L'enjeu majeur des cyber menaces

Jean-Louis Gergorin, ancien directeur du Centre d'analyse et de prévision (CAP) du ministère des Affaires étrangères, est le co-auteur de : *Cyber. La guerre permanente*, Paris, Cerf, 2018.

Thomas Gomart est directeur de l'Ifri.

Marc Hecker est directeur des publications de l'Ifri.

Jean-Louis Gergorin

Nous assistons actuellement à une révolution stratégique que je qualifierais de fusion entre Sun Tzu et Clausewitz, deux des plus grands penseurs stratégiques, le premier d'entre eux étant le plus célèbre en Occident. Clausewitz dit que la guerre est la continuation de la politique par d'autres moyens, puis que la guerre est une expression de violence en vue d'atteindre des objectifs de contrôle, d'influence, etc. Sun Tzu, voici 2 500 ans, a simplement écrit : « Vaincre sans croiser le fer est le comble du comble du guerrier. » Cela rejoint d'ailleurs ce que disait le professeur Mahbubani : la stratégie chinoise vise à gagner, à s'imposer en évitant la guerre. Les Chinois sont restés fidèles à Sun Tzu.

La cyberguerre est la fusion des deux pensées, parce qu'elle permet d'atteindre les objectifs de contrôle, d'influence que décrit Clausewitz, dans une manœuvre qui est la continuation de la politique par des moyens non violents – en tout cas au départ car, par exemple, si vous provoquez une catastrophe aérienne en bloquant les systèmes de navigation, cela devient très violent. En tout cas, la cyberguerre peut être pour l'essentiel non violente, et permettre d'atteindre exactement les mêmes objectifs de contrôle que la politique et la guerre, et ce beaucoup plus efficacement.

Qu'est-ce que la cyberguerre ?

Une autre chose importante est de savoir de quoi l'on parle quand on parle de cyberguerre, et je sais que cela n'est pas évident. La cyberguerre, c'est l'utilisation offensive, à des fins de contrôle, de l'ensemble des possibilités du numérique, et cela peut se faire de deux grandes façons. La première, c'est l'intrusion informatique (*hacking*), à des fins d'espionnage, de sabotage ou d'intimidation – et c'est la forme la plus répandue actuellement.

La « cyberintimidation »

La « cyberintimidation », on n'en parle pas beaucoup mais c'est absolument majeur. Je vous donnerai trois exemples récents dans l'ordre chronologique. Au mois de mai 2018, les responsables de la cybersécurité allemande ont signalé tout une série d'intrusions dans les systèmes énergétiques et électriques, tentatives semble-t-il déjouées. Il n'y a pas eu d'attribution officielle – c'est la doctrine du BSI, l'agence de cybersécurité allemande –, mais le patron de l'Office de protection de la Constitution a mis en cause la Russie, ce qui n'a été ni démenti, ni confirmé. Deuxième exemple : le Department of Homeland Security des États-Unis a publié en juillet 2018 un rapport très étayé d'où il ressortait que plus de 400 installations électriques américaines – de distribution et de production – avaient fait l'objet de pénétrations informatiques sans sabotage. Les Américains ont ainsi souligné que leurs ennemis auraient pu saboter, qu'ils ne l'ont pas fait mais ont donc démontré qu'ils pouvaient le faire, et pouvaient revenir. Je suis persuadé que ceux qui ont fait ça – les Américains ont clairement attribué la manœuvre au renseignement militaire russe, le GRU – ont voulu signaler qu'en cette période de tensions, de sanctions, eux aussi pouvaient agir au centre du système américain. Troisième cas, qui nous concerne très directement : Guillaume Poupard, patron de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a déclaré en janvier dernier que des pré-positionnements très importants – c'est-à-dire des pénétrations sans sabotage, comme celles décrites par les Américains, démontrant que l'entité qui a fait cela est capable de revenir et de saboter – avaient eu lieu en France et dans des pays alliés (Allemagne). Ce qui est capital stratégiquement. Nous sommes très attachés à notre indépendance, à la dissuasion, etc., et des entités étrangères ont ainsi montré qu'elles pouvaient nous paralyser, nous priver d'électricité pendant quelques heures par exemple.

La manipulation de l'information

Deuxième approche de ce qu'est une cyberguerre : la manipulation de l'information – très différente de l'intrusion informatique. Cette manipulation de l'information peut se faire par la manipulation des réseaux sociaux, vecteurs d'informations extraordinaires. Le problème des *fake news*, des infox, est très subjectif. Ce qui n'est pas subjectif, en revanche, c'est le problème, qui doit être mesuré objectivement, des faux profils sur les réseaux sociaux. Si vous dites que vous êtes Louis Durand, camionneur à Rouen et Gilet jaune et que vous animez un compte Facebook extrêmement actif et violent, mais qu'en réalité vous êtes John Stuart qui travaille avec M. Shillman (milliardaire américain d'extrême droite violemment engagé sur les réseaux sociaux contre l'Union européenne), ou

si vous êtes M. Popov travaillant à l'institut Internet Research Agency de Saint-Pétersbourg, et que vous vous faites passer dans un cas ou dans l'autre pour Louis Durand, vous pouvez, derrière ce faux profil, faire beaucoup de mal.

J'ai suivi moi-même (ayant trouvé cela dans des communautés de cybernautes), entre fin août et fin décembre 2018, un personnage qui sévit sur Twitter sous le nom de A. Dupond III, et qui a retweeté tous les messages de la cybersphère française les plus hostiles au président Macron et à sa politique (caricatures, photos de faux blessés pendant les affaires de Gilets jaunes…) – ce qui représente 40 000 tweets durant la période citée. Il commençait à 6h du matin et terminait à 10h le soir.

La manipulation numérique

Je terminerai par deux exemples de ce qu'est, dans la cyberguerre, la manipulation numérique de l'information. Je n'appellerais pas cela les *deep fakes,* mais les « infox profondes » : les manipulations numériques des vidéos par l'Intelligence artificielle, par ce qu'on appelle les « réseaux neuronaux ». Actuellement, il est quasiment impossible de détecter une fausse vidéo, et il est devenu techniquement possible de créer une fausse conversation – par exemple hier – entre Theresa May et Emmanuel Macron, en lui donnant toutes les apparences de la vérité ; les experts pourront la disséquer pour voir si elle ou vraie ou non en utilisant d'autres réseaux neuronaux. En temps d'élections, vous pouvez donc manipuler l'opinion publique en sortant une fausse vidéo. Vous pouvez également – c'est une nouvelle invention, apparue il y a deux ou trois mois –, truquer les informations d'un GPS, les informations des cartes de Google Maps, créer de fausses informations visuelles ou de navigation, ce qui peut avoir un effet déstabilisateur profond.

Thomas Gomart

Je soulignerai d'entrée le terme « menace » qui figure dans le titre de notre session : il traduit une évolution assez récente de notre compréhension du cyber. Jusqu'à l'affaire Snowden, le cyber était le plus souvent présenté comme un outil de libéralisation, d'individualisation extrême ; depuis Snowden un renversement s'est opéré, dans la mesure où cette affaire a fait prendre conscience, non aux spécialistes mais à l'opinion, de la puissance de ce qu'on pourrait appeler « le complexe militaro-numérique ». La dimension « opportunités ouvertes par le cyber » est aujourd'hui masquée par l'aspect « menaces », ce balancement nous renvoyant aux logiques militaires et aux racines libertaires. Cette dualité est à mon sens aujourd'hui dominante.

Qui menace qui ?

Deuxième remarque : quand on parle de menaces, qui les formule, qui les subit ? Il faut distinguer les trois types d'acteurs auxquels nous avons à faire face quand on parle de cyber, ainsi que les infrastructures qui peuvent être concernées par ces menaces. Les grands types d'acteurs sont d'abord les États – et on assiste un « retour des États » en matière de cybergouvernance tout à fait spectaculaire – ; ensuite ce sont les plates-formes – les GAFA, les BATX – ; et enfin les individus, les internautes, les utilisateurs. Au fond, on a trois couches que touchent des menaces de natures différentes : la couche matérielle – les infrastructures, les câbles sous-marins, les *data centers* par exemple –, la couche applicative qui regroupe les différentes applications, et la couche cognitive.

Ces trois acteurs, et ces trois couches, nous devons les garder en tête pour bien identifier le type de menaces auxquelles nous pouvons être confrontés.

Je vais citer assez naturellement Raymond Aron, qui pointe l'opposition – à mon sens au cœur de nos difficultés à penser le cyber – entre ce qu'il appelle pour le décideur « la conduite économique », forcément limitée, et ce qu'il nomme « la conduite diplomatico-stratégique » qui se fait « à l'ombre de la guerre ». Cette tension entre conduite économique et conduite diplomatico-stratégique doit être aussi au cœur de notre réflexion sur le cyber. Au fond, le point important, c'est la simultanéité de ces deux conduites, et la capacité que l'on a, ou non, à les suivre simultanément.

Puissance numérique et types de menaces

Je compléterai mon propos par quelques points rapides. Le premier concerne la notion de puissance numérique, pour tenter d'identifier les principales menaces. J'utiliserai l'image de l'échiquier et de la toile, et il faut penser les deux simultanément. Sur l'échiquier, les pièces ont une valeur les unes par rapport aux autres, s'inscrivent dans une hiérarchie – et cela reste une clé de lecture par exemple pour les rapports interétatiques de nature classique. Sur la toile, tout dépend au fond du nombre de points de contact que l'on peut avoir, et il peut être illimité.

Deuxième aspect de la puissance numérique : l'importance qu'il faut accorder au pouvoir de réseau. Le pouvoir de réseau est ce paradoxe que nous éprouvons tous, en utilisant nos outils de recherche : l'utilisation de standards par un nombre grandissant d'utilisateurs donne de la force à

ce standard, mais ce faisant réduit les options et choix possibles. Celui qui exerce le pouvoir de réseau prend dans cette logique un ascendant décisif.

Troisième remarque sur la puissance numérique : le numérique nous oblige au débat entre relations de souveraineté – celles qui permettent de prendre des décisions de nature collective – et relations de sociabilité – celles qui permettent de prendre des décisions individuelles. La littérature foisonnante sur le cyber pose la question : qui l'emportera, quel type de relations aura la primauté ?

Cela me conduit à tenter d'identifier les principales menaces. Je commencerai, en partant des acteurs précédemment définis, par le rapport d'État à d'État dans le numérique. Le problème principal est ici celui de l'attribution. On ne peut avoir dans le cyber des mécanismes d'attribution comparables à ceux du champ d'affrontement conventionnel, ou nucléaire : en attribuant explicitement une attaque, on révèle ses propres capacités de compréhension et de connaissance de l'autre. Un deuxième type de menace peut s'observer dans le rapport entre États et plates-formes : on est là dans une situation problématique pour les Européens, qui est apparue en filigrane dans les précédentes tables rondes : certaines plates-formes ont aujourd'hui des capacités d'investissement très largement supérieures à celles des États, et disposent d'un pouvoir marketing très puissant. J'en veux pour preuve l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, manière pour un certain nombre de plates-formes de se racheter une forme de vertu après la démonstration de leur collusion avec certains États, en particulier les États-Unis.

Troisième type de menace : il s'observe dans le rapport entre plates-formes et individus. La réponse des Européens est le fameux RGPD, ou Règlement général sur la protection des données, censé protéger les données de chaque consommateur par rapport aux grandes plates-formes. Mais je veux relever que tout n'est pas protégé, en particulier dans le domaine des données de sécurité.

Enfin, un quatrième type de menace s'observe dans le rapport entre États et individus. C'est là que les différences de régimes politiques pèsent le plus directement : se mettent en place des formes d'autoritarisme numérique avec la reconnaissance faciale, ou le crédit social que les autorités chinoises sont en train de développer, et qui auront des conséquences dans ce qu'on appelle les *smart cities*. Le volet proprement sécuritaire devient un élément constitutif de la *smart city*, et donc de la manière de gouverner.

Toutes ces questions sont décisives pour l'Europe, qui adopte pour l'instant un positionnement de nature éthique : il est important, évidemment, avec le débat sur l'avenir de l'Intelligence artificielle, mais pas suffisant. La question fondamentale, concernant les Américains en matière de cyber menace, est celle de leur capacité industrielle et militaire à réagir. Et le deuxième élément frappant – et c'est là aussi une « menace » lourde –, est que nous assistons aujourd'hui, sous tous les discours mettant en avant l'individualisation, à une reconcentration du numérique dans la main de quelques acteurs.

Quelles vulnérabilités concrètes ?

Marc Hecker

Ma question concerne les trois couches que vous venez de définir. Y a-t-il une hiérarchie de menaces au sein de ces couches ? Et ces couches sont-elles vulnérables de la même manière ? Je pense en particulier à la couche physique, ce qui devrait nous permettre de parler des espaces communs. Vous avez rappelé dans votre dernier ouvrage que 95 % des télécommunications et des données numériques transitaient par câbles sous-marins, et qu'il n'y a que 448 câbles qui arrivent autour de cent points terrestres. Ces câbles sont-ils vulnérables, et cette vulnérabilité matérielle est-elle sous-estimée par rapport à d'autres menaces, davantage mises en avant, pour la couche cognitive ou la couche logicielle ?

Thomas Gomart

Cette vulnérabilité a été pointée dans les travaux de la *Revue stratégique* ou de la *Revue de cyberdéfense*. Ces câbles peuvent être sectionnés, on l'a déjà vu ; ils peuvent être espionnés par sous-marins, et c'est aussi arrivé récemment. Une évolution industrielle est importante à noter : certaines plates-formes se dotent aujourd'hui de leurs propres moyens de devenir des câbliers, de poser leurs propres câbles, dans une forme d'intégration verticale qui ne dirait pas son nom. Cela pose la question d'une analogie possible avec le domaine de l'énergie : les Européens doivent bien séparer ce qui relève des couches d'infrastructures de ce qui relève des couches applicatives ou cognitives. La vulnérabilité des câbles est donc une réalité, comme celle, beaucoup plus dispersée, des *data centers*.

Jean-Louis Gergorin

Je voudrais lancer un cri d'alarme. Une des grandes caractéristiques des cyber menaces est qu'elles ne cessent d'augmenter, et qu'elles vont encore augmenter sous l'aspect d'intrusions informatiques. On va assister à un triplement du nombre d'objets connectés, on en aura plus de vingt milliards dans deux ou trois ans, ce qui augmentera de manière considérable

les risques. En plus, l'Internet des objets implique un vecteur de transmission de l'information qui va être la 5G, c'est-à-dire une capacité d'accélération considérable par les réseaux cellulaires ; et de ce point de vue là, la vulnérabilité augmentera aussi.

Il ne faut pas tomber dans une paranoïa qui proscrirait Huawei — il y a des tas de choses que fait Huawei et qui ne posent pas problème. En revanche, il existe des nœuds de sécurité que tout État souverain doit absolument conserver, et les Européens doivent pouvoir contrôler ces nœuds. Or les moyens qui sont affectés à ce problème (il va y avoir une loi dite « loi Huawei » en France, et des dispositions ont déjà été prises en Angleterre et en Allemagne) sont trop limités pour faire face même au seul problème de la 5G. Sans parler des autres cyber menaces.

Il faut être conscient de l'écart qui existe en matière de capacités cyber entre les différents États. En France, les organismes qui s'occupent de cyber au sens large, ANSSI, DGSE, commandement de Cyberdéfense, représentent 3 500 personnes. En Allemagne, il y en a un peu plus de 2 000. En Grande-Bretagne, tout est concentré alors que c'est quelque peu fragmenté en France et en Allemagne. Aux États-Unis il y en a 50 000 à la NSA. En Israël – voilà une grande puissance en devenir –, on dénombre 6 000 personnes dans l'unité 8 200. Si l'on considère maintenant les investissements technologiques annuels dans les start-ups cyber, ils représentent 30 millions en France – dollars ou euros… –, 42 millions en Allemagne, 300 au Royaume-Uni, 3 milliards aux États-Unis et 600 millions en Israël. L'effort à faire est donc majeur, et il doit commencer par un rapprochement franco-allemand, puisque les Britanniques sont liés par accords avec les Américains.

Quant aux réseaux sociaux, on a vu leur importance majeure dans la vie politique. Il est évident qu'on ne peut pas accepter une situation complètement asymétrique où les pays autoritaires contrôleraient Internet et l'utiliseraient aux fins de contrôle social. La Russie commence à s'inspirer de la Chine, qui contrôle tout Internet. Il existe un projet de loi britannique visant à responsabiliser les patrons des réseaux sociaux ; mais là aussi il nous faut une réponse européenne face aux réseaux sociaux, ou au minimum franco-allemande. C'est donc un double appel à l'action que je veux lancer : les dangers sont profonds et réels.

Marc Hecker

J'aimerais, pour conclure, rebondir sur vos propos, et vous demander à tous deux ce que sont vos recommandations pour l'Europe sur ces problématiques liées au cyber.

L'Europe face aux menaces cyber

Thomas Gomart

Il y a urgence à distinguer les données couvertes par le RGPD de celles qui ne le sont pas. Jean-Louis Gergorin invitait à une réflexion franco-allemande en la matière, et je partage son point de vue. Une étude de l'Ifri publiée en juillet dernier montre aussi à quel point il y a débat entre experts pour savoir s'il faut privilégier le franco-allemand ou s'il faut intégrer ces questions dans le cadre plus traditionnel P3 : le débat n'est pas tranché, et il mériterait à mon sens d'être élargi à l'ensemble des pays européens. Il y a une certaine urgence à mieux définir les données, sans croire que le RGPD nous protège de tout.

Jean-Louis Gergorin

Ma recommandation touche à la politique industrielle et technologique. La semaine dernière j'ai eu le privilège d'être invité à une réunion organisée par l'Union européenne où il y avait des Britanniques de très haut niveau – dont le patron de l'Agence de cybersécurité britannique et son directeur technique, lequel a fait le seul rapport existant exhaustif sur Huawei et la 5G. Ce que j'en retiens, c'est que nous avons nous-mêmes créé nos propres problèmes, personne n'ayant réagi devant le *dumping* de Huawei. Il y a à Bruxelles un Commissaire à la concurrence, il y a une politique de la concurrence, mais personne ne s'est préoccupé du fait qu'un acteur jouissait d'une position dominante, alors qu'Alcatel par exemple a été éliminé, que Nokia a été affaibli, et Siemens sorti du business. Voilà un problème industriel face auquel l'Union européenne a été déficiente.

Par ailleurs, il faut savoir que l'Europe dépense beaucoup. Elle a dépensé pour la politique d'innovation depuis 1960 80 milliards en euros actuels, alors que la DARPA américaine a dépensé sur la même période seulement 60 à 65 milliards d'euros, mais est à l'origine de beaucoup de choses dans le domaine de l'Intelligence artificielle (Internet, microprocesseurs, etc.). Il faut mieux dépenser notre argent, et débureaucratiser. Une initiative a été lancée par un Franco-Allemand pour débureaucratiser l'innovation, avoir des structures rapides, et qui sortent des mécanismes paralysés que nous avons actuellement. Les industriels sont ravis d'avoir des subventions supplémentaires, mais ce n'est pas ça qui nous permettra de réinventer l'avenir. Il faut que l'on change de méthode, et que l'on adopte des méthodes plus souples : c'est le sens de cette initiative, que je voulais saluer.