Penser la guerre économique : data is digital (I)

Auteur : Philippe MUELLER FEUGA

Ancien Responsable de la Mission Protection du secret (MPS/HFDS/SGDSN), et Auditeur au Contrôle général économique et financier des Ministères économique et financier (ER), Membre du Groupe de travail sur le rôle des territoires non coopératifs dans la déstabilisation de la finance mondiale. Membre du Working Group EFCSE - Gouvernance de l'information. Secrétaire général du Club des officiers de sécurité (ClOS).

21 Mars 2018

La guerre commerciale aura-t-elle lieu ? Contestation du « privilège exorbitant » du dollar comme monnaie de référence pour les transactions internationales, voire une possible guerre des monnaies dollar/yuan ? Hausse des droits de douane pesant sur les produits chinois, mais aussi européens, et autres mesures restrictives sur les secteurs technologiques en accord avec l'USTRi ou sur proposition du CFIUSii ? Le Président Donald Trump prend le risque d'engager une véritable guerre économique déjà amorcée par son retrait de l'accord de Paris sur le climat (juin 2017) et par sa décision de retirer les États-Unis (janvier 2018) de l'accord de libre-échange Trans-Pacific Partnership Agreement (TPP).

Ou faut-il y voir une volonté de rééquilibrage dans une guerre hybride globale non déclarée à plusieurs facettes (politique, économique, stratégique, tactique, psychologique, soft power, informationnelle, etc.) ? Paradoxalement, la Chine qui reste critique à l'égard des « valeurs éthiques » ou concepts occidentaux d'« équité commerciale » (dans les normes environnementales comme dans le domaine de la propriété intellectuelle – produits pharmaceutiques, licences, nouvelles technologies, etc.) apparaît tirer profit de ces deux retraits. Hésitante lors de la négociation du traité de libre-échange TPP (2015-2016), en bonne communicante, elle s'y montre désormais attentive en l'adoptant (mars 2018, Comprehensive and Progressive Agreement for Trans-Pacific Partnership ou CPTPP), après avoir pris la défense de l'Accord de Paris (avril 2016), et au final la voie du multilatéralisme contre un bilatéralisme imposé par « l'hégémonie » des Etats-Unis dans une confrontation jugée inévitable avec la Chine.

Quelle perception de la guerre économique ?

Alors qu'une guerre conventionnelle suivie d'une invasion par une puissance hostile apparaît « improbable »iii, les Etats-Unis se sentent menacés dans leur sécurité nationale soit par des missiles balistiques, nucléaires, chimiques ou biologiques et par des attaques terroristes ou de groupes armés, soit par des cyberattaques paralysant une partie des administrations, des entreprises et des infrastructures « vitales » ou « critiques » de leur économie organisée en réseaux et gérée par des systèmes informatiques (SI).

Selon l'amiral Michael S. Rogers, directeur de la National Security Agency (NSA) et commandant de l'US Cyber Command (US CYBERCOM), le scénario le plus défavorable impliquerait des « attaques destructrices » (outright destructive attacks) centrées sur certaines infrastructures critiques, couplées à une manipulation massive de données. Sont particulièrement vulnérables les systèmes bancaires ou les réseaux électriques, mais aussi ceux de l'assainissement, de la distribution

alimentaire, des communications, etc. dépendants d'automatismes et de l'Internet. Contrairement aux attaques militaires classiques, une cyberattaque peut être lancée instantanément de n'importe où, de manière la plus imprévisible avec une traçabilité difficile à reconstituer pour remonter vers ses auteurs ou hackers équipés des codes informatiques suite à une préparation par intrusions non décelées. Et la question n'est pas de savoir « si » conditionnel, mais « quand » et « comment », d'où une vigilance accrue en matière d'investissements étrangers, de coopération en R&D ou de transferts technologiques.

L'acte de guerre économique

Les conditions actuelles de la conflictualité limitent l'intervention directe traditionnelle (celle des armées) pour l'orienter vers une « stratégie indirecte » du type containment, moins par un protectionnisme classique que dans le contrôle des investissements « stratégiques ». En l'occurrence, illustrée par la dernière décision présidentielle (février 2018) suite à l'examen du dossier par le CFIUS, interdisant l'OPA sur Qualcomm spécialiste des technologies de la 5Giv, véritable rupture technologique vers l'ultra-connectivité sociétale, par un groupe chinois. Un tel contrôle aurait conduit à une captation du savoir-faire technologique de pointe, à un affaiblissement du fabricant américain, ce qui aurait laissé indirectement à la Chine la possibilité de déterminer les standards de la nouvelle génération de technologies mobiles avec des perspectives de marché intéressantes, voire de position dominante. Une stratégie de contrôle relevant davantage de la pensée du chinois Sun Tzu que du prussien Clausewitz !

La guerre des standards technologiques (competition between standards) n'est pas nouvelle, et participe à la même guerre économique sous d'autres aspects. La Chine apprend vite dans sa projection « globale », forte des expériences malheureuses antérieures. Comme dans le domaine des formats vidéographiques haute-définition, la compétition entre Sony et Toshiba (2002-2008) révélait l'enjeu du standard des DVDs haute définition (HD). Parmi d'autres exemples significatifs, ce furent les standards html:// et http:// des années 1990 permettant aux ordinateurs de communiquer entre eux avec une connectivité croissante à l'origine d'opportunités, mais aussi de menaces ou de cyberattaques. Leur nombre croissant peut être considéré comme une série d'« opérations » avant une « répétition générale » provoquant des dommages collatéraux importants, tels que subis par l'Estonie (2007) soumise à une attaque pilotée par des robots (botnets) depuis la Russie. La propagation de ransomware comme WannaCrypt ou NotPetya (2017) exploitant des failles de sécurité rend accessibles des bases d'informations « sensibles » comme les données personnelles, pouvant entraîner d'importantes pertes en capitalisation (Equifax en septembre 2017). Dans le monde des machines intelligentes et des communications entre équipements ou Internet des objets (IoT, applicable à l'automobile, aux smart cities, aux usines du futur mais aussi à des secteurs comme la santé, etc.), la connectivité accrue et le développement du cloud ou des plateformes soulignent le double enjeu au cœur de la « battle for digital supremacy » (The Economist, mars 2018) : celui du contrôle des standards universels et sécurisés, et celui de l'accès aux données. Or, data is digital. L'enjeu cardinal est celui de la captation et de la maitrise des données qui déterminent le web 4.0 marquée par la révolution de l'intelligence artificielle (IA) associée à l'intelligence humaine et au quantique, à un moment où les tensions pour le contrôle de l'Internet et le risque de sa balkanisation apparaissent en termes de souveraineté numérique.

Une telle connectivité situe l'acte de guerre économique dans une « guerre hors limites » précisée par deux officiers chinois, Qiao Liang et Wang Xiangsui qui éclairent la voie retenue vers la « souveraineté stratégique » selon des valeurs autres qu'occidentales (vision acceptable par le PCC, moins privacy versus security, mais ideology cum security). Soucieux de l'image de la relation entre pouvoir et violence pour atteindre un objectif et emporter la victoire, l'acte de guerre économique « hors limites » marque la nuance avec la conception Vom Kriege de Clausewitz qui peut conduire à la guerre

totale ou « à outrance » et à la mobilisation générale au profit des armées (ou économie de guerre). La nuance apportée par le « hors limites » est subtile : la guerre devient plus humaine, et les militaires n'ont plus le monopole de la guerre. Celle-ci est nécessairement une guerre hybride à dimension « globale », de tout instant et omnidirectionnelle aux multiples facettes en vue de contester « l'ordre mondial » traditionnel imposé par l'Occident. D'où l'impact des changements climatiques (« clean tech could become a trade battleground »), des technologies « propres » (solaire, éolien) pour répondre à une demande croissante en électricité (voitures électriques, data center, smart cities, etc.) corrélée aux innovations high tech comme le stockage de longue durée (batteries de nouveau type) susceptibles de révolutionner l'ensemble de la chaîne de valeurs mais pose la question de la cyber-sécurité des systèmes électriques… Ce qui risque d'entraîner une chute de la demande en hydrocarbures – sauf en gaz liquéfié (méthaniers versus gazoducs) –, et donc du prix du baril de pétrole, et une influence sur la géopolitique de l'énergie en général, de l'électricité en particulier : partenariat entre sociétés d'Etat Chine/Russie/Moyen-Orient, entre pays producteurs et consommateurs, dont importateurs sous l'angle des sanctions. Or, la Chine connaît la plus forte augmentation de la demande en gaz (+ 18% en 2017, soit le double de la croissance moyenne observée entre 2010 et 2016) alors qu'aux Etats-Unis, la production du gaz de schiste s'accélère, et les EU sont passés d'un statut d'importateur net à exportateur net.

L'acte de guerre économique « hors limites » conteste le concept d'équilibre des pouvoirs (balance of power) pratiqué durant la guerre froide avec la dissuasion nucléaire, et rejette le rôle attribué au système international depuis 1991 auquel la République populaire de Chine n'accorde aucune légitimité en raison de son approche idéologique du concept de la sécurité nationale. Le saut actuel qu'elle envisage trahi par ses objectifs extérieurs est celui des hautes technologies au service de sa puissance dans une perspective d'une cyberguerre aux effets comparables à des « armes à destruction massive » en raison de l'impact sur les secteurs vitaux des autres Etats, et par l'isolement de son cyberespace à la fois pour sa défense et pour la surveillance intérieure. Point de fragilité pour recruter les meilleurs talents même si statistiquement (selon des normes internes) la Chine forme de nombreux ingénieurs ou déposent de nombreux brevets… Une course aux nouvelles technologies numériques de seconde ou troisième génération (quantique) à forte intensité d'investissement est en cours entre les deux grandes puissances États-Unis et la Chine, les projets européens concernés par les technologies quantiques (Rydberg Quantum Simulators RYSQ, l'ingénierie quantique à l'UPSaclay, le Quantum Technology flagship) ne s'intégrant pas dans un acte stratégique de guerre économique. Une course à la cyber-dissuasion (cyber deterrence) semble plutôt ouverte avec la Russie dans ses rapports avec les pays baltes ou de l'Est européen, et celle-ci apparaît davantage comme supplétif des Chinois depuis 2001. Peu encline à une « concurrence responsable » faute d'une économie développée, les réseaux organisés y opèrent dans le « chaos informatique » issu du dark net à l'image du logiciel de rançon à 300 dollars en bitcoins WannaCry (mai 2017) capable de frapper rapidement plus de 150 pays, certes « de manière indiscriminée » en raison de la structure du web affectant le fonctionnement des hôpitaux au Royaume-Uni, des chemins de fer allemands, de la Banque centrale russe, du géant américain Fedex, des usines Renault, de la compagnie espagnole Telefonica, d'universités en Italie et en Grèce, etc. à partir d'une faille dans les systèmes Windows XP divulguée dans des documents piratés de la NSA.

L'acte de guerre « hors limites »

Dans ce contexte ultra-concurrentiel et chaotique, la Chine vise à combattre l'influence ou la superpuissance américaine hors frontières classiques, ce qui inclut tous les domaines et leurs combinaisons comme l'écologie, la psychologie, la criminalité, les réseaux, la technologie, les matières premières, l'aide économique, la culture, le droit international, etc. Si possible en évitant un conflit armé (sans l'exclure), même si l'objectif de soumission ou de suprématie est un « but stratégique de puissance » à moyen ou long terme (si possible pour 2049, centenaire de la prise du pouvoir par Mao

Zedong). Tous les secteurs sont concernés, appelés à assurer la « sécurité nationale » de la Chine dans une conception renouvelée de l'« empire du milieu » associé à un contrôle des données, non sans arrière-pensée politiquev.

Guerre économique, guerre électronique ou guerre numérique ? L'approche est forcément « hybride » et se décline en high tech au point de pouvoir parler de « dual-use tech cold war » en raison de l'émergence permanente d'armements de conception nouvelle en lien avec les nouvelles conditions de « compétition numérique » autour d'équipements électroniques, quels qu'ils soient, intégrés ou embarqués, tous transmetteurs d'informations à assurer (cyber-sécurité) et à contrôler. Plus précisément, la Russie et la Chine, mais aussi des pays comme l'Iran, Israël, la Corée du Nord travaillent sur l'autonomie de leurs réseaux dans un souci de souveraineté tout en œuvrant à tester l'architecture de ceux de leurs « concurrents » ou « rivaux ». De moindre coût que des armes sophistiquées ou une cyberdéfense difficile à organiser, malgré l'existence d'ingénieurs compétents ou de sociétés d'excellence comme Kaspersky, la recherche dans les systèmes à propagation de rayonnements électromagnétiques et de multi-captages de renseignements sont autant utiles pour les activités commerciales ou diplomatiques que militaires (notamment dans la constitution de « systèmes de systèmes » à base d'intelligence artificielle, dès by design).

L'importance donnée au cyberespace et aux technologies électromagnétiques n'exclut pas la recherche de systèmes de défense, voire de dissuasion (cyber deterrence) moins coûteux et à forte profitabilité comme le déni de service (DoS) ou la neutralisation des systèmes de transmission et des circuits de contrôle (survol de l'USS Donald Cook équipé du système de combat de dernière génération Aegis par un Su-24 en mer Noire, 12 avril 2014). Les guerres au Moyen-Orient, et en Syrie en particulier, permettent des tests grandeur nature. Plus généralement, et de manière insidieuse, il est possible d'intercepter le trafic radio sur les réseaux, le nombre et le type d'aéronefs, les trajectoires de vol, ainsi que le type d'arme utilisé, les objectifs ciblés et leur emplacement, etc. avec l'organisation de dysfonctionnements des systèmes électriques et électroniques d'une région, non sans graves conséquences sur la continuité d'activités du pays et le quotidien des populations. Ce qui rend la guerre « hors limites » et change fondamentalement la nature de la guerre menée par les armées en la fusionnant avec la guerre économique à des fins de puissance.

Dans cette cyberwar ou guerre de l'information (en tant que computing et data), les modes d'action se regroupent en trois étapes, avec des résultats encore aléatoires : i) l'action électronique utilise les rayonnements électromagnétiques à des fins d'attaque en perturbant les communications ciblées, en contribuant aux actions de « déception » (pour les activités en réseaux) ; ii) la sécurité ou défense électronique vise à garantir la liberté d'action dans l'utilisation des SI, sans perte dans la qualité de l'information ; iii) et la surveillance électronique contribue à alimenter l'intelligence économique. L'incertitude des résultats et la méconnaissance de certaines vulnérabilités conduisent à la conclusion : « The law of war is inadequate or irrelevant in the context of cyber conflict », selon Dennis C. Blair, ancien directeur du National Intelligence (2009-2010) directement rattaché au Président américain : si la guerre a des règles et des limites (Clausewitz, Vom Kriege), s'appliquent-elles à la cyberguerre avec ses multiples formes hybrides de cyberattaques, annoncées ci-dessus ?

Même si un groupe d'experts juridiques et militaires ont pubié le Manuel de Tallinn (2013), l'impact de l'ère de l'information sur les guerres conventionnelle ou économique est devenu le problème majeur en vue de protéger les actifs (assets) informationnels qui s'inscrivent dans le haut des bilans. Contrairement aux batailles du passé, la capacité de cyberattaques est imprévisible, car elle peut émaner à la fois d'acteurs étatiques et de groupes non étatiques (hackers, cyber-terrorisme, cybercriminalité, etc.) capables de paralyser des régions ou des sociétés entières comme déjà observées. La guerre, selon Clausewitz, est caractérisée à la fois par le moyen, la violence physique extrême et la fin en imposant sa volonté de puissance à un adversaire. La Russie actuelle y semble adepte sachant que « der Westen hat dem hybriden Krieg des Kreml wenig

entgegenzusetzen, denn er hält sich gewöhnlich ethnische Normen »vi. Côté Chinois, dans l'exposé de Qiao Liang et de Wang Xiangsui, les moyens utilisés n'importent plus car « hors limites ». Mais dans ce cas qu'est la différence entre guerre et concurrence ?

En réponse à ce contexte numérique globalisé, mais en décalage total avec l'approche consensuelle de l'Union européenne qui a conduit aux échecs des Stratégies de Lisbonne, à une perte de compétitivité et au pillage de ses actifs, à peine atténués par certains Etats membres à puissance relative comme la France, le Royaume Uni ou l'Allemagne, les Etats-Unis du Président Trump adoptent un comportement novateur de rupture sur les conditions concurrentielles, dominées par la concurrence déloyale (unfair competition) entre grandes puissances. Une concurrence exacerbée par l'usage et les manipulations dans le cyberespace d'algorithmes, de technologies avancées grâce à une IA efficace associée à des drones, des robots, etc. L'angle d'attaque s'élargit et se modifie perpétuellement, s'appuie de plus en plus sur l'anticipation autour de la cyber-résilience de l'environnement informationnel convoité.

Celui-ci devient la matrice de la puissance « hors limites » en trois volets stratégiques parfaitement compris par la Chine : l'accès et la maitrise de l'information « sensible », le contrôle des flux de certaines de ces données (bancaires, santé ou R&D) et la maitrise des technologies associées à l'IA (éducation et normes ou standard). « Guerre silencieuse et paix imprédictible »vii ? La guerre pour l'information accompagne celle de l'information par le contrôle des systèmes d'information (SI) en vue d'atteindre les informations stratégiques, confidentielles ou « sensibles ». Les menaces comme les exploits zero day indiquent que le retour de l'Etat est nécessaire, mais – selon les régions, notamment en France et dans l'Union européenne – reste inachevé, encore convaincu que seul le durcissement du contenant, c'est-à-dire des systèmes d'information (SI), est à retenir dans une vision obsolète top down. Aussi, à l'ère de l'Information Age, quelle stratégie faut-il adopter pour réussir dans un monde qui bascule irrésistiblement vers le virtuel et où les grandes puissances rivaliseront avec acharnement même si elles essaient d'éviter la guerre entre elles dans une « concurrence responsable » ?

Avertissement

La présente note a pour objectif d'interroger la notion même de « sécurité nationale » portée à l'échelle européenne, et de tenter de l'introduire dans la construction européenne à un moment où le doute sur l'efficacité des institutions européennes conduit à l'euroscepticisme.

Un de ses objectifs est d'élever la protection de toute « donnée sensible » au niveau de cette sécurité au-delà du périmètre « secret défense », c'est-à-dire du noyau dur de la DGA (direction générale de l'armement) et porté par l'IGI n° 1300, ainsi que par les textes règlementaires ayant pour objet la PPST (protection du patrimoine scientifique et technique) et les OIV (opérateurs d'importance vitale) définis dans les DNS (directive nationale de sécurité), ou les référentiels ad hoc de l'ANSSI sur la sécurité des systèmes d'information.

La présente note, comme les suivantes sur ce thème, est conçue de manière à être indépendante les unes des autres, tout en gardant une logique « d'indépendance et de puissance technologiques » en France, et peut-être pour l'UE, à solidifier.

[i] Cf. le rapport de l'US Trade Representative au Congrès américain, *On China's WTO Compliance*, janvier 2018. https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf

[ii] Le Committee on Foreign Investment in the United States (CFIUS) est un comité inter-administrations ayant le pouvoir d'examiner les investissements étrangers aux États-Unis pour des raisons de sécurité nationale, notamment les *« covered transactions »* qui pourraient entraîner le transfert du contrôle d'une entreprise américaine à une personne non-américaine.

[iii] *« Paix impossible, guerre improbable »* est le titre du premier chapitre de l'ouvrage de Raymond Aron, *Le grand schisme, (*1948) pour désigner la Guerre froide naissante, et pour qualifier l'apogée de la Guerre froide (1947-1962) ou l'ensemble de la période (1945-1991).

[iv] Cf. le rapport de l'Arcep sur la 5G https://www.arcep.fr/uploads/tx_gspublication/rapport-enjeux-5G_mars2017.pdf

[v] Inspiré du RGPD européen, l'article 37 de la nouvelle loi chinoise sur la cyber-sécurité, qui est entrée en vigueur en 2017, stipule que les informations personnelles et autres données *« importantes »* recueillies ou produites par les opérateurs intérieurs doivent être stockées sur le territoire chinois.

[vi] *« L'Occident n'a pas grand-chose à opposer à la guerre hybride du Kremlin, car celle-ci contient généralement des normes ethniques »*, *NZZ* du 17 mars 2018.

[vii] Cf. *« Cyberespace, nouvelles menaces et nouvelles vulnérabilités »*, Philippe Muller Feuga, *in* la revue *Sécurité globale*, nouvelle série, n° 9, mars 2017, pp. 83-95.