence à l'échelon européen : la Directive NIS, entrée en vigueur le 9 mai 2018, a introduit la notion plus large d'OSE (Opérateur de Service Essentiel), dont la définition englobe en l'élargissant celle des OIV. Du strict point de vue de l'opérateur en question, ce statut est plus un inconvénient qu'autre chose, dans la mesure où il implique surtout des contraintes réglementaires supplémentaires.

Le Règlement Général sur la Protection des Données (RGPD) applicable dans l'Union européenne depuis le 25 mai 2018 constitue une nouvelle étape importante dans la lutte engagée contre les menaces numériques.

Ce Règlement porte sur les données personnelles, définies comme une « information se rapportant à une personne physique identifiée ou identifiable. » La distinction entre « identifiée » et « identifiable » apparaît cruciale.

Elle permet de couvrir non seulement les informations sur quelqu'un dont on sait qui il est, mais aussi les nombreuses possibilités d'identification offertes par le numérique au moyen de données dont ce n'était pas la fonction au départ, et qui étaient auparavant muettes. Une photo anonyme, par exemple. À moins de tomber pile sur quelqu'un qui connaît la personne figurant sur la photo, celle-ci ne sert pas à grand-chose dans le seul monde physique. Mais il est désormais possible de mettre cette photo dans un moteur de recherche qui fera le lien avec un individu précis, pour autant qu'il existe une autre photo de lui sur Internet. Vous pouvez alors identifier cette personne, voir son profil ou celui de ses amis sur les réseaux sociaux. Et maintenant apprendre énormément de choses sur elle, directement ou indirectement.

Un autre aspect important du RGPD est l'aggravation des sanctions. Les amendes auparavant prévues par la CNIL étaient de 150 000 euros et 300 000 euros en cas de récidive. Pour une grande entreprise, ce n'est pas beaucoup. Dorénavant, les amendes pourront se monter à 4 % du chiffre d'affaires mondialisé, ce qui peut faire très vite grimper la facture. De plus, le RGPD étant un texte européen, une fuite de données qui se présenterait en Allemagne, en Espagne, en France et en Italie pourrait donner lieu à quatre contentieux.

Il est urgent en effet de repenser les sanctions. La comparaison entre les articles 226-4-1 et 317-4-1 du Code pénal est frappante. Le premier énonce : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une

ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende ». Le second, en revanche, condamne à 7 ans d'emprisonnement et 30 000 euros d'amende le fait de rouler avec un numéro d'immatriculation alloué à un autre véhicule. Autrement dit, le message est le suivant : voler l'identité de quelqu'un en ligne, atteindre à sa réputation, fragiliser sa vie personnelle et professionnelle n'est punissable 'que' d'un an de prison ; en revanche, dès qu'on touche à la voiture, plus question de plaisanter. Et les peines encourues s'alourdissent.

Le RGPD, enfin, renforce les obligations du responsable de traitement. Si une entreprise confie à un tiers à des fins de relance le fichier de ses anciens clients, et si ces données fuitent, l'entreprise de départ ne pourra plus se décharger de sa responsabilité sur ce fournisseur. Les grandes entreprises ne pourront plus se défausser sur leurs prestataires. Les effets de ce règlement s'étendront d'ailleurs hors d'Europe : toutes les entreprises de marketing téléphonique situées au Maghreb, par exemple, seront poussées par leurs donneurs d'ordre à faire attention.

La Chine a mis en place une réglementation similaire. L'Afrique aussi, avec la convention de Malabo. Les États-Unis aussi sont récemment intervenus dans le champ de la protection des données, avec notamment un *executive order* signé par Donald Trump.

Une troisième réponse, enfin, peut-être la plus structurante, est celle des agences de notations. Deux des trois grandes agences mondiales, S&P et Moody's, ont annoncé qu'elles prendraient en compte la protection des données dans leurs notations. Être exposé à une amende de 4 % de son chiffre d'affaires mondialisé, ou avoir investi dans des innovations qu'un concurrent peut récupérer et exploiter à votre place affecte gravement la solidité de votre entreprise. Pour une société, ou des dirigeants dont une partie de leur patrimoine est indexée sur des titres susceptibles d'être affectés par ces notes, c'est un sujet d'importance.

On a retrouvé en 2013 sur les ordinateurs de personnes affiliées à la mouvance djihadiste des éléments techniques servant à commander l'ouverture d'un barrage en amont de New York. C'est à ma connaissance le seul cas, heureusement avorté, d'actions qu'on puisse vraiment considérer comme une tentative de cyberterrorisme : l'utilisation du numérique pour provoquer des morts civiles et effrayer la population, avec des images spectaculaires en prime. Le projet n'a pas abouti, mais il n'y a malheureusement pas de raison de croire que les pratiques de ce genre ne se développeront pas.

Cyberterrorisme, attaques en déni de service, vols d'informations, rançongiciels… Face à ces menaces, renforcer sa cybersécurité demande d'avoir une vision d'ensemble des risques auxquels on est exposé et de la réponse qu'on entend apporter. Juxtaposer des systèmes côte à côte, lancer son système puis seulement ensuite se demander comment le sécuriser, n'aboutit qu'à du bricolage technique du point de vue de la cybersécurité.

Il est nécessaire aussi d'évaluer la valeur de ses informations pour proportionner intelligemment le système de sécurité qui sera retenu. Il en va comme d'une maison. Son habitant ne met pas tout dans le coffre-fort quand il s'absente. Il laisse éventuellement son mobilier de jardin à l'extérieur, il met le reste entre les murs, certains objets sont mis sous clef et d'autres dans un coffre-fort, voire dans celui d'une banque. Il y a eu alors en amont un arbitrage entre la valeur du bien, le risque de vol et le coût de la protection. Les choses ne sont pas différentes en matière de cybersécurité. Nous pourrions certes tous nous enfermer dans une cage de Faraday pour protéger la confidentialité de nos données. Mais ce ne serait pas très pratique et limiterait les gains que l'on peut tirer des usages numériques. Il nous faut donc conduire un exercice d'introspection pour savoir ce que l'on souhaite protéger et à quel prix. Une telle réflexion est indispensable : être efficace en matière de cybersécurité signifie protéger à leur juste niveau les données dont on dispose en fonction de leur valeur à un moment précis.

Cette valorisation fait partie d'une démarche personnelle pour les particuliers et d'une stratégie pour les entreprises qui identifient ainsi la valeur de leur patrimoine informationnel et de leurs capacités de production et de commercialisation. Dans un contexte de transformation numérique, cette analyse suscitée par la recherche de sécurité est assurément porteuse de création de valeur. Car elle conduit à désigner ce qui constitue le cœur stratégique de l'organisation.

Débat

***Franck Durand** : Lors d'un récent voyage en avion, j'ai voulu acheter une bouteille d'eau pendant un transfert. J'ai donc tendu 1,50 euro : la personne a refusé, il a fallu que je sorte mon smartphone pour qu'elle scanne ma carte d'embarquement avec mon nom et mon vol. Tout ça pour une bouteille à 1,50 euro. Il y a là quelque chose de nouveau. Chaque fois que je rentre dans un parking, ma plaque d'immatriculation est enregistrée. Des données sont partout captées sans que je puisse m'y opposer. C'est un premier point sur lequel j'aimerais avoir votre avis.*

Ma deuxième question porte sur le rapport entre technologie et régime politique. On a pu mettre en rapport l'invention de l'étrier et le développement de la féodalité : l'étrier donnant une meilleure stabilité au chevalier, celui-ci devient un guerrier bien plus intéressant, ce qui implique alors de l'entraîner, d'avoir des chevaux, etc. donc toute une économie et toute une société. Les évolutions technologiques que nous connaissons sont sans rapport avec la simple découverte de l'étrier. Elles sont gigantesques. Quelles hypothèses pouvons-nous faire alors sur le régime politique à venir ?

Nicolas Arpagian : Votre question renvoie à ce que le numérique rend possibles des pratiques difficilement

concevables auparavant. Un garagiste peut très bien demander à un employé de noter dans un cahier au fur et à mesure les numéros de plaque d'immatriculation des clients. Mais vous voyez bien que gérer et mettre en valeur un tel cahier manuscrit est très compliqué. De plus, l'un des intérêts de la numérisation est qu'elle permet de conserver les données de façon utilisable pour des finalités multiples ou qui n'existent pas encore. Dans le cas du parking, la finalité première peut être celle de la sécurité. C'est en tout cas celle qui prévaut dans les immeubles de bureau : on sait combien de personnes sont dans l'immeuble et donc combien doivent être évacuées en cas d'incident. Le problème étant bien évidemment que vous n'avez peut-être pas envie qu'il y ait une trace, par exemple, de votre passage à un entretien d'embauche. Mais ce que je voudrais souligner ici, c'est que la conservation des données, par exemple les numéros de plaques dans un parking, peut servir à de nombreuses autres fins. Un service personnalisé, par exemple : si vous êtes handicapé, on vous oriente sur les places dédiées, à proximité des ascenseurs.

Ceci pose la question du choix des finalités. On dit que les technologies sont agnostiques : elles ne sont pas bonnes ou mauvaises, ce sont les usages qui le sont. D'où la question centrale que je posais tout à l'heure : la question, ni juridique ni technique, de la confiance. Ai-je confiance dans l'entité qui va collecter les données ? Et corrélativement, est-ce que j'accepte le marché qui m'est proposé : céder mes données et livrer mon intimité en échange du service rendu ? Ceci demande un

vrai exercice d'introspection, que chacun devrait faire. Un choix doit être fait, le problème étant qu'on ne vous le donne pas toujours : dans le parking, c'est à prendre ou à laisser, donc vous êtes condamnés, si vous n'êtes pas d'accord, à vous garer dans la rue ou à aller à pied – et encore : votre plaque d'immatriculation sera alors probablement captée par d'autres systèmes de vidéoprotection.

On pourrait imaginer un service payant associé à une meilleure confidentialité. La question a été posée à Mark Zuckerberg durant son audition : pourquoi pas un Facebook payant, qui permettrait de profiter de ses fonctionnalités sans être espionné ? La réponse de Mark Zuckerberg a été, en gros, qu'il l'aurait déjà fait si cela l'avait intéressé, mais que ce n'est pas son modèle économique actuel.

Pierre-Jean Benghozi *(ARCEP[2]) : On voit bien qu'il y a une forme de porosité entre les questions de protection des données, de cybersécurité et de cybercriminalité. Du point de vue de l'action publique, comment voyez-vous l'équilibre à trouver entre la protection des utilisateurs, par exemple de leurs données personnelles, la protection des réseaux, le fait que ce sont les réseaux qui peuvent bloquer les attaques en déni de service, etc., et la protection des correspondances et des contenus des applications ? Au-delà du constat, il faudra bien prendre des décisions sur la position du curseur…*

2. Autorité de régulation des communications électroniques et des postes.

Nicolas Arpagian : Surtout qu'a priori certaines de ces décisions vous reviendront…

Pierre-Jean Benghozi *: C'est bien pour ça que je pose la question…*

Nicolas Arpagian : L'instance administrative spécialisée en matière de cybersécurité en France est l'ANSSI [3]. Ce n'est pas une agence indépendante. C'est une émanation des services du Premier ministre. Elle est compétente pour la sécurité technique, l'appréciation des éléments de chiffrement et d'intégrité, et a en charge la sécurité et la protection des infrastructures de l'État et la surveillance du maintien du niveau de sécurité des OIV. L'ANSSI attribue aussi le label qui permet aux sociétés de service de travailler auprès des opérateurs d'importance vitale.

Dans la loi actuellement en discussion au Parlement, il est important de savoir s'il ne faudrait pas se concentrer sur le réseau pour améliorer la sécurité. L'idée est la suivante : quand je bois de l'eau dans mon appartement, pas besoin d'être docteur en biologie, il me suffit d'avoir souscrit un contrat avec Suez, Veolia ou une régie municipale. C'est à ces entités de s'assurer que l'eau qu'elles me distribuent est potable. C'est peut-être de cette façon qu'il faudrait voir la sécurité des réseaux de communication : sans intervenir sur les contenus, peut-être serait-il possible d'intégrer aux flux des outils techniques, qui seraient accessibles à l'ANSSI ou

3. Agence nationale de la sécurité des systèmes d'information – www.ssi.gouv.fr

l'ARCEP pour contrôle et vérification. Regardez les antivirus vendus aux individus : beaucoup de gens les achètent, mais ne les activent pas, ne renouvellent pas leur abonnement, les installent mal, ne les mettent pas à jour. Quand vous achetez une voiture avec ABS ou des options, vous vous dites que si la voiture est vendue avec cette option, c'est que celle-ci est déjà installée, vous n'avez pas en plus à faire telle ou telle démarche. Eh bien, il en va de même avec les antivirus, sauf qu'on demande justement au consommateur de faire plusieurs choses en plus alors qu'il a d'autres soucis et qu'il n'y connaît peut-être rien. On réplique souvent que le consommateur n'a qu'à demander à un de ses amis « qui s'y connaît ». Comme garantie de sécurité, on a vu mieux…

Or tout le problème est qu'on demande aussi à la même personne de payer ses impôts sur Internet, de constituer son dossier médical en ligne, etc. Bref, de faire circuler sur le réseau des données toujours plus sensibles. C'est un peu comme si on laissait tout seul l'individu lambda s'occuper de sa voiture, de la qualité des freins, des suspensions, et qu'ensuite on lui demandait de courir un Grand Prix.

La question qu'on se pose est donc de voir s'il ne serait pas plus efficace, dès lors qu'on détient en tant qu'opérateur un certain nombre d'informations qui n'interviennent pas sur les contenus, mais qui sont des éléments strictement techniques, d'intégrer ces éléments dans le flux pour éviter les pandémies, d'une part, et

puis surtout parce que les gens n'ont ni l'envie, ni les compétences pour s'occuper de cela. Les gens veulent pouvoir utiliser le numérique, pas se spécialiser dans la sécurité. Surtout au regard du caractère extrêmement évolutif de la menace, et du caractère opportuniste des agresseurs, qui ont tous les avantages de l'attaque : choix de la cible (massive ou individuelle), de l'agenda, du mode opératoire et du tempo.

Cela permettrait aussi de remédier à un problème économique assez important. Les assureurs savent qu'avec Internet, il est possible de mettre à terre une entreprise. Le résultat est identique à celui des scooters à Paris. Étant donné qu'un scooter sur deux est volé, la prime d'assurance est très élevée : 50 % du prix du scooter plus la marge commerciale de l'assureur. De même, étant donné que toute votre entreprise peut s'écrouler à cause d'une attaque, votre police d'assurance vaut très cher, potentiellement 100 % de la valeur de ladite société si celle-ci risque de tout perdre lors d'une cyberattaque. Conséquence : vous ne vous assurez pas, parce que ça coûte trop cher, votre voisin non plus, probablement, et le niveau de sécurité ne progresse pas. Il y a donc toute une réflexion pour voir s'il ne serait pas préférable d'intégrer une hausse du niveau de sécurité à ce qui circule. Comme quand on distribue une eau traitée pour qu'elle soit potable. Cela permettrait de prémunir un certain nombre d'entreprises et d'utilisateurs contre par exemple 60 ou 65 % des risques, ou en tout cas une part importante. L'assurance, par conséquent, n'aurait à s'occuper que du reste – voire moins si vous avez

fait l'exercice d'introspection dont je parlais et que, finalement, vous décidiez de ne protéger que 15 % de vos données. Les primes d'assurance seraient alors plus réalistes et plus accessibles.

Stéphane Marchand *(délégué général d'Entreprise et Progrès) : Combien l'affaire Cambridge Analytica pourrait-elle coûter à Facebook ? Je voudrais aussi vous demander, pour rebondir sur la première question concernant les régimes politiques à venir, s'il n'est pas concevable que, face à l'angoisse croissante des citoyens concernant la protection des données, nous aboutissions à une sorte de réseau social ultra-étanche, complètement fermé, qui vivrait en autarcie, peut-être même avec sa propre monnaie. Le régime politique du futur ressemblerait à cela, ce qui ne serait pas une bonne nouvelle.*

Nicolas Arpagian : Je ne crois pas à un impact commercial à court ou moyen terme. D'une part, car une grande majorité des utilisateurs sont devenus dépendants de ce flux d'informations et d'interconnexions avec leur communauté. Sans parler des effets d'une drogue, ils sont en grand nombre accoutumés à ponctuer leurs journées de visites ou d'interactions sur cette plateforme. Ils ne semblent pas prêts à y renoncer. D'autre part, par ce que l'usage de la fonction « Facebook Connect » leur permet d'accéder à de nombreux services annexes dont ils ne sont certainement pas prêts à se priver. Les retraits de Facebook, outre quelques annonces de personnalités médiatiques, sont marginaux au regard de son audience.

En avril 2018, quelques jours après le début du scandale Cambridge Analytica, Facebook publiait d'excellents résultats pour le 1er trimestre 2018 : il comptait 2,2 milliards d'utilisateurs actifs mensuels et 1,45 milliard d'utilisateurs actifs quotidiennement. Dans les deux cas, c'est une augmentation de 13 % par rapport à l'année précédente. Ainsi de janvier à mars 2018, Facebook a gagné 11,9 milliards de dollars. C'est 4 milliards de dollars de plus qu'en 2017 à la même période.

On dit qu'il n'existe pas de droit international du numérique. Si, il y en a un : les conditions générales d'utilisation des grands acteurs et des grandes plateformes. C'est-à-dire leur version en anglais, comme cela est bien précisé, les autres n'étant que des traductions. Si vous avez un contentieux avec Google ou Facebook, il vous faudra aller devant des tribunaux étatsuniens. Il existe aussi une jurisprudence qui dit que vous pouvez éventuellement aller ailleurs. Mais on voit bien qu'il s'agit de lever l'index en s'excusant pour dire que ce serait quand même bien de ne pas réserver les procédures aux seuls tribunaux de Californie…

Je rappelle au passage que les deux commissions du Congrès américain devant lesquelles Mark Zuckerberg a été auditionné sont celles de la Justice et celles de l'Énergie et du Commerce. Il y a évidemment une portée politique dans ces auditions, mais le signal derrière est assez clair : quelles conséquences l'affaire Cambridge Analytica risque-t-elle d'avoir pour les affaires ?

Revenons au futur que nous promettent les réseaux sociaux et Internet. Il est vrai qu'on voit maintenant des entreprises qui prétendent avoir une véritable doctrine de société. Google dit : « *Don't be evil* ». Son vice-président soutient que si vous ne voulez pas qu'une information vous concernant soit rendue publique, vous devriez vous demander si vous devez avoir cette pensée ou commettre cet acte. La vie privée est censée être caduque – mais Mark Zuckerberg a quand même pris soin d'acheter les maisons autour de la sienne. Comme quoi même lui a encore une petite intuition de ce qu'est la vie privée. Il l'a d'ailleurs reconnu lors de son audition au Sénat, quand il a refusé de dire publiquement dans quel hôtel il était descendu à Washington.

Les dirigeants des grandes entités de l'Internet parlent d'égal à égal avec les chefs d'État. C'est à peine si, quand ils viennent en France, ils n'ont pas droit au cérémonial d'une visite d'État. Les pays européens sont dans une rivalité aberrante et utilisent l'optimisation fiscale pour s'attirer leurs faveurs.

Or, il ne faudrait pas oublier deux choses. Marissa Mayer alors Présidente de Yahoo! a très bien dit la première : si je ne respecte pas la loi américaine, c'est de la trahison. Autrement dit, ces grandes multinationales savent très bien à quel pays elles appartiennent. On l'a vu durant la crise de 2008 : mondiales durant la croissance, ces grandes entreprises américaines sont redevenues américaines dans la difficulté – elles savaient très bien à quel guichet s'adresser pour être sauvées.

Le second problème, alors, est que l'Europe manque singulièrement de répondant face à ces entreprises qui, malgré leur statut global, restent liées aux intérêts stratégiques américains. Baidu, VKontakte… : en Russie, en Chine, et, évidemment, aux États-Unis, il est possible de vivre dans un écosystème numérique entièrement composé d'entreprises nationales. Ce n'est absolument pas le cas pour les pays européens. L'Europe se caractérise dans ce domaine par des renoncements, une absence de volonté, un manque de clairvoyance particulièrement fâcheux. Nous sommes dans une situation de dépendance extrêmement dommageable et problématique pour des pays qui prétendent être à la pointe de l'économie de la connaissance.

Ce manque de volonté au niveau européen est particulièrement frappant en ce qui concerne la cybersécurité. Chaque pays essaye de se débrouiller dans son coin. Une structure a été mise en place au niveau européen, l'ENISA (www.enisa.europa.eu), mais ce n'est pas vraiment convaincant : elle est basée en Crète et à Athènes, avec un budget limité de 11 millions d'euros en 2018 pour une agence censée couvrir les vingt-huit pays de l'Union. À titre de comparaison, le budget du CSA, en France, est de 40 millions. Sur le plan européen, nous sommes essentiellement dans des dispositifs nationaux juxtaposés. Qui compliquent les interactions et rendent dépendants de la bonne coopération de chacun.

Je souhaiterais conclure sur le point suivant : la question de la cybersécurité et de l'encadrement de celle-ci ne doit

pas être confiée aux seuls techniciens. Ne confiez jamais un débat reposant sur des questions technologiques aux seuls techniciens. Un technicien, comme un industriel, s'autolimite rarement et à tendance à déployer intensément ses outils sans nécessairement intégrer tous les aspects de société. Il faut donc que les politiques, les citoyens, la société civile prennent en charge une véritable réflexion stratégique et philosophique pour participer au débat sur l'édification et le suivi du cadre normatif dans lequel ces usages peuvent être envisagés. Un monde dont le pilotage serait laissé aux seuls techniciens s'annonce guère hospitalier.

Nicolas Hoang *(directeur général délégué d'Eurobail) : Si on regarde plusieurs événements dramatiques qui ont eu lieu récemment, on se rend compte que les terroristes prennent soin d'annoncer à l'avance sur les réseaux sociaux qu'ils vont mener une action. Les réseaux coopèrent avec les services de police, mais on a l'impression que l'on dépense beaucoup d'argent dans la technologie et que, dans le même temps, les États ou les grandes sociétés ne sont pas capables de se défendre contre des menaces simples.*

Nicolas Arpagian : La grande difficulté – et c'était l'un des sujets clés de l'audition de Mark Zuckerberg devant les élus étatsuniens au printemps 2018 – c'est que les grandes plateformes revendiquent le statut d'hébergeur. Il serait plus cohérent de les considérer comme des éditeurs. Les fils d'actualité, par exemple, font de Facebook un véritable média, avec une politique

éditoriale, d'origine humaine ou algorithmique. Mais les plateformes refusent ce point de vue. Elles font un lobbying intense pour ne pas être assimilées à des éditeurs, pour une raison simple : les éditeurs sont dès publication responsables de leurs contenus.

Il y a ainsi un problème quand – en aval, en général, plutôt qu'en amont – des personnes ou des organisations revendiquent ou valorisent un acte terroriste. La politique de YouTube et de Google est qu'une vidéo, celle de l'attaque sur les Champs-Élysées, par exemple, doit être laissée si elle est donnée brute, sans montage ni commentaire. Ce serait alors une simple information, qu'il est légitime de laisser en ligne. En revanche, on interdit ceux qui se félicitent de ce que montre la vidéo et qui appellent à la haine ou à la violence.

On voit toute la difficulté : il y a bien une politique éditoriale consistant à laisser ou ne pas laisser une vidéo, mais dans le même temps les plateformes ne se jugent pas responsables, parce qu'elles ne seraient que des hébergeurs. Elles ne savent pas ce qui se passe sur leurs sites, sauf si un nombre conséquent d'internautes signalent un contenu – ce qui implique au passage que vous sous-traitez aux visiteurs le travail de surveillance. Evidemment ces sociétés ont opté dès l'origine pour des modèles économiques reposant sur l'automatisation des processus. Elles ne s'enthousiasment donc pas à l'idée de rémunérer des êtres humains pour mener des opérations de sélection éditoriale.

Néanmoins, Mark Zuckerberg a reconnu devant la Commission US une forme de responsabilité, et la possibilité de voir en Facebook un média. Si ces déclarations sont suivies d'effets, cela risque de changer un certain nombre de choses. Quoique : les réseaux sociaux étant gratuits et instantanés, les gens prennent directement la main, sans le filtre d'une rédaction, et il leur est très facile de contourner les interdictions. Sur Twitter, vous pouvez mettre un lien vers un autre compte si d'aventure le premier était fermé, et sur ce deuxième compte un lien vers un troisième, etc. Vous avez aussi des codes qu'il peut être compliqué de contrôler uniquement au moyen d'une machine. Les suprémacistes blancs utilisent un émoticon représentant un verre de lait pour indiquer le soutien à leur cause. De même, une aubergine peut, dans la communauté homosexuelle, signifier un sexe en érection. Le filtrage automatique pose alors problème. Si vous avez décidé d'utiliser le mot ou le symbole « chocolat » pour désigner une bombe, il peut être compliqué de demander à la machine de le repérer et, si c'est le cas, de bloquer les messages ou les comptes qui parlent de chocolat. Il faut un signalement – autrement dit, du renseignement humain. Il est vital de ne pas tomber dans une utopie technologique où l'on se contenterait de capteurs et de sondes. C'est comme pour les caméras de surveillance : à un moment, il faut des personnes pour aller arrêter les voleurs sur le terrain. De même, il faut des personnels immiscés dans les systèmes et les communautés terroristes, afin d'en connaître les codes et les pratiques. La technologie ne remplace pas le renseignement humain.

Maryse Artiguelong *(Ligue des Droits de l'Homme & Observatoire des libertés et du numérique) : Une souveraineté numérique européenne est-elle impossible ? Peut-être pouvons-nous actionner un certain nombre de leviers, en nous appuyant sur le scandale de Cambridge Analytica ?*

Nicolas Arpagian : Je ne suis pas fédéraliste dans l'âme. Et en général, par exemple pour la lutte contre le terrorisme, c'est le bilatéral qui fonctionne, l'échange entre deux pays qui collectent leurs données et les partagent afin de disposer d'éléments complémentaires. Le multilatéral est rarissime car pour être admis autour de la table, il faut être un contributeur et apporter des informations. Dans le domaine économique, les GAFAM et autres sont passés maîtres dans l'art de jouer les États européens les uns contre les autres. Les intérêts nationaux divergent car les pays sont en compétition dans le domaine économique, social et fiscal. Les États de l'Union européenne rivalisent pour attirer les emplois et les impôts. Cette absence d'unité est préjudiciable à une prise de parole forte de l'UE qui avance en ordre dispersé. Et ne bénéficie pas de la consolidation de ses ressources techniques, financières et commerciales.

Alfred Henry Lewis disait au début du XX^{e} que neuf repas nous séparent du chaos : les individus peuvent tenir trois jours avec leurs réserves, ou sans manger, avant que la faim ne les pousse à agresser les autres. On peut reformuler la question : pourrions-nous tenir ne serait-ce que trois jours sans technologie ? Car la

déstabilisation par le numérique, ce n'est pas simplement un univers sans Internet. C'est le fait que vous supprimez l'accès aux distributeurs de billets, qu'il n'y a plus d'électricité, que vous devez arbitrer avec les quelques ressources en énergie qui vous restent entre les hôpitaux, les banques, les casernes. Pouvons-nous tenir dans un univers ainsi dégradé sans nous agresser les uns les autres ? Indépendamment des attaques locales, il faut donc aussi imaginer ce type de scénario, qui peut d'ailleurs aller de pair avec une attaque conventionnelle. Nous devons être capables de stabiliser la situation et de revenir à la normale. Le monde numérique et le monde physique sont complètement entrelacés, et nous devons donc réfléchir à la façon dont notre société pourrait fonctionner durablement dans un monde dégradé. Car le jour où nous y serons confrontés, cela risque d'être une épreuve du feu.

Roberto di Cosmo *(professeur en informatique, Paris 7 & INRIA [4]) : Le problème de la sécurité vient aussi du fait que nous ne savons pas fabriquer des logiciels sans erreurs. Nous savons produire des puces sans aucune erreur, alors qu'elles renferment des milliards de composants, mais nous n'arrivons pas à faire de logiciels sans erreurs. Je crois que nous ne mettons pas assez de ressources dans la formation des informaticiens. Nous n'investissons pas suffisamment dans la formation d'informaticiens de haut niveau. Et nous devrions orienter les meilleurs vers cette filière. Plus généralement, la*

4. Institut national de recherche en informatique et en automatique

culture informatique des citoyens ou des différents responsables est faible. J'ai par exemple fondé un projet, Software Heritage, dont le but est de constituer une archive de tous les codes sources de la planète. Il s'agit là d'un instrument de souveraineté numérique incroyable. Or quand j'ai fait le tour des entreprises et des décideurs français, on m'a suggéré de me tourner vers les Américains. Par conséquent, Microsoft collabore au projet, mais nous n'avons aucun sponsor français… C'est une occasion ratée, et j'aimerais bien savoir pour quelle raison l'informatique, les connaissances en programmation, ne sont pas appréciées au même niveau que les autres disciplines.

Nicolas Arpagian : Ce que vous dites me rappelle ce qui est arrivé au Professeur Louis Pouzin, qui dans les années 1970 a développé la commutation par paquets. En France, personne n'a été intéressé, mais deux Américains, Vinton Cerf et Robert Kahn ont tout de suite repris l'idée, et l'ont exploité à partir des États-Unis…

Il y a en effet un manque de culture technique en France. Je n'ai pas vraiment d'explication à proposer. Mais je constate que la technique et l'informatique ne font pas partie, en général, du *cursus honorum* de nos élites. Je le déplore.

La culture technique, ce n'est pas nécessairement rentrer dans l'intimité de la machine. C'est comprendre ce qui est envisageable, ce qui est matériellement

faisable. C'est surtout faire preuve de curiosité. Il faut arrêter avec les raisonnements du type : « j'étais nul en maths, tout ça ce n'est pas pour moi. » Je crois aussi qu'il faudrait changer notre approche de la formation continue : celle-ci est dans les esprits plutôt réservée aux gens en situation d'échec professionnel ou en reconversion. Alors qu'elle devrait être naturelle pour régulièrement actualiser nos compétences dans un monde où les techniques évoluent constamment. Cela concerne tous les domaines de l'informatique aux sciences de la vie en passant la construction. Il est vain de croire qu'un diplôme passé il y a vingt ans, même au sein d'un établissement prestigieux, assure deux décennies plus tard une connaissance fine de l'environnement technologique et de ses perspectives. Cette mise à jour régulière est une condition nécessaire de ce que les militaires désignent sous le sigle MCO : le Maintien en Conditions Opérationnelles. Un tel maintien, face à une concurrence qui s'internationalise, s'intensifie et s'accélère, est une exigence minimum. Et le socle attendu pour acquérir les connaissances qui permettent d'aborder les enjeux à venir dans les meilleures conditions.

Retrouvez l'intégralité du débat en vidéo sur
www.institutdiderot.fr

Les publications de l'Institut Diderot

Dans la même collection

- L'avenir de l'automobile - Louis Schweitzer
- Les nanotechnologies & l'avenir de l'homme - Etienne Klein
- L'avenir de la croissance - Bernard Stiegler
- L'avenir de la régénération cérébrale - Alain Prochiantz
- L'avenir de l'Europe - Franck Debié
- L'avenir de la cybersécurité - Nicolas Arpagian
- L'avenir de la population française - François Héran
- L'avenir de la cancérologie - François Goldwasser
- L'avenir de la prédiction - Henri Atlan
- L'avenir de l'aménagement des territoires - Jérôme Monod
- L'avenir de la démocratie - Dominique Schnapper
- L'avenir du capitalisme - Bernard Maris
- L'avenir de la dépendance - Florence Lustman
- L'avenir de l'alimentation - Marion Guillou
- L'avenir des humanités - Jean-François Pradeau
- L'avenir des villes - Thierry Paquot
- L'avenir du droit international - Monique Chemillier-Gendreau
- L'avenir de la famille - Boris Cyrulnik
- L'avenir du populisme - Dominique Reynié
- L'avenir de la puissance chinoise - Jean-Luc Domenach
- L'avenir de l'économie sociale - Jean-Claude Seys
- L'avenir de la vie privée dans la société numérique - Alex Türk
- L'avenir de l'hôpital public - Bernard Granger
- L'avenir de la guerre - Henri Bentegeat & Rony Brauman
- L'avenir de la politique industrielle française - Louis Gallois
- L'avenir de la politique énergétique française - Pierre Papon
- L'avenir du pétrole - Claude Mandil
- L'avenir de l'euro et de la BCE - Henri Guaino & Denis Kessler
- L'avenir de la propriété intellectuelle - Denis Olivennes
- L'avenir du travail - Dominique Méda
- L'avenir de l'anti-science - Alexandre Moatti
- L'avenir du logement - Olivier Mitterand
- L'avenir de la mondialisation - Jean-Pierre Chevènement
- L'avenir de la lutte contre la pauvreté - François Chérèque

- L'avenir du climat - Jean Jouzel
- L'avenir de la nouvelle Russie - Alexandre Adler
- L'avenir de la politique - Alain Juppé
- L'avenir des Big-Data - Kenneth Cukier & Dominique Leglu
- L'avenir de l'organisation des Entreprises - Guillaume Poitrinal
- L'avenir de l'enseignement du fait religieux dans l'École laïque - Régis Debray
- L'avenir des inégalités - Hervé Le Bras
- L'avenir de la diplomatie - Pierre Grosser
- L'avenir des relations Franco-Russes - S.E Alexandre Orlov
- L'avenir du Parlement - François Cornut-Gentille
- L'avenir du terrorisme - Alain Bauer
- L'avenir du politiquement correct - André Comte-Sponville & Dominique Lecourt
- L'avenir de la zone euro - Michel Aglietta & Jacques Sapir
- L'avenir du conflit entre chiite et sunnites - Anne-Clémentine Larroque
- L'Iran et son avenir - S.E Ali Ahani
- L'avenir de l'enseignement - François-Xavier Bellamy
- L'avenir du travail à l'âge du numérique - Bruno Mettling
- L'avenir de la géopolitique - Hubert Védrine
- L'avenir des armées françaises - Vincent Desportes
- L'avenir de la paix - Dominique de Villepin
- L'avenir des relations franco-chinoises - S.E. Zhai Jun
- Le défi de l'islam de France - Jean-Pierre Chevènement
- L'avenir de l'humanitaire - Olivier Berthe - Rony Brauman - Xavier Emmanuelli
- L'avenir de la crise du Golfe entre le Quatar et ses voisins - Georges Malbrunot
- L'avenir du Grand Paris - Philippe Yvin
- Entre autonomie et Interdit : comment lutter contre l'obésité ? - Nicolas Bouzou & Alain Coulomb
- L'avenir de la Corée du Nord - Juliette Morillot & Antoine Bondaz
- L'avenir de la justice sociale - Laurent Berger

Les Notes de l'Institut Diderot

- L'euthanasie, à travers le cas de Vincent Humbert - Emmanuel Halais
- Le futur de la procréation - Pascal Nouvel
- La République à l'épreuve du communautarisme - Eric Keslassy
- Proposition pour la Chine - Pierre-Louis Ménard
- L'habitat en utopie - Thierry Paquot
- Une Assemblée nationale plus représentative - Eric Keslassy
- Où va l'Égypte ? - Ismaïl Serageldin
- Sur le service civique - Jean-Pierre Gualezzi
- La recherche en France et en Allemagne - Michèle Vallenthini
- Le fanatisme - Texte d'Alexandre Deleyre présenté par Dominique Lecourt

- De l'antisémitisme en France - Eric Keslassy
- Je suis Charlie. Un an après... - Patrick Autréaux
- Attachement, trauma et résilience - Boris Cyrulnik
- La droite est-elle prête pour 2017 ? - Alexis Feertchak
- Réinventer le travail sans l'emploi - Ariel Kyrou
- Crise de l'École française - Jean-Hugues Barthélémy
- À propos du revenu universel - Alexis Feertchak & Gaspard Koenig
- Une Assemblée nationale plus représentative - *Mandature 2017-2022* - Eric Keslassy
- L'avenir de notre modèle social français - Jacky Bontems & Aude de Castet
- Handicap et République - Pierre Gallix
- Réflexions sur la recherche française... - Raymond Piccoli

Les Dîners de l'Institut Diderot

- La Prospective, de demain à aujourd'hui - Nathalie Kosciusko-Morizet
- Politique de santé : répondre aux défis de demain - Claude Evin
- La réforme de la santé aux États-Unis : quels enseignements pour l'assurance maladie française ? - Victor Rodwin
- La question du médicament - Philippe Even
- La décision en droit de santé - Didier Truchet
- Le corps ce grand oublié de la parité - Claudine Junien
- Des guerres à venir ? - Philippe Fabry
- Les traitements de la maladie de Parkinson - Alim-Louis Benabib

Les Entretiens de l'Institut Diderot

- L'avenir du progrès (actes des Entretiens 2011)
- Les 18-24 ans et l'avenir de la politique

Quelles menaces numériques dans un monde hyperconnecté ?

Notre sécurité se trouve aujourd'hui gravement mise en péril par le numérique, sans même souvent que nous en prenions conscience.

La mondialisation pousse à l'interconnexion. La menace numérique connait une forme de démocratisation. Nicolas Arpagian souligne en particulier le danger que porte l'apparition d'outils « simples à utiliser, faciles d'accès » qui permettent à leurs acquéreurs pour un coût modique d'espionner et de lancer des attaques.

L'auteur explore méthodiquement les réponses les plus récentes à ces menaces d'un type nouveau.

Dominique Lecourt
Directeur général de l'Institut Diderot

Nicolas Arpagian : Directeur de la stratégie d'Orange Cyberdéfense, Nicolas Arpagian a fondé le cycle « Sécurité numérique » à l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Il enseigne aussi à l'École nationale supérieure de la police (ENSP) et est l'auteur, notamment, de « La Cybersécurité » aux Presses Universitaires de France. Il est membre du Conseil d'orientation de l'Institut Diderot.

INSTITUT DIDEROT

ISBN 979-10-93704-49-4
9791093704494
ISSN 2496-4948 (en ligne)
ISSN-L 2272-835X (imprimé)

FONDS DE DOTATION POUR LE DEVELOPPEMENT DE L'ECONOMIE SOCIALE REGI PAR LA LOI N°2008-776 DU 4 AOUT 2008 - SIRET N° 513 746 651 00019
86-90, rue Saint-Lazare 75009 Paris / T. +33 (0)1 55 50 65 60 / contact@institutdiderot.fr / www.institutdiderot.fr

Réalisation www.idcomm.fr - Imprimé sur papier issu de forêts gérées durablement.