INSTITUT DIDEROT

LES DÎNERS DE L'INSTITUT DIDEROT

# Cyber :
## quelle(s) stratégie(s) face à l'explosion des menaces ?

Jean-Louis GERGORIN & Léo ISAAC-DOGNIN

INSTITUT DIDEROT // www.institutdiderot.fr / @InstitutDiderot

LES DÎNERS DE L'INSTITUT DIDEROT

# Cyber :
## quelle(s) stratégie(s) face à l'explosion des menaces ?

**Jean-Louis GERGORIN & Léo ISAAC-DOGNIN**

Retranscription des débats lors du dîner du 3 mars 2020

# Sommaire

# Avant-propos

Pour atteindre ses objectifs, la guerre a toujours tiré parti de toutes les ressources technologiques existant dans la société. Elle a même été le moteur de nombreux progrès pour son usage propre dont les retombées civiles n'ont été que d'heureux effets collatéraux. Il était donc prévisible que les technologies numériques, comme celles qui les ont précédées, trouveraient leur emploi au service des conflits entre États.

En premier lieu, ce fut en complément de l'action des forces traditionnelles, dans un but d'information pour espionner l'adversaire, ou pour neutraliser des ressources ennemies dont le fonctionnement repose désormais largement sur des systèmes et des réseaux eux-mêmes numériques. Dans ce sens, c'est une avancée technologique comme une autre.

Mais le cyber signe aussi et surtout l'avènement d'une forme nouvelle de conflictualité.

Selon Carl von Clausewitz, la guerre est la poursuite de la politique par d'autres moyens, notamment la diplomatie. Il était bien conscient qu'il existe un espace

entre la guerre déclarée et la paix officielle et que celle-ci ne signifie pas l'absence d'intentions, voir d'actes hostiles. Désormais cet espace trouve, à travers le cyber, un puissant moyen d'expression. Il élargit le champ du possible au point de définir un nouvel état des relations internationales, distinct à la fois de la guerre et de la paix, probablement le plus durable et le plus fréquent.

Le cyber permet aux pays de défendre leurs intérêts, par des moyens indirects et peu chers, en créant ou amplifiant des forces ou des événements de nature à affaiblir la cible et d'améliorer leur rapport de force avec elle. L'opération cyber, au contraire d'un acte d'agression matériel, risque peu d'engager dans une escalade conduisant à la guerre en raison de l'incertitude qui peut planer sur l'identité de l'agresseur ; des soupçons peuvent au demeurant être suscités à l'égard d'autres responsables potentiels, y compris des groupes d'individus nationaux.

Ces techniques, compte tenu de leurs caractéristiques de discrétion, leur faible coût, leur progressivité et le caractère fréquemment réversible de leurs effets, peuvent même être utilisés contre des pays amis, c'est-à-dire par tout le monde et contre tout le monde.

Le cyber crée ou amplifie donc un espace flou entre guerre et paix, actions régaliennes et initiatives privées, militaires et civiles, États souverains s'affranchissant des règles internationales et grandes sociétés de haute technologie prétendant imposer leurs propres normes aux États.

Cette évolution, s'ajoutant à d'autres de même sens

internes aux pays, menace de leurs effets entropiques, les États dans leur forme actuelle et tout spécialement les démocraties.

Jean-Louis Gergorin et Léo Isaac-Dognin éclairent pour nous ce nouveau monde pour nous permettre de le mieux comprendre, d'infléchir son évolution ou, à défaut, de nous y adapter.

Jean-Claude Seys
Président de l'Institut Diderot

# Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ?

## INTRODUCTION

**Jean-Louis Gergorin**

Le cyber n'est pas une guerre au sens classique, avec déclaration, drapeaux, tambours et décorations. C'est un combat de l'ombre, toujours en dessous du seuil de la guerre ouverte. Le cyber n'est pas la cyberguerre. Les Anglo-saxons parlent de *cyberwarfare*, d'un mode de combat, plutôt que de *cyberwar*. Les universitaires utilisent, pour leur part, le terme de cyberconflictualité. Mais le terme est un peu pédant. Avec Léo Isaac-Dognin, nous avons donc retenu dans notre ouvrage [1] le terme « cyber », comme beaucoup d'experts. Au masculin : le cyber. Pas « la cyber », qui ferait penser à la cybersécurité, ensemble à la fois plus large et plus étroit car la protection contre le *hacking*, l'intrusion informatique, va plus loin que la lutte contre les actions numériques des états, sans pour autant couvrir l'autre volet du cyber qu'est la manipulation de l'information numérique.

1. Jean-Louis Gergorin et Léo Isaac-Dognin, « Cyber. La guerre permanente », Paris, Les Éditions du Cerf, coll. « Idées », 2018.

Quelle est alors cette menace qui, de façon évidente, ne cesse d'augmenter ? Le cyber, c'est l'utilisation des moyens numériques à des fins d'influence et de contrôle, sur le plan géopolitique, économique, et même sociétal.

Ces moyens numériques peuvent être divisés en deux grandes familles, qui se recoupent de plus en plus. D'une part, l'intrusion informatique : ce qu'on appelle le *hacking*, le fait de pénétrer un ordinateur, un système d'information, pour le saboter ou l'espionner. D'autre part, la manipulation de l'information numérique, essentiellement via les plateformes de médias et les réseaux sociaux.

Ces deux modes d'influence et d'action s'interpénètrent de plus en plus, comme le montrent deux exemples. Le premier est l'élection présidentielle américaine de 2016 : selon le gouvernement et la justice américaine, des *hackers* russes appartenant à un service officiel russe, un service de renseignement militaire, auraient hacké le système d'information du Comité national démocrate et l'ordinateur du directeur de campagne de Hillary Clinton. Les informations, authentiques, qui y ont été glanées ont ensuite été communiquées à Wikileaks, qui les a sorties à des moments critiques. Des comptes fictifs sur les réseaux visant à déstabiliser Hillary Clinton diffusaient au même moment ces informations. Tous les sondages et toutes les analyses faites par des politologues s'accordent pour dire que cela a eu un effet négatif sur la campagne de la candidate démocrate. Ces informations, je le répète, étaient authentiques, notamment ses discours chez

Goldman Sachs, qui n'étaient pas totalement convergents avec ses discours à l'attention de l'électorat ouvrier, ce qui n'a pas été très apprécié dudit électorat. Le second exemple est tiré du conflit entre, d'un côté, l'Arabie Saoudite, les Émirats arabes unis et leurs partenaires du Conseil de coopération du Golfe, et, de l'autre, le Qatar. Ce conflit a commencé par une intrusion informatique : la publication, sur le site de la Qatar News Agency, de faux propos de l'émir du Qatar faisant l'éloge de l'Iran, du Hezbollah, du Hamas, des Frères musulmans… et d'Israël ! Cela a lancé une campagne d'opinion contre le Qatar aux Émirats et en Arabie Saoudite, qui n'avait pas encore officialisé son rapprochement avec Israël. Le conflit commence donc par une intrusion informatique. Celle-ci a permis une manipulation de l'information numérique et la diffusion de fausses nouvelles, ce qui a lancé un conflit et des opérations cyber ultérieures comme le *hacking* de courriels de l'ambassadeur des Émirats arabes unis à Washington. On voit bien ici que les deux dimensions de piratage et de manipulation de l'information sont utilisés de concert pour atteindre un même objectif.

Les progrès de la technologie, notamment de l'intelligence artificielle, permettent aussi des manipulations de l'information numérique qui ressemblent au *hacking*, mais qui n'en sont pas : ce sont des transformations de l'information existante par des techniques permettant de produire des faux. La plus célèbre de ces techniques est celle des *deep fakes*, des vidéos complètement artificielles d'une personne et quasiment indétectables, faites à

partir d'une base de données suffisamment importante. À supposer, par exemple, qu'une banque d'images de moi-même ou de mon coauteur soit disponible en ligne ; il serait possible de faire une vidéo de cette séance dans laquelle nous tiendrions des propos totalement différents D'autres formes de manipulation existent : on peut par exemple *hacker* un système comportant des algorithmes d'intelligence artificielle, de façon à fausser ces algorithmes et donner d'autres résultats.

Ces menaces cyber explosent. Lors des deux dernières années, en France et en Europe occidentale, le nombre des *ransomwares*, ou rançongiciels, c'est-à-dire les intrusions informatiques visant à obtenir des rançons en bloquant les données d'un système, a été multiplié par quatre. C'est spectaculaire et les sommes en jeu sont importantes. Aux États-Unis, les *ransomwares* auraient rapporté 150 millions de dollars en six ans [2]. Des chiffres plus importants circulent, et, de surcroît, beaucoup de victimes de ces rançons ne le disent pas. Le chiffre doit donc être de beaucoup supérieur. C'est une activité très rentable. La manipulation de l'information aussi explose. Beaucoup de pays créent des faux comptes. Ce genre d'opérations n'est plus l'apanage des très grandes puissances. Beaucoup de puissances moyennes s'y mettent, et d'acteurs privés. En témoigne le fait que Graphika, une start-up spécialisée dans la détection des manipulations numériques de l'information, dont

2. https://searchsecurity.techtarget.com/news/252479119/FBI-144-million-in-ransomware-payments-made-over-6-years

Camille François, une de mes anciennes étudiantes, est *chief innovation officier*, après avoir commencé par travailler pour le Congrès américain, a maintenant une clientèle privée : les entreprises doivent se prémunir contre les campagnes de désinformation que pourraient lancer leurs concurrents sur Facebook ou Twitter. Si vous êtes dans les cosmétiques, il peut être tentant pour votre concurrent de multiplier les faux comptes individuels sur les réseaux sociaux disant que vos produits sont mauvais, irritants, dangereux pour la santé, etc.

Comme dit Kissinger, en paraphrasant les philosophes des Lumières, l'espace numérique est aujourd'hui l'illustration la plus parfaite de l' « état de nature » ayant nécessité la création institutions politiques. Autrement dit, pour le moment, c'est la jungle. Nous le sentons tous, et le but de notre discussion serait d'y voir un peu plus clair sur les façons d'y remédier.

## I – LES TROIS NIVEAUX DU CYBERESPACE
**Léo Isaac-Dognin**

Avant de vous présenter plus spécifiquement ce qu'est le cyberespace, j'aimerais partager avec vous un chiffre qui illustre bien l'explosion des attaques informationnelles (qui, avec les attaques informatiques, constituent les deux grands ensembles de la menace cyber). En 2017, à la suite des élections présidentielles américaines, Facebook a supprimé des centaines de milliers de comptes ; cela

semble beaucoup, mais en 2019, ce sont six milliards de comptes qui ont été supprimés, c'est-à-dire près de 17 millions de comptes par jour et trois fois le nombre de vrais comptes existant sur le site. En seulement deux ans, nous avons donc complètement changé de dimension et les acteurs du numérique ont dû s'adapter.

Pour revenir au cyber, je souhaite, dans cette première partie de notre présentation, reposer les bases de ce qu'est l'espace cyber. L'espace cyber est souvent apparenté à un cinquième théâtre de guerre, à côté des théâtres « traditionnels » que constituent la terre, la mer, l'aérien et l'espace.

Comment le théâtre cyber est-il structuré ? On peut distinguer trois couches, qui créent autant de niveaux de vulnérabilité.

La première est la partie matérielle du cyber : les câbles sous-marins océaniques par lesquels circulent les données, les serveurs, les disques durs, les composants dont sont faits les ordinateurs et les smartphones.

Deuxième niveau, la couche logique ou applicative. Ce sont les logiciels, soit tout ce qui permet de se servir des différents composants matériels pour effectuer des calculs, faire transiter des données et restituer l'information.

La troisième couche est ce qu'on appelle la couche sémantique ou cognitive. Il s'agit du « contenu », tandis que les deux premières couches représentent les « contenants ».

Ce niveau est celui des informations que l'on retrouve sur les sites web et les réseaux sociaux, mais aussi les serveurs confidentiels. L'attaque Stuxnet découverte en 2010, ayant permis de détruire des centrifugeuses iraniennes, avait une importante dimension cognitive : les informations restituées aux chercheurs sur leurs écrans de contrôle dans les centrales paraissaient normales, les *hackers* avaient réussi à afficher sur ces écrans de fausses données pré-enregistrées pour que personne ne s'aperçoive que les centrifugeuses étaient en train de dysfonctionner et de tourner à des vitesses bien supérieures à celles auxquelles elles pouvaient résister.

Ce bref rappel de la distinction entre les trois couches du cyberespace est important, car la manière dont cet espace est perçu structure fortement la manière dont les acteurs, étatiques ou non, agissent et réagissent dans le cyberespace. Prenons deux exemples :

1) On a longtemps considéré, dans le monde occidental, que ce qui importait était les deux premières couches, à savoir l'infrastructure matérielle et les logiciels. Car il n'y a pas à regarder le contenu : dans une démocratie, ce qui est dit n'a pas à être régulé. On s'intéresse donc surtout à l'infrastructure et aux logiciels. Et, en général, les agences de cybersécurité occidentales, en France par exemple, se sont structurées ainsi, en se concentrant sur les deux premières couches. En revanche, les Russes ont compris dès la fin des années 1990 que le cyberespace, qu'ils appellent, eux, la sphère informationnelle, comprend en réalité ces trois couches et ont donc développé des

stratégies défensives et offensives intégrant ces trois éléments. La campagne orchestrée pendant les élections présidentielles américaines de 2016 a joué sur les trois niveaux : piratage de comptes mails, diffusion massive d'information sur les réseaux sociaux et, bien qu'on en parle moins, prépositionnement sur des infrastructures critiques, à savoir non seulement les machines de vote, mais surtout le réseau énergétique. Ce qui, comme il a été plus tard, a paralysé la réaction de l'administration américaine, qui craignaient des conséquences sur les machines à vote et les infrastructures énergétiques du pays.

2) Sur le plan économique, les dirigeants politiques et industriels ont, pendant des années, concentré leur attention sur les deux dernières couches – les logiciels et les contenus numériques – considérant les infrastructures comme un bien à faible valeur ajoutée dont il convenait de délocaliser la production. Ils se rendent aujourd'hui compte de la valeur stratégique de cette couche matérielle, et l'on observe de réels changements de doctrine concernant l'importance de la sécurité en matière d'infrastructure, en tout cas des composants critiques.

Les trois niveaux du cyberespace doivent dorénavant être pris en compte. La cyberguerre, notre sujet, est l'utilisation offensive de toutes ces couches à des fins soit de contrôle, soit d'influence.

## II - UNE RÉVOLUTION DE L'ARMEMENT

**Jean-Louis Gergorin**

L'arme numérique est une révolution majeure, au même titre que les grandes révolutions antérieures qui ont complètement transformé les capacités d'action : la poudre, la vapeur, l'aviation, les missiles, le nucléaire. Ces révolutions jouent toujours sur une ou plusieurs des caractéristiques suivantes : la portée, la vitesse, la puissance, la précision, la furtivité et l'accessibilité. Sur tous ces éléments, le numérique apporte une transformation fondamentale.

**Léo Isaac-Dognin**

En effet, la portée de l'arme numérique est évidemment mondiale, voire plus : j'aime toujours donner pour exemple le fait que la Station spatiale internationale a connu une intrusion numérique en 2008, un des astronautes ayant utilisé une clef USB contenant un virus. En réalité, le plus intéressant est que le numérique oblige à repenser la notion de portée : elle n'est plus limitée par la distance ou des facteurs géographiques, mais par la manière dont les infrastructures sont configurées, par la facilité d'accéder à un réseau ou à un autre.

La vitesse, elle, est instantanée. Les attaques sont souvent bien avancées, voire achevées, avant que la victime s'en aperçoive. Ceci dit, il faut tempérer : les opérations avancées ne sont pas l'affaire de quelques jours. Elles peuvent demander plusieurs mois de préparation, chose importante en matière de stratégie de défense.

Le cyber ne vient pas démultiplier la puissance comme a pu le faire l'invention du missile balistique nucléaire. Certes, le numérique peut créer des dégâts, on peut mettre à plat une centrale nucléaire, mais, d'un point de vue stratégique, l'intérêt des actions cyber est leur dimension réversible : une coupure de courant provoquée par une attaque, comme il s'est produit dans l'ouest de l'Ukraine en 2015, a un effet immédiat semblable à celui de la destruction d'une centrale, mais l'attaquant, et la victime, peuvent rétablir la situation et revenir à la normale, si l'on met de côté les effets collatéraux qu'une coupure de plusieurs heures a pu avoir sur différents services comme les hôpitaux. D'un point de vue géopolitique, c'est très important. Selon les normes actuelles, cela ne justifie pas le même type de réaction de la part de la victime, ou de ses alliés, qu'une attaque cinétique. Cette réversibilité est source de grandes difficultés pour les doctrines actuelles de dissuasion, parce qu'elle permet des attaques en dessous du seuil de la guerre ouverte.

La précision des attaques numériques renforce ce problème. La meilleure comparaison pour penser les attaques numériques est celle du marketing. Celui-ci a énormément bénéficié du numérique, qui en ouvrant la possibilité du microciblage, permet aux promoteurs d'atteindre une personne très précise. La précision des armes numériques est très similaire. Elle permet, là aussi, de rester en dessous du seuil de guerre ouverte en orientant les attaques sur des cibles précises, en évitant dans la plupart des cas un effet de masse.

Il est, en outre, très difficile de déterminer qui est derrière une attaque. Les acteurs jouent énormément sur cette furtivité, qui permet de mener des attaques sous faux drapeau. On se rappelle ainsi qu'en 2015, il s'est affiché sur TV5 une revendication du «cybercalifat». Il a fallu attendre quelques mois pour que les responsables français, faisant exception à la doctrine française de ne jamais attribuer publiquement d'attaques numériques, révèlent qu'il s'agissait en fait d'un groupe de *hackers* russes dans le contexte des attaques de Charlie Hebdo, cherchaient à surfer sur la crainte de l'État islamique en France. Il s'avère que les autorités américaines feront face au même groupe de *hackers* russes, surnommé *Fancy Bear*, un an plus tard lors de la campagne présidentielle de 2016.

Concernant l'accessibilité, enfin, il suffit de comparer les coûts : un seul F-35 dépasse les 100 millions de dollars, tandis qu'une attaque sophistiquée demande au maximum quelques millions de dollars. Il s'agit là d'une attaque de très haut niveau planifiée pendant des mois. On voit tout de suite que l'arme numérique est beaucoup plus accessible que ce soit pour les États ou les acteurs non-étatiques.

Comme le disait un ancien directeur technique de l'état-major américain, le cyber, c'est comme un match de football où tous les spectateurs seraient sur le terrain et où personne ne porte de maillot : tout le monde peut participer, de façon anonyme, et on ne sait jamais tout à fait qui est en train d'attaquer. D'autant plus que,

notamment grâce à l'intelligence artificielle, n'importe qui peut se faire passer pour un autre, en imitant les comportements informatiques d'autres adversaires.

On comprend, à partir de ce qui vient d'être dit, que le rapport coût/efficacité de l'arme numérique est considérable. Cela encourage les acteurs à l'utiliser ou, en tout cas, à s'en doter plutôt que de se lancer dans des programmes d'armement extrêmement coûteux par rapport aux avantages qu'ils peuvent conférer. D'autant plus que dans le domaine du numérique, il y a une prime à l'offensive : cela coûte très peu d'attaquer par rapport au gain possible, et la faille informatique qui permet de le faire peut disparaître d'un moment à l'autre, poussant à l'utiliser le plus rapidement possible.

On voit de la même façon que l'arme numérique a un caractère asymétrique lui aussi assez impressionnant. Elle permet de cibler les vulnérabilités d'un adversaire, dont il n'a potentiellement pas connaissance, et ainsi de rééquilibrer un désavantage stratégique sur le plan des rapports de force conventionnels. Il y a ainsi un pouvoir égalisateur du numérique, qui n'est pas sans rappeler celui de l'atome. Un acteur comme la Corée du Nord, indépendamment de la bombe, pèse sur le plan international bien au-delà de son poids objectif, grâce aux capacités cyber qu'elle a développées.

Le numérique crée ainsi un environnement «VUCA» : volatil, incertain (*uncertain*), complexe et ambigu. Les consultants aiment bien cet acronyme, ça permet de

dire au client que l'environnement concurrentiel est compliqué et qu'il faut forcément nous faire confiance… Mais le fait est qu'avec le numérique, c'est vrai, les choses bougent très rapidement, une start-up peut en quelques années prendre une part importante du marché, des acteurs géopolitiques sont capables, très rapidement, de peser sur la scène internationale et de rattraper des décennies de retard technologique et économique.

## III - LA GÉOSTRATÉGIE DU CYBER

**Jean-Louis Gergorin**

L'importance stratégique de la révolution numérique a été perçue de façon à la fois inégale et différente par les différentes nations. Dans les années 1990, seuls trois pays l'ont saisie : Israël, la Russie et la Chine. Ces trois nations ont très vite compris que le numérique ne serait pas simplement un nouveau moyen d'espionnage, cela tout le monde l'avait vu, mais qu'il serait aussi un outil d'influence, une arme stratégique.

Il y a un point commun à ces trois pays : leur sentiment d'avoir besoin d'une stratégie asymétrique. Une stratégie asymétrique consiste à se concentrer sur des domaines où quand on frappe, on est nettement supérieur à l'adversaire, quand bien même celui-ci serait globalement plus fort.

Ainsi Israël, même si ce pays a la première force conventionnelle de la région, et une force nucléaire, a toujours le

sentiment d'être une petite nation isolée dans un ensemble hostile et bien plus important démographiquement. Le numérique est donc apparu comme un moyen supplémentaire d'agir, au niveau mondial de surcroît.

Dans le cas des Chinois et des Russes, l'aiguillon a été le rapport aux États-Unis. Les années 1990 sont les années de l'hyperpuissance américaine. Les Russes et les Chinois ont alors vu dans le numérique la possibilité de compenser leur infériorité au moyen d'une stratégie asymétrique. Il y a des textes chinois de l'époque qui décrivent le numérique comme une arme dont il est question dans la semi-mythologie chinoise racontant l'ère des Royaumes combattants, au V^e^ siècle avant Jésus-Christ, et qui pour nous serait l'équivalent de la fronde de David contre Goliath. Jiang Zemin, le successeur de Deng Xiaoping et le dirigeant de la Chine dans les années 1990 jusqu'en 2002, a tenu au tournant du siècle un discours, qui n'a pas été rendu public, disant que le numérique devait être une priorité, notamment parce que l'Amérique étant totalement numérisée, il s'agit là d'une vulnérabilité qu'il faut être prêt à exploiter. On voit que dès les années 1990, les Chinois ont développé une vision stratégique approfondie concernant le numérique, et l'ont poursuivie.

Du côté de la Russie, l'armée soviétique, puis russe, a traditionnellement toujours eu une excellente réflexion stratégique. Après la chute des années 1990, celle-ci a connu un renouveau avec l'arrivée de Vladimir Poutine qui marque le début d'une résurrection nationale, une réhabilitation de l'État et une volonté de rétablir le rang

de la Russie. Le numérique est apparu comme un outil au service de cette ambition.

Israël, Chine, Russie : dans chacun de ces trois pays, le numérique est apparu pour des raisons différentes comme une nécessité vitale.

Les États-Unis, en revanche, qui étaient évidemment dominants technologiquement, n'y ont vu qu'un moyen de conserver leur hégémonie sans faire la guerre. Comment ? Par l'ubiquité du renseignement. Savoir tout sur tout. C'est ce qui a abouti à faire de la NSA une paire de grandes oreilles couvrant tout ce qui se passe dans le monde, rassemblant des quantités astronomiques d'informations, de façon à protéger et promouvoir les intérêts américains. C'est tout à fait irréaliste : la NSA accumule des informations impossibles à traiter en temps réel, et même en temps différé, et qui n'ont d'intérêt que si l'on a déjà une idée de ce qu'on cherche. Les Américains ont emprunté cette voie après le 11 septembre, avec cette tendance qui est la leur, face à un problème, de chercher une solution technologique plutôt que politique. Ils ont donc pensé que le cyber, sous la forme du renseignement, allait être la solution. Le budget de la NSA a connu une croissance très forte, le *Patriot Act* lui a donné des capacités d'interception inédites sur le plan légal, et les Américains ont un peu vécu dans l'illusion que cela suffirait. Ils ont cependant dû constater vers la fin des années 2000 que les Russes et les Chinois les rattrapaient très vite, et ils se sont trouvés confrontés au défi du programme nucléaire

iranien. La question iranienne a fait l'objet d'un débat intense au sein de l'administration américaine, entre les néoconservateurs, qui défendaient une solution militaire, et ceux, notamment le Secrétaire de la Défense de George W. Bush, Robert Gates, qui ont dissuadé les autorités politiques de recommencer l'expérience irakienne. Il a donc fallu trouver autre chose, et cela a été le projet Stuxnet. Celui-ci a vu le jour à la fin de la présidence de G.W. Bush, mais a été lancé sous Barack Obama. Il s'agit probablement d'une des choses que le premier a annoncées au second lors de la passation des pouvoirs en janvier 2009. Stuxnet est un tournant historique : c'est l'équivalent de Hiroshima dans le domaine nucléaire. Il s'agit de la première utilisation du cyber à des fins de destruction physique. Obama a été extrêmement séduit par cette idée. C'était un moyen de faire la guerre sans la faire. Stuxnet a mis hors d'état de nuire 2 000 centrifugeuses iraniennes. Cela n'a pas arrêté le programme iranien, mais a ouvert une brèche : tous les autres États ont commencé à s'intéresser aux potentialités destructrices du cyber.

L'un des résultats de ce développement du cyber sera, je crois, la mise en place de stratégies de « cyber coercition » : réagir à des actions jugées hostiles d'un adversaire en lui montrant qu'on peut lui faire beaucoup de mal. C'est ce qu'a fait la Russie avec l'Estonie. À la suite du déplacement du Monument aux morts de la Seconde Guerre mondiale, des « patriotes russes », selon la version officielle russe, ont paralysé les principaux systèmes informatiques des services publics estoniens.

On voit que les Russes ont bien saisi toutes les conséquences stratégiques de l'apparition du cyber. J'en veux pour preuve l'article publié par le général Valeri Guérassimov, chef d'état-major des armées russes dans une revue discrète, VPK (acronyme de « Courrier du complexe militaro-industriel »), le 27 février 2013 [3]. Guérassimov écrit, entre autres, que « *désormais, la partie la plus importante des conflits se déroulera avant le déclenchement formel des hostilités.* » C'est exactement ce que nous voyons. Il étudie aussi les formes hybrides à venir, mélanges de guerre ouverte, de déstabilisations, de trêves et de sanctions économiques. Cet article permet ainsi de comprendre la pensée stratégique russe comme une réponse à ce que les stratèges et les responsables politiques russes considèrent comme ayant été une agression, à savoir les révolutions de couleur. Face à cette agression, Guérassimov dit que la réponse sera d'utiliser des moyens comme le numérique et de gagner la guerre de l'information. Tout ce qui se passe actuellement en matière géopolitique se trouve déjà décrit en 2013 dans cet article. Le conflit syrien, par exemple : on ne sait plus si c'est la guerre ou la paix, la Turquie et la Russie se font la guerre par intermédiaires interposés, les Turcs interviennent directement contre les Syriens qui sont les alliés des Russes, et en même temps Erdogan et Poutine se parlent tout le temps… Nous ne sommes pas du tout dans le schéma où un ambassadeur en frac vient remettre une déclaration de guerre.

3. On trouve une traduction anglaise de cet article sur : https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.

La Russie a donc développé ses forces en matière de cyber, essentiellement confiées, au sein de l'état-major général, au GRU, la Direction générale du renseignement. Les inculpations par la justice américaine contre ceux qu'elle accuse d'avoir monté les opérations de déstabilisation lors des élections présidentielles visent notamment des lieutenants-colonels dont on peut voir qu'ils ont fait des doctorats de cryptologie ou de mathématique appliquée. Autrement dit, un personnel extrêmement bien formé et sophistiqué. On retrouve dans cet intérêt russe pour le cyber ce que les Soviétiques dans les années 1970 appelaient le « contrôle réflexif » : la capacité de changer les perceptions de l'adversaire, soit de manière positive, en lui faisant penser que la réalité du paysage stratégique est différente de celle qu'il croit, soit de manière destructrice, en faisant en sorte qu'il ne sache plus distinguer le vrai du faux.

La Chine, pour sa part, a orienté sa stratégie dans deux directions : 1) se protéger, avec la constitution d'une véritable cybermuraille de Chine, où tout est contrôlé, filtré et susceptible d'être interrompu ; 2) un gigantesque effort d'espionnage économique, le plus grand transfert de technologie qui ait jamais été opéré dans l'histoire.

Les autres pays se sont adaptés, notamment face au développement de la cybercriminalité, qui de tous les métiers du crime dans l'histoire est le plus rentable et le moins dangereux : les perspectives de gain sont importantes, tandis que le nombre de cybercriminels en prison se compte sur les doigts d'une main.

En France, le « Livre Blanc » de 2008 est le premier à faire du cyber un enjeu majeur. Trois mesures ont été prises dans la foulée : la création de l'ANSSI ; la mise en place d'un commandement militaire cyber, dont l'amiral Arnaud Coustillière a été le premier titulaire, et qui maintenant est devenu un commandement opérationnel, le Comcyber, enfin, les crédits de la direction technique de la DGSE ont été considérablement augmentés afin que la France tienne son rang dans le cyber renseignement. Il y a donc eu des changements majeurs en France, mais sur une position défensive ou contre-offensive, pas hégémonique ou offensive.

Et puis vous avez des puissances moyennes ou régionales qui jouent remarquablement du pouvoir égalisateur du cyber, avec des performances remarquables. Parmi elles, Israël, bien entendu, qui sur le plan technologique est presque qualitativement au même niveau que les trois cyber superpuissances que sont les États-Unis, la Russie et la Chine.

Pour vous donner une idée, l'investissement dans les start-ups cyber en 2019 a été de quatre milliards de dollars aux États-Unis, d'un milliard pour Israël, de trois ou quatre cents millions au Royaume-Uni et de pas tout à fait cent millions pour la France et l'Allemagne réunies. Autrement dit, les Français et les Allemands investissent chacun un vingtième de ce qu'investissent les Israéliens dans les start-ups cyber. Ces écarts sont spectaculaires.

L'Iran aussi a développé des capacités cyber dès le milieu

des années 2000, qui lui permettront de répliquer après l'attaque Stuxnet en provoquant des interruptions de services à Wall Street, ce qui a dissuadé Barack Obama de reprendre les offensives cyberdestructrices contre l'Iran. De la même façon, quelqu'un comme Sheldon Adelson, un milliardaire israélo-américain à la tête de Sands, un empire de casinos, qui avait dit qu'il fallait résoudre le problème nucléaire iranien en faisant exploser une bombe nucléaire dans le désert iranien, s'est moins fait entendre après que la comptabilité de sa société a été effacée par une cyberattaque ultérieurement attribuée à des *hackeurs* iraniens.

Les Coréens du Nord ont aussi des capacités cyber importantes qui servent non seulement à l'espionnage, mais aussi au contournement des sanctions : la Corée du Nord est un État cybercriminel qui n'hésite pas à recourir aux rançongiciels, ou à se faire faire des virements bancaires. Les Coréens du Nord ont ainsi réussi à détourner de l'argent de la banque centrale du Bangladesh grâce à un faux ordre de transfert.

Il y a enfin un dernier pays, un autre pays communiste, qui émerge depuis peu sur la scène cyber : le Vietnam, très actif, paraît-il, dans le renseignement économique, mais aussi la criminalité.

## CONCLUSION

**Léo Isaac-Dognin**

Une tendance très importante que l'on constate depuis plusieurs années est la mise en œuvre de stratégies de prépositionnement. Il s'agit d'une mise en œuvre très concrète des stratégies de cybercoercition que nous avons évoquées : des acteurs, pour la plupart étatiques car cela demande des moyens techniques importants, prépositionnent des implants sur des infrastructures critiques, avec pour message : « *N'agissez pas à l'encontre de nos intérêts, car nous pouvons facilement attenter aux vôtres.* » Une coupure de courant à Moscou se paiera d'une coupure de courant à New York, et vice versa. La capacité à faire ce type de prépositionnement à une échelle massive est importante si l'on souhaite peser sur la scène internationale. Il y avait le cercle des puissances nucléaires, il y a dorénavant le cercle des cyberpuissances. La France, pour en faire partie, doit se doter de ce type de capacité.

Elle doit aussi améliorer la protection de ses PME. C'est là que se situe actuellement le principal risque. Les grandes entreprises et les États se sont bien rendus compte du danger et ont commencé à se protéger, mais la chaîne logistique et économique reste fragile en raison de la vulnérabilité des PME. La convention cyber que le ministère de la Défense a signé en novembre 2019 avec nos huit principaux industriels est une bonne chose, mais il faut l'élargir aux PME.

Une tendance majeure, actuellement, est l'émergence d'une fracturation de l'espace numérique mondial. La Chine construit sa grande cybermuraille, avec un réseau quasiment autonome depuis plusieurs années. Beaucoup de pays, dont la Russie, réfléchissent de plus en plus à mettre en place une architecture permettant d'isoler leur réseau Internet du réseau mondial. Cela aura des conséquences géostratégiques importantes, par exemple sur les flux d'informations de certains pays ou régions vers d'autres.

Je terminerai enfin sur l'intelligence artificielle. Mark Zuckerberg, devant le Sénat américain, a dit qu'il y avait une course à l'armement dans ce domaine. La phrase lui a sûrement été soufflée par ses avocats, mais c'est exact. D'un point de vue défensif comme offensif, ceux qui maîtriseront la capacité à tirer parti des systèmes autoapprenants pour leur force cyber auront un réel avantage dans les prochaines années.

**Jean-Louis Gergorin**

Finissons sur une dernière comparaison. La DARPA, l'agence d'innovation de rupture de la défense américaine, a dépensé depuis sa création en 1958 environ 65 milliards d'euros actuels ; les communautés européennes ont commencé à avoir un programme de recherche à la même période ; elles ont depuis dépensé environ 80 milliards. Même si les objectifs de ces fonds ne sont pas tout à fait comparables, on voit que l'écart n'est pas celui qu'on aurait pensé.

Or, pendant cette période, alors que la DARPA a, par ses challenges, été à l'origine, entres autres, de l'invention du microprocesseur, d'Arpanet, ancêtre d'Internet, du calcul parallèle et les réseaux neuronaux… les programmes européens, si utiles qu'ils aient pu l'être, n'ont pas été à l'origine d'innovations disruptives majeures. Ceci illustre un problème fondamental : nous avons de l'argent, mais nous ne savons pas le dépenser efficacement.

# Débat avec la salle

**Général François Chauvancy** [4] **:** *Vous avez évoqué la question de la manipulation des esprits. Au fur et à mesure, celle-ci a un petit peu disparu de votre discours au profit des questions techniques. Or la guerre, c'est quoi ? Ce n'est pas uniquement tuer des gens et détruire des infrastructures. C'est gagner. Le cyber serait la guerre permanente. Mais comment répondre à cette guerre permanente et, finalement, comment la gagner ? Nous avons une vision trop technicienne de la guerre et pas assez orientée vers les buts de guerre, qui est une affaire idéologique.*

**Jean-Louis Gergorin :** La guerre de l'information est évidemment essentielle. D'autant plus, puisqu'il faut bien prendre en considération la technique, que c'est techniquement bien plus simple : il suffit pour semer la dissension de se créer des comptes sur Internet et d'avoir, au besoin, des compétences en intelligence artificielle, pour répandre des fausses nouvelles voire, plus fort encore, des informations exactes. La rapidité de

4. Directeur de *La Revue d'Études,* Demos Group.

diffusion de l'information rend cette stratégie redoutable. Imaginez qu'une information compromettante pour un candidat apparaisse juste avant une élection. Elle sera reprise et retweetée sur tous les réseaux sociaux en quelques heures maximum. Même en cas de rectification convaincante, celle-ci arriverait probablement trop tard. Le mal aura été fait.

Ce que le numérique apporte à la guerre de l'information est donc phénoménal. Mais je suis d'accord avec vous pour dire qu'il faut avoir en tête le but visé. Le but stratégique, ici, c'est le contrôle, l'influence. Sans avoir à se battre. C'est un des grands préceptes de Sun Tzu : le summum, pour un stratège, est de vaincre sans combattre.

Beaucoup de choses ont été faites en France, mais je pense qu'elles sont trop fragmentées. Le défi cyber est aussi important qu'un autre défi qui a nécessité tout un mode d'organisation, le défi terroriste. Une coordination nationale du renseignement et de la lutte nationale contre le terrorisme a été créée, ce qui est une très bonne chose. Dans un article que j'ai coécrit avec l'amiral Edouard Guillaud, ancien chef d'état-major des armées, et Bernard Barbier, ancien directeur technique de la DGSE [5], nous disons qu'il nous faut aussi un coordinateur national cyber, qui n'aurait pas à interférer avec l'action opérationnelle des services, mais dont la fonction serait d'élaborer une vision stratégique

5. Bernard Barbier, Edouard Guillaud et Jean-Louis Gergorin, « Cybercoercition : un nouveau défi stratégique », *Le Monde*, 28 janvier 2020, disponible sur : https://www.lemonde.fr/idees/article/2020/01/28/cybercoercition-un-nouveau-defi-strategique_6027444_3232.html.

de l'ensemble du cyber dans tous ses aspects. La question de l'information serait incluse dans cette stratégie. Elle est délicate. Peut-on censurer Internet ? Qui doit réguler les réseaux sociaux ? Réagir aux fausses nouvelles ? Est-ce qu'on délègue ça aux réseaux sociaux ? Il faut que quelqu'un soit en charge. Or, au sein de l'administration personne n'est clairement responsable ni de définir ni de mettre en œuvre une stratégie cohérente vis-à-vis des réseaux sociaux et face aux campagnes de désinformation.

Il faudrait donc que quelqu'un soit en charge. Sans pour autant que cela devienne un ministère de la pensée. C'est un vrai défi. Mais il est temps de l'aborder. Il faut un responsable dans l'appareil politique, qui puisse dialoguer et avoir un rapport de force avec les réseaux sociaux et les GAFAM. Des gens comme Mark Zuckerberg ou les dirigeants de Google considèrent qu'ils sont un État supranational. Ils parlent aux gouvernements comme naguère les Templiers aux monarques, avant que ça tourne mal.

**Georges Malbrunot** [6] **:** *Vous avez beaucoup insisté sur les acteurs étatiques : la Chine, la Russie et Israël. Mais le principal danger n'est-il pas la privatisation du cyber par un certain nombre d'opérateurs ? Un acteur majeur dans le domaine est la société israélienne NSO. Celle-ci a beaucoup fait parler d'elle en vendant des logiciels d'espionnage à Mohammed ben Salmane et à d'autres*

6. Spécialiste du Moyen-Orient, grand reporter au service étranger du journal *Le Figaro*.

*émirs du Golfe. J'interrogeais à ce sujet un ancien ambassadeur de France en Israël et aux États-Unis, qui est associé de NSO, sachant que NSO a quand même contribué au contrôle d'un certain nombre d'opposants en Arabie Saoudite et ailleurs. Il m'a répondu qu'il était bien conscient de ces problèmes, mais qu'il nourrissait l'espoir de civiliser ces activités. D'où la question que je vous pose : peut-on civiliser ce genre d'activité ? Peut-on mettre sur pied une doctrine d'emploi et peut-être aussi réguler la privatisation ?*

**Jean-Louis Gergorin :** D'un côté, vous avez bien entendu raison. Quand Léo parlait d'un pouvoir égalisateur du numérique, celui-ci ne joue pas simplement entre nations, mais entre de nombreuses entités : les nations, certes, mais aussi les multinationales, les GAFAM et des petites entreprises extrêmement performantes spécialisés dans le cyber. Cependant, les États contrôlent quand même ce théâtre d'opérations. Le modèle qui me vient à l'esprit pour décrire ce qui se passe, c'est celui des corsaires et des pirates. Il y a certes beaucoup de pirates, mais d'une façon ou d'une autre, ils sont contrôlés ou marginaux relativement aux États, quand ils ne sont pas tout bonnement des corsaires autorisés ou directement employés par ceux-ci.

Les services israéliens, par exemple, savent parfaitement ce que font ces acteurs privés. Il y a une osmose totale. Entre parenthèses, je serai plus dur que vous concernant les rapports de NSO et de l'Arabie Saoudite, puisque c'est le craquage par NSO du WhatsApp de Jamal Kashoggi

qui a entraîné la décision fatale de l'éliminer dans les circonstances épouvantables que vous connaissez.

De même, le FSB russe protège des organisations cyber criminelles et ne peut pas ignorer complètement ce que font ces groupes.

On a ainsi un petit peu la même relation que la reine Elizabeth avec ses corsaires attaquant les galions espagnols.

Face à cela, le 12 novembre 2018, le lendemain de la commémoration des cent ans de l'Armistice, notre président de la République lancé l'Appel de Paris pour la paix, la sécurité et la confiance dans le cyberespace. La liste des signataires s'engage à une série d'actions : coopérer contre la cybercriminalité, protéger l'accessibilité et l'intégrité d'Internet, défendre les processus électoraux et la propriété intellectuelle, etc. À l'heure actuelle, 74 pays, je crois, ont signé, ainsi que plusieurs grandes sociétés numériques comme Microsoft. Petit problème cependant : les États-Unis, la Russie, la Chine, la Turquie, Israël, l'Inde, entre autres, n'ont pas signé. Il risque d'être compliqué de traduire cet appel en action.

**Michel Crinetz** [7] **:** *Une question dont je m'étonne qu'elle n'ait pas encore été posée : la société Huawei constitue-t-elle une réelle menace ou s'agit-il seulement d'un storytelling gonflé par Monsieur Trump ?*

7. Ancien commissaire-contrôleur des assurances au ministère des Finances, à la commission de contrôle des assurances puis à l'autorité de contrôle prudentiel.

**Léo Isaac-Dognin :** Il y a beaucoup de débats autour de la capacité à certifier les infrastructures – en l'occurrence, les composants qui seraient éventuellement fournies par Huawei. Je vais en dire un mot, mais j'insisterai aussi sur le fait que si même on arrivait à implémenter ce type de certification technique de la sûreté des infrastructures, le contexte légal et politique chinois continuerait de constituer le risque primordial.

Nous ne devons pas prendre de retard dans la mise en place de la 5G. Si certains pays décident que cela nécessite d'utiliser des composants fournis par Huawei, ces composants doivent être configurées de façon à être auditables le plus facilement possible. L'Europe, si elle se coordonne, sait peser sur le plan réglementaire et obliger ces infrastructures à être conçues de telle sorte à ce qu'elles soient *secure by design*, c'est-à-dire sécurisée par conception, auditables rapidement, avec un maximum de composants open source. Il faut aussi que le chiffrement soit plus systématique et plus robuste. Si quelqu'un pénètre les infrastructures, mais que les données y sont chiffrées, il n'obtient pas grand-chose.

Mais même si on parvenait à faire cela vis-à-vis de Huawei, nous serions quand même exposés. Pourquoi ? En 2017, la Chine a passé une loi sur la cybersécurité permettant au gouvernement de mandater l'accès aux infrastructures de toute entreprise basée en Chine. Ainsi, même à supposer que le groupe Huawei ait la meilleure volonté du monde et, comme l'a proposé son fondateur, accepte d'ouvrir l'accès total à son code et se soumettre

à toutes les obligations européennes ou américaines, il est évident que le jour où le gouvernement chinois lui demandera l'accès à telle ou telle infrastructure, contenu, composant ou code informatique, Huawei le lui donnera. Sans parler du fait que les autorités n'auraient jamais les ressources suffisantes pour auditer tous les composants. Le danger se situe donc dans cette loi, et dans le rapport de force que le régime chinois exerce vis-à-vis de ses entreprises. Une solution serait la proposition par Huawei de créer une entreprise séparée en Europe. Reste à voir si Huawei le peut et si l'entreprise est capable en pratique de s'extraire de ses obligations et de sa subordination au gouvernement chinois.

**Jean-Louis Gergorin :** Je me référerai pour ma part à un éminent stratège, Napoléon, qui affirmait que ce qui compte face à un adversaire potentiel ne sont pas ses intentions, au sujet desquelles on peut perdre un temps fou et se tromper, mais ses capacités. Or il se trouve que les autorités chinoises ont une capacité absolue de pouvoir sur Huawei. À la fois parce que cette entreprise est en Chine, sur le plan légal, et que des chefs d'entreprise ou des universitaires peuvent disparaître s'ils déplaisent au pouvoir. Autrement dit, ce qui compte, c'est que si une autorité chinoise veut soit pénétrer Huawei, sans que les dirigeants le sachent, soit forcer certains responsables de Huawei à faire certaines choses, ils n'auront aucun mal à le faire. Concernant la 5G, il s'agit ainsi de quelque chose d'absolument fondamental. Nous avons parlé des implants dans les réseaux électriques qui aboutissent à une paralysie mutuelle assurée entre Russes et Américains.

Mais la 5G, c'est un implant permanent. Ceci alors que l'activité d'un pays en sera de plus en plus dépendante. Concrètement, confier la 5G à un équipementier que nous ne contrôlons pas signifie s'exposer un jour à des interruptions de service, potentiellement vitales. Afin de maintenir son indépendance nationale, la France finance une force de dissuasion, mais dans le même temps nous accepterions que nos infrastructures majeures puissent être à volonté sélectivement interrompues par un pays étranger ? Ce n'est pas acceptable. Même si nous avons d'excellentes relations avec lui, c'est une question de capacité : c'est donner à un pays étranger important, qui peut être un concurrent, notamment dans le domaine industriel, le pouvoir d'interrompre sélectivement telle ou telle infrastructure, telle ou telle usine. D'autant plus quand, pour reprendre ce que disait Guillaume Poupard, le directeur de l'ANSSI, dans un entretien avec *Les Échos* [8], les autorités chinoises peuvent faire pression sur Huawei, tandis qu'il n'y a pas à craindre que le gouvernement suédois contraigne Ericsson à interrompre ses services en France.

**Pierre Joxe** [9] **:** *Le bouleversement des rapports de force qui se prépare est presque incommensurable avec celui qui a lieu depuis trente ans. En matière de renseignement, il y a certes toujours le problème des moyens. Il y a aussi celui des risques qu'on est prêt à*

8. https://www.lesechos.fr/tech-medias/hightech/les-conflits-de-demain-vont-etre-numeriques-tous-les-grands-etats-sy-preparent-dit-le-patron-de-lanssi-1164596.
9. Ancien ministre de l'Intérieur et de la Défense, ancien président de la Cour des comptes.

*prendre, aussi important que les moyens : est-on prêt à y consacrer des milliards, des hommes, des réseaux, etc. ? Mais à part ça, la donnée technologique et scientifique établit des inégalités croissantes dont on a l'impression qu'elles vont devenir gigantesques. Devant cela, on est abasourdi par les chiffres que vous avez donnés : une puissance moyenne comme Israël consacre un milliard de dollars au cyber, les États-Unis en consacrent quatre, et l'Allemagne et la France, à eux deux, seulement cent millions ! Ces chiffres sont précurseurs d'une déchéance, d'une dégringolade, presque d'une disparition s'il n'y a pas de changement rapide. Qui est aveugle ou ignorant devant cette réalité ?*

**Jean-Louis Gergorin :** C'est fondamentalement un problème culturel. Nous avons une vision colbertiste de l'innovation, du développement, marquée par les grands programmes. Et nous avons eu raison. Il fallait le faire. Les Chinois le font, les Israéliens l'ont fait. Mais le numérique, c'est totalement différent. L'innovation s'y fait par les start-ups, par des développements très rapides : on teste des idées, il y a des échecs, on va très vite. Le génie israélien est d'avoir créé un écosystème à partir de leur fameuse unité de renseignement, l'unité 8200. Ils sélectionnent dans l'enseignement secondaire tous ceux qui sont les plus doués pour faire du *hacking* : ceux qui sont forts en mathématiques et les bidouilleurs. Ceux-ci font leurs trois ans de service, puis ils sont systématiquement encouragés à aller dans les start-ups, ce qui est d'ailleurs leur intérêt, puisqu'ils peuvent bien y gagner leur vie. Le modèle est tellement performant,

qu'un pays très différent, le Royaume-Uni, l'a adopté avec succès. Le GCHQ, l'unité de renseignement britannique, de bonne qualité, et qui, au passage, a deux fois plus de moyens que nous en France dans le même domaine, stimule la création autour d'elle d'un écosystème. Nous essayons de faire la même chose autour de l'ANSSI, ou à Rennes, mais nous avons pris beaucoup de retard, et y mettons beaucoup moins de moyens.

Une des premières licornes européennes en matière de cyber est Darktrace, une start-up britannique créée par des anciens du GCHQ. D'après les informations que j'ai eues, elle sera probablement sélectionnée pour assurer la sécurité des Jeux olympiques à Paris. Le problème, cependant, comme Bernard Barbier, l'amiral Guillaud et moi-même l'avons souligné dans notre article du Monde, est qu'il ne s'agit que de service : nos grandes entreprises dans le domaine proposent du service aux entreprises, ces sociétés les aident à se protéger, mais avec des outils qui ne sont pas français, ni même européens, mais essentiellement américains ou israéliens. C'est une dépendance impressionnante.

**Léo Isaac-Dognin :** Je compléterai ce qui vient d'être dit sur un point : il y a un endroit où peut encore trouver de très gros financements : l'Union européenne. En matière d'innovation, le budget est mal piloté. Mais la Commission a annoncé 20 milliards d'euros d'investissement et il me semble qu'il y a cette fois-ci ce qui avait manqué aux précédentes occasions, c'est-à-dire une vraie stratégie industrielle, une vision qui permet de coordonner, d'inves-

tir efficacement ces fonds, tout en étant prêt à prendre le niveau de risque que d'autres pays sont prêts à prendre. La Commission a en effet récemment publié un « Livre blanc » [10] qui, enfin, esquisse les priorités et propose une analyse assez réaliste des forces et faiblesses européennes, identifiant notamment l'avantage que l'on a en matière de données industrielles. Car on peut penser que l'Europe est toujours en retard sur plein de sujets, mais, au final, nous avons quand même les entreprises les plus numérisées du monde, avec, par conséquent, une masse de données qui constitue déjà un réel atout concurrentiel international pour nos entreprises. L'idée portée par le nouveau commissaire à la politique industrielle et au numérique, Thierry Breton, bien qu'elle n'ait pas été formulée ainsi, est d'essayer de créer une forme de RGPD permettant de maintenir les données industrielles en Europe, comme on commence à le faire pour les données des utilisateurs. Cela pourrait faire une vraie différence. Mais il faut pour cela parvenir à coordonner toute une industrie derrière. Les fonds existent, jusqu'à présent ils ont été mal utilisés, mais j'ai bon espoir pour l'avenir.

**Jean-Louis Gergorin :** Les choses sont en effet en train de changer à Bruxelles. La nomination de Thierry Breton à la Commission européenne est un excellent choix. Ce qu'il a réussi chez Atos, et ses grandes ambitions pour le numérique, c'est exactement ce qu'il faut faire. Mais il reste limité par les procédures, ainsi que par la philosophie de juste retour pour les États-membres.

10. Voir : https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_273.

Il est aussi limité par le principe même, celui de la redistribution. Dans un séminaire récent, le créateur de la *Joint European Disruptive Initiative* (JEDI), André Loesekrug-Pietri, et moi-même avons promu auprès d'un des principaux responsables de la recherche à la Commission la nécessité de procédures agiles inspirées de celles de la DARPA. Ce à quoi il nous a répondu que sa mission fondamentale est de satisfaire ses *stakeholders*, c'est-à-dire les agences nationales… Maintenant, je suis persuadé que Thierry Breton dans sa volonté d'efficacité sera amené à redéfinir les méthodes de stimulation de l'innovation. Il faut s'attaquer à ce défi majeur : pas seulement dépenser de l'argent, mais savoir mieux cibler ces investissements, pour être De la même façon, Thierry Breton a récemment répondu dans une émission radiophonique, je crois, concernant l'efficacité des dépenses qui allaient être faites, que sa fonction consistait à redistribuer aux États. Autrement dit, à redistribuer aux agences, aux bureaucraties nationales. Il y a un sacré défi : pas simplement dépenser de l'argent, mais comment le dépenser et comment être efficace.

**Léo Isaac-Dognin :** …Et choisir des gagnants. Il faut que l'Europe accepte de choisir des gagnants dans certains domaines du marché numérique qui seront par essence, quoiqu'il arrive, oligopolistiques. A court et moyen terme, l'industrie numérique sera dominée par des mastodontes internationaux tels que les GAFAMs américains et BATX chinois, et la question pour l'Europe est : souhaite-t-on que certains de ces mastodontes soient européens et si oui, quels domaines faut-il cibler ?

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

# Les publications de l'Institut Diderot

## Dans la même collection

- 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
- La souveraineté numérique - Pierre Bellanger
- Le Brexit et maintenant - Pierre Sellal
- Les Jeux paralympiques de paris 2024 : une opportunité de santé publique ? Professeur François Genêt & Jean Minier en collaboration avec Philippe Founy
- L'intelligence artificielle n'existe pas : et maintenant ? - Luc Julia

## Les Carnets des Dialogues du Matin

- 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
- Quelles menaces numériques dans un monde hyperconnecté ? Nicolas Arpagian
- L'avenir de la Bioéthique - Jean Leonetti
- Données personnelles : pour un droit de propriété ? Pierre Bellanger et Gaspard Koenig
- Quels défis pour l'Algérie d'aujourd'hui ? - Pierre Vermeren
- Turquie : perspectives européennes et régionales - S.E. Ismail Hakki Musa
- Burn-out - le mal du siècle ? - Philippe Fossati & François Marchand

- L'avenir de la loi de 1905 sur la séparation des Églises et de l'État. Jean-Philippe Hubsch
- L'avenir du bitcoin et du blockchain - Georges Gonthier & Ivan Odonnat
- Le Royaume-Uni après le Brexit Annabelle Mourougane - Fréderic de Brouwer & Pierre Beynet
- L'avenir de la communication politique - Gaspard Gantzer
- L'avenir du transhumanisme - Olivier Rey
- L'économie de demain : sociale, solidaire et circulaire ? Géraldine Lacroix & Romain Slitine
- La transformation numérique de la défense française Vice-amiral Arnaud Coustillière
- L'avenir de l'indépendandance scientifique et technologique française Gérard Longuet

## 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
- Le système de santé privé en Espagne : quels enseignements pour la France ? Didier Bazzocchi & Arnaud Chneiweiss
- Le maquis des aides sociales - Jean-Pierre Gualezzi
- Réformer les retraites, c'est transformer la société Jacky Bontems & Aude de Castet
- Vers un droit du travail 3.0 - Nicolas Dulac
- L'assurance santé privée en Allemagne : quels enseignements pour la France ? Arnaud Chneiweiss & Nadia Desmaris
- Repenser l'habitat. Quelles solidarités pour relever le défi du logement dans une société de la longévité ? - Arnaud Chneiweiss & Nadia Desmaris

# Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ?

Le cyber n'est pas une guerre au sens classique, avec déclaration, drapeaux, tambours et décorations. C'est un combat de l'ombre, toujours en dessous du seuil de la guerre ouverte.

Quelle est alors cette menace qui, de façon évidente, ne cesse d'augmenter ? Le cyber, c'est l'utilisation des moyens numériques à des fins d'influence et de contrôle, sur le plan géopolitique, économique, et même sociétal.

Ces moyens numériques peuvent être divisés en deux grandes familles, qui se recoupent de plus en plus. D'une part, l'intrusion informatique : ce qu'on appelle le *hacking*, le fait de pénétrer un ordinateur, un système d'information, pour le saboter ou l'espionner. D'autre part, la manipulation de l'information numérique, essentiellement via les plateformes de médias et les réseaux sociaux.

À l'invitation de l'Institut Diderot, en l'espace de ces quelques pages, Jean-Louis Gergorin et Léo Isaac-Dognin nous font l'amitié de nous montrer pourquoi et comment chaque rouble, dollar ou euro dépensé dans des opérations de cyber sabotage ou de guerre de l'information a un rapport coût-efficacité extrêmement attractif avec des risques limités ; ce qui encourage à les utiliser toujours davantage…


**Jean-Louis GERGORIN**

Ancien chef du Centre d'Analyse et de Prévision du Quai d'Orsay, ancien membre du comité exécutif d'EADS, Chargé de cours à Sciences Po Paris, co-auteur de « Cyber la guerre permanente » (Le Cerf).

**Léo ISAAC-DOGNIN**

Chef de projet IA & Big data chez Capgemini Invent, enseignant à Sciences Po Paris, co-auteur de « Cyber la guerre permanente » (Le Cerf).



INSTITUT DIDEROT

La présente publication ne peut être vendue.

ISBN 979-10-93704-73-9

ISSN 2496-4948 (en ligne)
ISSN-2608-1334 (imprimé)

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