Les représentations du cyberespace : un outil géopolitique

Alix Desforges[1]

Malgré une popularité croissante, le cyberespace reste un objet d'étude aux contours flous. Il n'y a pas une seule définition mais de multiples qui peuvent considérablement varier, y compris dans les milieux universitaires et militaires [Betz et Stevens, 2011]. L'acception la plus fréquente du cyberespace au sein du grand public est celle d'un synonyme de l'Internet. En revanche, dans les milieux universitaires et militaires, le cyberespace prend un sens plus opérationnel, sans pour autant faire l'objet d'un consensus. Le cyberespace est désigné tour à tour comme un *environnement* [Harknett *et al*., 2010], un *domaine* [Carr, 2009], un *théâtre d'opérations*, un *espace* [Kempf, 2012], un *substrat* [Demchack, 2012], un *milieu*, ou un *moyen* [*medium* dans le texte — Libicki, 2012]. Il est pourtant devenu un concept stratégique au plus haut niveau des États, utilisé dans le cadre de doctrines militaires et de négociations internationales même si, au sein d'un même État, ces définitions peuvent varier en fonction des entités.

Si l'Internet est aisément définissable et identifiable[2], le cyberespace apparaît plus englobant et plus virtuel. Il évoque tout à la fois un « monde » virtuel, dématérialisé, sans frontières, anonyme, de libertés, de partage et de communication, mais également un « espace » dangereux et nébuleux dans lequel des comportements réprimés en société peuvent s'exprimer sans répression. Certains y voient la promesse d'un accroissement de la démocratie, du progrès économique et d'un monde pacifié, mais il annonce aussi l'avènement d'une surveillance généralisée,

1. Chercheuse à la chaire Castex de cyberstratégie (Cercle des partenaires de l'IHEDN/ Fondation Airbus Group), doctorante à l'Institut français de géopolitique, université Paris-VIII.

2. Voir le lexique au début de ce numéro.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

un Big Brother ultime et un outil absolu pour le contrôle des foules et leur manipulation – une représentation réveillée par la publication des documents d'Edward Snowden quant aux pratiques de la NSA en matière de renseignement. Le cyberespace est empreint de représentations dont ces quelques exemples illustrent le fort antagonisme.

En dépit de la multiplicité des définitions, il est possible de noter des éléments communs. Tout d'abord, l'Internet. Il semble indispensable à l'existence même du cyberespace de par l'interconnexion mondiale des réseaux qui le génèrent. Ensuite, la majorité des définitions comporte une référence spatiale. Qu'il soit « espace », « monde », « milieu », « environnement », le terme cyberespace semble avoir une dimension géographique[3]. Malgré ces emprunts au vocabulaire géographique, le cyberespace ne constitue pas un espace géographique et ce n'est pas non plus un lieu, un milieu, un monde ou même un territoire. Pourtant, la représentation du cyberespace comme une entité spatiale semble particulièrement prégnante dans l'analyse des conflits pour son contrôle, sa maîtrise ou sa sauvegarde. Pour beaucoup de chercheurs[4], il s'agirait ainsi d'une entité à part, souvent qualifiée de « virtuelle », qu'il conviendrait de relier au « réel » pour analyser les conflits qui en découlent. Et, alors que le préfixe cyber- prolifère à travers l'ensemble de la littérature stratégique, il semble de plus en plus nécessaire de revenir sur cet « ensemble d'idées plus ou moins logiques et cohérentes » [Lacoste, 1995] associé au cyberespace et qui « décrit, exprime une partie de la réalité, de façon floue ou précise, déformée ou exacte » : les représentations. Car ces représentations sous-tendent des discours, justifient des actions, fédèrent ou au contraire divisent les acteurs du conflit.

Loin d'avoir pour ambition de proposer une définition du cyberespace, cet article a pour objectif de donner un aperçu des principales représentations dont il fait l'objet. Le cyberespace ne constitue pas à lui seul une seule représentation mais un système complexe de représentations qui s'enchevêtrent, s'agrègent et s'opposent. Il conviendra ensuite de les analyser afin de mesurer et comprendre leurs fonctions dans les rivalités de pouvoirs relatives au cyberespace. La mobilisation ou non de celles-ci dans le cadre de stratégies politiques, économiques et/ou militaires sera mise en lumière au travers d'exemples.

3. On retrouve notamment cette dimension géographique dans le champ lexical utilisé, un champ lexical essentiellement emprunté à la mer.

4. Voir les recherches menées en relations internationales par Joseph Nye (Cyberpower).

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

Cyberespace, un monde libre ?

En 1984, dans son roman *Neuromancien*, William Gibson décrit le cyberespace comme

> une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts des mathématiques... Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable. Des traits de lumières disposés dans le non-espace de l'esprit, des amas et des constellations de données. Comme les lumières de villes, dans le lointain... [Gibson, 1984].

Cet ouvrage de science-fiction fait partie d'un genre littéraire appelé « cyberpunk » dont Gibson est le fondateur. Ce genre littéraire décrit un monde violent, sombre, proche de l'apocalypse et où la technologie informatique et l'intelligence artificielle sont au cœur du fonctionnement de la société. Dans les années 1970 et 1980, l'émergence croissante de l'informatique réveille les angoisses d'une surveillance ultime, d'un Big Brother et du risque de voir un jour la machine dépasser l'homme. Le mouvement cyberpunk illustre parfaitement ces angoisses. Bien que marginal dans la littérature, il a influencé de nombreux domaines notamment dans les communautés du jeu vidéo, de la bande dessinée ou encore du cinéma. Ainsi, les travaux d'Alan Moore et David Lloyd, auteurs de la bande dessinée *V pour vendetta*, dont le masque fétiche du personnage principal représentant Guy Fawkes, est aujourd'hui la marque du mouvement Anonymous[5]. Au cinéma, son empreinte est présente dans plusieurs films qui ont connu un vif succès au moment de leur sortie en salles : *Matrix*, *Tron*, *Terminator*, etc. Comment ce terme, apparu au sein d'une communauté littéraire marginale, est parvenu à s'imposer en quelques années dans le vocabulaire quotidien et à s'imposer comme un concept stratégique ?

En 1948, lorsque le mathématicien Norbert Wiener crée la cybernétique[6] (mot qui inspira William Gibson pour créer le terme cyberespace), il s'inspire du mot grec *kubernetes* signifiant *pilote de navire* pour nommer la science dont il est le

5. Mouvement très hétéroclite né sur l'Internet, les Anonymous est un exemple de ce que l'on nomme « hacktivisme ». Ils sont l'auteur de plusieurs attaques informatiques utilisées à des fins de militantisme politique, économique et social. Ils défendent notamment une vision libertaire du cyberespace.

6. Science de l'action orientée vers un but, fondée sur l'étude des processus de commande et de communication chez les êtres vivants, dans les machines et les systèmes sociologiques et économiques (Larousse).

fondateur. De ce même mot sont également dérivés les termes *gouvernail*, *gouverneur* ou encore *gouvernement* qui revêt une signification très politique. D'ailleurs, de la cybernétique émerge une idée éminemment politique. Alors que la Seconde Guerre mondiale vient de s'achever, Wiener développe l'idée que l'information et la communication sont résolument nécessaires au fonctionnement de la société. Il écrit : « La communication est le fondement de la société et ceux dont le travail consiste à maintenir libres les voies de communication sont ceux-là mêmes dont dépend surtout la pérennité ou bien la chute de la civilisation » [Wiener, 1948].

Il s'agit d'une façon d'affirmer, par le biais d'une légitimation scientifique, que la démocratie constitue la meilleure forme d'organisation des sociétés humaines alors que la guerre froide en est à son commencement. La communication perçue comme une « valeur d'émancipation » et synonyme de libertés n'est donc pas née du développement de l'Internet. Dominique Wolton indique, dans son ouvrage *Internet et après ? Une théorie critique des nouveaux médias*, que l'association entre les notions de communication et de liberté débute dès la Renaissance. L'explosion des réseaux de communication, en particulier depuis l'avènement de l'Internet dans les années 1990, ne fait que renforcer cette représentation.

De *L'Homme numérique* [Negroponte, 1997] à *La Galaxie Internet* [Castells, 2002], les réseaux de communication constitueraient ainsi le moteur d'une nouvelle société, celle de l'information. Le passage d'une société qui serait non plus dominée par l'exploitation des matières premières (ère industrielle) mais par les technologies de l'information et de la communication fait d'ailleurs l'objet d'études académiques dès le début des années 1970[7]. Dans le monde politique aussi les conséquences des réseaux sur la vie quotidienne ont fait l'objet de nombreux rapports officiels (en France et à l'étranger) à partir des années 1990. L'explosion de la communication permettrait l'émergence de rapports sociaux plus égalitaires et pacifiés car plus directs et plus fluides. La démocratie en serait alors favorisée et enrichie. Dès 1968, Joseph Licklider et Robert Taylor, figures emblématiques du projet ARPANet[8] (précurseur de l'Internet), estiment que « les

7. Fondée en 1981, la revue *The Information Society Journal* lui est consacrée.

8. Un mythe commun admet que c'est l'exigence d'un réseau permettant d'assurer un commandement central y compris en cas d'attaque nucléaire sur le sol américain qui est à l'origine de la volonté de création d'ARPANet. Si la capacité de fonctionnement du réseau lors d'un endommagement d'une partie de celui-ci a été encouragée dans le développement d'ARPANet, c'est de la frustration des informaticiens qui souhaitaient avoir accès à des capacités de calculs plus importantes qu'est véritablement née l'idée de l'Internet. Il est certain que des militaires ont pu voir dans les recherches de l'ARPA sur la constitution d'un réseau non centralisé une opportunité de disposer d'un niveau moyen de commandement redondant. D'ailleurs, il semblerait que cette rumeur soit née après la publication d'une étude de la RAND Corporation sur

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

hommes communiqueront de façon plus efficace avec la machine qu'en face à face. Les individus en ligne seront plus heureux, car les gens avec lesquels ils interagiront auront été choisis. La communication sera plus effective et productive et donc plus agréable » [cités par Flichy, 2001]. Les nombreux écrits qui ont fleuri dans la presse sur le rôle primordial qu'auraient joué les réseaux sociaux dans les révolutions arabes ont illustré cet enthousiasme même si quelques voix se sont élevées pour corriger cette image.

La libre circulation de l'information et le principe de transparence qui en découle seront d'ailleurs l'une des volontés des concepteurs de l'Internet qui ont baigné dans l'atmosphère contestataire des campus californiens et le mouvement New Age des années 1960 et 1970 : « Un bon système doit être ouvert, c'est-à-dire transparent » [Breton, 2000]. À l'inverse, toute tentative de dissimulation et « toute volonté de cloisonner les systèmes » sont perçues comme une menace pour le bon fonctionnement du réseau, et au-delà de la société, car elles constituent une entrave à la libre circulation de l'information.

En fait, ce sont de nombreux marqueurs de la contre-culture américaine que l'on retrouve dans cette vision utopique du cyberespace : partage, gratuité, refus de l'autorité, etc. Mais l'impact de l'histoire américaine sur cette utopie est plus profond. La liberté d'expression vantée dans le cyberespace – caractéristique essentielle de son utopie – se trouve sacralisée à l'image des libertés publiques dans le premier amendement de la Constitution américaine. L'influence de ce contexte historique (influence de la construction politique des États-Unis) et géographique (la Californie des années 1960) spécifique atteint l'architecture même de l'Internet et son mode de fonctionnement : une architecture décentralisée et sans processus de contrôle.

Conséquence de la promotion d'une vision idéalisée du cyberespace, la société de l'information est portée en véritable projet politique. Al Gore, qui porta le projet des autoroutes de l'information (*Global Information Infrastructure*) aux États-Unis, déclara d'ailleurs devant l'Union internationale des télécommunications en 1994 :

> La *Global Information Infrastructure* (GII) ne sera pas seulement une métaphore de la démocratie en fonctionnement ; elle encouragera dans la réalité le fonctionnement de la démocratie en rehaussant la participation des citoyens à la prise de décision. Elle favorisera la capacité des nations à coopérer entre elles. J'y vois un nouvel âge athénien de la démocratie forgée dans les forums que la GII créera.

---

les possibilités d'échanges sécurisés en cas d'attaque nucléaire sur le territoire américain, qui évoque la piste d'ARPANet.

En France aussi, les responsables politiques développent des discours optimistes et militants pour le développement de cette société de l'information. Plusieurs rapports évoquant le sujet sont remis aux autorités publiques entre 1994 et 1997, témoignant de l'intérêt croissant des politiques pour ce sujet[9]. Dans un discours d'août 1997, Lionel Jospin, alors Premier ministre, explique à son tour :

> L'essor des nouveaux réseaux d'information et de communication offre des promesses sociales, culturelles et, en définitive, politiques. La transformation du rapport à l'espace et au temps qu'induisent les réseaux d'information permet des espoirs démocratiques multiples, qu'il s'agisse de l'accès au savoir et à la culture, de l'aménagement du territoire ou de la participation des citoyens à la vie locale[10].

Plus proche de nous, et même si dans les discours politiques l'accent est davantage mis sur les possibilités de développement économique (une préoccupation majeure en temps de crise économique), le développement des réseaux est toujours perçu comme « facteur d'égalité » et un « enjeu démocratique » selon les termes de François Hollande lors d'une allocution en février 2013 sur l'ambition numérique de la France.

À un discours aux accents prophétiques s'oppose une vision beaucoup plus pessimiste de ce monde virtuel. Au fantasme de rapports sociaux harmonieux permis par l'Internet répond la crainte que la technologie ne dépasse l'humanité et conduise à l'avènement d'un Big Brother ultime. Et ce ne sont certainement pas les révélations d'Edward Snowden à l'été 2013 qui auront fait taire ces craintes. Les pessimistes affirment que, loin de se montrer égalitaire, l'Internet contribuerait au renforcement des inégalités sociales existantes en permettant aux élites de renforcer leur domination. En d'autres termes, la « fracture numérique » persisterait, qu'elle soit territoriale, sociale ou générationnelle [Desforges, 2012].

La représentation d'un cyberespace généré par les infrastructures de communication comme espace de liberté, facteur de progrès économiques et sociaux et symbole même de la démocratie a été largement mobilisée dans le discours américain relatif à la gouvernance de l'Internet. La gouvernance de l'Internet est assurée par les différents acteurs impliqués dans son fonctionnement, c'est-à-dire non seulement les États mais également la société civile et le secteur privé. Certains États comme la Chine et la Russie militent pour voir le rôle des gouvernements

9. Le rapport Théry sur les autoroutes de l'information en 1994, le rapport Breton sur les téléservices en France en 1994, le rapport Miléo sur les réseaux de la société de l'information en 1996 et le rapport Martin/Lalande en 1997 sur l'Internet.

10. Discours M. Lionel Jospin, Premier ministre, sur les enjeux de l'entrée de la France dans la société de l'information, Université de la communication à Hourtin du 25 au 29 août 1997.

accru en souhaitant confier les rênes de l'Internet à l'ONU (où seuls les États sont représentés). En matière de gouvernance, les débats sont souvent résumés de façon dichotomique, opposant la représentation d'un cyberespace libre, comme aux États-Unis, aux pratiques de contrôle de l'information dans le cyberespace en vigueur en Russie et en Chine. La Conférence mondiale des télécommunications internationales, organisée par l'Union internationale des télécommunications à Dubaï en décembre 2012, en a été la parfaite illustration. Face aux déclarations russes en faveur d'une gouvernance de l'Internet gérée par l'ONU, les États-Unis ont su mobiliser cette vision libertaire du cyberespace pour maintenir le *statu quo* sur cette question alors même que leur rôle prédominant dans la gouvernance est de plus en plus critiqué, y compris par les pays de l'Union européenne[11]. Pourtant, pour Bertrand de La Chapelle, membre du conseil d'administration de l'Internet Corporation for Assigned Names and Numbers (Icann) qui gère les questions relatives à l'adressage et au nommage de l'Internet « [cette vision] est [...] erronée et simplificatrice » [de La Chapelle, 2012]. Elle est également dangereuse car elle revêt une « capacité autoréalisatrice » :

> La tension entre ces deux visions peut dégénérer en un nouvel affrontement géopolitique si les discours caricaturaux ne sont pas freinés et si l'accent n'est pas mis sur des objectifs au fond communs : généralisation de l'accès, préservation de l'interopérabilité globale et équilibre entre accès à l'information, protection de la vie privée et exigences de sécurité.

Cependant, grâce à cette simplification discursive mobilisant la représentation d'un cyberespace libre, cinquante-quatre pays (parmi lesquels les États-Unis, le Royaume-Uni et la France) ont refusé de signer le texte révisant le règlement des télécommunications internationales (RTI). Fleur Pellerin, ministre de l'Économie numérique, déclarait alors : « Internet est un bien commun, qui doit rester libre et ouvert. Nous ne pouvions pas signer un texte qui soulevait de telles inquiétudes auprès des organisations non gouvernementales et des acteurs du numérique[12]. »

La représentation d'un cyberespace comme espace de liberté a été dans ce cadre un outil puissant de la stratégie américaine pour mettre un frein aux velléités russes et chinoises de contrôle sur le réseau mais aussi pour conserver leur position dominante dans la gouvernance de l'Internet alors que celle-ci est de plus en plus critiquée. Cependant, la succession de révélations d'Edward Snowden quant aux pratiques du renseignement américain depuis le début de l'été 2013 a fortement

11. Voir les réactions suscitées par la fermeture de Megaupload en janvier 2012 sur une décision de la justice fédérale américaine.

12. Frédéric Bergé, « Le sommet de Dubaï entérine la fragmentation de l'Internet mondial », 17 décembre 2012, *01net*. <www.01net.com/editorial>

affaibli la portée de ce discours et de nouveaux acteurs, au premier chef le Brésil, comptent désormais s'attaquer avec détermination à la position des États-Unis.

Un territoire au-delà du réel ?

Cette représentation libertaire et utopique participe à faire de ce cyberespace une entité à part, souvent qualifiée de virtuelle. Pas de distance, pas de frontières, le cyberespace contribuerait à dissoudre « tout ce qui gêne : le territoire, les institutions, notamment l'État, et le corps physique » [Musso, 2003] et à l'avènement d'une entité hors du monde physique. Et malgré un discours niant *a priori* toutes les notions géographiques (sans frontières ni distance), on assiste à l'émergence d'une représentation spatialisée, voire territoriale dans certains cas, du cyberespace [Flichy, 2001].

Selon Yves Lacoste, le territoire désigne « l'étendue sur laquelle vit un groupe humain qu'il considère comme sa propriété collective ». Pour l'État, il s'agit de « la portion de l'espace terrestre délimitée par ses frontières et sur laquelle s'exercent son autorité et sa juridiction » [Lacoste, 2003]. S'il est établi que le cyberespace ne représente pas une portion de l'espace terrestre, il aurait néanmoins, pour des acteurs, certaines caractéristiques territoriales : une population (les internautes) et son propre mode de gouvernance (l'autorégulation). Au début des années 1990, cette représentation d'un cyberespace comme territoire est d'abord portée par les pionniers de l'Internet comme la représentation d'un espace indépendant, hors des lois du monde physique [Desforges, 2013].

La « déclaration d'indépendance du cyberespace[13] » rédigée en 1996 par John Perry Barlow, cofondateur de l'Electronic Frontier Foundation[14], est un élément manifeste de cette représentation. Cette déclaration consacre la liberté d'expression comme son principe fondateur et enjoint aux gouvernements « des pays industrialisés » de ne pas interférer dans les affaires de ce cyberespace. Dans cette représentation, le cyberespace devient un territoire à part entière. Si son auteur s'est depuis ravisé, ce texte fait partie des éléments constitutifs du processus de territorialisation du cyberespace et demeure une référence pour certains acteurs. Par exemple, le mouvement des Anonymous l'a reprise et modifiée en 2012, pour

13. Site internet : <https://projects.eff.org> (consulté le 27 mai 2012)

14. L'EFF, créée en 1990, est un important lobby pour la défense des « libertés dans le monde digital » aux États-Unis, selon leur site Internet.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

dénoncer les textes SOPA[15] et ACTA[16] sur le respect des droits d'auteur en ligne qu'ils jugent contraires à la liberté d'expression. Et, de façon générale, on observe de vifs débats au sein des démocraties (principalement aux États-Unis mais pas seulement) dès qu'il est question de liberté d'expression dans le cyberespace. Elle y est sacralisée sur le modèle de la Constitution américaine comme en témoigne la polémique créée en France par des propos homophobes, antisémites et racistes sur Twitter avec les hashtags[17] #simonfilsétaitgay, #unbonjuif et #simafillerameneunnoir à la fin de l'année 2012.

La représentation du cyberespace comme entité spatialisée réapparaît au début des années 2000 dans le discours des États-nations. Face aux développements des usages et à l'augmentation de la cybercriminalité[18] et des menaces, les États cherchent à affirmer leurs frontières et leur souveraineté dans cet *espace*. Il s'agit avant tout pour eux d'assurer la protection de leurs citoyens, la sécurité de leur territoire, la protection de leurs intérêts, mais, pour certains, il s'agit également de protéger leur régime politique *via* des mesures de contrôle et de surveillance. Le cyberespace représente pour les dirigeants des États un véritable défi car il vient remettre en question l'exercice de leur pouvoir et leur autorité. En outre, au-delà du monde civil, on observe plus récemment dans le monde militaire une certaine forme de spatialisation du cyberespace qui est considéré par plusieurs armées comme le cinquième domaine des opérations militaires après la terre, la mer, l'air et l'espace. S'il est mis sur le même plan que ces théâtres d'opérations, il faut toutefois noter qu'à la différence des autres il n'existe pas en dehors de l'action humaine. Les États-nations réactivent cette représentation spatialisée du cyberespace pour justifier le développement de leurs moyens d'action dans cet espace qui semble échapper à leur droit et leur souveraineté.

Plus largement, le secteur des télécoms est considéré par les États comme relevant des éléments essentiels de la sécurité du territoire, de l'indépendance nationale, du maintien de l'ordre ou encore de l'identité culturelle. Les États ont

15. *Stop Online Piracy Act* (SOPA) est une proposition de loi américaine visant à réglementer les droits d'auteur en ligne. À la suite de vifs débats et notamment d'un lobby des principaux fournisseurs de contenus américains, les discussions relatives à ce projet ont été suspendues.

16. *Anti-Counterfeiting Trade Agreement* (ACTA) est un accord international sur la propriété intellectuelle dont les droits d'auteur sur l'Internet.

17. « Suite signifiante de caractères sans espace commençant par le signe #, qui signale un sujet d'intérêt et est insérée dans un message par son rédacteur afin d'en faciliter le repérage. Son usage est particulièrement répandu dans les réseaux sociaux fonctionnant par minimessages » (FranceTerme).

18. La cybercriminalité désigne « l'ensemble des infractions pénales qui sont commises *via* les réseaux informatiques » (ministère de l'Intérieur).

d'ailleurs un rôle premier dans le développement des réseaux de télécommunication qui à leurs débuts sont très souvent impulsés par les États eux-mêmes.

Ces deux représentations spatialisées du cyberespace émergent et sont mobilisées pour des objectifs contradictoires. Elles s'affrontent et se confrontent d'ailleurs avec plus ou moins de radicalité. Elles légitiment des attaques informatiques (dans le cas des Anonymous), justifient le développement de moyens financiers, humains et techniques (pour les États) que certains dénoncent comme une militarisation du cyberespace, ou encore mobilisent des acteurs autour d'un projet (gouvernance de l'Internet). Mais, malgré les apparences, cette représentation spatiale du cyberespace n'est pas nouvelle. Les travaux de sociologues [Flichy, 2001 ; Musso, 2003] montrent qu'au-delà du cyberespace c'est dans la naissance du concept de réseau qu'il faut chercher les origines de cette représentation spatiale. Lorsque le concept de réseau émerge et devient une grille de lecture du monde à partir du XIX^{e} siècle, les réseaux techniques semblent dès lors constituer une nouvelle strate qui viendrait se superposer au territoire sur lequel ils sont installés et en modifierait le rapport espace/temps.

Comme le montre l'intérêt croissant des États pour la thématique, le cyberespace est perçu comme un facteur de risques et de menaces. Dès la fin des années 1990, et surtout à partir du milieu des années 2000 suite à l'intensification des attaques informatiques visant des États, ces derniers ont identifié la cybermenace comme relevant d'une question de sécurité nationale.

De la construction d'une cybermenace

En 1993, John Arquilla et David Ronfeldt prophétisaient que la cyberguerre arrivait [Arquilla et Ronfeldt, 1993]. S'ils ont fait figure de précurseurs, on assiste, depuis le milieu des années 2000, à la montée en puissance des discours étatiques concernant le cyberespace et ses menaces. Le cyberespace, identifié par les États comme « champ de confrontation » [Livre blanc sur la défense et la sécurité nationale, 2013], devient le vecteur de nouvelles menaces : les cybermenaces. Pourtant, tout comme celui de cyberespace, le terme cybermenace est relativement flou. Comme le note Myriam Dunn Cavelty, l'utilisation massive du préfixe cyber- (qui devient même parfois un adjectif en soi) consiste avant tout à désigner une action qui se fait par l'utilisation d'ordinateurs.

Le Livre blanc français de 2013 identifie trois types de cybermenaces : la cybercriminalité « qui ne relève pas spécifiquement de la sécurité nationale » ; « les tentatives de pénétration de réseaux numériques à des fins d'espionnage » ; et « les attaques visant le sabotage de systèmes d'importance vitale ».

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information, identifie quant à lui un quatrième type de menace : la déstabilisation conduite par des attaques de type défacement[19], déni de service[20] ou publication d'informations dérobées. Il indique que, « au même titre que les manifestations de rue, les attaques informatiques sont devenues un moyen d'exprimer une protestation[21] ».

Mais cette typologie est moins simple qu'il n'y paraît car la menace est protéiforme. Les mêmes techniques d'attaque pouvant être utilisées dans le cadre d'un acte cybercriminel ou d'une attaque à but d'espionnage. Ce caractère protéiforme de la menace ne facilite pas son appréhension, contribue un peu plus à en faire un objet aux contours flous et donc à produire des discours confus sur l'état de la menace. Car, malgré une intensification des attaques informatiques, peu nombreuses sont celles ayant eu des conséquences significatives du point de vue de la sécurité nationale, du moins parmi celles qui ont été portées à la connaissance du public.

Les pays les plus développés sont également les plus vulnérables de par la croissance des interconnexions des réseaux informatiques nécessaires à la vie de la nation. Considérés comme le « système nerveux » des États, les réseaux sont devenus un enjeu de premier plan pour ces derniers. Cette métaphore organiciste des réseaux n'est pas nouvelle et s'inscrit dans l'émergence du concept de réseau. « Symbole de circulation et de continuité, le réseau renvoie immédiatement à son contraire, la panne, l'arrêt, la crise, la saturation, le bouchon, le court-circuit, et finalement la mort » [Musso, 2003], comme en témoigne le vocabulaire – « virus », « antivirus », « ver ». Leur caractère *vital* renforce ainsi un peu plus le sentiment d'insécurité et légitime les politiques mises en place à l'échelle nationale pour assurer leur protection.

De nombreux États ont placé les questions de cybersécurité et de cyberdéfense au premier plan de leur agenda politique en les liant aux questions de sécurité nationale [Dunn Cavelty, 2008]. En France, le fait que le Livre blanc sur la défense et la sécurité nationale de 2008 place la sécurité des systèmes d'information au même niveau stratégique que la dissuasion nucléaire illustre l'importance prise par ces questions pour des décideurs stratégiques et politiques. Et, aux États-Unis, il

19. Le défacement consiste à modifier les pages d'un site pour faire apparaître une revendication.

20. Les attaques en déni de service consistent à rendre inaccessible un site Web en le saturant de requêtes.

21. Audition de M. Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information devant la Commission de la défense nationale et des forces armées de l'Assemblée nationale le 16 juillet 2013.

n'est pas rare d'entendre que le niveau de cybermenaces a désormais dépassé celui du terrorisme.

Un sentiment d'insécurité globale

L'aspect global et diffus de la menace contribue à renforcer le sentiment d'insécurité au sein des instances traitant de cette question. L'idée que la menace peut venir de partout et frapper n'importe qui, et qu'elle est peut-être déjà là sans qu'on le sache, produit un puissant sentiment d'insécurité permanente, d'autant plus qu'il est difficile d'identifier clairement l'ennemi (cybercriminels, groupes de hackers agissant à des fins politiques, entreprises, États, etc.).

L'asymétrie de cette menace décrite dans la majorité des ouvrages traitant de la question est un autre facteur de ce sentiment d'insécurité globale. Le fait qu'un adolescent du fond d'un garage puisse mettre à mal les systèmes d'un État ou d'une grande entreprise est une idée encore répandue dans le grand public. Et, comme le note très justement Olivier Kempf, « cette perception est renforcée par toute la littérature, écrite ou filmée, qui est pleine de ce genre de scénarios » [Kempf, 2012, p. 138]. Sans remettre en cause la possibilité d'une telle situation, il semble toutefois nécessaire d'en relativiser l'éventualité. En effet, des attaques informatiques capables de mettre à genoux tout un pays nécessitent d'abord un certain niveau de connaissances (planification, techniques d'attaque, enquête de terrain) et de moyens (humains, financiers, technologiques). Si certaines failles sont relativement faciles à exploiter, l'interconnexion des systèmes qui sont désormais de plus en plus complexes et de plus en plus protégés n'est pas de nature à faciliter une attaque d'envergure. Ainsi, le niveau de connaissances, l'organisation, les outils et les moyens nécessaires à la réalisation d'une telle attaque ne sont pas à la portée du premier venu. Olivier Kempf parle alors de « resymétrisation du cyberespace ». Toutefois, s'il semble évident que les investissements réalisés par les acteurs comme les États et les grandes entreprises participent à limiter à la fois le nombre et la portée des attaques informatiques réussies, ils semblent moins efficaces face aux attaques ciblées, aussi nommées *Advanced Persistent Threat* (APT). Avec des techniques aussi simples et simplistes que le *phishing*[22] ou une pièce jointe piégée dans un mail, les attaquants parviennent non seulement à pénétrer les systèmes des États et des grandes entreprises, mais souvent à y rester pendant plusieurs semaines voire des mois sans y être détectés. Ainsi, la « resymétrisation » induite par les progrès en matière de défense des systèmes d'informations trouve ses limites en matière de sensibilisation et dans les usages informatiques et Internet à ce jour.

22. Le *phishing* est une technique qui consiste à récupérer des identifiants et mots de passe.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

La prolifération d'une sémantique anxiogène

La difficulté d'appréhension de la menace s'illustre également à travers la prolifération lexicale constatée dans ce domaine. Tout est cyber-quelque chose et les nombreux désaccords de définitions témoignent des réelles difficultés, y compris pour les spécialistes, à caractériser clairement la menace. Les vifs débats autour du terme cyberguerre sont, à ce titre, symptomatiques de ces difficultés. Les frontières floues entre les différentes menaces contribuent à renforcer un peu plus ce brouillard sémantique et ont notamment pour conséquence de produire un discours aux accents catastrophistes. Comme le note Bertrand Boyer,

> entretenant les peurs et les craintes liées aux nouvelles technologies, jouant sur la confusion entre la guerre (entre États), la criminalité (fût-elle organisée) et la compétition économique, elles [les publications alarmistes] contribuent à l'enracinement de la croyance en une arme absolue capable d'offrir une réponse à tout type d'attaque [Boyer, 2012].

En outre, de nombreuses références à des événements historiques particulièrement anxiogènes sont également utilisées par les politiques mais aussi certains experts pour désigner ces menaces. Le recours à des expressions comme « Cyber Pearl Harbor » ou « 11 Septembre numérique » contribue ainsi un peu plus à entretenir le sentiment d'une insécurité globale. Si ces expressions concourent à la sensibilisation de l'opinion publique aux enjeux de cybersécurité et de cyberdéfense, elles pourraient également créer une attente des populations à de fortes réactions en cas d'attaque et contribuer à l'escalade des tensions. L'agitation de cette représentation permet cependant de justifier politiquement l'augmentation constante des moyens humains et financiers dévolus à ces questions dans un contexte marqué par les restrictions budgétaires. Jean-Yves Le Drian, ministre de la Défense, annonçait au dernier Forum international sur la cybersécurité, en janvier 2014, la mise en place d'un « plan Défense cyber » d'un budget d'un milliard d'euros en arguant que « devant des menaces majeures, qui peuvent aller jusqu'à de véritables actes de guerre, militaires ou non directement militaires, il y a un enjeu de premier ordre pour la défense, la souveraineté et la sécurité de notre nation[23] ». Cette surenchère dans le discours sert également les intérêts des industriels du secteur (grands groupes comme PME) qui s'installent sur un marché particulièrement florissant. Pour Guy Anderson, analyste chez Jane's IHS, « la cybersécurité est perçue comme un bateau de sauvetage pour l'industrie

23. H. Meddah, « Au FIC, Le Drian soigne sa cyberdéfense », *L'Usine digitale*, 22 janvier 2014.

quand les dépenses de défense baissaient fortement dans les pays occidentaux[24] ». Aussi les principaux industriels de défense ont-ils diversifié leur offre de biens et services vers des produits de cybersécurité notamment par le rachat d'entreprises spécialisées.

Conclusion

Le terme cyberespace n'est pas neutre. Il véhicule plusieurs représentations dont certaines, contradictoires, sont à l'origine de plusieurs conceptions du cyberespace retranscrites notamment dans les stratégies des États. Ces représentations deviennent alors un véritable outil géopolitique. Certains États, dont la Russie, ont d'ailleurs choisi dans leur stratégie de ne pas utiliser le terme de cyberespace pour lui préférer le concept d'« espace informationnel ». Le recours à un concept plus large permet à la Russie d'aller au-delà même du cyberespace pour permettre un contrôle sur l'information de façon globale et sans distinction du vecteur par lequel celle-ci est distribuée. Sans être un territoire à part, les acteurs des conflits du cyberespace le considère souvent comme un monde virtuel (en opposition au réel) généré par l'interconnexion des réseaux. Mais les conflits géopolitiques dont le cyberespace est l'objet et/ou le vecteur n'en sont pas moins réels et sont le reflet de rivalités de pouvoir existantes par ailleurs. Il s'agit avant tout d'une nouvelle forme d'expression des conflits.

Bibliographie

ARQUILLA J. et RONFELDT D. (1993), « Cyberwar is coming ! », *Comparative Strategy*, vol. 12, n° 2, p. 141-165.

BETZ D. et STEVENS T. (2011), *Cyberspace and the State, Toward a Strategy for Cyberpower*, The International Institute for Strategic Studies, Routledge, Londres.

BOYER B. (2012), *Cyberstratégie : l'art de la guerre numérique*, Nuvis, Paris.

BRETON P. (2000), *Le Culte de l'Internet. Une menace pour le lien social ?*, La Découverte, Paris.

DE LA CHAPELLE B. (2012), « Gouvernance Internet : tensions actuelles et futures possibles », *Politique étrangère*, *Internet : outil de puissance,* n° 2/2012, Institut français des relations internationales, Paris, p. 250.

DESFORGES A. (2012), « Internet : un nouveau monde interactif et libre ? », *L'Atlas des utopies*, hors-série *Le Monde-La Vie*, p. 160-161.

24. « La cybersécurité devient un secteur stratégique pour l'industrie de la défense », LaTribune.fr, 8/03/2012.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

DESFORGES A. (2013), « Les frontières du cyberespace », *in* GIBLIN B. et DOUZET F. (dir.), *Des frontières indépassables ?*, Armand Colin, Paris.
DUNN CAVELTY M. (2008), *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age*, Routledge, Abingdon.
FLICLY P. (2001), *L'Imaginaire d'Internet,* La Découverte, Paris.
GIBSON W. (1984), *Neuromancien*, La Découverte, Paris.
KEMPF O. (2012), *Introduction à la cyberstratégie*, Economica, Paris.
LACOSTE Y. (2003), *De la géopolitique aux paysages, dictionnaire de la géographie*, Armand Colin, Paris.
LACOSTE Y. (dir.) (1995), *Dictionnaire de géopolitique*, Flammarion, Paris.
MUSSO P. (2003), *Critique des réseaux*, PUF, Paris.
WIENER N. (1948), *Cybernetics or Control and Communication in the Animal and the Machine,* John Wiley, Oxford.