Chapitre 21

Le cyberespace, un champ d'affrontement géopolitique

Bien loin du pacifique village global rêvé par les utopistes au tout début de l'Internet, le cyberespace est désormais perçu à la fois comme une menace et une ressource dans la plupart des conflits géopolitiques contemporains. Pour les armées de nombreuses nations, dont la France, il est même devenu un enjeu stratégique majeur et un champ de confrontation à part entière. Cette représentation laisse peu de place à la vulnérabilité, pourtant intrinsèque au cyberespace, et encourage le renforcement des capacités défensives et le développement d'un véritable arsenal offensif et de commandements militaires spécialisés.

Or le cyberespace représente un véritable défi stratégique. Contrairement aux autres domaines militaires que sont la terre, la mer, l'air et l'espace, ce milieu, né de l'interconnexion globale des systèmes d'information et de communication, n'est pas un milieu naturel. Il est entièrement façonné par l'homme et surtout en reconfiguration rapide et permanente. C'est donc un domaine difficile à appréhender et encore plus à représenter, en raison de sa géographie complexe et changeante, et pour part intangible. On ne sait pas encore très bien ce qu'est un terrain militaire dans le cyberespace, et il n'existe pas vraiment de cartes d'état-major du cyberespace.

C'est aussi un milieu dans lequel les paradigmes stratégiques classiques comme la dissuasion, la riposte, l'anticipation ou encore le contrôle des armes ne sont pas directement transposables, en raison de ses spécificités propres. Les cyberattaques sont particulièrement difficiles à anticiper, à détecter, à attribuer, à contrer, à qualifier et à décourager. La réponse stratégique ou tactique est ainsi particulièrement complexe à élaborer et à mettre en œuvre, tout comme la coopération internationale dans la résolution des crises et la conduite des opérations militaires.

Le cyberespace présente de nouvelles menaces sécuritaires mais aussi de nouvelles opportunités (surveillance, espionnage, manipulation de l'information) pour les États comme pour les groupes non étatiques, les dissidents, les criminels, les entreprises, les individus. Les activités transfrontières

qu'il facilite représentent un défi à l'exercice des pouvoirs régaliens par les États, confrontés à un enchevêtrement de juridictions qui contraint leur action. Enfin et surtout, les enjeux politiques, économiques, militaires et démocratiques sont complètement entremêlés et difficilement dissociables car les réseaux sont partagés entre la société civile, les gouvernements et les entreprises[1]. La rupture stratégique est telle qu'elle oblige à adapter les règles d'application du droit international et repenser les cadres de la sécurité collective.

Jusqu'à récemment, ces questions, perçues comme très techniques, étaient aux mains d'une communauté d'experts de culture scientifique. Les révélations en cascade sur les pratiques offensives des États, notamment par Edward Snowden à partir de juin 2013, et la multiplication de cyberattaques de plus en plus sophistiquées et médiatisées les ont fait entrer avec fracas dans la sphère politique, médiatique et stratégique. La prolifération des conflits géopolitiques pour, dans et par le cyberespace, rend sa compréhension désormais incontournable dans l'analyse des conflits du monde contemporain.

Qu'est-ce que le cyberespace, la cyberguerre, les cyberconflits ? Quels en sont les ressorts et les enjeux ? Comment assurer la sécurité collective à l'ère des réseaux informatiques ?

Cyber quoi ? Le grand brouillard sémantique

Le terme de brouillard est souvent utilisé pour désigner le cyberespace et reflète bien le flou qui entoure les définitions multiples que l'on peut en trouver, et que l'avènement du *cloud* ne manque pas d'épaissir. Le Pentagone a proposé pas moins d'une douzaine de définitions au cours des dernières années, avant de recruter une équipe de chercheurs qui a mis un an à en élaborer une, si sophistiquée que personne ne l'utilise[2].

Il est en effet difficile d'englober dans une seule définition les différentes dimensions que le terme recouvre, et dont la combinaison rend le cyberespace si unique.

Le cyberespace est d'abord et avant tout un environnement d'information créé par l'interconnexion planétaire des systèmes d'information et de communication, où les données sont créées, stockées et surtout partagées entre des utilisateurs. Il désigne à la fois l'infrastructure matérielle à la source de cet environnement, soit les différents éléments qui composent l'Internet, et l'espace immatériel où circulent les flux de données, les informations, les

1. Pour un panorama plus complet des enjeux, voir « Cyberespace : enjeux géopolitiques », *Hérodote*, n° 152-153, 2014.
2. Singer P. W. et Allan Friedman, 2014, *Cybersecurity and Cyberwar*, Oxford, Oxford University Press, p. 13.

idées, les interactions entre les personnes qui sont derrière les ordinateurs. Le cyberespace, c'est ainsi à la fois l'Internet, un réseau de réseaux informatiques, et l'espace d'information et de communication qu'il génère entre des individus de toutes nations, à une vitesse quasi instantanée qui bouleverse le rapport à la distance[1].

Pour en faciliter la compréhension, on offre souvent une représentation simplifiée en trois couches. La couche physique, appelée aussi couche inférieure, comprend l'infrastructure matérielle qui est à la base de l'Internet, le gigantesque réseau de réseaux informatiques : les câbles de fibre optique, les routeurs, les serveurs, la technologie cellulaire, les satellites, les ordinateurs personnels, smartphones, tablettes et autres objets connectés. Cette couche matérielle est ancrée dans le territoire et répond aux contraintes de la géographie physique et politique; on peut relativement aisément la cartographier. La deuxième couche est la couche logique (ou syntaxique), qui comprend les services (protocoles, programmes, applications) qui permettent d'assurer la transmission des données entre deux points du réseau et donc de faire voyager l'information jusqu'à son destinataire, en conservant son intégrité. Or les routes empruntées par les données changent tout le temps dans un système totalement décentralisé et ultra-dynamique, mais aussi non sécurisé et manipulable. Sa cartographie est particulièrement complexe mais néanmoins instructive (voir les travaux de Dyn Research et CAIDA). La troisième couche est la couche sémantique ou cognitive, appelée aussi couche supérieure. C'est l'espace de l'information, des réseaux sociaux, des discussions et des échanges instantanés dans le monde, c'est aussi l'espace de l'influence, de la propagande et de la guerre informationnelle.

Mais le cyberespace, c'est aussi une métaphore puissante, qui fait l'objet de représentations géopolitiques profondément contradictoires : celle, issue de la littérature de science-fiction, pensée dès 1984 par le romancier William Gibson et formulée par les pionniers de l'Internet, d'un territoire indépendant, libre de contraintes et de régulations, qui véhicule un idéal de démocratie, à préserver de l'ingérence des États; ou celle d'un territoire de menaces et d'opportunités, un champ de bataille pour les États, un territoire à maîtriser, à contrôler et dans lequel il faut positionner ses forces voire « planter son drapeau[2] ».

Comprendre les représentations qui sous-tendent l'usage des métaphores est essentiel à l'analyse des stratégies des acteurs et des dynamiques de conflit. Or l'usage à profusion du préfixe « cyber » devant toutes sortes de termes – tout comme les amalgames et analogies hasardeuses qui

1. Douzet Frédérick, 2014, « La géopolitique pour comprendre le cyberespace », *Hérodote*, n° 152-153.
2. Dossé Stéphane, 2010, « Vers une stratégie de milieu pour préparer les conflits dans le cyberespace ? », *DSI*, n° 59.

fleurissent bon train dans les discours politiques et les médias – n'aide pas à dissiper le brouillard, bien au contraire. Il peut masquer la réalité des enjeux, en conférant un caractère virtuel à des menaces ou des actions qui sont bien réelles, même si elles opèrent *via* des réseaux informatiques.

Les chercheurs et experts sont partagés sur l'usage même du terme cyberguerre. Dans son ouvrage *Cyber War Will Not Take Place* (2013), Thomas Rid dénonce son usage abusif, rappelant les trois caractéristiques qui permettent de qualifier une guerre. Elle doit être violente, donc impliquer l'usage de la force, elle doit potentiellement causer des morts, et elle doit être instrumentalisée à des fins politiques. Or l'analyse des principales cyberattaques connues montre qu'elles se résument essentiellement à des actes de sabotage, d'espionnage et de subversion. Et malgré la surenchère alarmiste dans la dénonciation du risque de cyberterrorisme, de Pearl Harbor numérique ou de cyber-Armageddon, force est de constater que les cyberattaques n'ont, à ce jour, directement tué personne.

D'autres arguent cependant qu'il ne s'agit que d'une question de temps avant qu'une cyberattaque majeure puisse causer des morts et être qualifiée d'acte de guerre. Et beaucoup soulignent que la cyberguerre a déjà commencé, alors que les capacités cyber sont utilisées en appui d'autres moyens pour mener des opérations militaires. Or, si les opérations menées par les États dans le cyberespace flirtent parfois avec les limites de la déclaration de guerre (voir Stuxnet contre les centrales nucléraires iraniennes), elles sont pour l'instant restées sous le seuil de son déclenchement qui, comme nous le verrons, reste à définir.

Les États-Unis, mais aussi la France, la Grande-Bretagne et d'autres ont néanmoins déclaré qu'une cyberattaque majeure pourrait être considérée comme un acte de guerre et justifier une réponse par tous les moyens nécessaires, y compris les armes conventionnelles. Une telle situation reste inédite. Mais les formes et les contours de la guerre évoluent, et le terme « cyberguerre » recouvre souvent une acception bien plus large, dont l'anglais permet d'exprimer la nuance (*cyberwarfare*). Il englobe généralement toutes les actions menées *via* les réseaux informatiques, potentiellement combinées avec d'autres moyens d'action, dans le cadre de conflits géopolitiques plus ou moins ouverts, entre des acteurs étatiques et/ou non étatiques. La notion de cyberconflit est encore plus large, puisqu'elle désigne selon Daniel Ventre toute forme de conflit qui « s'exprime de façon totale ou partielle dans le cyberespace, qu'il s'y déroule ou l'utilise comme un véhicule[1] ».

Depuis la fin des années 2000, les incidents cyber se multiplient et prennent de l'ampleur (Estonie en 2007, Géorgie en 2008, Stuxnet en 2010, Saoudi Aramco en 2012), alors que l'expansion rapide et continue des

1. Ventre Daniel, 2012, *Cyber Conflict. Competing National Perspectives*, Londres, Wiley-ISTE, p. 77.

systèmes d'information et de communication accroît la surface d'attaque des États qui prennent de plus en plus conscience de leurs vulnérabilités et du risque complexe auxquels ils font face.

Les menaces pour les États dans le cyberespace

Dans le cyberespace, non seulement les États, mais aussi des individus, des groupes politiques, des organisations criminelles ou des terroristes peuvent s'emparer de technologies qui sont largement accessibles et à faible coût pour mener à distance différents types d'opérations. Ces technologies renforcent ainsi le pouvoir des petits acteurs, qui nourrit l'idée d'une menace asymétrique, diffuse et imprévisible. Mais elles renforcent aussi le pouvoir des États.

Les protagonistes peuvent perturber les instruments de communication et d'information d'un État ou d'une armée pour entraîner des dysfonctionnements, les rendre inopérants, empêcher l'accès à des ressources ou manipuler l'information. Ils peuvent aussi saboter des installations, des armes voire des infrastructures critiques, avec des conséquences potentiellement dramatiques ; espionner pour obtenir un avantage stratégique ou préparer une future attaque ; influer sur l'opinion ou les troupes (opérations psychologiques, propagande, campagnes de dénigrement, déni de service, défacement) ; mobiliser et recruter à des fins politiques (terrorisme, subversion, levée de fonds, coordination d'actions).

En 2007, des attaques massives en déni de services (DDoS) ont paralysé les serveurs des banques, médias, sites gouvernementaux et autres services publics de l'Estonie, suscitant une prise de conscience générale. Menées en représailles suite au déplacement d'un monument à la gloire de l'Armée rouge du centre-ville vers la périphérie de Talinn, ces attaques peu sophistiquées qui consistent à lancer de multiples requêtes simultanées afin de saturer les serveurs, émanaient de hackers patriotes russes, fort probablement soutenus par le gouvernement russe qui a toujours nié toute implication. La plupart des États ont alors réalisé qu'ils étaient mal préparés face à ce nouveau type de menaces et ont développé des cyberstratégies et des capacités pour répondre aux vulnérabilités créées par leur dépendance croissante aux systèmes d'information et de communication.

Pour autant, les attaques les plus sophistiquées et les plus difficiles à prévenir et détecter émanent principalement des États, qui disposent, pour les plus avancés, des ressources techniques, financières et humaines pour les concevoir et les mener à bien. En 2012, le *New York Times* révélait les détails de l'attaque Stuxnet, un virus informatique très sophistiqué lancé en 2010 afin de ralentir secrètement le programme nucléaire iranien qui

n'était pourtant pas connecté à l'Internet, ce qui a nécessité le recours à du renseignement et des moyens humains. Élaboré par les services américains, en collaboration avec les services israéliens, le virus s'est accidentellement retrouvé sur l'Internet où les entreprises de cybersécurité ont tôt fait d'identifier sa mission. L'une des conséquences inattendues de cette arme d'un nouveau genre est la prolifération de cyberarmes de moindre intensité, dérivées des techniques rendues publiques de Stuxnet. Les organisations criminelles ont ainsi récupéré et adapté des technologies sophistiquées développées par un État qu'elles utilisent à leur profit ou au service d'autres États ou acteurs commanditaires. Dans le cyberespace, l'arme peut parfois se retourner contre l'État qui en est à l'origine.

L'attaque Stuxnet est souvent considérée comme le premier acte connu de cyberguerre, en raison de la nature de son action (sabotage) et son attribution à un acteur étatique. Sorte de troisième voie entre une diplomatie coercitive et une attaque armée, ce sabotage d'un nouveau genre hors du cadre des conflits armés n'a pas fait l'objet de représailles immédiates mais a encouragé l'Iran à déclarer mettre sur pied une « cyberarmée », soit à développer des capacités offensives. Depuis, les révélations d'Edward Snowden ont montré l'étendue des activités offensives des États-Unis et l'ampleur inégalée de leur arsenal.

D'autres États sont connus pour mener des actions offensives de grande envergure *via* les réseaux informatiques, aux premiers rangs desquels la Chine, Israël, la Russie, l'Iran et la Corée du Nord. Dès 2007, les Israéliens auraient ainsi hacké le système de défense aérien de la Syrie, préalablement à une série de bombardements. En 2008, un an après les attaques contre l'Estonie, des attaques ciblées contre les serveurs de la Géorgie précèdent l'intervention armée russe.

La « guerre *cool* » entre les États-Unis et la Chine

La Chine, en particulier, a fait l'objet d'accusations virulentes d'abord par le Congrès américain et la presse – notamment autour de la publication du très médiatisé rapport Mandiant qui révélait l'intrusion non détectée depuis des mois de hackers chinois dans les systèmes informatiques de multiples entreprises et médias américains –, puis directement par le président Barak Obama à partir de 2013. Les accusations d'espionnage et de vol de propriété intellectuelle ont conduit à une escalade des tensions entre les deux pays, avec la mise en examen par la justice américaine de cinq officiers de l'armée chinoise et la suspension, en représailles, du groupe de travail bilatéral sur les questions cyber par le régime chinois pendant près de deux ans. Les analogies historiques ont fleuri dans les médias et les

discours stratégiques, produisant un nouveau concept de « guerre *cool* », une lutte silencieuse faite d'attaques de basse intensité dont le double sens du terme « *cool* » suggère qu'elle est moderne et relativement détendue, « fraîche » plutôt que froide et « branchée » nouvelles technologies.

Dans le but d'assurer son développement économique et la modernisation de son armée, la Chine mène de longue date une stratégie d'acquisition tous azimuts de l'information de haut niveau scientifique, technologique, économique, politique et stratégique. Elle exploite de plus en plus à ces fins toutes les ressources du cyberespace, avec des attaques très nombreuses et souvent peu sophistiquées qui laissent des traces visibles, même si elles tardent parfois à être détectées. En 2015, les États-Unis ont accusé la Chine d'avoir piraté l'agence de gestion du personnel (Office of Personnel Management) et volé les données de 4,5 millions d'employés américains, alors que des hackers chinois déclaraient par ailleurs avoir volé des informations stratégiques dans le secteur de la défense américaine.

Bien qu'elles engendrent des tensions géopolitiques au plus haut niveau, ces attaques ne relèvent en rien d'actes de guerre. Pourtant, dans le but de dramatiser les enjeux et faire pression sur la Chine, l'administration Obama crée une sérieuse ambiguïté en qualifiant l'espionnage chinois de menace sur la sécurité nationale, et en liant souvent dans le même discours l'espionnage et le risque de cyberattaque sur les infrastructures vitales des États-Unis. Or une telle attaque est fortement improbable, étant donné l'interdépendance économique entre les deux pays et les risques de représailles encourus par la Chine. Ce lien discursif ajoute à la confusion des enjeux et dessert l'argument principal des États-Unis dans le bras de fer avec la Chine.

L'administration américaine insiste en effet sur la distinction entre espionnage stratégique – qui est légitime – et le vol de propriété intellectuel et de secret des affaires donnant un avantage compétitif sur le plan économique, qui est illégal aux États-Unis et contraire aux règles du commerce. De son côté, la Chine ne reconnaît pas une telle distinction – qui est justement difficile à défendre si l'on estime que l'espionnage économique est une question de sécurité nationale – et nie toute implication dans l'espionnage en général. Elle dénonce les capacités technologiques très supérieures des États-Unis et les attaques multiples dont elle fait l'objet de la part de la NSA, s'appuyant sur les révélations de Snowden.

Mais la montée en puissance de la Chine dans le cyberespace inquiète les puissances occidentales. En 2010, la Chine a détourné vers son territoire plus de 15 % des routes mondiales de l'Internet pendant 18 minutes en 2010, un « *traffic hijacking* » qui pourrait être le résultat d'une erreur ou bien une démonstration magistrale de ses capacités. Elle investit massivement dans les hautes technologies et la recherche sur l'Internet du futur, avec comme ambition de devenir une puissance d'innovation. Avec près

de 700 millions d'internautes, la Chine entend se positionner comme une grande puissance du cyberespace et revendique sa place dans les négociations sur la gouvernance de l'Internet, l'application du droit international au cyberespace et l'adaptation des normes de sécurité collective.

L'exploitation du cyberespace par les stratèges russes

Les Russes ont démontré un véritable savoir-faire dans la manipulation des outils cyber et une certaine maturité dans leur intégration à leur stratégie politique, économique et militaire. Ils seraient passés maîtres dans l'art de la guerre hybride, qui combine la guerre conventionnelle, le recours aux opérations spéciales, la guerre informationnelle et les cyberattaques. Lors de l'intervention en Ukraine en 2014, les services russes auraient utilisé leur excellente connaissance des réseaux pour infiltrer les systèmes d'information et de communication et récolter des informations stratégiques. Ils sont soupçonnés par le gouvernement ukrainien d'être à l'origine des pannes de courant qui ont plongé 700 000 foyers de l'ouest de l'Ukraine dans le noir en décembre 2015, après que des *malwares*[1] ont été retrouvés dans le réseau d'alimentation électrique[2]. Si elle est avérée, cette attaque serait une première du genre.

En octobre 2015, des navires russes ont été repérés à plusieurs points du globe manœuvrant à proximité des câbles sous-marins qui transportent l'essentiel du trafic Internet, suscitant la nervosité des militaires et officiers du renseignement américains qui redoutent une attaque sur ces infrastructures critiques[3] en cas de tensions ou de conflit ouvert[4]. Les officiels américains ont coutume de saluer les compétences techniques russes en matière offensive en disant : « Tout ce qu'on sait faire, les Russes savent le faire aussi[5]. » Les attaquants russes seraient particulièrement habiles pour masquer leurs traces et développer un arsenal très sophistiqué (techniques d'intrusion, virus, outils de chiffrement et de déchiffrement, etc.).

1. *Malware* ou logiciel malveillant : il existe un très grand nombre de logiciels malveillants, le ver informatique, le virus, le cheval de Troie en sont des exemples. Ils ont pour but d'infiltrer un ordinateur ou un réseau afin d'entraver son bon fonctionnement ou d'en prendre le contrôle (Desforges A., Déterville E., 2014, « Lexique sur le cyberespace », « Cyberespace : enjeux géopolitiques », *Hérodote*, n° 152-153, p. 24).
2. L'enquête est encore en cours. Voir : www.voanews.com/content/russia-suspected-in-first-ever-cyberattack-on-ukraine-power-grid/3135485.html
3. Une infrastructure critique ou vitale est une infrastructure identifiée par l'État comme essentielle à la vie de la Nation (ex. : réseaux de distribution d'énergie, d'eau, infrastructures de santé, finances, etc.).
4. Sanger David E., Schmitt Eric, 2015, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort", *The New York Times*, 25 octobre.
5. Assertion répétée en diverses occasions dans les meetings de haut niveau.

Mais c'est d'abord et avant tout l'héritage soviétique en matière d'organisation humaine et d'art de la manipulation psychologique qui distingue les offensives russes dans le cyberespace.

Les attaques émanent ainsi rarement directement des agents qui s'abritent derrière des « proxies » qui mènent les attaques pour leur compte, à savoir des hackers individuels ou appartenant à des groupes organisés de type mercenaires ou mafias. Si certains recherchent le profit, beaucoup sont aussi animés de motivations politiques et idéologiques et se considèrent comme des « hackers patriotes. » L'attaque contre l'Estonie en 2007 a ainsi été revendiquée un groupe de jeunes pro-Kremlin – revendication qui reste invérifiable – lié à l'organisation « Nashi », créée par Vladimir Poutine mais financée par des entrepreneurs russes et indépendante du gouvernement[1].

Les hackers russes utilisent des techniques d'« ingénierie sociale » particulièrement sophistiquées pour mener à bien leurs attaques. Elles consistent par exemple à récolter des informations sur une personne par des voies multiples (sources ouvertes, renseignement, socialisation au club de gym ou *via* les réseaux sociaux), puis la manipuler pour arriver à pénétrer un réseau ou un ordinateur. La plus grande vulnérabilité des systèmes est souvent le facteur humain. Les attaquants réussissent à se faire passer pour quelqu'un ou usent d'astuces psychologiques pour gagner la confiance d'un utilisateur et le pousser à cliquer sur une pièce jointe contenant un malware, insérer une clé USB infectée dans son ordinateur ou révéler ses codes d'accès.

Enfin, ces techniques s'insèrent dans une approche beaucoup plus globale du cyberespace, où la guerre d'influence fait rage. Contrairement aux pays européens, la Russie – comme la Chine d'ailleurs – a développé ses propres réseaux sociaux et moteurs de recherche qui proposent des contenus politiques, culturels et linguistiques à destination de la Russie et son étranger proche, reconstituant ainsi dans le cyberespace la zone d'influence soviétique[2]. Le pouvoir russe mène des opérations d'influence et de propagande particulièrement poussées afin de dérouter ses ennemis, discréditer ses adversaires et susciter l'adhésion populaire à ses opérations militaires et politiques.

1. www.wired.com/2009/03/pro-kremlin-gro/ et Kévin Limonier, intervention à Milipol 2015.
2. Limonier Kévin, 2014, « La Russie dans le cyberespace : représentations et enjeux », *Hérodote*, n° 152-153.

Des liens complexes entre le public et le privé

Les opérations offensives susceptibles de dégénérer en conflit ouvert ne se limitent toutefois pas aux actions entre États, car le secteur privé est omniprésent dans le cyberespace. Et c'est sans doute là un changement de paradigme essentiel dans le domaine de la défense. Les opérateurs privés ont développé et possèdent l'essentiel de l'infrastructure de l'Internet. Près de 90 % des ordinateurs dans le monde opèrent sous un système développé par Microsoft, qui se trouve, de fait, un opérateur clé pour détecter le trafic suspect, prévenir et contrer les attaques. Mais surtout, la surface d'attaque ne cesse d'augmenter en raison de la dépendance croissante aux réseaux informatiques et les vecteurs d'attaques sont bien trop nombreux pour que les États puissent faire face seuls. Ils s'appuient de plus en plus sur le secteur industriel pour développer les techniques, les outils mais aussi les services pour défendre leurs systèmes et leurs infrastructures vitales, majoritairement opérées par le secteur privé.

Les réseaux informatiques sont partagés entre les militaires, les civils et les entreprises, et les mêmes techniques peuvent servir à des attaques stratégiques comme à de l'espionnage économique ou de la criminalité. Le nombre de cyberattaques est en expansion continue et les services de l'État sont dépassés par le nombre. Ils concentrent leurs investigations sur les attaques qui visent des cibles sensibles ou utilisent les techniques les plus sophistiquées, et qui produisent un impact majeur avec un effet stratégique. Les partenariats entre les secteurs public et privé sont donc essentiels pour défendre efficacement le territoire.

Le secteur privé développe aussi des outils offensifs (exploits, outils de surveillance, etc.), que les États acquièrent mais que les entreprises utilisent aussi parfois pour défendre plus agressivement leurs réseaux. La difficulté à protéger les données personnelles des cyberattaques et prévenir le vol de propriété intellectuelle ou le secret des affaires a ouvert la voie à tout un marché lucratif de la cyberdéfense « active », une version plus musclée de la cybersécurité aux contours flous à en juger par la prolifération de définitions contradictoires. D'après les enquêtes menées auprès des entreprises, la pratique du « *hack back* », qui consiste à retourner l'arme contre l'adversaire pour identifier l'attaquant et répondre, serait courante, même si elle est illégale dans la plupart des pays. Les pratiques des États évoluent également dans un sens où la distinction entre les pratiques défensives et offensives s'estompe au profit de l'objectif final de sécurité.

La complexité des liens public-privé dans le domaine est particulièrement bien illustrée par le problème de l'exportation des technologies de surveillance intrusive. Développées par le secteur privé, ces techniques sont utilisées par une multitude d'acteurs (gouvernements, entreprises, individus, groupes politiques) pour collecter des données personnelles sur

l'Internet. Un rapport de l'Union européenne souligne les risques d'abus, une fois que ces technologies auront franchi les frontières de l'UE et donc sa zone de juridiction[1]. Elles font aussi l'objet de discussions dans le cadre des Accords de Wassenaar de 1996 sur la réglementation des exportations d'armes conventionnelles et des biens et technologies à double usage.

Enfin, le secteur privé est non seulement une ressource mais aussi une cible dans les attaques entre États. Le gouvernement américain anticipait depuis des années le risque d'une attaque sur des sites gouvernementaux ou des infrastructures vitales. L'offensive contre Sony Pictures en novembre 2014, attribuée par le FBI à la Corée du Nord, est arrivée comme une surprise monumentale[2]. Il a d'ailleurs fallu plusieurs semaines à la Maison Blanche pour qualifier l'attaque contre l'industrie majeure du divertissement comme un acte de « cybervandalisme », un terme à consonance plus dramatique que « cybercrime » mais qui reste sous le seuil de la guerre. Le président Obama a toutefois déclaré en personne que cette attaque majeure conduirait à des représailles, dont certaines seraient visibles et d'autres non. L'Internet coréen a par la suite subi une coupure de plusieurs heures, une démonstration de force claire, bien que non revendiquée par les États-Unis.

Ce cas illustre l'extrême entremêlement des enjeux. S'attaquer à des infrastructures critiques très bien protégées demande des ressources importantes. Cibler une entreprise comme Sony Pictures ou TV5Monde est beaucoup plus abordable pour une multiplicité d'acteurs et peut provoquer un retentissement médiatique planétaire au service d'un effet stratégique. Les entreprises sont ainsi soumises à des risques de criminalité, d'espionnage ou de sabotage de la part de tous types d'acteurs, y compris des États. Elles peuvent être la cible de rivalités de pouvoir géopolitiques (attaques, dénigrement, terrorisme) et subir par ailleurs les dégâts collatéraux des pratiques ou des politiques gouvernementales, notamment la perte de confiance de leurs utilisateurs liées à la surveillance intrusive. La gestion du risque cyber pour les entreprises doit ainsi s'inscrire dans une approche globale du risque, qui inclut le risque géopolitique. Pour les États, la surface d'attaque n'en est que plus importante, d'autant que ces attaques peuvent émaner non seulement d'acteurs étatiques mais aussi d'acteurs non étatiques, dont le comportement est d'autant moins prévisible.

1. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-12-15_Intrusive_surveillance_EN.pdf

2. L'entreprise a subi un piratage massif qui nécessité de lourdes interventions sur ses systèmes d'informations. Elle a assisté impuissante à la divulgation de données personnelles et de conversations électroniques sensibles qui ont conduit sa vice-présidente à la démission et ses personnels à une *class action* (recours collectif). En raison de menaces terroristes, elle a renoncé à la sortie en salle du film *The Interview*.

Menace asymétrique et acteurs non étatiques

L'exemple le plus déroutant de ces nouveaux défis pour les États est peut-être l'utilisation du cyberespace par Daech. Les terroristes n'attaquent pour l'instant pas les infrastructures critiques dans le but de causer des morts civils, ce qui n'exclut pas qu'ils y viennent un jour. Ils privilégient pour l'heure des modes d'action qui requièrent moins de moyens et offrent, quasiment à coup sûr, un fort impact médiatique. Cela ne signifie pas qu'ils soient dénués d'intérêt ou de compétences pour le cyberespace. Le groupe Daech en a au contraire démontré une grande maîtrise des codes, des techniques et des usages.

Le groupe terroriste utilise le cyberespace pour diffuser de la propagande sur les réseaux sociaux par des vidéos très travaillées qui s'inspirent de la scénographie hollywoodienne et donnent l'illusion de ses moyens techniques et financiers[1]. Les scénaristes de la propagande manient le *teasing* comme dans les séries télévisées et usent habilement de la violence pour créer l'effet surprise, le choc et la sidération de leur public. Les réseaux sociaux sont l'instrument privilégié pour pousser les jeunes à la radicalisation puis les recruter, en détournant les outils de communication et de marketing développés à des fins commerciales. L'organisation repère les jeunes intéressés et influençables puis entre en contact avec eux *via* Facebook ou d'autres réseaux sociaux pour les convertir à sa cause et organiser leur départ vers la Syrie. Les réseaux servent aussi à lever des fonds ou planifier des opérations. Le groupe aurait recruté des centaines de professionnels bien formés (reporters, infographistes, *community managers*, reporters, etc.) qui constituent l'élite de l'organisation et seraient payés jusqu'à 7 fois plus que les soldats, d'après les interrogatoires menés auprès de certains prisonniers comme Abu Hajer ou Abu Abdullah al Maghribi[2]. Le dispositif de propagande serait constitué de 36 agences autonomes coordonnées depuis le QG de Raqqa.

Cette menace est particulièrement complexe à contrer pour les États[3]. Il est très difficile de savoir d'où part la propagande, où sont les individus et les serveurs impliqués et donc qui, quand, comment et où frapper pour être efficace, sans se tromper de cible et sans plonger dans le noir les services de renseignement qui opèrent *via* les réseaux. Les blocages techniques des sites qui diffusent des vidéos terroristes ou la suppression des comptes

1. Bonifait Bastien, Douzet Frédérick, 2015, « Propagande de l'État islamique, une stratégie médiatique efficace », *Revue de Défense nationale*, 19 novembre (http ://fr.calameo.com/read/000558115fab11dd04042) ; Bonifait Bastien, *L'utilisation du cyberespace par l'E.I., une menace et un défi pour les démocraties européennes à travers l'exemple français*, Mémoire de Master 2, IFG Paris 8 (disponible sur : www.cyberstrategie.org) ;
2. TTU, Lettre d'informations stratégiques et de défense, n° 1000, 9 décembre 2015 ; Winter Charlie, 2015, *The Virtual « Caliphate » : Understanding Islamic State's Propaganda Strategy*, Quilliam.
3. Douzet Frédérick, 2016, « Le cyberespace, troisième front de la lutte contre Daesh », *Hérodote*, n° 160, 1er trimestre.

Twitter propagandistes se révèlent d'une efficacité très limitée en raison de la capacité d'adaptation rapide dont font preuve les terroristes : ils recréent des comptes sur lesquels ils migrent avec leurs abonnés, passent par des réseaux chiffrés et anonymisés et utilisent de multiples relais de diffusion qui débordent les capacités de traitement des services. Les données permettant l'identification et la localisation des protagonistes, voire leur inculpation, lorsqu'elles sont traçables, sont pour l'essentiel entre les mains des plateformes privées de réseaux sociaux (Twitter, Google, Facebook), principalement américaines. La collaboration avec les plateformes est cruciale pour traquer les terroristes, récolter des preuves mais aussi lutter contre la propagande.

Comment contrer la diffusion de la propagande dans le cyberespace ? Comment tirer partie des opportunités qu'offre l'espace numérique pour traquer les terroristes et les neutraliser, mais aussi pour prévenir la radicalisation des jeunes susceptibles de se retourner contre leurs concitoyens ? La distinction entre la menace intérieure ou extérieure devient de plus en plus complexe. Ces menaces nécessitent une approche globale qui implique une coopération poussée entre les gouvernements à l'échelle internationale, mais aussi au sein des gouvernements, et avec les acteurs privés et la société civile, ce qui nécessite une réelle évolution de la culture et des pratiques de bien des services étatiques de sécurité et défense.

Coopération internationale et prévention des conflits

Face aux acteurs non étatiques et au risque d'escalade des conflits liés à un incident cyber, les États ont besoin de renforcer la coopération internationale et de redéfinir les cadres de la sécurité collective. Le centre d'excellence de l'OTAN de Tallinn est le centre névralgique de la réflexion juridique sur droit international et cyberespace. La plupart des États, y compris la Chine et la Russie, reconnaissent désormais que le droit international s'applique au cyberespace. Mais les modalités sont toujours en discussion.

Un premier manuel assez controversé, publié en 2013 par un groupe d'experts du centre, expose un certain nombre de recommandations tout en laissant ouvertes quelques questions cruciales : quel est le seuil au-delà duquel une cyberattaque peut être considérée comme un acte de guerre ? Qu'est-ce qu'une contre-mesure dans le cyberespace ? Qu'est-ce qu'une attaque armée ? Le droit international s'applique-t-il en cas de cyberattaque majeure en temps de paix ?

De nombreuses spécificités du cyberespace rendent les mécanismes et principes du droit international complexes à mettre en œuvre, comme par exemple la responsabilité de l'État pour fait internationalement illicite et la

légitime défense. Ainsi, l'attribution n'est pas toujours possible à effectuer ou prouver, ce qui rend souvent impossible l'imputation d'un acte à un État et par conséquent l'engagement éventuel de sa responsabilité. De même, la difficulté à prévoir l'effet d'une contre-mesure dans le cyberespace et ses éventuels dégâts collatéraux rend difficile le calcul de la proportionnalité de la réponse. Et la qualification d'une cyberattaque en attaque armée, qui justifierait la légitime défense, n'est pas simple. La réponse par des moyens conventionnels à une cyberattaque comporte par ailleurs de sérieux risques d'escalade des conflits, ce que nombre d'experts extérieurs ont souligné. Ce premier document a toutefois eu le mérite de lancer la discussion, et de démontrer qu'il ne fallait pas la laisser exclusivement aux mains des juristes.

Le groupe des experts gouvernementaux de l'ONU (UN GGE) a publié en juillet 2015 un rapport de consensus sur une série de normes de comportement responsables des États dans le cyberespace, ainsi que des mesures de confiance, des engagements de coopération internationale et des principes d'applicabilité du droit international[1]. Malgré les difficultés inhérentes à sa mise en œuvre, ce texte représente une véritable avancée dans les discussions, d'autant qu'il réunit 20 pays dont les plus grandes puissances du cyberespace comme les États-Unis, la Chine, la Russie, la France, l'Allemagne et le Royaume-Uni[2]. Parmi les principes importants, les États se sont notamment mis d'accord sur le fait qu'ils ne devaient pas utiliser les technologies d'information et de communication (TIC) pour endommager volontairement des infrastructures vitales. Ils ne doivent pas attaquer directement ou indirectement les équipes d'intervention d'urgence en informatique (Computer Emergency Response Teams CERT/CSIRT). Le rapport stipule également que les États doivent respecter les résolutions de l'ONU sur les droits de l'homme et les libertés fondamentales sur Internet. Les États ont également pris des engagements en termes d'assistance mutuelle, d'échange d'information et de renforcement de leurs capacités pour améliorer la sécurité de leurs systèmes.

Le rapport rappelle les principes du droit international que les États signataires reconnaissent, notamment le principe de souveraineté de l'État dans le cyberespace et la non-intervention dans les affaires d'autres États, qui est un enjeu crucial pour la Chine et la Russie qui défendent le principe de contrôle souverain des données et de l'information dans leurs efforts diplomatiques. En revanche, bien que le document souligne le droit inhérent des États à prendre des mesures en accord avec le droit international et le respect de la charte de l'ONU, il n'évoque pas explicitement le droit à la « légitime défense ». La délégation chinoise s'y est opposée, elle a dénoncé dans les négociations le risque de militarisation du cyberespace et la

1. www.un.org/ga/search/view_doc.asp ?symbol=A/70/174
2. Le rapport de 2013 avait permis d'établir que le droit international s'appliquait au cyberespace, ce qui a constitué le point de départ des discussions suivantes.

nécessité d'encourager un règlement pacifique des conflits. La Chine a d'ailleurs signé avec la Russie en mai 2015 un « cyber pacte » de non-agression. Cet accord est un peu paradoxal de la part de deux pays qui dénoncent de concert la militarisation du cyberespace et se défendent d'y mener des actions offensives.

L'effet de surprise est toutefois venu du « cyber pacte » entre les États-Unis et la Chine, négocié au plus haut niveau lors de la visite du président Xi Jinping aux États-Unis en septembre 2015. Les tensions étaient alors à leur comble, l'administration américaine avait clairement laissé entendre que des sanctions pourraient être prises contre les entreprises chinoises qui avaient bénéficié de cyberespionnage aux dépens des entreprises américaines. Le régime chinois a dépêché un envoyé de haut niveau, Meng Jianzhu, responsable de la sécurité de l'État, pour des négociations en urgence en amont de la visite du président Xi.

L'accord comprend deux engagements de bonne conduite et la création de nouveaux mécanismes de coopération bilatérale. Les deux États s'engagent à coopérer lorsqu'une requête d'assistance est formulée pour contrer une activité malveillante sur leur territoire respectif. Ils s'engagent également à ne pas commettre ou soutenir sciemment, par des moyens cyber, de vol de propriété intellectuelle, secrets commerciaux ou autres données économiques confidentielles dans le but de procurer à leurs entreprises un avantage compétitif. À ces fins, un mécanisme de dialogue bilatéral de haut niveau sera créé pour lutter contre la cybercriminalité et assurer le suivi des demandes d'entraide, accompagné d'une hotline pour prévenir les risques d'escalade d'incidents cyber. Un groupe d'experts de haut niveau sera également constitué pour dialoguer sur les normes de comportement responsable des États dans le cyberespace.

Ce pacte constitue une avancée importante dans la régulation des activités des États dans le cyberespace et l'amélioration de la coopération internationale pour lutter contre la cybercriminalité. Il vise à encourager la retenue dans les activités offensives et la mise en place des mécanismes de dialogue pour prévenir l'escalade des conflits entre États. Il reste à voir, toutefois, quelles seront les mesures effectivement prises et le comportement des autorités chinoises. Les obstacles restent importants de part et d'autre. Comme nous l'avons vu, les Chinois refusent d'opérer une distinction entre espionnage stratégique et espionnage économique (vol de données et propriété intellectuelle) et le président Obama a clairement laissé entendre que l'option des sanctions restait ouverte si les pratiques chinoises ne correspondaient pas à l'esprit de l'accord. En matière d'assistance mutuelle, les Chinois déplorent souvent que les Américains refusent de partager des informations sensibles dans leurs requêtes d'assistance. Le rejet par les États-Unis de requêtes chinoises d'assistance liée au contrôle des contenus sur le web pourrait aussi poser problème. Enfin, la mise en œuvre de la

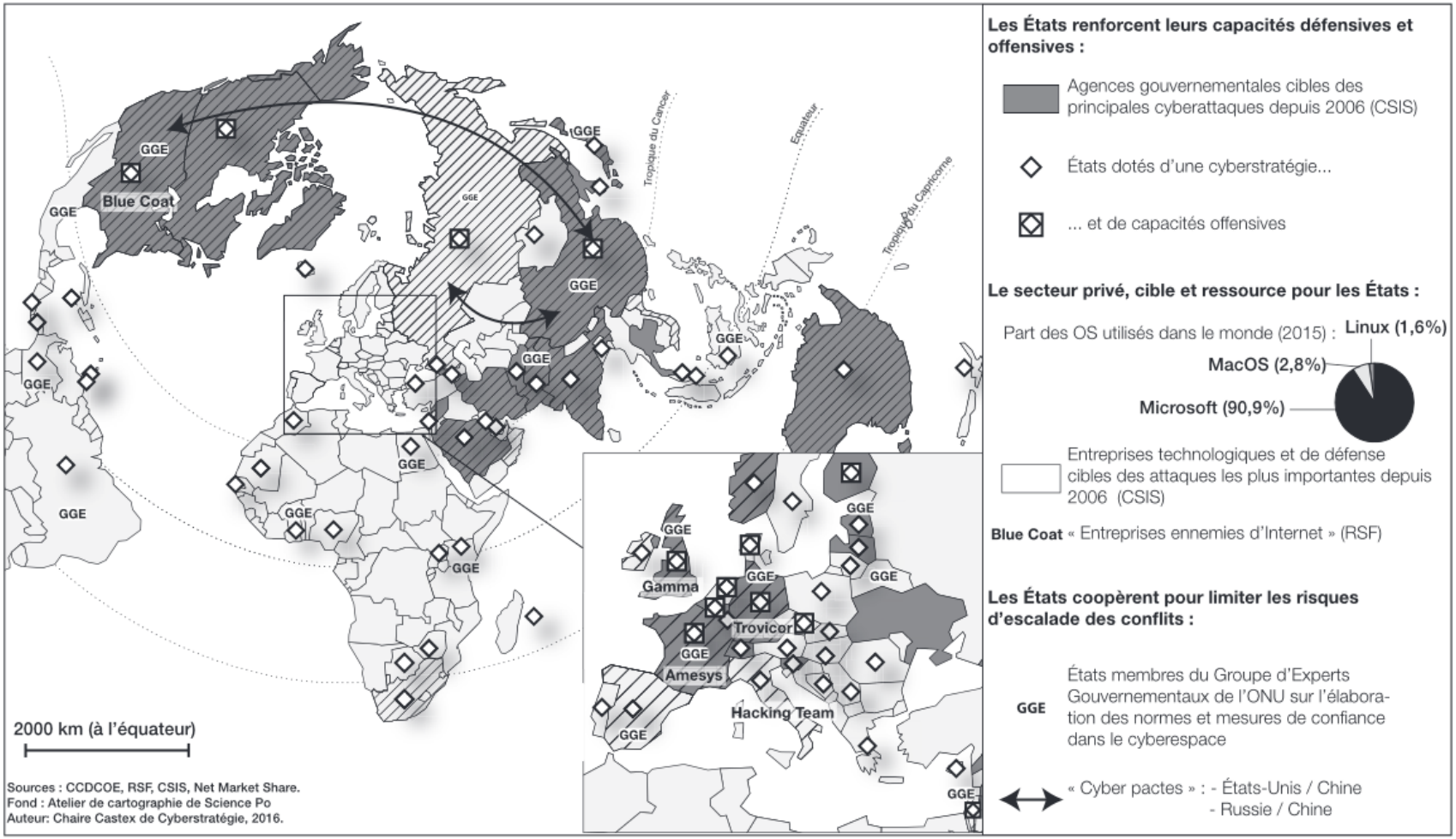

Figure 25 Le cyberespace, un champ d'affrontement géopolitique

hotline nécessitera que les deux pays, aux larges bureaucraties, puissent faire fonctionner efficacement leur processus interministériel.

Les discussions autour des normes de comportement responsables des États sont limitées par les difficultés inhérentes à l'environnement du cyberespace. L'application de nombre de ces règles est difficile – parfois impossible – à vérifier, ce qui peut faire douter de leur valeur. Bien des questions de définitions et de terminologie restent entières. Elles nécessitent d'être abordées en gardant à l'esprit que la technique évolue très vite et qu'elles doivent être suffisamment précises pour être utiles mais suffisamment flexibles pour ne pas être trop vite obsolètes. Ces discussions sont néanmoins indispensables car si ces normes non contraignantes n'empêcheront jamais personne de les transgresser, elles guident l'action des États et assurent un minimum de prévisibilité de leur comportement, ce qui peut réduire les risques pour la paix et la stabilité internationales.

Conclusion

Le cyberespace est ainsi devenu un champ d'affrontements géopolitiques mais aussi un vecteur d'attaque et d'influence, et même un enjeu de ces conflits. Il est essentiel de retenir qu'il ne s'agit pas d'un territoire virtuel mais bien d'une dimension nouvelle des conflits géopolitiques. Les cyberconflits et la cyberguerre ne se déroulent pas en dehors du contexte géopolitique de leurs protagonistes. Ils résultent de l'action des êtres humains pris dans des rivalités de pouvoir sur leur territoire, qui utilisent le cyberespace comme outil de puissance tout en s'exposant à ses vulnérabilités.

La plupart des conflits ont aujourd'hui une dimension cyber en raison de l'omniprésence des systèmes informatiques interconnectés dans tous les outils de nos sociétés, tous les équipements de nos armées et dans tous les aspects de notre vie sociale, économique et politique. Pour comprendre les conflits dans le monde, il est dès lors indispensable pour les géographes de se forger une culture sur les questions cyber, car elles occupent une place de plus en plus grande dans tous les conflits géopolitiques et deviennent partie prenante de l'analyse géographique. Mais il est aussi indispensable d'étudier la géographie du cyberespace et les dynamiques spécifiques des cyberconflits comme un champ d'études à part entière, malgré les multiples défis techniques et méthodologiques auxquels il faut faire face, car c'est désormais un domaine hautement stratégique.