PROGRAMME ASIE

LA CYBERSÉCURITÉ GLOBALE ET LA GUERRE FROIDE 2.0

Par EMMANUEL MENEUT /

Maître de conférences dans les Universités catholiques

SEPTEMBRE 2021

ASIA FOCUS #166

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

La critique du paradigme libéral de J. Mearsheimer en 2018 dans son ouvrage *The Great Delusion : Liberals Dreams and International Realities* et la réponse en 2020 de J. Ikenbery avec son livre *A World Safe For Democracy, Liberal Internationalism and The Crisis of Global Order* (qui inspire la nouvelle administration Biden) s'accordent sur la séquence historique du « Siècle américain, 1917–2017 ». Les États-Unis émergent comme une grande puissance dans une société internationale multipolaire à partir de 1917 avec leur engagement dans la Grande Guerre, la mise en place d'un premier ordre libéral à travers la Société des Nations et la prévalence du Droit sur la force. L'isolationnisme américain et l'échec de cet ordre en 1939 ont convaincu les États-Unis en 1945 d'être une superpuissance désormais « responsable » du nouvel ordre international bipolaire, c'est-à-dire concernée par le maintien de l'équilibre stratégique. Mais, en parallèle de cette posture « réaliste » pendant la guerre froide et jusqu'en 1991, le bloc de l'Ouest s'est développé en termes d'interdépendances économiques sous le leadership de la superpuissance américaine. Cette croissance peut être appréhendée comme un second ordre libéral limité géographiquement. Après l'effondrement de l'Empire soviétique, la société internationale est devenue unipolaire et cet ordre libéral a été globalisé jusqu'en 2017 sous la direction de l'hyperpuissance américaine hégémonique. Plus précisément, les consommateurs profitaient de la délocalisation des usines, les entreprises profitaient de la conquête de nouveaux marchés à l'étranger et l'outil diplomatico-militaire américain fournissait la sécurité requise par ces interdépendances économiques étendues à l'ensemble des pays membres des Nations unies, y compris pour les « régimes illibéraux ». Le fil conducteur de cette chronologie est la définition classique d'une puissance comme étant un pays dont l'économie est capable de produire et d'exporter des biens et des services à travers des chaines de valeurs globalisées. Cependant, cette puissance devient « responsable » au sein de la société internationale lorsqu'elle est aussi capable de fournir la sécurité requise par ces chaines de valeurs. Par exemple en 2003, lorsque les militaires ont proposé à G. W. Bush une cyberattaque de certaines banques abritant les avoirs de S. Hussein, le président fut dissuadé par Wall Street de porter atteinte à la crédibilité des institutions financières qui sont un levier essentiel de la politique étrangère. Les sanctions unilatérales prises contre l'Iran par le président Trump[1] en sont l'illustration. Ainsi, le concept que nous allons étudier est celui d'une « puissance responsable », telle un

1. Richard CLARK, *Cyber war : the next threat to national security and what to do about it*, HarperCollins, 2010, p. 320

fournisseur de sécurité pour les biens et les services qu'elle produit et exporte. Dans le contexte actuel d'affirmation de la puissance technologique chinoise, ce rôle de fournisseur de sûreté et de sécurité de services, notamment dans le secteur digital, induit une reconfiguration des alliances et des relations internationales. En effet, la dualité civile et militaire de la technologie numérique conduit à la constitution de pôles de cyberpuissances et non pas à l'accroissement de leur interdépendance. Le mécanisme d'équilibre des puissances est de nouveau activé d'une façon similaire au début de la guerre froide, mais avec des caractéristiques propres : l'émergence de l'entreprise digitale comme acteur central de la sûreté et de la sécurité d'un pays et donc de son statut de puissance responsable. La globalisation comme conjonction de la diffusion des valeurs libérales, de l'intensification des interdépendances et du développement des organisations internationales qui assurait le succès du processus de paix démocratique devient caduque dès lors que les acteurs de la société civile doivent s'articuler avec les intérêts de leur État de référence. Selon J. Mearsheimer, si la nécessité de la survie de l'État s'étend aux acteurs de la société civile, cela rend impossible cette conjonction centrale du modèle libéral.

LES CARACTÉRISTIQUES DE LA CYBERSÉCURITÉ

Les menaces sur les infrastructures en réseau ne sont pas nouvelles. Dès les années 1960, le réseau téléphonique aux États-Unis faisait l'objet de menaces de coupure généralisée. Cependant, la numérisation de toutes les infrastructures d'une société systématise cette typologie de menaces et accroit le couplage entre les entreprises et l'État. La connectivité de toutes les infrastructures et des objets les plus courants (voiture autonome) ou les plus spécifiques (centrifugeuse pour l'enrichissement d'uranium de la centrale de Natanz) conduit à un nouveau défi pour la société internationale : la cybersécurité globale.

La continuité du spectre sécuritaire et le couplage État/entreprise

Dans la théorie de la firme classique, nous avons la définition d'un acteur de la société civile, l'entreprise qui intervient sur un marché en concurrence avec d'autres entreprises. Les biens produits et les services fournis par une entreprise peuvent n'avoir aucun impact en cas de dysfonctionnement. Ils sont simplement inutilisables, mais sans conséquence sur l'utilisateur. Les dysfonctionnements sont sans gravité et de plus très rares. L'entreprise n'a donc pas besoin de mettre en place des processus spécifiques dont la

structure de coût n'est pas couverte par le revenu de ses ventes. Au début de l'ère automobile, il n'y avait qu'un seul modèle de couleur noire la Ford T, son moteur « increvable », sa robustesse légendaire sur tous les types de routes et de chemins de terre, ainsi que son carburateur polyvalent pour tous les types de carburants disponibles (y compris l'alcool) ont fixé les attributs des produits de la révolution industrielle. Il n'y avait pas d'enjeux en termes de sécurité ou de sûreté.

Toujours dans le cas où les impacts sur le client sont faibles, si la récurrence des dysfonctionnements est importante, l'entreprise peut mettre en place un processus d'assurance qualité qui rend possible l'amélioration du produit ou du service et sa commercialisation. C'est le cas du secteur automobile avec l'introduction par les constructeurs japonais des méthodes de Edwards Deming et Taiichi Ohno qui donneront l'organisation du progrès permanent de la qualité des voitures (le kaizen) des marques telles que Toyota. En effet, en 1989, une enquête conduite par le MIT sur les facteurs de compétitivité des constructeurs automobiles déclenche un voyant rouge au tableau de bord des entreprises américaines : les indicateurs concernant les processus d'études et de fabrication font apparaitre des écarts pouvant aller jusqu'à un facteur 2 entre les constructeurs japonais et américains et explique ainsi la domination du marché par les entreprises japonaises. La structure de prix peut alors augmenter, justifiée par la qualité du produit ou du service, afin de couvrir la nouvelle structure de coûts. Le prix pourra ensuite diminuer grâce à la conquête de nouvelles parts de marché.

Cependant, d'autres dysfonctionnements peuvent avoir un impact sérieux sur les utilisateurs. Mais, la rareté de leur occurrence rend possible leur commercialisation par une entreprise dès lors que celle-ci met en place des processus de sécurité qui rendent acceptable le risque encouru par les clients. C'est par exemple le cas des acteurs du secteur de l'énergie nucléaire ou du transport automobile. Dans les années 1960, l'avocat Ralph Nader met en cause[2] les négligences de l'industrie automobile dans la problématique croissante de la mortalité routière, ce qui conduit à la mise en place d'une loi sur la sécurité routière en 1966 contraignant les constructeurs automobiles, notamment avec le retrait du modèle Corvair de General Motors jugée trop dangereuse. La production de cette sécurité augmente de façon structurelle les coûts de conception/fabrication, ce qui conduit l'entreprise à la nécessité d'accroitre significativement sa part du marché pour assurer sa profitabilité. Cela se traduit par la structure oligopolistique du marché automobile. C'est aussi le cas par exemple du secteur nucléaire et du transport aérien. Les processus de sécurité requièrent généralement un processus d'assurance qualité comme préalable.

2. En 1965, Ralph Nader publie son livre *Unsafe at any speed* d'enquête sur les pratiques de disqualification des automobilistes dans les accidents alors que les voitures sont en cause.

Enfin, si l'impact d'un dysfonctionnement est grave pour le client et si sa fréquence est significative, aucune entreprise ne pourra envisager de produire ses biens ou ses services très longtemps sans une intervention significative de l'État qui imposera une réglementation pour ce type d'activité avec des impôts ou des taxes pour assurer son financement. L'entreprise sera obligée de produire des biens ou des services conformes à la réglementation étatique. C'est la nécessité du bien ou du service qui justifie en dernière instance une telle activité. On retrouve dans ce domaine la plupart des activités régaliennes fournies par l'État dont le transfert à une entreprise soulève de nombreux problèmes en termes de rentabilité et de confiance des citoyens. L'État produit cette confiance à travers la mobilisation de ressources spécifiques dans un cadre réglementaire propre, c'est la sûreté. L'obligation de résultats peut parfois conduire à invoquer la sûreté de l'État pour recourir à des moyens exceptionnels, par exemple après les attaques terroristes du 11 septembre aux États-Unis. Ce sont les services de renseignements américains et les forces armées qui luttent quotidiennement contre les réseaux djihadistes qui rendent possible l'activité des compagnies aériennes. Les aéroports et les compagnies collaborent aussi étroitement pour partager l'information avec les services étatiques. Les entreprises et l'État articulent de fait la circulation du renseignement sur le risque encouru et la neutralisation de la menace. La sûreté s'appuie aussi sur les processus de sécurité et de qualité.

La digitalisation des infrastructures et des objets de la société avec la généralisation de la menace cyber établit une continuité entre les préoccupations de qualité, de sécurité et de sûreté et la nécessaire articulation entre les acteurs concernés : les entreprises et l'État. Les voitures connectées qui seront commercialisées dans un futur proche devront nécessairement être résilientes aux cyberattaques et l'État devra contribuer significativement à la sûreté des infrastructures qu'elles utilisent. Le concept de cyberattaque a émergé après la première cyberguerre contre l'Estonie en 2008. Selon l'OTAN et son manuel de Tallin, une cyberattaque est une opération dans le cyberespace dont la conséquence probable est susceptible de blesser ou de tuer des personnes, ou d'endommager ou de détruire des biens. Cette définition recouvre les notions de qualité, de sécurité et de sûreté. Ainsi, une entreprise ne peut pas fournir des services via le cyberespace sans l'appui de l'État.

Le large éventail des cybermenaces et l'émergence de la Chine

La loi des réseaux qui établit que la valeur d'un objet connecté est directement proportionnelle au nombre d'utilisateurs connectés conduit nécessairement à une

interconnectivité généralisée des réseaux. Cependant, cette justification économique de l'interconnectivité a pour conséquence que l'ensemble des objets connectés sont des cibles potentielles. Ainsi, les Américains ont découvert que les chargeurs rapides pouvaient être facilement transformés en incendiaires. Un chargeur rapide fonctionne avec un petit logiciel (firmware) qui échange des données avec l'appareil connecté pour être chargé (voiture électrique, vélo électrique, smartphone, Personal Electronic Device, etc.) Ces paramètres permettent au chargeur de calculer la vitesse optimale de la charge de la batterie de l'appareil connecté. Le piratage d'un smartphone ou d'une voiture électrique permet de transmettre au logiciel du chargeur des données fausses et son calcul va le conduire à délivrer une puissance électrique supérieure à ce que la batterie peut absorber, ce qui provoquera son embrasement. Une équipe de cyberguerriers peut ainsi facilement porter atteinte à l'intégrité d'une personne physique ou à plusieurs étant donné les conséquences de l'embrasement de la batterie d'une voiture électrique[3]. Il existe actuellement 234 modèles de chargeurs rapides dans le commerce. Sur un échantillon de 35 chargeurs, 18 modèles peuvent être facilement transformés en incendiaires. Cela concerne 8 fournisseurs différents de chargeurs rapides qui doivent revoir la conception et la fabrication de leurs produits pour leur sécurisation[4]. C'est un problème de réglementation. L'État sera alors chargé de contrôler la conformité des chargeurs, voir d'accréditer certains fournisseurs au détriment d'autres. Mais la menace peut être beaucoup plus complexe et intrusive. C'est le défi politique de la cybersécurité : comment gérer le risque cyber de l'écosystème des entreprises du secteur numérique au cœur des activités qui constituent la société ?

Ainsi, pendant la crise de la Covid-19, lors des premiers confinements, le collectif de pirates chinois APT41 a entrepris d'exploiter largement les nouvelles vulnérabilités introduites par la pratique du télétravail. Selon un rapport de la société américaine de cybersécurité Fire Eye, des vagues de cyberattaques entre le 20/01/2020 et le 11/03/2020 ont exploité les failles des routeurs CISCO, du contrôleur de trafic Internet et des logiciels de gestion de terminaux à distance Citrix Netscaler et Zoho. Une vingtaine de pays ont été ciblés et environ 75 entreprises dans les secteurs de la finance, de la défense et de l'énergie. Ces cyberattaques ont ciblé des failles « zero days » qui venaient d'être identifiées par APT41 et pour lesquelles un patch correctif était en cours de distribution. Le retard à la mise à jour des correctifs est devenu une vulnérabilité majeure des entreprises selon le CISA[5]. Ce groupe de pirates pratique autant les attaques criminelles

3. Une batterie de voiture électrique peut brûler pendant 24 heures et requiert plus de 11 000 litres d'eau pour être refroidie et éteinte. De plus, un feu de batterie « éteint » peut se rallumer jusqu'à 3 fois dans la même journée (Barthélemy Dont, *Les voitures électriques, futur cauchemar des pompiers*, site https://korii.slate.fr/tech/, consulté le 12/10/2020.
4. Catalin Cimpano, *Badpower : l'attaque informatique qui veut mettre le feu*, site https://www.zdnet.fr/, consulté le 22/07/2020.
5. FORBES, « Les 10 plus grosses attaques de 2019 », FORBES, 06/01/2020

pour des réseaux que l'espionnage pour des États. Ces vagues de cyberattaques ont récupéré des données sans demande de rançon, ce qui signale l'origine étatique du commanditaire de ces pratiques. Le volume et la criticité des informations collectées n'ont pu être évalués publiquement[6]. En 2019, c'est la ville de la Nouvelle-Orléans qui avait été touchée par une cyberattaque de grande ampleur qui bloqua les services administratifs pendant plusieurs jours. Mais la cyberattaque la plus significative cette année-là fut la découverte de la possibilité de prendre le contrôle à distance de la caméra des smartphones, ce qui transforme tout un chacun en espion à son insu[7] !

Cette activité d'espionnage à travers le cyberespace est établie depuis les années 1990 et le tournant stratégique chinois après la première Guerre du Golfe. En avril 1997, la Commission militaire centrale (CMC) crée un corps d'une centaine de membres pour déterminer les stratégies et les directions technologiques à suivre pour utiliser le piratage des ordinateurs comme levier stratégique. À la même époque, le célèbre ouvrage des deux colonels Qiao & Wang *La Guerre Hors Limites* indiquait déjà les nouvelles possibilités de conflits ouvertes par le développement des autoroutes de l'information et des réseaux informatiques : « La première règle de la guerre hors limite est qu'il n'y a pas de règle et rien n'est interdit »[8]. La guerre hors limite est une guerre asymétrique qui est une possibilité de conflit à un coût limité : « si nous voulons nous assurer la victoire dans les guerres à venir, nous devons mener une guerre affectant tous les domaines de la vie du pays concerné sans que l'action militaire en soit l'élément dominant ». Plus largement, en 2003, la CMC approuve le cadre conceptuel des 3 arts de la guerre : psychologique, médiatique, juridique à travers le cyberespace.

Pour répondre à cette problématique, nous devons identifier la spécificité du risque associé à la connectivité introduite par le cyberespace.

La caractéristique de la cybermenace : un monde ouvert

La propriété cognitive qui permet de distinguer la sécurité fournie par une entreprise et la sûreté assurée par les services étatiques est la nature de l'ensemble des dysfonctionnements auxquels ils sont confrontés. Une entreprise produit de la sécurité par rapport à un ensemble de dysfonctionnements ou de pannes qu'elle connait ou qu'elle peut décrire, voire imaginer. Ainsi, l'entreprise peut anticiper et élaborer des plans de contingence afin de répondre aux problèmes. Lorsqu'un composant de voiture présente un défaut de fabrication grave, par exemple les pneumatiques, le constructeur peut rappeler les véhicules concernés grâce à la traçabilité de sa production et le suivi de ses

6. "Chinese hackers undertake largest cyber espionage in recent years amid Covid19 panic", site : Website news18, consulté le 29/03/2020,
7. FORBES, « Les 10 plus grosses attaques de 2019 », FORBES, 06/01/2020
8. « The first rule of unrestricted warfare is that there are no rules, and nothing is forbidden. »

clients. L'ensemble des menaces possibles auxquelles doit se préparer une entreprise peut être explicité et elle peut se préparer pour y faire face, elle évolue dans un environnement décisionnel fermé. Au contraire, la présence de l'État devient incontournable lorsque l'ensemble des menaces auxquelles doit faire face une entreprise est imprédictible. Lorsque les voitures connectées représenteront une part importante du marché automobile, le problème de leur résilience face au risque de piratage informatique sera une préoccupation quotidienne de l'État, car les scénarios de cyberattaque sont pratiquement inimaginables. La cyberattaque peut cibler un nombre très important de voitures et conduire à une saturation de la circulation ou à un embrasement de milliers de voitures au même moment dans une ville dense. Au contraire, elle peut cibler une seule voiture afin de nuire à son conducteur. Enfin, elle peut cibler une voiture et la transformer en arme pour commettre une attaque terroriste. Sans oublier la possibilité de faire d'une voiture connectée un environnement d'espionnage des passagers. Il est pratiquement impossible de construire l'ensemble exhaustif des scénarios de cyberattaque. De plus, si les conséquences d'une cyberattaque sont graves pour les conducteurs (perte de contrôle du véhicule), elles peuvent toucher un très grand nombre d'utilisateurs et leur occurrence peut être fréquente. L'anticipation d'une cyberattaque est très difficile, par essence l'attaquant mettra tout en œuvre pour bénéficier de l'effet de surprise et le cyberespace offre en permanence de nouvelles vulnérabilités aux attaquants. En effet, l'essence du cyberespace c'est d'être un espace permanent d'innovations. Selon R. Evertt, la diffusion d'une rupture technologique suit une courbe en « S ». Elle est donc très rapide (phénomène social non linéaire) et imprédictible. La sûreté est donc un processus qui traite de menaces dans un environnement décisionnel ouvert.

Le dilemme de cybersécurité : une course permanente aux cyberarmes

Cette propriété a des conséquences pour les dirigeants politiques. Les ruptures technologiques déterminent un espace décisionnel propre. Ainsi, les armes nucléaires ont constitué un ensemble de possibilités stratégiques où la confrontation directe de deux superpuissances nucléaires n'est plus une option. Cet espace décisionnel repose sur la doctrine de la destruction mutuelle assurée (MAD : mutual assured destruction) qui conditionne les stratégies possibles et donc l'espace décisionnel des dirigeants politiques. La conséquence est la recherche permanente de l'équilibre des capacités nucléaires, tout d'abord à travers un phénomène de course aux armes atomiques puis de contrôle des armes nucléaires afin de maintenir une parité acceptable pour les deux superpuissances. De plus, la nature des armes nucléaires est leur caractère défensif. Elles ne sont pas

utilisables comme des armes offensives (hormis les deux seules bombes atomiques contre Hiroshima et Nagasaki qui ont été utilisées avec une stratégie d'emploi de bombes aériennes conventionnelles). La conséquence est leur rôle dissuasif et stabilisateur. Il suffit de construire des armes nucléaires fiables (qui ont fait l'objet de nombreux tests) avec une organisation résiliente (les forces armées nucléaires) pour qu'elles dissuadent un attaquant potentiel d'escalader une agression comme l'a illustré la crise des missiles de Cuba en 1962 entre Kennedy et Kroutchev.

Les cyberarmes sont aussi une rupture technologique. Mais, à la différence des armes nucléaires, elles donnent l'avantage à l'offensive. Autrement dit, dès que vous concevez une nouvelle stratégie d'attaque informatique, vous construisez la cyberarme idoine et vous l'utilisez avant que votre adversaire identifie les vulnérabilités que vous avez identifiées. Vous pouvez espionner et vous préparer pour une prochaine attaque conventionnelle. Les cyberattaques sont quotidiennes, elles ne connaissent aucun répit, c'est une activité permanente qui occupe des dizaines de milliers de cyberguerriers des deux côtés du Pacifique.

Plus précisément, la défense n'est pas possible, car le nombre de vulnérabilités d'une infrastructure numérique ou d'un produit digitalisé dépasse les capacités de test et de fiabilisation des constructeurs. Ceux-ci renoncent donc à fournir des produits « sûrs ». L'État, dans l'obligation de fournir la sûreté nécessaire au bon fonctionnement des infrastructures de la société, n'a pas d'autre option que de pratiquer aussi des cyberattaques contre ses adversaires potentiels afin de les dissuader d'utiliser effectivement les vulnérabilités de ses infrastructures tant civiles que militaires. Les cyberattaques sont généralisées et leur performance conduit à une « dissuasion offensive » qui produit un équilibre stratégique… instable.

Pratiquement, cela signifie que les États doivent fournir une sûreté qu'ils ne sont pas capables de produire sans réintroduire dans la société internationale le concept d'équilibre des puissances cher aux réalistes. Les entreprises sont alors en première ligne pour développer la sécurisation des infrastructures et des produits afin de crédibiliser un niveau de sûreté insuffisant. Cependant, les entreprises se trouvent liées de facto à un État de référence comme des acteurs essentiels de la sûreté. Il ne s'agit plus simplement d'un complexe militaro-industriel qui produit des armes nucléaires fiables, mais de partenaires de l'État dans les domaines de la sûreté et de la sécurité. L'équilibre des puissances conduit alors à associer les entreprises aux rivalités politiques de la société internationale. Cette tendance est illustrée en mai 2019 par le président Trump lors du

bannissement du marché américain des infrastructures de la 5G du constructeur télécom chinois Huawei alors qu'il est le meilleur fournisseur actuellement au niveau mondial en position de monopole sur de nombreux produits essentiels à un réseau 5G performant.

En résumé, les cyberarmes donnent l'avantage à l'offensive, la défense est limitée. La sûreté défensive produite par l'État est donc limitée. Si la sûreté produite par l'État n'est pas suffisante pour permettre les activités numériques des entreprises à travers le cyberespace, alors c'est la sécurité produite par les entreprises qui devra y remédier afin d'entretenir la confiance des utilisateurs dans ces services. Si la puissance de l'État est seulement défensive, dans le secteur numérique, c'est l'entreprise qui produit la sécurité. L'alternative pour l'État c'est d'adopter une posture offensive afin de suppléer aux limites intrinsèques de la production de la sécurité par les entreprises. C'est le dilemme de cybersécurité d'une cyberpuissance au sens de J. Nye : un pays capable d'obtenir des résultats politiques grâce à l'utilisation de ressources informationnelles et électroniques interconnectées à travers le cyberespace[9].

Les conséquences du dilemme de cybersécurité

Pour rappel, le dilemme de sécurité est un concept défini par J. Herz en 1951 pour expliquer et rendre compte des effets de la course aux armes atomiques. C'est « une notion structurelle dans laquelle les efforts des États pour assurer leurs besoins de sécurité ont la tendance, quelle que soit l'intention, de conduire à une insécurité croissante pour les autres[10] ». Ainsi, en 1994, les Américains autorisent la Chine à se connecter aux réseaux des autoroutes de l'information de la National Science Foundation, le prototype de l'Internet issu des recherches de la DARPA. En 2005, la Chine est le second pays avec le plus d'internautes connectés, plus de 100 millions. En 2018, ils sont plus de 800 millions, c'est le premier pays connecté. Pour « protéger » sa population de l'influence des stratégies de guerre de l'information des agences de renseignement américaines, les dirigeants chinois ont élaboré pendant cette période le Great Fire Wall (GFW) qui bloque l'accès aux entreprises numériques : Facebook, Wikipedia, Twitter, YouTube, etc. Cette protection s'accompagne aussi de piratage des courriels des dissidents chinois, notamment ceux de Google. La conséquence est la confrontation directe entre cette entreprise et le gouvernement chinois qui « l'expulsera » de son marché. Cette « protection » de la population chinoise contre les influences extérieures est interprétée par la secrétaire d'État H. Clinton comme une menace : « Un nouveau rideau est en train de s'abattre sur l'information dans une grande partie du monde… Dans un monde

9. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), p. 44–71.
10. John Herz, "Idealist Internationalism and the Security Dilemma." *World Politics*, Vol. 2, No. 2, Cambridge University Press, 1950, p. 157–180

connecté, une attaque contre les réseaux d'une nation peut être une attaque contre toutes les nations… En répétant avec force ce message, nous pouvons créer des normes de comportement entre les États et favoriser le respect des réseaux Internet mondiaux… La lutte contre le terrorisme ne doit pas devenir une excuse pour que les gouvernements violent systématiquement les droits et la vie privée de ceux qui utilisent Internet à des fins pacifiques ». Pour la secrétaire d'État américaine, la « protection » de la population chinoise des « intrusions » américaines dans la sphère publique est une « menace » sur les droits fondamentaux. Pendant la campagne présidentielle de 2017, les dirigeants américains s'élèveront de façon véhémente contre les intrusions russes et leurs tentatives d'influencer les électeurs…

Selon. R. Jervis, le facteur contributif au dilemme de sécurité est l'augmentation du « nombre de moyens par lequel un État essaye d'augmenter sa sécurité et diminue ainsi la sécurité des autres »[11]. Il y a deux variables critiques dans le modèle de Jervis : la capacité de discernement entre les armes offensives et défensives d'une part, et le coût de la défense par rapport à l'attaque d'autre part. Si un acteur dépense 1$ pour développer une arme et que l'adversaire doit dépenser une somme supérieure pour se protéger, alors l'arme procure un avantage à l'attaquant et la défense n'est pas une option viable. La course aux armes offensives est alors une structure sociale qui va s'imposer aux acteurs. C'est l'un des facteurs contributifs à la course aux cyberarmes que nous observons désormais publiquement depuis la cyberattaque Stuxnet contre les centrifugeuses de la centrale iranienne de Natanz en 2009. De plus, le développement d'un firewall géant et l'intrusion dans les serveurs d'une entreprise étrangère sont des technologies duales. En effet, elles sont utilisables de façon défensive et offensive. Ainsi, l'incertitude sur les capacités de l'adversaire rend très difficile la coopération entre les cyberpuissances. Selon R. Jervis, « il faut que la défense soit aussi efficace que l'attaque et la différenciation entre ces deux postures explicites afin de permettre aux États de maintenir un statu quo stable et de ne pas se comporter en agresseurs[12] ». Or, nous avons vu que le cyberespace est un environnement d'innovations permanentes qui sont imprédictibles. Les cyberarmes peuvent atteindre un nombre élevé de cibles à l'échelle d'un pays, et ce, sans contrainte sur la distance, avec une grande précision dans le ciblage, sous un voile d'opacité quant à leur conception et fabrication, et sous un anonymat quasi total pour l'attaquant. Ainsi, selon B. Buchanan, la course aux cyberarmes et leurs caractéristiques constitue un nouveau dilemme de sécurité : le cyberdilemme de sécurité[13]. Les facteurs qui entretiennent ce cyberdilemme sont l'avantage à l'offensive que procurent les cyberarmes (ou l'impossibilité de la défense contre les cyberarmes), l'incertitude radicale sur les

11. R. Jervis, Cooperation under the Security Dilemma, *World Politics*, 30(2), 1978, p167-214
12. Jervis, R. (1978). Cooperation under the Security Dilemma. World Politics, 30(2), 167-214.
13. B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press, 2017, p. 15-30.

attaquants et la peur pour la survie du régime qui caractérise les dirigeants politiques tant illibéraux que libéraux.

Ce dilemme de cybersécurité conditionne l'espace décisionnel des dirigeants politiques. Ceux-ci sont confrontés en permanence à l'alternative entre une sécurité limitée (car la défense coûte plus cher que l'attaque [14]) produite par des entreprises du secteur numérique ou une sûreté offensive produite par l'État (le *cyber command* et les agences de renseignement) et un équilibre des puissances instable. Ce dilemme conditionne la stratégie et le comportement d'une cyberpuissance. De plus, cette structure sociale, similaire au dilemme de la course aux armes nucléaires (l'alternative entre continuer d'accumuler de coûteuses armes atomiques ou coopérer pour le contrôle de la course aux armes à un point d'équilibre accepté par les deux superpuissances) a le même effet sur les relations internationales. Ce dilemme de cybersécurité concerne les infrastructures et les capacités digitales critiques pour les économies et la survie des régimes des cyberpuissances.

En effet, la particularité de la connectivité des infrastructures c'est qu'elle conduit à une extension du cyberespace comme environnement décisionnel global où tous les actifs d'une société, des bases de données bancaires aux infrastructures, sont vulnérables.

Le cas du GPS : le découplage sino-américain

Prenons l'exemple du service de positionnement dans l'espace et dans le temps fourni par le système de positionnement global ou global position system (GPS). Après la phase de recherche et de développement dans les années 1960, l'armée américaine plaça en orbite son premier satellite pour le positionnement et la navigation en 1978 et la première version du GPS américain devint opérationnelle en 1993. Ainsi, les systèmes d'armes américains tiraient une part de leur efficacité de l'exploitation de ce signal global dans l'espace et le temps tel que le système antimissile Patriot popularisé lors de la première Guerre du Golfe. En 2000, le GPS militaire fut étendu au domaine civil. De même, des entreprises voyaient leur coût diminuer grâce à l'intégration de ce signal dans leur produit ou service tel que le transport maritime dont l'heure d'arrivée au port des porte-conteneurs devint prédictible et le suivi des cargaisons étendu à l'ensemble des mers et des océans. Cependant, les armées clientes des systèmes d'armes américains ou les entreprises étrangères, notamment chinoises, sont devenues dépendantes directement du Pentagone qui peut dégrader la qualité du signal de positionnement en fonction de son besoin stratégique. Cette dépendance conduit quelques grandes puissances à chercher

14. Le génie logiciel, ou l'ensemble des pratiques de développement du logiciel s'applique aussi au développement des cyberarmes. Ce que l'on observe pour les logiciels civils, accroissement des fonctionnalités et diminution du coût, s'applique aussi aux cyberarmes qui bénéficient des effets de la réutilisation, de la modularité et de l'accroissement du savoir-faire au sein d'institutions spécialisées de cybersoldats et d'un écosystème de nombreuses entreprises.

leur autonomie stratégique. La Chine est donc en quête d'une alternative au GPS américain depuis 1994[15]. La crise du détroit de Taiwan en 1995-96 fut un réveil stratégique pour la Chine. La Chine a décidé de construire la chaine de valeur de tous les composants du GPS et des moyens de l'utiliser[16]. Le premier lancement d'un satellite pour le GPS chinois Beidou eut lieu en 2000 avec pour périmètre le voisinage asiatique de la Chine et une précision d'une centaine de mètres. À cette époque, elle avait déjà lancé plus d'une centaine de satellites avec un taux de succès de 90%. Ce système est désormais global avec sa 3e version. La précision du signal à destination des civils est de 0,41 m vs 0,5 m pour le GPS américain et de 10 cm pour le signal militaire[17]. Dans la région Asie-Pacifique, la précision du service GPS de Beidou est supérieure au GPS américain. De plus, Beidou offre un service de messagerie de 1 200 caractères chinois[18]. La précision du signal de positionnement du GPS chinois permettra aux usines d'accroitre leur productivité grâce à une robotisation accrue qui requiert une capacité de localisation précise. Le GPS s'inscrit dans un portefeuille de technologies qui vient amplifier l'offre de la technologie 5G. Ce couplage ouvre des perspectives pour la voiture autonome et interconnectée, les villes intelligentes et l'Internet des Objets (IoT), les transactions financières, etc. De plus, cette interconnectivité permet de construire des bases de données gigantesques sur le comportement des utilisateurs et qui seront à l'origine du développement de nouveaux services. Ce système GPS chinois renforce sa position dans le secteur des applications et des appareils mobiles tels que les drones et les smartphones. Aujourd'hui, 70% des smartphones en Chine (Huawei, Xiaomi, Galaxy) utilisent le signal GPS du système Beidou[19]. Le service de positionnement de Beidou génère un marché de 58 milliards de dollars en 2020[20]. Le japonais SONY a mis sur le marché des circuits de réception du signal GPS chinois pour les objets connectés et les produits d'électroniques portables avec la caractéristique d'avoir la consommation la plus basse du marché. Cependant, l'utilisation du signal du système Beidou requiert un circuit intégré particulier, il ne suffit pas de télécharger une application logicielle. Ainsi, l'iPhone ne permet pas d'utiliser le signal GPS chinois[21]. En l'absence du composant électronique spécifique, les Chinois « patriotes » qui

15. Xinmei Shen, "Apps claiming to use chinese satellite navigation system Beidou see a surge in downloads, but they might just use GPS", site : Scmp.com/abacus, visité le 06/08/2020
16. Anjani Trivedi, "GPS watch out, here comes China's system", site : https://techxplore.com/, visité le 12/08/2020
17. Anjani Trivedi, "GPS watch out, here comes China's system", site : https://techxplore.com/, visité le 12/08/2020
18. Don Giolzetti, "China charts a path with iconic Beidou satellite system", site : https://www.channelnewsasia.com/commentary/china-tech-bifurcation-space-technology-beidou-satellites-603246, visité le 01/10/2020
19. Lewin Day, "Not just GPS : new options for global positioning", site : https://hackaday.com/, visité le : 06/08/2020 ; et Xinmei Shen, "Apps claiming to use chinese satellite navigation system Beidou see a surge in downloads, but they might just use GPS" ; et "Apps claiming to use chinese satellite navigation system Beidou see a surge in downloads, but they might just use GPS", site : Scmp.com/abacus, visité le 06/08/2020
20. Don Giolzetti, "China charts a path with iconic Beidou satellite system", site : https://www.channelnewsasia.com/commentary/china-tech-bifurcation-space-technology-beidou-satellites-603246, visité le 01/10/2020
21. Xinmei Shen, "Apps claiming to use chinese satellite navigation system Beidou see a surge in downloads, but they might just use GPS", site : Scmp.com/abacus, visité le 06/08/2020

ont téléchargé des applications Beidou se retrouvent de fait à utiliser le signal du GPS américain[22]. Le GPS introduit un double rapport de dépendance, d'une part sur les fournisseurs du service de positionnement et d'autre part sur l'outil diplomatico-militaire. Le GPS chinois renforce donc la dépendance à la politique internationale de la Chine. Les fournisseurs de récepteurs utilisant un signal GPS ont débuté le développement des capacités de fonctionnement multisignaux, quelle que soit l'origine du signal GPS. Les systèmes GPS existants peuvent être rendus interopérables[23]. Les récepteurs des utilisateurs avec un positionnement multimode qui reçoivent simultanément les signaux américain, russe et chinois vont désormais pouvoir bénéficier des points forts de chaque fournisseur de positionnement[24]. Un utilisateur, entreprise ou particulier, de signal GPS peut utiliser l'un ou l'autre des services américain ou chinois de positionnement. Mais cette dépendance signifie la nécessité pour l'État de référence de cet utilisateur de rendre ses intérêts vitaux compatibles avec ceux de son fournisseur de service. Il peut même utiliser les deux fournisseurs de signal GPS avec un système interopérable. Mais il doit alors s'adapter aux « conditions de l'équilibre des puissances » sino-américain. Actuellement, la Turquie qui a acheté le système antimissile russe S400 est confrontée à cette situation, car elle est aussi membre de l'OTAN et ses systèmes d'armes sont interopérables avec les forces américaines.

De plus, le segment satellitaire du système GPS est une cible des armes de guerre électroniques et le segment au sol du système GPS est une cible des cyberarmes. La globalité du système GPS conduit naturellement à la convergence du cyberespace et des forces spatiales. C'est une conséquence stratégique de la loi économique des réseaux[25].

Les armes de la guerre électronique ont atteint un niveau de développement qui permet d'envisager leur utilisation conjointe avec les cyberarmes afin de porter atteinte à l'intégrité du signal GPS et sa disponibilité. Plus précisément, les techniques de leurrage du signal GPS (*spoofing*) et de détournement des utilisateurs peuvent être des armes stratégiques de grande ampleur[26]. La convergence des armes de la guerre électronique avec celle du cyberespace est une nouvelle rupture stratégique similaire à l'introduction de la bombe H après la bombe A dans l'espace décisionnel des dirigeants politiques. Le domaine de l'espace est celui de la défense contre les missiles et les attaques des réseaux de communication dont le GPS. Le domaine du cyberespace est celui des cyberattaques et

22. Xinmei Shen, "Apps claiming to use chinese satellite navigation system Beidou see a surge in downloads, but they might just use GPS", site : Scmp.com/abacus, visité le 06/08/2020
23. Anjani Trivedi, "GPS watch out, here comes China's system", site : https://techxplore.com/, visité le 12/08/2020
24. ABC Bourse, « Le GPS chinois finalisé avec un ultime satellite », site : https://www.abcbourse.com/marches/le-gps-chinois-finalise-avec-un-ultime-satellite_506964
25. Ethan Brown, "A combat role for the space force : why the newest armed service should own cyber warfare", site : https://mwi.usma.edu/a-combat-role-for-space-force-why-the-newest-armed-service-should-own-cyber-warfare/, visité le 16/07/2020
26. Lewin Day, "Not just GPS : new options for global positioning", site : https://hackaday.com/, visité le : 06/08/2020

de la guerre de l'information. Ces systèmes duaux, à la fois militaire et civil, sont constitués par des partenariats public et privé très structurants pour leur stratégie de développement et vers une intégration de plus en plus poussée. Fournir un service de positionnement global GPS requiert aussi de conquérir l'espace et la 5G et introduire de nouvelles vulnérabilités aux cyberarmes et aux armes électroniques. La convergence de ces deux domaines soulève la question de la sécurité associée aux fournisseurs de signaux GPS de façon structurante pour les relations internationales.

LES CONSÉQUENCES SUR L'INTERDÉPENDANCE UTILISATEUR/ FOURNISSEUR DE SERVICES NUMÉRISÉ

L'interdépendance politique entre des utilisateurs d'un service sur un territoire avec un régime politique et un fournisseur du service sur un autre territoire avec un autre régime politique peut difficilement conduire à un régime de coopération lorsque ce service est le référent d'un processus de sécurisation face à des menaces imprédictibles.

La cybersécurité n'est pas une problématique technologique, mais organisationnelle

La conséquence d'une cyberattaque sur le GPS est l'atteinte à l'intégrité des données de positionnement, dans l'espace et dans le temps voire à leur disponibilité. La conséquence d'une cyberattaque, informatique ou électronique, sur le GPS est donc la confiance de l'utilisateur à l'égard du fournisseur de service.

Plus précisément, une chaine de valeur numérisée, tel qu'un système GPS, est vulnérable à la défaillance de quelques-uns seulement des fournisseurs ou des sous-traitants de l'écosystème associé.

Cette menace fait désormais partie des opinions communes de la population. Ainsi, dans le célèbre roman d'anticipation *La flotte fantôme : le troisième conflit mondial est déjà là !* de l'été 2021 sur la prochaine guerre sino-américaine par deux consultants du Pentagone, la vulnérabilité de l'écosystème des fournisseurs de circuits intégrés, notamment pour le GPS, est décrite comme suit, tout d'abord concernant la rupture technologique :

« Les composants des premiers microprocesseurs qui avaient équipé tous les appareils depuis les premiers ordinateurs jusqu'aux avions à réaction des années 1960 étaient visibles à l'œil nu. Mais à l'orée du XXIe siècle, les microprocesseurs étaient capables de

contenir des millions de transistors dans un espace de quelques millimètres carrés à peine. Et chaque puce se divisait elle-même en une multiplicité de circuits secondaires, appelés blocs, qui remplissaient chacun une fonction différente. »

Puis son impact sur l'écosystème des entreprises de fabrication et sa localisation en Chine :

« Quand l'industrie des microprocesseurs avait décollé, on était passé d'une petite poignée d'entreprises à plus de 2000 compagnies, dont la plupart basées en Chine et qui créait chacune 5000 nouveaux modèles de puces chaque année. Ces nouveaux processeurs étaient le fruit du travail de plusieurs milliers de personnes sur différents sites, chaque équipe s'occupant d'un bloc particulier, le créant tantôt de A à Z, ou bien le sous-traitant, d'autres fois encore l'achetant en externe à un spécialiste. Et chacun de ces nouveaux blocs était alors intégré à des millions de puces, qui étaient à leur tour incorporées à des objets allant du grille-pain au missile Tomahawk. »

La vulnérabilité exploitable est explicitée, la complexité qui rend impossible la fiabilisation des circuits :

« Tout cela avait abouti à un dangereux mélange : les puces étaient devenues si complexes qu'aucun ingénieur, seul ou en équipe, n'était capable de comprendre comment leurs composants fonctionnaient concrètement ; le processus de conception était si fragmenté que personne ne pouvait contrôler toutes les personnes impliquées ; et les processeurs étaient produits et achetés en si grand nombre qu'on ne pouvait même plus tester un petit pourcentage d'entre eux, ce qu'aucun acheteur, pas même les grandes entreprises du complexe militaro-industriel américain, n'avait d'ailleurs tenté de faire. L'efficacité l'emporte toujours sur la sécurité. »

Enfin, la menace qui exploite la vulnérabilité est désignée :

« Pendant longtemps, c'était la notion de *kill switch*, une sorte de coupe circuit secrètement intégré dans une puce, capable de paralyser sur demande tout un système informatique, qui avait inquiété les analystes militaires ».

La conséquence pour l'État est la nécessité de sécuriser l'ensemble d'un écosystème d'entreprises. La sécurisation face à une menace imprédictible dans un « monde ouvert » s'appuie sur un processus permanent d'analyse du risque de chaque acteur de la chaine de valeur. L'analyse du risque cyber doit donc être généralisée à des pans entiers de l'économie et c'est l'État qui la rend obligatoire, car l'enjeu concerne la sécurité économique et nationale du pays.

La cybersécurité est donc le résultat de la conformité des entreprises à la réglementation étatique, à une culture de la sécurité des entreprises qui permet de rendre opérationnelle l'articulation avec la sûreté étatique et un processus permanent de suivi du risque cyber au plus près de l'évolution des menaces. Ce processus de sécurisation concerne tous les acteurs des chaines de valeur vitales d'une économie et la cartographie globale des systèmes d'information. La propriété recherchée est la résilience des infrastructures face à une cyberattaque tant informatique qu'électronique. La conséquence de cette approche est la nécessaire confiance qui s'établit entre tous les acteurs concernés par une chaine de valeur et les infrastructures associées. Il s'agit d'une véritable communauté de sécurité.

En effet, la principale cause de succès d'une cyberattaque c'est un comportement inadapté de la part d'un collaborateur sur la chaine de valeur. Une cyberattaque requiert la collecte d'informations qui rendent possible l'intrusion des systèmes d'information. C'est la phase « d'ingénierie sociale » dont l'exemple le plus connu est une approche d'un employé via un courriel de *phishing* (hameçonnage). Ce type de courriel semble provenir d'un expéditeur digne de confiance alors qu'il a été piégé afin de collecter des données critiques. Chaque collaborateur d'une entreprise doit donc acquérir les bons comportements pour protéger son employeur et fournir la sécurité attendue par les clients. Il doit faire preuve de « loyauté » à l'égard des *stakeholders* de l'entreprise.

L'État doit aussi « défendre » cette communauté de sécurité de façon « offensive » contre les cyberattaques des autres cyberpuissances. Ainsi, l'Union européenne a pris des sanctions contre des cyberguerriers russes, chinois et nord-coréens. Le groupe de cyberguerriers chinois APT 10 a piraté des entreprises européennes, notamment britanniques, pendant 7 ans : IBM, Fujitsu, Tata, NTT, Dimension Data, Computer Science corp., DXC, HPE. La sécurité d'État chinoise (le Guanbu) a participé à cette opération ainsi que l'entreprise chinoise HAITA Tech Dvt[27]. En décembre 2018, les États-Unis avaient mis en accusation les cybersoldats Zhu Hua et Zhang Shillong du groupe APT 10 pour avoir volé des fichiers de 45 entreprises dans une douzaine de pays dans les secteurs aéronautique, télécommunications, électronique, naval, énergie[28]. L'Union européenne a sanctionné 4 cybersoldats supplémentaires, 2 autres groupes de cybersoldats chinois et 1 groupe nord-coréen : Chosun Expo[29].

Le critère de succès pour une cyberpuissance qui fournit des services et des produits digitaux, c'est la loyauté des entreprises à l'égard des intérêts vitaux de l'État et sa capacité à dissuader ses adversaires. Dès lors, comment mettre en place un régime de

27. Laurent Lagneau, « L'UE prend des sanctions contre des pirates informatiques russes, chinois et nord-coréen », site : opex360.com, visité le : 31/07/2020
28. Laurent Lagneau, « L'UE prend des sanctions contre des pirates informatiques russes, chinois et nord-coréen », site : opex360.com, visité le : 31/07/2020
29. Ce groupe avait déjà été identifié lors de la cyberattaque Wanacry en 2017 où le groupe de cybersoldats APT 38 ou Lazarus était aussi impliqué

cybersécurité entre des entreprises et des États pour lesquels la sûreté est uniquement déterminée par les intérêts nationaux qui sont parfois exclusifs ?

La sécurisation des infrastructures digitales tant civiles que militaires est structurante, elle est permanente et conditionne l'espace décisionnel des dirigeants politiques. Ceux-ci réactivent progressivement les mécanismes d'alliances et de zones d'influences. Le *hedging* tel qu'il est pratiqué en Asie de l'Est n'est désormais plus pertinent. Un pays ne peut plus simplement assurer sa sécurité vis-à-vis de la Chine en signant un traité d'alliance avec les États-Unis et en même temps développer ses interdépendances avec les entreprises chinoises. Si la population d'un pays utilise massivement le signal GPS chinois, alors de fait l'État de ce pays s'alignera sur les intérêts stratégiques chinois. Une dispute entre ce pays et la Chine conduirait celle-ci à prendre en otage la population en coupant le GPS. Les Américains devraient alors prendre le risque d'entrer en conflit armé avec la Chine afin de rétablir le bon fonctionnement du GPS, ce qui semble relativement disproportionné. Les États-Unis ne peuvent pas raisonnablement intervenir avec leurs forces armées en fonction d'intérêts fonctionnels critiques, mais seulement locaux sans que les intérêts vitaux américains soient directement menacés. Utiliser les forces armées américaines à cause des smartphones taiwanais risque d'être difficile à justifier. L'opinion publique américaine ne soutiendrait pas un tel usage de la force armée. Il n'y a pas eu d'intervention américaine en 1956 pour les Hongrois ou plus récemment pour Hong Kong…

Des relations internationales structurées par une stratégie de « prise d'otage de population »

Le réseau satellitaire du GPS chinois est désormais finalisé. La Chine est donc autonome du GPS américain. La complétude de la 3e version du système GPS chinois Beidou est un jalon important de l'accès de la Chine au statut de superpuissance. C'est une avancée importante vers le découplage de la Chine des États-Unis. L'objectif stratégique de Beijing est de diminuer sa dépendance technologique à l'égard des Américains. Cette volonté stratégique est ancienne, affirmée par Deng Xiaoping dès 1986 avec le programme 863 et renforcée avec le plan « Made in China 2025 ». C'est le 11e plan quinquennal 2006–2010 qui réalise l'intégration des mécanismes de marché avec les institutions spatiales chinoises afin de mettre en place l'écosystème des entreprises pour favoriser le développement des capacités spatiales et de les rentabiliser sur le marché mondial[30]. La Chine réalise alors 1 lancement tous les 2 mois : elle a mis en orbite 456 satellites en 2020 contre 9 en 2002, elle a réussi 3 missions de vol spatial habité et 2 missions lunaires. La Chine met au point une nouvelle génération de satellites dès 2007, notamment pour le

30. Les opérateurs d'état de satellites sont China DBSat et China Satcom qui travaillent notamment avec des groupes hongkongais privés APT Group et AsiaSat.

GPS avec une précision de 10 mètres et une mesure temporelle de l'ordre de la dizaine de nanosecondes. En 2020, la version actuelle de Beidou est constituée de 35 satellites, 5 géostationnaires, 27 en orbite moyenne, 3 géosynchrones. Seulement 3 de ces satellites ont connu des problèmes techniques. Le GPS chinois est performant pour le guidage de missiles, la navigation maritime et aérienne, la coordination des capacités inter armes et l'identification des cibles. Les avantages du découplage sont soulignés par de nombreux spécialistes des relations internationales comme Di Dongsheng de l'Université de Renmin : « to a certain extent, China joining the US led market system was necessary, but one cannot walk the same path forever. One must decide the right time to leave »[31]. Ainsi le service de communication et le signal GPS fournis par Beidou permettent à l'APL de disposer de son propre système de messagerie fiable, de ciblage propre et d'autres fonctions critiques pour son autonomie stratégique.

La réalisation de cette ambition chinoise d'autonomie face aux États-Unis alimente le dilemme de cybersécurité. C'est une permanence et désormais il est peu probable que la Chine accepte de s'accommoder des contraintes libérales de la société internationale afin de préserver le statu quo. Elle a refusé le jugement de la Cour internationale de justice de La Haye dans son différend avec les Philippines au sujet des îlots en mer de Chine. Le développement du GPS chinois permet d'accroitre la dépendance des populations qui utilisent ce service. Les États de ces populations s'alignent progressivement sur les intérêts stratégiques de la Chine fixés par le PCC. Les capacités américaines pour fournir la sécurité à ses alliés face à la montée en puissance de la Chine sont inexorablement sapées.

Ces nouvelles relations internationales entre des acteurs d'une société civile et des États extérieurs dans le domaine de la cybersécurité ressemblent à la situation d'une prise d'otage. Un État voit sa population prise en otage par un autre État via ses entreprises digitales et les services qu'elles fournissent à cette population. L'enjeu est alors de trouver une porte de sortie acceptable pour les parties prenantes. L'État dont la population est prise en otage ne peut pas sacrifier la cybersécurité de sa population, cela serait une victoire à la Pyrrhus, car il perdrait de fait sa légitimité. S'il « libère » sa population en cédant aux preneurs d'otages, il renonce à un pan de sa souveraineté, c'est aussi une défaite. Cette stratégie de diplomatie coercitive où la population est prise en otage sous l'effet des cyberattaques requiert de la part de chaque pays de réduire ses vulnérabilités et d'équilibrer ses dépendances. C'est la réactivation de l'équilibre des puissances qui conduit à une régionalisation des relations internationales à travers des alliances autour des cyberpuissances.

31. Don Giolzetti, "China charts a path with iconic Beidou satellite system", site : https://www.channelnewsasia.com/commentary/china-tech-bifurcation-space-technology-beidou-satellites-603246, visité le 01/10/2020

Une reconfiguration des alliances

Le Pakistan a ouvert des perspectives de coopération avec le fournisseur de GPS chinois[32], le Laos et la Thaïlande. Tous ces pays participent au programme des Routes de la Soie[33]. Plus généralement, une centaine de pays en Afrique, Europe de l'Est, Asie du Sud-Est, qui participent aux projets du programme des Routes de la Soie (Belt and Road Initiative ou BRI) telles que des installations aéroportuaires, des aéroports, des infrastructures pour les différents modes de transport : routier, ferré, aérien, maritime, etc. sont désormais des utilisateurs du signal GPS chinois[34]. Le programme spatial est une composante critique du programme des BRI comme le réseau de fibre optique Transit Europe Asia (TEA) qui connecte un couloir entre l'Asie de l'Est, la Chine, les pays d'Asie centrale, la Russie et le continent européen. Le GPS chinois induit et renforce une régionalisation des relations sinocentrées, car il s'accompagne de dépendances tant économiques que sécuritaires. La technologie, plus précisément les services numériques dans une société digitalisée sont des leviers de permutation des alliances. La Chine, à travers ses entreprises, devient un fournisseur de services numériques et donc de sécurité de façon similaire à un producteur de pétrole. À la différence de ceux-ci, la Chine est indépendante en termes diplomatico-militaires. Elle devient de fait un pays fournisseur de sécurité et donc une opportunité pour « consommer » cette sécurité via une alliance.

La solution technique est l'utilisation par les produits électroniques et les services de tous les signaux GPS disponibles. Toutefois, cette pratique augmente le coût des produits et parfois de manière dissuasive. Elle a surtout pour conséquence de rendre les utilisateurs dépendants de l'équilibre entre les cyberpuissances qui fournissent les signaux GPS. L'alternative est une organisation internationale qui permet aux cyberpuissances de se comporter comme des cyberpuissances responsables : c'est-à-dire, des États dont les entreprises fournissent des produits et des services et qui garantissent leur fiabilité en excluant l'instrumentalisation de ces services dans le cadre d'une diplomatie coercitive. Dans le secteur pétrolier, les grands producteurs forment un « cartel » via l'OPEP et les importateurs dissuadent le recours à l'arme pétrolière via l'AIE qui offre une assurance contre un embargo pétrolier via des réserves stratégiques obligatoires pour tous ses pays membres. Ou le retour de la « Guerre froide » comme structure politique entre deux grandes cyberpuissances qui conditionne ainsi les « alliances » et les alignements des pays en fonction de leurs intérêts respectifs.

32. Ran Chengqi, "China satellite navigation office, Cooperation perspective with Pakistan".
33. Don Giolzetti, "China charts a path with iconic Beidou satellite system", site : https://www.channelnewsasia.com/commentary/china-tech-bifurcation-space-technology-beidou-satellites-603246, visité le 01/10/2020
34. Anjani Trivedi, "GPS watch out, here comes China's system", site : https://techxplore.com/, visité le 12/08/2020

UN NOUVEL ENVIRONNEMENT DÉCISIONNEL ET LA GUERRE FROIDE 2.0

La rivalité entre les fournisseurs de signaux GPS va se faire sur la confiance. Dans quelle mesure la nécessité de la globalisation des marchés participe-t-elle à la coopération entre les fournisseurs de signaux GPS en matière de sécurité ? Une alliance diplomatico-militaire sino-américaine est-elle envisageable afin de garantir la fourniture d'un signal GPS pour les civils malgré un affrontement entre ces deux puissances en mer de Chine ?

Aujourd'hui, les institutions en charge de la dimension « sûreté » de la cybersécurité sont en place aux États-Unis et en Chine. Face à la puissance américaine concrétisée par la création de son *cyber command* en 2009 et son autonomie comme force armée en 2018 ; la Chine a aujourd'hui mis en place une organisation idoine. En décembre 2015, Beijing a créé son alter ego au *cyber command* américain : le Strategic Support Force (SSF) ou la Force de soutien stratégique (FSS) couvrant le cyberespace, le renseignement et les communications spatiales et la guerre électronique. Le SSF intègre notamment des départements de l'APL 3 (General Staff 3 qui assure la reconnaissance des cibles) et de l'APL 4 (General Staff 4 qui utilise les moyens radars et assure les contremesures de guerre électronique). Le SSF devient le Network System Force (NSF) avec un responsable de niveau hiérarchique : adjoint de commandant de théâtre d'opérations. Le NSF est désormais le quartier général de la cyberguerre : c'est la cyberforce chinoise (Wang Jun)

Cette institution est complétée par l'Information Engineering University comme centre de formation des cyberguerriers. De plus, les entreprises, telles que Qihoo 360, produisent les outils tant matériels que logiciels qui renforcent les capacités d'attaque et de défense des réseaux militaires chinois. L'ensemble de l'écosystème des entreprises électroniques et digitales de la Chine peut participer aux besoins des forces armées et des agences de renseignement chinoises.

Les capacités cyber et de guerre électronique de la Chine sont utilisées pour la reconnaissance : collecte de données techniques et opérationnelles pour l'exploitation du renseignement et la planification des attaques. De même, ces capacités sont déployées pour l'attaque des réseaux de contrôle, de commandement, de communication, de transport aérien, de distribution d'énergie, de la logistique de l'adversaire. Les États utilisent l'espace pour la collecte de renseignement et les communications. Klein définit les informations spatiales comme des données provenant des capacités spatiales à la fois

dans l'espace et à la surface terrestre[35]. Les armes sol/espace ont pour fonction de dénier à l'adversaire l'accès aux renseignements d'origine spatiale. La Chine a testé son missile antisatellite avec succès en 2007. En 2009, le commandant de la force aérienne chinoise déclara que la militarisation est historiquement inévitable. En 2015, la Chine développa ses technologies de brouillage de satellites. En 2018, elle possède ainsi toutes les armes antisatellites. La Chine a envoyé plus de satellites que les États-Unis et son système GPS est global et actif en permanence. L'objectif stratégique est d'empêcher une intervention américaine sur un théâtre d'opérations que la Chine a choisi dans son voisinage. Ses capacités lui permettent de rechercher l'établissement de la domination informationnelle et cela dès le début d'un conflit. Ses capacités servent aussi à amplifier l'efficacité des attaques conventionnelles et à saper les réseaux militaires et civils de l'adversaire. En 2012, le système de distribution d'électricité américain a subi plusieurs cyberattaques qui ont conduit les entreprises à demander le bannissement des matériels et des logiciels chinois[36].

Il s'agit de contourner la puissance conventionnelle d'un adversaire sur le théâtre d'opérations choisi à travers les armes conventionnelles, mais aussi des attaques non conventionnelles : la manipulation des médias, l'utilisation des trafics telle que ceux de la drogue, la prise de contrôle de marchés financiers (par exemple celui des matières premières/commodités), la désinformation des organisations internationales. La Chine possède des capacités très développées. Par exemple, l'unité spéciale de l'APL n°61 398 qui pratique les cyberattaques via des applications pour les smartphones, grand utilisateur de signal GPS (plus de 9 applications sur 10 sur un smartphone requièrent un signal GPS pour fonctionner de façon normale) représente environ 50 000 cyberguerriers basés à Chengdu au quartier général du centre de commandement de la région ouest[37]. La Chine élabore aussi des cyberattaques avec des pays tiers comme la Corée du Nord en tant qu'allié ou intermédiaire[38]. Le credo stratégique du NSF est « fighting the fight that fits one's own weapons and making the weapons to fit the fight. » Face à cette affirmation de la cyberpuissance chinoise, l'éventail des réponses de la nouvelle administration des États-Unis semble relativement limité.

35. John J. Klein, *Space Warfare: Strategy, Principles, and Policy*, London, New York, Routledge, 2006, 60 pages.
36. Saikiran Kannan, "Inside China's cyber war room : how PLA is plotting global attacks", site : https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06, visité le : 06/08/2020
37. Saikiran Kannan, "Inside China's cyber war room : how PLA is plotting global attacks", site : https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06, visité le : 06/08/2020
38. Saikiran Kannan, "Inside China's cyber war room : how PLA is plotting global attacks", site : https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06, visité le : 06/08/2020

En conclusion, les caractéristiques des cyberarmes et la connectivité généralisée des sociétés établissent une continuité du spectre sécuritaire, des enjeux de la qualité à la sûreté en passant par la sécurité des produits et des services. Les États et leurs écosystèmes d'entreprises digitales doivent concourir ensemble à la cybersécurité de la population. La principale caractéristique de la cybermenace c'est qu'elle provient d'un environnement d'innovation permanente et imprédictible. Le large éventail des cyberarmes et l'émergence de la puissance chinoise dans la société internationale rendent possible le recours à la guerre asymétrique. Cela conduit au dilemme de cybersécurité, une course permanente aux cyberarmes et une pratique quotidienne des cyberattaques, car elles offrent un avantage à l'offensive. L'alternative des dirigeants devient : laisser les entreprises produire une cybersécurité limitée accompagnant leurs produits et services sans intervenir afin de préserver les chaines de valeur globalisées ; ou compléter celles-ci avec une cybersûreté offensive dont la conséquence sera l'intensification du mécanisme d'équilibre des forces avec les autres cyberpuissances et la réduction des interdépendances économiques. L'étude du service de positionnement chinois BDS (Beidou) illustre les conséquences du dilemme de cybersécurité avec la mise en place d'une nouvelle configuration des alliances. Aujourd'hui, il y a plus d'une centaine de millions d'utilisateurs du service de positionnement BDS autour des infrastructures du programme Belt and Road Initiative, ce qui représente 120 pays clients, soit 20% du marché global de ce service. Les dirigeants politiques de ces pays évoluent donc dans un environnement décisionnel où l'enjeu de la cybersécurité est le risque de prise d'otage de leur population par une cyberpuissance fournisseuse d'un service critique pour leur économie à travers un écosystème d'entreprises digitales incontournables. C'est une problématique organisationnelle d'élaboration d'une communauté de sécurité plutôt qu'un défi technologique. Les relations internationales sont alors structurées par une menace permanente de « prise d'otage » de la population d'un État s'il porte atteinte aux intérêts stratégiques d'une cyberpuissance. Ces cyberpuissances qui fournissent des produits et des services numériques sont, de fait, des fournisseurs de sécurité et les populations utilisatrices deviennent des leviers de politiques internationales pour la mise en place d'alliances. Ces alliances seront conditionnées par les infrastructures et les services digitaux fournis par les cyberpuissances. Les capacités digitales croissantes de la Chine sont alors un défi stratégique structurel pour la cyberpuissance américaine. C'est le retour du mécanisme d'équilibre des puissances (la diplomatie coercitive et les alliances), les capacités nucléaires des deux cyberpuissances américaine et chinoise rendent toujours improbable leur confrontation directe et plus prégnante leur confrontation

indirecte dans les « zones grises » (par exemple la cyberguerre). La nouvelle dimension de cette situation est l'importance des écosystèmes d'entreprises digitales au cœur des complexes militaro informationnels des deux cyberpuissances qui ouvre une période de Guerre froide 2.0.

ASIA FOCUS #166

LA CYBERSÉCURITÉ GLOBALE ET LA GUERRE FROIDE 2.0

Par EMMANUEL MENEUT / Maître de conférences dans les Universités catholiques

SEPTEMBRE 2021

ASIA FOCUS

Collection sous la direction de Barthélémy COURMONT, directeur de recherche à l'IRIS, maître de conférences à l'Université catholique de Lille, et Emmanuel LINCOT, chercheur associé à l'IRIS et professeur à l'Institut Catholique de Paris – UR « Religion, culture et société » (EA 7403) et sinologue.
courmont@iris-france.org — emmanuel.lincot@gmail.com

PROGRAMME ASIE

Sous la direction de Barthélémy COURMONT, directeur de recherche à l'IRIS, maître de conférences à l'Université catholique de Lille
courmont@iris-france.org

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES
2 bis rue Mercoeur
75011 PARIS / France

T. + 33 (0) 1 53 27 60 60
contact@iris-france.org
@InstitutIRIS
www.iris-france.org