CYBERESPACE, NOUVELLES MENACES ET NOUVELLES VULNÉRABILITÉS

Guerre silencieuse et paix imprédictible

Philippe Muller Feuga

ESKA | « Sécurité globale »

2017/1 N° 9 | pages 83 à 95

ISSN 1959-6782
ISBN 9782747226783

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-securite-globale-2017-1-page-83.htm

Pour citer cet article :

Philippe Muller Feuga, « Cyberespace, nouvelles menaces et nouvelles vulnérabilités. Guerre silencieuse et paix imprédictible », *Sécurité globale* 2017/1 (N° 9), p. 83-95.
DOI 10.3917/secug.171.0083

Cyberespace, nouvelles menaces et nouvelles vulnérabilités

Guerre silencieuse et paix imprédictible

*Philippe Muller Feuga**

Depuis le premier réseau (né avec Arpanet en 1969) aux dix nœuds (nodes) de 1974, dissocié de l'usage militaire en 1980, l'Internet[i] a évolué au cours de ces quatre dernières décennies vers des activités civiles par la création de la *« toile »* ou *world wide web* (1989), avec une accélération exponentielle conduisant au cyberespace. Reconnu comme un *« nouveau monde »*, institutionnalisé à Davos en février 1996 à un moment où des Big Five (GAFA + T)[ii] n'existaient qu'Apple et Amazon, tout était déjà *« inventé »* en tant que système d'échanges créatif, mais menacé par ses propres vulnérabilités intrinsèques ouvrant la voie aux manipulations de *hackers* ou de black hats (dès 1988 le ver Morris sévit), qui déstabilisent tout responsable face aux menaces persistantes avancées (APT, *Advanced Persistent Threats*).

La *Déclaration d'indépendance du cyberespace* (*Declaration of the Independence of Cyberspace*) publiée par John Perry Barlow, l'un des cofondateurs de l'EFF[iii] issu du mouvement libertaire *open source* d'origine californienne, rappelait aux gouvernements que *« Vous n'avez aucune souveraineté là où nous sommes rassemblés »*[iv], autrement dit que la réglementation et l'application de la loi par l'Etat ne s'y appliquent pas, auquel fait écho aujourd'hui la notion de *« neutralité du Net »*.

Ce nouvel espace est au coeur des échanges socio-économiques actuels, objet de cyberattaques ou de piratages mais aussi source de conflits potentiels. Les enjeux de puissance et de souveraineté disparus en 1989-91 avec la fin de l'Histoire refont surface dans un contexte de morosité économique mondiale, voire sur fond de chaos. Analysés dès 1993, non sans arrière-pensées budgétaires pour la Défense américaine, par l'étude *« Cyberwar is coming »* financée par la Rand Corporation, la cyberwar est présentée

comme le Blitzkrieg du XXIe siècle par effacement du *« brouillard de la guerre »* ou *Kriegsnebel* selon Karl von Clausewitz (1834), brouillard d'incertitudes dû à l'insuffisance d'informations (*der Krieg ist das Gebiet der Ungewissheit*) désormais compensée par l'Internet, tandis que, version civile, le cybernet appartient à la cybercriminalité.

Force est de constater que dans le *« projet »* européen ces deux *« guerres silencieuses »* sont totalement oubliées, y compris dans la *Stratégie de Lisbonne* énoncée en mars 2000 visant à faire de l'Union européenne à échéance 2010 *« l'économie de la connaissance la plus compétitive et la plus dynamique du monde, capable d'une croissance économique durable accompagnée d'une amélioration quantitative et qualitative de l'emploi et d'une plus grande cohésion sociale »*, stratégie revisitée en 2005 et en 2009 devant le constat d'échec et la perte de compétitivité.

Exemple même de stratégie totalement déconnectée des réalités par une vision technocratique *top down* à court terme, bâtie sur l'euphorie de la première bulle technologique apparue fin 1998, visant notamment en France à l'intégration des TIC comme priorité (rapport de Gérard Théry en février 1994 reprenant l'expression du vice-président américain Al Gore d'*« autoroutes de l'information »*) tout en en ignorant les risques.

Ce cyberespace peut être décliné comme un domaine aux contours insaisissables, né de l'imaginaire de Gibson dans *Neuromancer* (1984), mais caractérisé par un *« potential for unintended cascading effects »* (2016)[v] que la France découvre lentement lors de la publication des *Livres blancs de la Défense* de 2008, et d'avril 2013 et de la loi de programmation militaire (LPM, décembre 2013). Une première stratégie de cybersécurité est élaborée début 2011 *« peu après la découverte d'une attaque informatique à des fins d'espionnage contre les ministères économiques et financiers »* selon la présentation de la *« Stratégie nationale pour la sécurité économique »* (octobre 2015). Le mot cyberespace y est cité 42 fois, sans en définir les contours que propose l'ANSSI, autorité nationale française rattachée au SGDSN : *« espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques »*.

L'approche est essentiellement technocentriste de son contenant comme observé dans les nouvelles règles qui s'appliquent aux opérateurs d'importance vitale (OIV) ce qui dénote un trouble dans la compréhension du cyberespace et de ses véritables enjeux, vingt ans après les Etats-Unis. Elle conduit aux mesures, certes nécessaires mais insuffisantes, visant à renforcer la sécurité et la défense des systèmes d'information (SI), soutenues par le paramètre géographique (le territoire national), le cyberespace étant alors présenté comme le cinquième domaine après la terre, la mer, l'air et l'espace sur lesquels se déploient des forces et une pensée stratégique dans le contexte d'une *« paix imprédictible »*. Mais sans vision globale

stratégique, dans une conception erronée ou *« exagérée sous l'effet d'un clair de lune »* (Clausewitz) qui rappelle les conditions de l'*« organisation des nouvelles frontières »* (1919) et la construction de la ligne Maginot.

L'approche de l'Internet est donc biaisée dès ses origines, en France comme en Europe, par l'intérêt immédiat porté sur les fragilités du contenant ou à l'outil plutôt qu'à son contenu. Dès lors une définition est à retenir : *« Le Cyberespace est un domaine caractérisé par l'utilisation de l'électronique et du spectre électromagnétique à des fins de stocker, modifier, et échanger des données par l'intermédiaire des systèmes gérés en réseau et des infrastructures physiques associées. En effet, le Cyberespace peut être considéré comme une interconnexion des êtres humains par des ordinateurs et la télécommunication, sans souci de la géographie physique »*[vi] : elle désigne la *« donnée »* ou *data* comme autre cible potentielle car celle-ci, au coeur de la connaissance et des enjeux contemporains, n'est pas neutre.

Elle dépasse le débat actuel européen autour de la cybersécurité vers celui de la menace qui pèse sur toute donnée *« sensible »*, confidentielle ou stratégique couverte par le *« secret défense »*.

La *data* devient l'unité de base de l'Information age qui succède aux révolutions industrielles. Source de nouvelles valeurs au coeur des enjeux de compétitivité actuels, objet de toutes les convoitises en tant que nouvelles richesses des Nations, elle est menacée dans le contexte actuel de morosité économique. Il s'agit d'aller chercher de la valeur avec un effet de levier extraordinaire grâce aux avantages comparatifs qu'elle procure sur l'emploi et la croissance par la transformation digitale de la société (1).

Sans pour autant déprécier le rôle de l'Etat ou de l'autorité qui doivent l'accompagner ce qui exige, compte tenu des vulnérabilités nouvelles, une mutation dans l'organisation interne des entreprises et des pouvoirs publics soumis encore à un gap culturel, héritage d'une pensée unique dépassée (2).

I. Nouvelles richesses des Nations

Le cyberespace évoque à la fois le réel et le virtuel avec le basculement du premier vers le second sous le double effet de la numérisation ou transformation digitale (*digital age*) et de l'expansion de systèmes informatiques organisés en réseaux (la toile, ou *web*) au sein de l'Internet. Le premier produit de l'information numérique ou *data*, le second permet le partage, le stockage et l'échange de la *data* entre utilisateurs ou internautes, connectés ou non selon l'instant d'usage, non sans menaces.

Nouvelle matière première convoitée et avantages comparatifs

La diffusion et le stockage de l'information bénéficient constamment des innovations

technologiques et techniques qui améliorent les langages, le traitement ou l'exploitation des données. Le développement des accès à haut-débit, puis à très haut débit vers la toile (ou world wide *web*) sous l'action d'applications toujours plus nombreuses depuis le premier courrier électronique privé ou professionnel (*e-mail* inventé en 1972) ou la multiplication de pages *web* (standard html), unité de consultation mesurée en unité de stockage[vii], crée une véritable rente virtuelle captée notamment par les acteurs de l'oligopole américain du *web*.

Les technologies numériques et l'usage de l'IP (*Internet Protocol*) participent aux processus cognitifs et transforment fondamentalement les modèles hérités des âges fordiens tant dans les coûts marginaux de stockage (Amazon), de duplication de l'information (Google), de la diffusion de la connaissance (*knowledge age*), de coûts de traitement, etc. que par les économies d'échelle (à l'origine de plus de la moitié de la croissance de la productivité européenne) et les progrès qu'elles engendrent, obtenus dans tous les composants par la réduction des coûts unitaires et l'accroissement des performances selon la loi de Moore (doublement des performances tous les deux ans).

La numérisation accrue des contenus et des services, transforme un simple espace d'échanges statiques d'informations comme les *web* logs devenus blogs (*web 1.0*) en un espace de plus en plus interactif dans les domaines de la connaissance et du marketing, entre internautes et sur les réseaux sociaux (*web 2.0*) à partir des années 1996-98.

L'*Industrial age* s'efface devant l'*Information age* dont la *data* devient la matière première par excellence et dont il faut assurer l'accès et la sécurité. Au rythme des tendances ou *« tech trends »* qui structurent les activités économiques selon la loi de Robert Metcalfe – *« l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs »* – (1992), le cyberespace participe à la création de métadonnées ou *Big Data*, gisements inépuisables car renouvelables par la connectivité accrue des objets et des personnes, mais aussi des machines entre elles grâce à l'intelligence artificielle (IA), en rappelant que le premier apport est aléatoire (données de l'internaute), le second repose sur l'automatisation des systèmes de commande ou de contrôle industriels (type SCADA)[viii], sur les systèmes de système, etc. mais reste prédéterminés par l'homme avec ses risques d'erreurs.

Convoitée et donc menacée, la donnée éminemment désirable s'inscrit dans le haut de bilan de toute entreprise en tant que nouvel actif à saisir, copier, accaparer par prise de contrôle ou à piller dans une guerre économique *« hors limites »*[ix] ou *unfair competition* qui ne dit pas son nom, sans déclaration de guerre, sans morts mais avec des victimes suite aux pertes d'emploi liées à la perte de compétitivité.

Le cyberespace autorise non plus le partage de documents (page *web*), mais aussi celui

des données (*web* of *data*) entre internautes (standard http) ou entre machines (standard uri), voire les deux dans un réseau global : il laisse poindre le *web 3.0* (*semantic web*), et laisse soupçonner le *web 4.0* par connexion des intelligences (*intelligence web* ou *metaweb*) ou l'hyperconnectivité du monde organisée en réseau P2P (*person-to-person*) ou P2M (*person-to-machine*). L'Internet révolutionne ainsi le quotidien, le social et l'économie, induit des changements majeurs des paradigmes issus des révolutions industrielles dans des secteurs verticaux tels que l'industrie, la santé, l'énergie, l'environnement, l'éducation, etc. ou horizontaux comme la domotique, les villes ou réseaux intelligents appelés smart cities ou smart grids, les véhicules interconnectés, etc.

L'Internet des objets (*IoT*) nourrit le *Big Data* et crée ce nouveau monde du cyberespace tout en occultant les menaces. Par la digitalisation de la société, de nouveaux acteurs bousculent les business models, notamment dans l'*Industrie 4.0* vantée en Allemagne. Dans le domaine de l'*IoT* industriel, une société comme General Electric traite 50 millions de données collectées provenant de 10 millions de capteurs industriels, soumises à ses *data scientists* qui analysent les données marketing pour développer des solutions *IoT*, parfois en lien avec des *designers*. L'apparition de nouveaux types de données en de grands volumes avec les innovations *data*-driven pose la question des conditions de l'interopérabilité dans un monde ouvert avec ses menaces imprédictibles.

Environnement informationnel

Les améliorations apportées à la puissance, à la vitesse de traitement des données (algorithmes) ou à la capacité des supports donnent lieu à des problèmes de sécurité croissants qui conduisent à sécuriser non pas uniquement les systèmes d'information (SI), mais la donnée et l'utilisateur (principe de la blockchain). Dans cette *« destruction créatrice »*, l'affichage d'une information numérique est le résultat d'une harmonie entre couches et sous-couches superposées (layers) des SI, chacune d'entre elles ayant un rôle précis, mais chacune d'entre elles pouvant comporter des failles utilisées par des cyberattaquants. Retenons trois couches : la couche physique ou matérielle (*hardware assets*) construite autour de codes et de systèmes d'exploitation des matériels et logiciels où se situent les principales vulnérabilités en termes de blocage ou de manipulation.

Celle-ci supporte la couche logique des programmes (*logic network layer*) avec leurs codes appelés à numériser l'information, l'utiliser et l'acheminer selon les protocoles de l'Internet (adresse IP) au travers l'URL (adresse d'une page *web*), considérés *« comme des données mixtes, qui peuvent comporter à la fois des données de connexion et des mots faisant référence au contenu de correspondances échangées ou d'informations »*[x] ; et la couche cognitive ou sémantique composée de la *cyber-persona layer*, sous-couche d'identification sous forme digitale d'un individu ou d'une entité, chacun pouvant avoir plusieurs cyber-iden-

tités par son ou ses *e-mails*, adresses d'ordinateur ou de terminal, de téléphones portables, etc. en raison de la mobilité croissante des systèmes).

Or, toute architecture SI dans ses couches historiques comportent des vulnérabilités, et un *hacker* se nourrit de ces failles logicielles à durée plus ou moins limitée prêt à les exposer sur le *web* ce qui peut déclencher des cyberattaques, des dénis de service (DDoS) ou à les marchander sur le dark *web*, partie du deep *web* non référencée du cyberespace. Car la valeur de la *data* s'accroît et engendre désormais une cybercriminalité moins risquée que le trafic de stupéfiants ou des armes, celle-ci se nourrit d'elle-même avec des *hackers* qui, sans être des génies, s'adaptent et savent exploiter toute brèche (*« exploits »*) de l'environnement informationnel en pleine évolution, comme les systèmes embarqués utilisés au quotidien ou tout terminal branché sur l'Internet via un réseau wi-fi passant aux attaques multivectorielles et prenant pour cible la *data* selon sa valeur, de la prise de contrôle de sites *web* de confiance à celle de logiciels d'exécution de fichiers selon les *« métiers »*.

Avec la généralisation du *cloud computing*, des *datacenters*, l'utilisation d'*application programming interfaces* (API) non sécurisées de *webservices* ou de communications inter-organisationnelles de ces API par des passerelles B2B en parallèle à l'Internet mobile et des systèmes Byod, et quel que soit le budget consacré, ou quel que soit le rôle d'organismes comme l'ANSSI, des CERT[xbis] (ou CSIRT) mis en place en 1988 dans la plupart des pays lors des premières attaques, ou d'expertises – comme le CDSE ou le Clusif en France –, il est impossible que les DSI puissent avoir une connaissance précise de leur architecture composée du millefeuilles des évolutions techniques de l'Internet, à commencer lors du passage de l'analogique ou numérique (années 1990), combinée à des négligences humaines.

Et il n'est pas certain que même les autorités en aient une meilleure en donnant la priorité à la sécurisation des deux premières couches (sécurité physique et sécurité logique) facilement manipulables et falsifiables, preuve d'une dissonance cognitive déterminent la troisième, la plus stratégique. C'est le syndrome Krupp : innover et s'adapter en permanence aux attaques tout en développant des systèmes de blindage ou en l'occurrence de sécurité, vite obsolètes.

Les entreprises sont menacées au coeur de leurs actifs, mais les menaces demeurent asymétriques, car de plus en plus imprévisibles faute d'être identifiées, ou menaces *zero-day* (*zero day exploit attack*) qui peuvent être particulièrement destructrices, comme Stuxnet en 2010 ou Flame en 2012 avec un risque systémique. Ce qui exige la définition d'une véritable cyberstratégie au niveau de l'Etat pris dans un dilemme cornélien entre d'une part l'accroissement des contrôles sécuritaires, et d'autre part l'accroissement de la productivité par *« reduce frontline productivity by slowing employees' ability to share information »*.

Ce qui peut provoquer un effet *« cyberbacklash »* (effet boomerang) qui décélère la digitalisation et conduit à terme à un décalage technologique dus aux coûts supplémentaires engendrés par la cybersécurité, avec risques de pertes de compétitivité, et de désavantages comparatifs que subit la France (6e puissance dépassée en 2016 par le Royaume Uni, et une industrie qui pèse 10% dans le PIB contre 21% en Allemagne).

Comment l'expliquer si ce n'est par une approche erronée de certains responsables qui se sont focalisés sur la *« transversalité des TIC »*, et non par une approche stratégique globale du futur ? L'Etat stratège a privilégié la stratégie de mise en oeuvre d'une cyberligne Maginot, choix également retenu par la Chine et la Russie dans des conditions particulières. Mais une stratégie globale doit privilégier davantage privilégier la construction d'un *« écosystème de confiance »* dans l'environnement informationnel qui reste à structurer autour des secteurs stratégiques souverains définis dans le cadre du changement du paradigme post industriel.

II. Le retour des Etats pour faire face aux menaces ?

Vingt ans après la déclaration de 1996, les défis du cyberespace restent au coeur du Forum économique mondial (WEF) de Davos où les coûts liés au piratage et vol de données sont évoqués. L'expansion du cyberespace conduit à s'interroger sur le dilemme *« privacy versus security »* après l'épisode de San Bernardino (mars 2016), libertés publiques et vie privée *versus* surveillance et défense ou sécurité. Mais ne nous égarons pas : le *digital age* n'efface en rien le rôle des Etats et leur souveraineté comme l'ont cru les penseurs généreux du punk net, les tenants de l'open source à l'époque du *web 1.0* ou le mouvement hacktiviste *Anonymous*. Le cyberspace a pris le visage de Janus, et si le cyberespace est présenté comme opposé aux Etats, à leur souveraineté et prérogatives et hors champs territoriaux comme semble l'attester les cyberattaques, les enquêtes permettent d'arrêter des *hackers* attestant d'une certaine efficacité, le *web* étant aussi une arme pour les autorités.

Face aux menaces, le retour inachevé de l'Etat

Dans le cyberespace, l'angle d'attaque se modifie et s'appuie de plus en plus sur l'anticipation autour de la cyberrésilience de l'environnement informationnel que doit intégrer tout Etat stratège. En France, il a conduit, certes, au succès du programme Ariane, mais aussi aux échecs du Plan Calcul, voire du programme *Cyclades*. Le premier était essentiellement technique répondant à un choix stratégique visant à assurer l'indépendance et la souveraineté de la France (lanceurs), voire de l'UE ; à un moment où l'Internet se construisait, toujours, dans une vision *top down*, les seconds ont fait l'impasse sur l'élément humain dans une approche technocentriste pour favoriser une administration (les télécommunications). Or,

les mesures prises restent inachevées, et de toute évidence aucun gouvernement n'a encore réussi à relever le défi de l'environnement informationnel et de la souveraineté numérique.

L'Etat stratège global doit inverser les facteurs, et privilégier l'approche bottom up auprès des acteurs économiques. Ce sont des données qui *« parlent »* au réel, données personnelles (identité, santé) ou toute autre information plus ou moins confidentielle (industrie, affaires) ou sensible (bancaire) collectée, véritables mines (*data mining*) pour les moteurs de recherche conquérants en termes de compétition déloyale (unfair competition), et données *« stratégiques »*. Si avec la croissance des fraudes et autres menaces, les autorités s'adaptent à la cybercriminalité. Les actes de malveillance sont gérés avec une certaine efficacité en termes de fraudes ou d'infractions, le contexte terroriste ayant conduit à cette prise de conscience dans des conditions tragiques, mais davantage sous un angle politique qu'économique avec l'adoption de textes sécuritaires après l'adoption de la LPM (2013).

Mais l'approche reste parcellaire, et mérite une réponse stratégique plus globale tant sur le plan de la protection des données, à commencer par les données personnelles. Que ce soit pour le *« droit à l'oubli »* ou le *Safe Harbor* pour lequel la CJUE a su réagir en octobre 2015, la réglementation européenne s'impose aux grands acteurs du numérique qui, dans un premier temps californien, ont voulu imposer leurs valeurs tout en dictant leurs conditions générales d'utilisation (CGU) désormais sous la surveillance des CNIL nationales. Comme quoi la dimension extérieure dans la construction européenne peut retrouver toute sa place, et peut-être réconcilier les citoyens avec les institutions européennes.

Fondamentalement, la place de la souveraineté dans le champ régalien reste la défense, la police et la sécurité, la justice ainsi que la fiscalité même si la notion de *« neutralité du Net »* avec quelques réserves reste affirmée par les régulateurs des télécommunications. D'autres exemples récents montrent que l'approche territoriale, donc de souveraineté, deviennent possibles en s'appuyant sur les réalités tangibles des trois couches, notamment sur les données de localisation parfaitement recensables ou indicatives. Sur le plan fiscal ou juridique, le dossier Apple dans un contexte de concurrence fiscale entre États membres de l'UE, ou les actions menées contre Google pour abus de position dominante, de même que les conceptions différentes en matière de *copyright* ou de propriété intellectuelle montrent que l'UE peut réagir aux exigences extraterritoriales des Etats-Unis. S'il n'existe pas en droit, le concept de *« souveraineté européenne »* s'exprime sur les territoires nationaux des Etats membres en attendant de franchir l'étape du fédéralisme.

Il est vrai qu'il est exacerbé par les révélations de *« lanceurs d'alerte »* montrant le rôle des États-Unis et du Royaume Uni (entre autres) dans la captation de nos don-

nées, privées ou professionnelles avec leurs services de renseignements respectifs, la NSA et le GCHQ. Avec la publication de la directive européenne (avril 2016), la question peut être élargie en matière de secret d'affaires car celle-ci reste trop limitée à la définition de l'accord sur les ADPIC de Marrakech (1994), et ne correspond pas à l'attente des entreprises européennes en termes de protection de leurs actifs face à l'arsenal juridique américain.

Si le temps des conflits frontaux associés aux conquêtes territoriales semble en partie révolu (malgré l'Ukraine, la Syrie ou la mer de Chine), celui du rejet du bloc occidental est conduit par les BRICS à la recherche d'un nouveau centre de décision, et la course à l'innovation supplante la course aux armements dans le cyberespace comme s'y sont engagées la Chine et la Russie. L'oligopole américain du *web* est bien entendu visé : en lien avec les organismes de gouvernance, soutenus officiellement par les Etats-Unis (IETF sur le plan technique créé en 1986, le W3C en terme de compatibilité créée en 1994, et l'ICANN créé en 1998 pour l'adressage IP et les noms de domaine de premier niveau) qui apparaissent comme une justification de l'extra-territorialisation du droit américain (ne serait-ce que dans les clauses d'utilisation de nombreux sites, plateformes ou réseaux sociaux), par ailleurs observé dans d'autres dispositifs comme l'ITAR ou l'OFAC.

Les rivalités existent autour de prise de contrôle, comme celle de l'ICANN au-delà de la question de l'appartenance ou non de l'Internet ou du cyberespace aux « global commons », espaces d'intérêt commun. Pour d'autres espaces comme la mer, l'espace aérien ou stratosphériques, mais aussi en matière de télécommunications (UIT, institution spécialisée des Nations Unies créée en 1865) et le statut particulier de l'Antarctique, force est de constater que des droits internationaux s'y appliquent, avec des points d'entrée physiques (ports en droit public maritime, ou aéroports en droit international de l'aviation civile, comme pour l'espace ou des activités spatiales) en lien avec les souverainetés nationales. Dans le cyberespace, il existe aussi des points physiques d'entrée.

Encore faut-il que l'Etat stratège, même au niveau européen, raisonne en termes de puissance et donc de stratégie face aux menaces. A défaut, c'est un management de l'environnement informationnel qui doit se mettre en place sur le plan national. La France aurait pu définir une stratégie globale mais le SGDSN n'a pas su se montrer à la hauteur des attentes notamment sur les données sensibles lors de la réforme (inachevée) de l'IGI n° 1300 sur la protection du secret de la défense nationale en posant la question des OIV et des acteurs des secteurs stratégiques et en s'appuyant sur certaines mesures prises par des sociétés du secteur de la défense comme Safran, Thalès, etc. Certes le rôle de la Défense et de la DGA en particulier est structurant par l'organisation de l'environnement informationnel grâce à l'approche par la donnée et sa liaison au facteur humain.

C'est une nécessité dans la défense des actifs informationnels. Ce management de l'environnement informationnel *« de confiance »* à construire est une approche qui modifie complètement la hiérarchie et la structure organisationnelle en *« silos »*. Avec l'expansion du cyberespace et ces *fins de mondes*, il s'agit d'agir pour transformer les anciens paradigmes et répondre aux exigences de réactivité, de rapidité, se réactivité ou d'adaptabilité, bref l'introduction d'une *« agilité institutionnelle »* : qui d'un DSI peut affirmer qu'il contrôle l'ensemble du millefeuille informatique (SI) de sa société ? Qui d'un DRH peut affirmer que les personnes employées sont au-dessus de tout soupçon, même parmi les accréditées ?

Qui d'un DMO peut affirmer connaître la cartographie des informations sensibles chez lui ? Relevant de la confidentialité, il s'agit de gérer l'environnement informationnel du cyberespace : ceci passe par la nécessité d'évaluer ses actifs informationnels, de les classer selon leur sensibilité en lien avec la gestion d'identité (IAM, *Identity and Access Management*) pour l'accès aux applications internes et externes corrélé à ce qui est plus ou moins *« sensible »* ou *« stratégique »* comme actif à protéger en rapport avec le *« métier »*.

Pour une stratégie globale

L'adaptation de cette nouvelle doctrine à notre dépendance technologique et aux effets des *« guerres asymétriques »* sur le plan de l'information est appelée à réduire deux grandes vulnérabilités : l'absence d'un circuit décisionnel court au sein de l'Etat, et entre l'Etat et le monde des entreprises dans une approche *bottom up* ; et l'absence d'une prise en compte des composants (munis de *back door* ?) dans les nouvelles technologies qui accroissent nos vulnérabilités. La première exige de repenser l'intelligence économique dont les vicissitudes depuis l'âge d'or d'Alain Juillet alors hébergé par le SGDSN illustre une réflexion également inachevée, ne serait-ce qu'en matière de gestion des REF, renseignements économiques et financiers ; la seconde de définir une stratégie globale confiée au SGDSN à l'autorité affirmée, notamment sur des procédures comme l'IEF gérée par la DGTrésor.

Le pillage de nos actifs ou leur *« sabordage »*[xi] peut être endigué si une véritable politique se met en place, à l'exemple de la DGA ou du HFDS du ministère de l'Ecologie. Mais de toute évidence aucun gouvernement n'a réussi à relever ce défi par l'absence d'une réelle coordination des politiques industrielles, du suivi des engagements de sociétés étrangères ou de l'évaluation d'un risque majeur en termes de participation stratégique (TDF), ou de fragilité de nos infrastructures d'importance vitale alors que le fournisseur chinois Huawei, implanté au coeur des réseaux, a été interdit de postuler à des appels d'offre pour l'Internet à bande large aux Etats-Unis. Cette politique doit intégrer les activités duales comme la cryptologie, imagerie, drones, etc.

Dans ce contexte *« hors limites »*, les vulnérabilités s'élargissent : la menace n'est plus ponctuelle mais peut être indirecte ou collatérale, pour neutraliser un réseau en copiant les caractéristiques techniques d'automates programmables industriels (API) de Siemens, de Veolia, etc. et créer de nouvelles peurs[xii]. L'approche peut être plus discrète par une sorte d'infiltration rampante dans l'espace des données : la prise de contrôle par les Chinois de chaîne d'hôtels en est une : le groupe hôtelier Jin Jiang a déboursé 1,3 MdsUS$ (mars 2015) pour l'achat du deuxième groupe hôtelier européen (et ses données clients) alors que le ministre des Affaires étrangères souhaite faire de la France la plateforme de son groupe en Europe.

Aucune cartographie nationale de ces risques n'existe, or le contrôle peut s'étendre aux aéroports, à tout réseau. La menace sur la sécurité des infrastructures vitales apparaît bien plus insidieux que la menace atomique ou la bombe N ou bombe à rayonnement renforcé (1979-1985). La prise de contrôle de réseaux électriques ou *black out* (Ukraine, décembre 2016) n'est qu'un aspect de vulnérabilité d'un Etat que l'Estonie (avril 2007) a déjà expérimenté. Tout dépend de la *« qualité »* de la cible, des *« buts de guerre »* comme celui du virus *« malicious »* Stuxnet conçu par la NSA en collaboration avec Israël utilisé contre l'arsenal nucléaire iranien : plus discret, plus propre que l'attaque sur le réacteur irakien Osirak (1981).

Or, les attaques de l'été 2016 par leur ampleur peuvent laisser penser à des tests ou des répétitions soit comme réponse, soit pour avoir des informations sur la résilience des réseaux *« ennemis »*. Mais visage de Janus, cela peut être aussi une arme de dissuasion si les contre-mesures de l'Etat visé peuvent répondre en déstabilisant les réseaux adverses.

Plus grave, la conduite de la guerre devient de plus en plus dépendante du cyberespace et de la guerre électronique. Les systèmes gérés en réseau sont créés par l'utilisation de l'énergie électromagnétique, et même des réseaux qui ne sont pas directement reliés au cyberespace peuvent être potentiellement neutralisés comme cela est arrivé en mer Noire pour le bâtiment *USS Donald Cook* en 2013 survolé par un Sukhoï-24 (avril 2014) qui a utilisé l'énergie électromagnétique pour interroger ou perturber les composants électroniques américains.

Les opérations menées par la Russie sont des champs d'expérimentions low cost permettant de tester des armes, mais aussi des contre-mesures à moindre coût. Or, les menaces visent les systèmes de systèmes nés de l'hyperconnectivité décrite comme la numérisation du champ de bataille infocentré et infovalorisé où tous les éléments militaires sont reliés (type programme *Scorpion*).

Conclusion

Faut-il être *« condamné au silence »* (1955) s'il n'existe pas de visionnaire comme le brigadier général William L. Mitchell (né à Nice, 1879-1936) rayé des cadres en 1925 pour avoir proposé de créer une armée de l'air indépendante de la marine et de l'armée de terre américaines, ainsi qu'un département de la défense pour superviser ces trois entités, *« accusing senior leaders in the Army and Navy of incompetence and almost treasonable administration of the national defense »* (accusation contre les chefs des armées *« comparable à une trahison dans l'administration de la défense nationale »*), et allant jusqu'à prévoir l'attaque de Pearl Harbor (1941) ?

La situation géopolitique à partir des années 1990 change singulièrement les rapports de forces internationaux, et la perception des menaces qui en découle avec l'expansion du cyberespace. Or, un cyber-Pearl Harbor reste possible si la pensée stratégique ne s'inscrit pas dans un concept stratégique global, *« hors limites »* et si elle considère la révolution numérique comme un outil supplémentaire pour lequel il faut construire une cyber-ligne Maginot.

Appliqué à la France ou à l'UE, ce sera une *« étrange défaite »* industrielle qui commence à se profiler. Enjeux de pouvoir plus global dans un monde nouveau autour de la donnée ? Nouvelles menaces sans la guerre ? Guerre silencieuse et paix imprédictible ? La guerre économique ou d'un nouveau genre, non pas par une occupation du territoire, mais par une neutralisation des réseaux dans une cyberguerre prenant la forme d'un contrôle du cyberespace, du monde virtuel par une captation et une appropriation illégitime de nos actifs informationnels. C'est de la capacité des pouvoirs publics en lien avec les partenaires privés de comprendre et de maîtriser les enjeux de la transformation numérique, mais ceci conduit à une remise en cause doctrinale fondamentale sur les questions de sécurité et de défense nationale.

Bibliographie

Arquilla John et Ronfeldt David, *Cyberwar is coming*, Comparative Strategy 12 (1993), Rand Corporation.

Arquilla John et Ronfeldt David, *Networks and netwar : The Future of terror, crime and Militancy*, Rand Corporation, 2001.

Bellanger Pierre, *La souveraineté numérique*, Ed. Stock, Paris, 2014.

Boyer Bertrand, *Cyberstratégie, l'art de la guerre numérique*, Ed. Nuvis, Paris, 2012.

Clarke A. Richard et Robert K. Knake, *Cyber War*, HarperCollins Publ., New York, 2010.

Del Valle Alexandre, *Les vrais ennemis de l'Occident*, L'Artilleur, Paris, 2016.

Desportes Vincent, *La guerre probable*, Ed. Economica, Paris, 2008.

Durieux Benoît, *Clausewitz en France*, Ed. Economica, Paris, 2008.

Esambert Bernard, *La guerre économique mondiale*, Olivier Orban, Paris, 1991.

Gibson William, *Neuromancer*, Ace, 1984.

Harbulot Christian, *Sabordage*, Ed. François Bourin, Pariss, 2013.

Hassid Olivier et Lucien Lagarde, *Menaces mortelles sur l'entreprise française*, Ed. Nouveau monde, Paris, 2016.

Kempf Olivier, *Introduction à la Cyberstratégie*, Ed. Economica, Paris, 2015.

Morin-Desailly Catherine, *L'Union européenne, colonie du monde numérique ?*, Sénat, Rapport, 2013.

Nye S. Joseph, *Soft Power*, New York, Public Affairs, 2004.

Qiao Liang et Wang Xiangsi, *La guerre hors limites*, Rivages Payot, Paris, 1999.

Notes

* DEA de l'Institut d'Etudes Politiques de Paris,
Ancien Responsable de la Protection du secret de la Défense,
Ancien Auditeur au Contrôle général économique et financier,
Ministères économique et financier

Héraclite d'Ephèse : « rien ne dure à part le changement ».

[i] Vinton Cerf, un des pères de l'Internet n'a jamais caché qu'il s'est inspiré des recherches de Louis Pouzin sur le *Cyclades* (1973-1975) en milieux universitaires et de ses protocoles pour mettre au point internet et son protocole TCP/IP.

[ii] Google est créé en 1998, Apple en 1976, Facebook en 2004, Amazon en 1994 et Twitter en 2006.

[iii] Electronic Frontier Foundation.

[iv] *« You have no sovereignty where we gather »*, février 1996 à Davos.

[v] In *Strategic Cyberspace Operations Guide*, US Army War College, Juin 2016.

[vi] Selon la publication du National Military Strategy for Cyberspace Operations.

[vii] En termes de capacité de stockage, un méga-octet (Mo) = un million d'octets, un giga-octet (Go) = un milliard d'octets, et untéra-octet (To) = un trillion d'octets, ou en anglais terabytes (Tb).

[viii] Une seule entreprise peut connaître 25 vulnérabilités *zero-day* dans ses systèmes de gestion type Scada.

[ix] Selon les termes d'une réflexion stratégique menée par deux colonels de l'AP de Chine *« la Guerre hors limites »* (paru en 1999) portant sur tous les aspects de la *« guerre asymétrique »* observée dans chacun des domaines, économique, financier, religieux ou environnemental, et appartenant à une réflexion plus large sur les ambitions *« globales »* chinoises.

[x] Selon la définition de la CNIL suite au décret de janvier 2016 sur les données de connexion.

[xbis] CERT : Computer Emergency Response Team.

[xi] Christizn Harbulot, *Sabordage. Comment la France détruit sa puissance*, Editions François Bourin, Paris, 2013.

[xii] Cf. *« La guerre psychologique »*, ouvrage établi par l'état-major français lors de la guerre d'Indochine qui mériterait d'être réactualisé.