ARMÉE DE L'AIR

Penser les Ailes françaises

La tribune de l'air
et de l'espace

n°32
Juillet 2015

RÉFLEXIONS SUR LE CYBER : QUELS ENJEUX ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

Centre d'études stratégiques aérospatiales

Sommaire

Directeur de la publication :
GBA Patrice Sauvé, directeur du CESA

Rédacteur en chef :
Cdt Jean-Christophe Pitard-Bouet,
chef de la division études et rayonnement du CESA

Maquettage :
M. Emmanuel Batisse
M. Philippe Bucher
Clc Zita Martins Nunes
Av1 Antoine-David Da Silva Manteigas

Diffusion :
M. Pierre d'Andre
Clc Mathieu Cornu

Correspondance :
CESA
1 place Joffre – 75700 Paris SP 07 – BP 43
Tél. : 01 44 42 83 96 Fax : 01 44 42 80 10
www.cesa.air.defense.gouv.fr

Photogravure et impression :
Imprimerie EDIACA
Établissement d'impression, de diffusion et
d'archivage du commissariat des armées

Tirage : 2 500 exemplaires

Le cyber espace et les opérations aériennes : De l'analogie à la synergie

Allocution du Général d'armée aérienne Denis Mercier,
Chef d'état-major de l'armée de l'air,
prononcée le 10 février 2015, devant les auditeurs de l'Institut National des Hautes Études de la Sécurité et de la Justice

Introduction

L'analogie est un jeu dangereux et peut être parfois un écueil.

Je vais pourtant, si vous me le permettez, débuter mon discours en osant une analogie.

J'affirme devant cette assemblée réunie que les opérations aériennes et les opérations cyber sont analogues par nature et par essence.

Cette affirmation se fonde sur des faits concrets et non sur des sentiments.

L'Air et le cyber espace ont une dimension planétaire, partageant une même perméabilité :

- Un acte suspicieux dans le cyber espace entraîne les mêmes réactions que lorsqu'un aéronef se comporte de manière suspicieuse dans le flot du trafic aérien : quand ce cas se produit, nous avons besoin de trouver rapidement « l'aiguille dans la botte de foin » ;

- Les cycles de réaction et de prise de décision doivent d'être brefs. Plus le cycle est court, meilleure sera la posture face à l'ennemi ;

- À l'instar de la guerre aérienne, dans le cyber espace, c'est la nature des cibles qui détermine le niveau stratégique ou tactique de l'opération à mener ;

- Si l'air fut le champ bataille du XX^{e} siècle, le cyber espace est celui du XXI^{e} siècle.

Aussi semblables qu'elles puissent être, les opérations aériennes et les opérations cyber sont également liées par une relation interdépendante et omniprésente :

- D'une part, le cyber dépend de plus en plus des moyens 3D (satellites, antennes) ;

- D'une autre part, les opérations aériennes deviennent de plus en plus dépendantes du cyber parce qu'elles ont toujours été à la pointe de la technique.

À cause de cette interdépendance, et afin d'être capables de combattre dans le cyber espace aussi bien que dans les airs, nous, l'armée de l'air française, devons d'abord comprendre cet environnement redéfini.

Ensuite, nous avons à élaborer un projet opérationnel à même d'inclure le cyber dans n'importe quelle opération aérienne.

En parallèle, nous avons aussi à tenir compte de la dualité propre à toute activité dans le cyber espace.

C'est seulement grâce à cette approche globale que nous serons en mesure de concevoir un futur système de combat aérien efficace.

Plus que la défense du cyber espace, comment l'armée de l'air fait-elle pour appréhender son environnement cyber dans le but de le défendre ?

Avant de pouvoir parler de défense du cyber espace ou d'attaques cyber, une question se pose : comment l'armée de l'air fait-elle pour comprendre son environnement cyber afin de l'aborder et de s'en imprégner pleinement ?

- Nous interagissons dans le cyber espace au sein même des structures de notre armée. Nous sommes aussi en connexion permanente avec les armées et avec diverses agences gouvernementales voire même avec des entreprises. Mais nous échangeons également avec des partenaires et des alliés à l'échelle internationale dans des relations bilatérales ainsi que dans des relations multilatérales.

- J'ai assisté il y a quelques semaines au symposium OTAN qui réunissait les CEMAA et nous avons beaucoup discuté des opérations transfrontalières à l'intérieur de la zone OTAN. Si vous le permettez, je vais, de nouveau, utiliser une analogie : les interconnexions mentionnées requièrent des procédures identiques aux opérations aériennes transfrontalières organisant les opérations de transit d'un espace aérien souverain à un autre.

- Il n'y pas d'espace aérien sans contrôle, assuré par les contrôleurs aériens et par l'ensemble des moyens qui garantissent ce contrôle. De même, la surveillance et le contrôle des systèmes d'information sont nécessaires dès l'instant que nous planifions des opérations dans le cyber espace.

- Dans les deux domaines, il est quasiment impossible de suivre toutes les traces radar ou cyber, il faut alors établir un seuil acceptable dans la détection ; les signaux faibles seraient détectés tandis que la plus grande partie des fausses alarmes serait rejetée. Dans le cyber comme dans l'air, un but demeure : préserver notre activité opérationnelle.

- Je suis moi-même pilote de défense aérienne. Dans la défense aérienne, la règle d'or est de détecter, d'identifier et de catégoriser. À l'issue de ces actions, vous avez alors le droit de venir en aide, d'ignorer ou de détruire le signal initial intercepté.

- C'est la même chose avec le cyber ! Rien ne ressemble plus à un virus qu'une mise à jour de logiciel. Là aussi, la règle d'or (c'est-à-dire détecter, identifier et catégoriser la menace potentielle) est cruciale.

- Cela requiert la mise en place d'une base de données solide et suppose l'actualisation continuelle de votre fine connaissance des menaces

éventuelles. C'est seulement à ce moment-là que vous pouvez commencer à construire votre défense aérienne active et passive. La même logique lie les contre- mesures et l'antivirus.

- Quand votre système d'armes tombe en panne dans votre avion de chasse, vous avez toujours un plan B. Vous connaissez la procédure à suivre et les réactions à avoir si un moteur, un instrument de navigation ou une arme est défaillant.

- La redondance ou la résistance sont deux notions primordiales communes aux domaines de l'air et du cyber.

- Plus important encore, la planification et la conduite des opérations aériennes, capacité clef de leur succès, repose sur un centre permanent de commandement et de conduite. Les crises dans l'espace cyber ont besoin de structures similaires, capables de gérer des cyber-attaques en temps réel, de réagir et de donner des ordres afin que des mesures concrètes soient prises et que des actions pertinentes soient menées.

- Je suis persuadé que nous pouvons optimiser la synergie entre les deux types de structures car après tout, les opérations dans l'espace cyber sont inhérentes à toute opération aérienne.

Les opérations cyber dans les opérations aériennes

En effet, dans le cadre d'opérations aériennes, le cyber est à la fois une arme et un milieu à l'instar des éléments aériens, maritimes ou terrestres.

- C'est un choc de culture. Pourtant, chaque stade de préparation d'une opération aérienne (ou interarmées) devrait inspirer la manœuvre cyber.

- Je veux dire par là que nous devons prendre en compte chaque étape : le processus de ciblage cyber, les règles d'engagement cyber, les effets recherchés ou indésirables d'une cyber-attaque et l'évaluation de ces effets.

Toutefois, des différences marquées existent entre les armes aériennes et les armes cyber.

Une des plus remarquables est la dualité présente dans tout type d'activité cyber.

À l'inverse des bombes laser ou de toute autre catégorie de bombes intelligentes, lors d'une cyber-attaque, la probabilité de dommages collatéraux qui pourraient toucher des réseaux civils ou des consommateurs est très élevée.

Une autre différence réside dans le tempo. Dans la puissance aérienne, la réactivité se mesure en minutes et la précision en secondes. Le facteur temps dans le cyber espace est, au contraire, rarement maîtrisé, notamment dans le cas d'une bombe logique par exemple.

Enfin, une cyber-attaque est la plupart du temps une arme à emploi unique car aussitôt le virus actif, il est exposé puis rapidement traité. Pour ce qui est du domaine air, nous utilisons encore des armements ou des tactiques aériennes conçues il y a parfois une centaine d'années car elles sont néanmoins toujours efficaces. Les manœuvres basiques de combat aérien de Guynemer ou de Fonck sont toujours valides !

Notre défi est d'étudier la relation entre les deux domaines pour que nous puissions exploiter leur complémentarité.

- Prenons l'exemple de l' « aveuglement » des radars par le biais de moyens cyber lorsque des avions de chasse entrent dans une zone de combat aérien. Cela peut représenter un avantage ou provoquer une catastrophe, tout dépend de la qualité de la coordination et du camp dans lequel la cyber-défense est la plus forte.

- Nous pouvons explorer plus en avant la combinaison d'actions cyber et d'opérations menées par les forces spéciales pour focaliser l'attention de l'adversaire sur des activités particulières.

- Ces deux exemples montrent le soutien que le cyber peut apporter dans le cadre d'opérations aériennes. Nous pourrions tenter d'imaginer ce qu'une opération aérienne pourrait apporter à une manœuvre cyber interarmées.

La destruction physique (par air) de moyens de communication cyber et de centres de transmissions pourrait par exemple amplifier les effets des opérations psy-ops /non-cinétiques.

CONCLUSION : des plate-formes connectées à un système de systèmes

Comment pouvons-nous, dans cet environnement cyber qui comprend les opérations aériennes, donner forme au futur système de combat aérien ?

- Commençons par regarder nos opérations actuelles. Nos plates-formes de renseignement et de surveillance (Rafale, drones, satellites, AWACS etc…) recueillent ainsi un nombre croissant de données diffusées en temps réel ou différé vers d'autres plates-formes. Les capacités de ces capteurs et de ces effecteurs, quels qu'ils soient, sont évidemment essentielles.

- Mais le vrai défi réside dans l'organisation de ces échanges de données perdues dans l'océan du *Big Data.* Réfléchir à un système de combat aérien futur en se concentrant uniquement sur les capacités de différentes plates-formes, ordinateurs ou aéronefs, même s'ils sont connectés les uns aux autres, serait une grave erreur.

- Le mot clé ici est "système".

- Pour cela, nous devons définir quels systèmes sont en action. Les systèmes d'information ; les systèmes de réseaux ; les systèmes de commandement et de contrôle ; les systèmes de données ; les systèmes de sécurité ;

- Ensuite, nous avons à mesurer jusqu'où vont les interconnexions entre ces systèmes et il nous faut étudier le caractère global de leurs influences.

En gardant tout cela en tête, je voudrais mettre l'accent sur le fait que le futur de l'armée de l'air repose sur la conception d'un système global de systèmes et non sur une simple association de plates-formes performantes.

- Nous avons une chance unique mais courte dans la durée : celle de commencer maintenant à forger le futur système de combat aérien équipé de capacités cyber.

- Robuste, résistante et cohérente, l'architecture de ce système de systèmes doit prendre en compte les faiblesses et les vulnérabilités du cyber espace tout comme les synergies cyber en terme de commandement et de conduite mais aussi en termes de performance.

Pour finir, aujourd'hui, et pour les décennies à venir, le succès d'une défense aérienne dépendra de la qualité de la fusion des données relatives à la menace. Le résultat de cette équation repose sur ce que nous appelons la « *Recognized Air Picture » (RAP),* établie par les structures de commandement et de conduite air.

- Je crois que cette expertise particulière et cruciale doit être étendue aux activités cyber en lien avec des opérations aériennes.

- Je soutiens l'idée de *« Recognized Cyber Picture »*, semblable à la « *Recognized Air Picture »,* intégrée à un système de systèmes, capable de détecter et de sélectionner parmi des milliards d'octets/bytes des éléments précieux et d'adapter intelligemment la réactivité des différents systèmes.

Le futur des capacités de l'armée de l'air est là, dans cette prise en compte du cyberespace dans nos systèmes de combat de plus en plus interconnectés.

Une cyberstratégie à inventer

Monsieur François-Bernard Huyghe
Docteur d'État en Sciences Politiques
Chercheur à l'Institut des relations internationales et stratégiques

S'il est un domaine où notre pays n'est pas absent, au moins en termes de réflexion théorique, ou d'intentions politiques, c'est la cyberstratégie[1]. En attendant peut-être que la France se dote d'une « quatrième armée », après l'air, la mer et la terre, pour lutter dans le champ de bataille numérique, nous sommes tous bien conscients de la nécessité d'un art de vaincre adapté à ce milieu. Mais comment peut-on gagner « dans » le cyberespace ? Là où la guerre ne consiste plus à porter son territoire derrière la frontière de l'autre, où il n'y a pas de capitales ennemies à occuper ni de cibles à bombarder et où ne servent guère les gros bataillons[2].

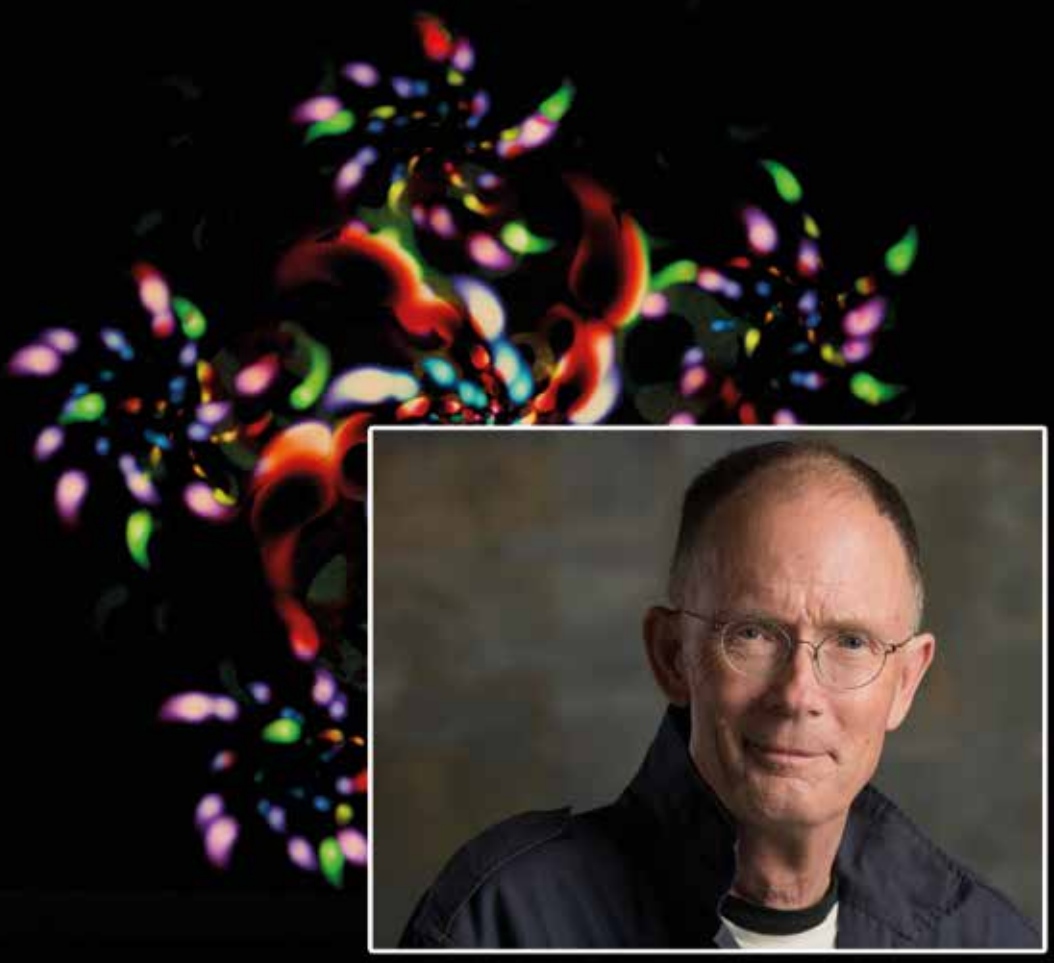
L'origine du terme cyberespace est un livre de science fiction de 1984, (le *Neuromancien* de William Gibson). Il est forgé à partir de « cybernétique » (initialement science du « gouvernail » ou des automates) plus « espace ». Il renvoie à « *une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain* ». L'expression, vite popularisée, s'est imposée pour désigner le « monde » né de la connexion des ordinateurs échangeant des données et de tout ce qui les fait fonctionner, matériel ou immatériel.

Cette interface au croisement du numérique (qui réduit toute information à une série de bits reproductibles, transportables, combinables comme à l'infini) et des réseaux qui en assurent la circulation parle à l'imagination : un monde derrière les écrans, comme le pays des merveilles d'Alice est de l'autre côté du miroir.

1. On songe à la place de la cyberstratégie dans les Livres blancs depuis 2008, au « pacte cyber » de 2014, à l'existence de deux chaires de cyberstratégie en France, à l'abondance des publications...
2. Nous tenterons de répondre à cette question dans *Gagner le cyberconflit*... co-écrit avec N. Mazzucchi et O. Kempf, et à paraître prochainement aux éditions Economica.

MODERN MASTERWORK

w1ll1am g1bs0n



neuromancer

Pour qu'un tel monde existe, il faut trois composantes :

- des « choses », des écrans, des câbles, des antennes..., soumis quelque part au pouvoir d'une autorité ;

- des « codes », applications, algorithmes, protocoles..., ce qui veut dire qu'en ce domaine des innovations et informations nouvelles, par exemple sous forme d'un algorithme inédit comme un maliciel, peuvent très rapidement bouleverser des rapports de force ;

- des « signes » qui ont du sens pour un destinataire, un cerveau humain, donc avec une part d'imprévisibilité et de subjectivité qui touche la nature et l'ampleur des effets obtenus (désordre, peur, agressivité, mobilisation...).

Il est donc convenu, pour les désigner de parler de couche matérielle, logicielle et sémantique du cyberespace.

Les choses sont quelque part (par exemple un câble sous-marin formant une dorsale d'Internet passe dans telles eaux territoriales où il est possible d'y prélever des flux d'informations). Les codes ont été fabriqués par quelqu'un (qui a pu, par exemple, installer une « porte de derrière ») et ils peuvent subir l'action d'autres codes (tel un système de contrôle informatique type SCADA qui peut être déréglé par un logiciel malveillant). Quant aux signes, ils s'adressent à des gens chez qui ils suscitent des réactions : ils savent ou croient des choses, et sont amenés à prendre des décisions, en fonction de ce que leur montrent leurs ordinateurs et de leur interprétation. Maîtriser des infrastructures de communication, inventer des algorithmes redoutables et agir sur autrui par écran interposé : déjà se dessinent des pistes.

Le cerveau humain, cible ultime

La cyberstratégie, par essence humaine, s'applique à un espace technique, produit artificiellement, et sa finalité reste dans le monde réel : obtenir quelque chose de quelqu'un par la force et la ruse.

Au final, la cible ultime reste bien ce cerveau humain. En stratégie classique, la violence vise à agir sur la volonté de l'ennemi, soit, radicalement, en le tuant, soit en l'amenant à se rendre, à poser les armes, à accepter vos condi-

tions de paix, etc. Dans le cyberespace, par des moyens informatiques, il est possible d'agir sur un adversaire (ou une victime) en diminuant des capacités (en lui volant des connaissances précieuses, en empêchant ses outils de décision et de coordination de fonctionner), en le trompant ou en l'influençant.

Pour ce faire, le numérique offre des possibilités inédites de pénétrer dans un système adverse pour y voler des données confidentielles (espionnage) et aussi pour empêcher ledit système de fonctionner correctement (sabotage). Ce dernier point vaut qu'il s'agisse de paralyser une chaîne d'enrichissement de l'uranium iranienne (opérations dite Stuxnet menée en 2012) ou une chaîne de télévision francophone (TV5 condamnée à l'écran noir au mois d'avril 2015). Enfin, il est possible de mener une action psychologique ou symbolique (que certains nomment « de subversion ») contre des organisations ou des communautés cibles. Dans des genres très différents les *Anonymous* qui peuvent « *défacer* » ou submergent de demandes (*Divided Denial Of Access*) des sites d'organisations adverses le font toute la journée, mais aussi les pirates informatique pro Bachar El Assad de la *Syrian Electronic Army*.

Ajoutons un dernier élément : l'imaginaire. Dès les années 90, Internet avait suscité les prédictions les plus triomphales : « toutes » les informations possibles seraient disponibles et tous pourraient communiquer avec tous ; toutes les frontières et les délais seraient abolis, nos systèmes politiques, économiques et culturels en seraient révolutionnés, etc. Mais il a aussi nourri toutes les craintes : les « *cavaliers de l'infocalypse* » (pédophiles, nazis, terroristes, trafiquants en tout genre) allaient y proliférer, mais surtout des attaques destinées à piller, à créer du chaos ou à manipuler les foules menaceraient nos biens, nos institutions et nos valeurs. Demain la cyberguerre (notion fort douteuse) allait bouleverser l'équilibre international, des actions « cyberterroristes » permettaient à une poignée d'hommes de mettre à genoux nos sociétés ouvertes de l'information, si dépendantes, justement, de leurs systèmes d'information. Outre-Atlantique, se poursuit l'attente du « Pearl Harbour informatique » (ou du Cybergeddon, cyber + Armageddon, la fin du monde) – comprenez la peur d'une attaque contre les systèmes informationnels d'un pays qui paralyserait une fonction vitale comme l'approvisionnement énergétique.

Pour le moment, personne n'est mort d'une cyberattaque, aucun pays n'a dû se soumettre à un autre sous la contrainte d'un virus informatique particulièrement puissant et les terroristes préfèrent globalement utiliser des Kalachnikov plutôt que des McIntosh.

Mais en même temps, il semble évident qu'il y aura une composante cyber dans la plupart des conflits. Ceci vaut qu'il s'agisse d'affrontements militaires classiques (quel belligérant se priverait d'essayer de pénétrer de paralyser les systèmes adverses avec un algorithme plutôt qu'avec un commando ou un missile ?) ou de conflits idéologiques (quelle guerre des idées ne se prolonge pas sur les réseaux sociaux ?). Et, bien sûr, dans un système comme le nôtre dépendant de plus en plus de la circulation de l'information numérisée, les enjeux économiques sont énormes.

Vulnérabilités et conflits

Le cyberespace permet de plus en plus d'agir dans les secteurs, géopolitiques militaires, idéologiques ou économiques comme l'ont compris les acteurs qui l'utilisent, souvent en dissimulant leur identité. Parallèlement, l'abolition de la barrière entre producteurs et consommateurs d'informations dans les réseaux sociaux et le Seb 2.0 facilite l'entrée sur le champ de bataille et fait encore davantage de l'information à la fois un enjeu et une arme, un objectif et un bouclier. Plus une société devient « de l'information », plus elle est dépendante de données, de systèmes, de réseaux et de dispositifs lointains par définition vulnérables. Plus il est tentant de se livrer à la prédation ou à la perturbation par électrons interposés.

D'où une tendance lourde. Si des cas de cyberattaques ont été signalés dans les années 1990, à partir de la seconde moitié des années 2000 naît vraiment l'univers conflictuel voire chaotique que nous connaissons.

Aujourd'hui lire dans la presse (comme c'est le cas le jour où nous écrivons ces lignes) « *cyberattaque préoccupante contre la Maison Blanche* » relève de la routine : nous avons parfaitement intégré qu'il n'y a plus guère de grande organisation ou institution qui ne constitue une cible, et que l'on peut voir son système informatique pénétré à distance (pour vous voler des donner précieuses, mais peut-être aussi vous humilier, vous défier, vous lancer un avertissement), qu'il faudra s'adapter et que cela se reproduira sans doute plus tard, sans que cela implique la guerre finale ou le chaos total.

Tous les grands types d'acteurs, États, organisations, groupes activistes et individus, ont investi le cyberespace avec une énergie et avec une inventivité croissantes. Au prix d'une complexité préoccupante. À commencer par la difficulté qu'il y a à déterminer l'identité et le but véritable des acteurs,

protégés par le brouillard qui entoure toute attaque : d'où venait-elle (pas forcément de celui qui la revendique) et que visait elle qu'elle ait réellement atteint ? La chose est bien moins claire que lorsque des tanks violent une frontière.

Bref, si la nécessité d'une cyberstratégie s'impose dans tous les pays, elle soulève partout les mêmes questions – Comment protéger ses infrastructures vitales ? Comment faire coopérer acteurs privés ou publics ? Faut-il se doter d'armes informatiques offensives ? Que faut-il avouer ou laisser croire en ce domaine ? Jusqu'où aller dans la protection de sa souveraineté numérique et dans le respect de celle des autres ? Comment se reposer sur le droit ou sur ses alliés ? À partir de qu'elle nocivité de l'attaque se considérer comme victime d'un acte de guerre ? Quid du facteur temps (temps de préparation, décèlement, résilience) ? Tous y apportent des réponses qui reflètent à la fois leurs intérêts et leurs cultures stratégiques.

Pour ne donner qu'un exemple, le Département de la Défense américain qui classe la cyber menace au sommet des dangers à combattre vient de publier sa nouvelle cyberstratégie[3]. Il se donne pour objectifs la défense de ses propres réseaux et des intérêts vitaux du pays face à des attaques de perturbation, mais aussi la maîtrise de ses propres armes informatiques pour mener des opérations (qu'il faut bien parfois présumer offensives) dans le Cyberespace. Significativement aussi, il considère son usage comme susceptible d'aider à contrôler l'escalade des conflits et de s'intégrer dans toutes les options militaires. Sans oublier la question des alliances dans le cyber.

Visiblement, la dimension cyber sera désormais partout dans le conflit, non pas sous forme d'une hypothétique cyberguerre qui remplacerait la guerre tout court, mais comme une vulnérabilité obsession, un moyen d'attaque et de défense y compris civile, une composante à intégrer à des modes de lutte plus classiques, mais aussi une option nouvelle ouverte au politique pour envoyer un message (pression, avertissement, menace, punition...) et agir sur la volonté politique de l'autre.

---

3. *The DOD Cyberstrategy*, avril 2015, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Puissance technologique et anticipation psychologique

En croisant les grilles que nous venons de présenter, il commence à s'esquisser quelques tendances d'une future cyberstratégie. Elle suppose une démarche, d'ailleurs bien entamée en France, et qui ne se borne pas à dresser des défenses de plus en plus solides contre des attaques de plus en plus imprévisibles. Elle demande de la continuité politique et une vision à long terme.

Il faudra bien sûr de l'excellence technique, toujours plus de coopération entre secteurs privé et public, de la sensibilisation des acteurs, de l'anticipation (y compris dans le choix des matériels, des logiciels, du stockage de données « dans les nuages », qui répondent à des critères nationaux ou au moins européens de sécurité), toujours plus de réactivité.

Il faudra aussi davantage de renseignement, ne serait-ce que pour déceler qui pourrait vouloir s'en prendre à nous par écran interposé et dans quel but. Il faudra certainement aussi intégrer un élément psychologique, de la crédibilité : une attitude (une posture, diront les militaires) qui décourage de futures agressions, moins par l'étalage de moyens informatiques (affaiblis aussitôt que révélés, sans doute éphémères face à la prochaine innovation agressive), que par la crainte qu'un pays de notre niveau technologique, ayant la volonté de se défendre, ne puisse exercer une rétorsion, même contre ceux qui se croient à l'abri derrière des écrans lointains.

Enfin et surtout, nous aurons besoin de réinventer des règles pour nous adapter à un monde de l'innovation technique et du changement stratégique. Le défi n'est pas seulement lancé à nos capacités scientifiques mais aussi à notre souplesse mentale. Avantage au rapide et à l'inventif. Est-ce une nouvelle qu'il faille redouter ?

Enjeux et moyens de notre souveraineté numérique

Allocution de Monsieur Pierre Bellanger,
président directeur général et fondateur de Skyrock,
devant l'Institut des Hautes Études de Défense Nationale

Merci mon Général de votre invitation.

Bonsoir à tous. C'est un honneur d'être devant vous ce soir et en ce lieu.

Je viens vous parler de souveraineté numérique. C'est-à-dire de la maîtrise de notre destin sur les réseaux informatiques. Nous vivons, sans vraiment le savoir, une situation d'une exceptionnelle gravité. Les maladies les plus dangereuses sont celles qui ne tourmentent que lorsqu'il est trop tard. Nous en sommes là.

Ici est le lieu de la réflexion et du partage sur les questions de défense nationale. Il me faut donc tenter de parler à la hauteur de cette exigence. Des radios libres de jadis qui m'ont fait courir sur les toits de Paris, jusqu'à cet amphithéâtre Foch, l'engagement est le même. C'est le combat pour la liberté. L'équation est simple : la garantie de la liberté, c'est le droit. La garantie du droit, c'est la souveraineté. Qui s'intéresse à la souveraineté numérique comprend vite que ce pays est atteint au cœur, asservi et saigné comme un animal. Vient alors en mémoire, la somme des courages de nos aînés pour nous donner ce pays libre. Voici que c'est maintenant à notre tour.

Maîtriser notre destin sur les réseaux informatiques. C'est un univers complexe. Comment donc trouver un guide simple à notre action ?

Il nous faut une boussole. Elle nous est donnée en trois mots qui résonnent en ce lieu : « *Ne pas subir* ». Devise du grand soldat Jean de Lattre de Tassigny. Ce sera notre cap. Ne pas subir une volonté autre que la nôtre dans le cyberespace. Affirmer notre République sur les réseaux.

Pour commencer, prenons la mesure du changement en cours.

La performance des systèmes informatiques double tous les ans à prix égal. C'est une progression à facteur multiplicatif constant dont les effets ne cessent par conséquent de s'accélérer. Ce type de croissance dite exponentielle était inconnu jusqu'à présent dans l'histoire des techniques.

Entre 1995 et 2015, les progrès conjugués des micro-processeurs, du stockage et de la bande passante ont multiplié par un million la puissance des machines. Mais c'est surtout le progrès de la vitesse d'exécution des logiciels qui donne à cette dynamique une accélération sans précédent : le logiciel progresse 43 fois plus vite que la machine. Ainsi ces vingt dernières années, la performance conjuguée des logiciels et des machines a été multipliée par 43 mille milliards de fois et doublera dans douze mois. Cette croissance exponentielle est multipliée par une seconde exponentielle : l'effet réseau.

L'effet réseau statue que la valeur d'une machine est proportionnelle au carré du nombre de machines auquel elle se connecte. On le comprend, la valeur d'un téléphone dépend du nombre de personnes avec lequel il nous permet de communiquer. Cette loi est une machine exponentielle à créer de la valeur.

Dix machines connectées : chacune vaut 10 au carré, soit 100. Une onzième s'ajoute, chacune vaut alors 11 au carré, soit 121. Vingt-et-un pour cent de croissance de valeur avec le seul ajout d'une machine ! Le nombre de machines et d'appareils reliés au réseau est passé de 200 millions en 2000 à 15 milliards en 2015 et sera de 40 milliards en 2020. C'est vertigineux. Et c'est au-delà de notre compréhension.

Nous ne savons pas nous représenter les exponentielles. Un exemple : plions une feuille de papier en deux, puis en quatre, cinquante fois de suite. Quelle est l'épaisseur finale du pliage ? La réponse étonne : 114 millions de kilomètres, soit les ¾ de la distance de la Terre au Soleil.

Quel est l'effet de cette accélération sur la société ?

Les efforts, les projets, les investissements recherchent le meilleur rendement, c'est-à-dire la croissance de valeur la plus rapide. C'est ce que leur donne l'effet réseau.

L'effet réseau reconfigure la société : les machines informatiques se lient en réseau ; les réseaux de machines se lient en réseau : c'est Internet ; les documents se lient en réseau : c'est le Web ; les personnes se lient en réseau : ce sont les réseaux sociaux. Et maintenant les objets se connectent à leur tour.

Le réseau des réseaux informatiques, Internet, chaque jour plus productif, efficace et rapide, devient le grand concentrateur de valeur. Il capte ainsi la valeur de la société, de toutes les industries, de tous les services, car il les remplace par une meilleure productivité, un meilleur rendement et surtout un meilleur service.

L'effet réseau s'applique aussi à l'humanité. Trois milliards de connectés, déjà 40 pour cent de la planète, et 5 milliards prévus en 2020. Jamais autant d'individus dans le monde n'ont eu autant de possibilités, de choix, d'informations et d'échanges. Jamais, il n'y eut une telle puissance informatique disponible pour chacun et en réseau.

Notre émancipation est égale au carré de toutes les émancipations auxquelles elle se connecte. L'humain est un devenir constant. L'amélioration de chaque connecté accroît notre propre valeur et celles de tous les autres. Ainsi l'humanité peut faire un saut évolutif sans précédent avec le réseau. Ce qui nous changera tous intimement et collectivement. Le réseau est notre chance.

La révolution industrielle nous a donné le moteur, l'électricité, et la ressource de l'énergie fossile. La révolution numérique nous donne le processeur, l'information, et la ressource des données.

Expliquons-nous sur ce dernier point.

Nous manquons d'informations. Cette carence paraîtra folle dans le futur. Comment faisaient-ils ? Comment faisons-nous pour remédier à l'incertitude ? Une réponse principale : le gaspillage.

C'est l'exemple de l'escalator fonctionnant en permanence jusqu'à ce que, muni d'une cellule photo-électrique, il ne se déclenche qu'à l'arrivée d'un utilisateur.

Notre société entière a fonctionné comme cet escalier mécanique tournant à vide. Puisqu'on n'estime pas les besoins alimentaires et que l'on n'a pas d'information sur chaque étape de la distribution, la moitié de la nourriture est perdue entre la fourche et la fourchette. Un tiers de l'essence consommée est gâchée en recherche de place pour se garer et donc par l'absence d'échanges d'informations entre les véhicules circulants et les emplacements libres. La France dépense plus de 30 milliards d'euros par an en pétrole pour l'automobile. L'information dynamique sur le stationnement vaut donc 10 milliards d'euros, 11 % du déficit du budget de l'État.

La dilapidation des vies humaines, elle, est sans coût mesurable. Selon certaines études, sur les seuls patients hospitalisés, l'emploi des données permettrait de réduire la mortalité de 20 pour cent.

En ce siècle, on change de modèle. On résout l'incertitude non plus par le gaspillage mais par l'information. Le gain de productivité et de ressources à tout niveau est immense. Chaque État, chaque collectivité, chaque entreprise, chaque individu peut faire mieux et plus avec moins, grâce à plus de données.

Pour la France, si ce gaspillage généralisé équivaut à 10 % de notre économie, cela représente environ 200 milliards par an. C'est une estimation basse de la valeur de nos données. La grande optimisation par les données va permettre d'allouer cette richesse perdue et stérile en gain de croissance, de qualité de vie, d'environnement et de bien-être collectif.

Nous connaissons les quatre dimensions : la largeur, la longueur, la hauteur, le temps. Voici la nouvelle dimension supplémentaire : l'information. L'environnement muet et inerte d'aujourd'hui va être métamorphosé. Pour l'imaginer, remplacez les étiquettes et les inscriptions imprimées sur tout ce qui nous entoure par des capteurs intelligents, émetteurs et récepteurs, en échange constant et se réajustant mutuellement en permanence. Ce qui les relie tous, c'est le réseau.

Le réseau est la prochaine étape du progrès humain, c'est la clef de la réponse aux défis sociaux, économiques et écologiques auxquels nous faisons face. Nos sociétés s'épuisent dans une impasse. Voici une révolution d'une magnitude incommensurable. Voici la sortie de notre crise sans fin.

Le réseau est notre chance. Il n'y aura que le réseau et tout est le réseau. Ce qui est connecté à une chance de croître, ce qui est déconnecté disparaît.

Voici donc le réseau dans sa majesté mutante. Mais quelle est la stratégie au cœur de sa propre évolution ?

Au sein du réseau, la valeur migre vers le rendement maximal, c'est celui du logiciel, la première industrie du numérique. Et cette industrie est dominée par une nouvelle catégorie d'entreprise : le réseau de logiciels ou résogiciel. Le résogiciel concentre à son profit la double exponentielle d'Internet - progrès informatique et effet réseau - en la coiffant par une accélération plus rapide encore.

Voilà comme il procède : il commence par un service à succès, puis en associe d'autres. On verra donc les résogiciels dépasser la centaine de services coordonnés entre eux : moteur de recherche, carte, courrier, agenda, traducteur, carnet d'adresses, réseau social, plate-forme vidéo, commerce en ligne, intermédiaire de paiement, etc…

Chacun des services se coordonne avec les autres et les rend plus utiles et plus pratiques. Une heure de rendez-vous sur un message nous conduit à un agenda lié à un carnet d'adresses qui ouvre sur une carte géolocalisée indiquant la durée de parcours et décalant d'autant une réunion en prévenant les autres participants.

C'est ce qui fait que l'effet réseau s'applique aussi aux services. Un service associé à cent autres vaut cent au carré soit 10 000. Un service concurrent isolé, même meilleur, est broyé. L'alliance de services développe ensuite ses propres infrastructures pour être plus pertinente et plus rapide.

Puis, pour rapprocher ses propres machines des utilisateurs et pour gagner ainsi en qualité et vitesse, le résogiciel investit les réseaux de télécommunications. Ensuite, le meilleur service oblige à maîtriser le logiciel qui pilote la machine de l'utilisateur : son système d'exploitation. Pour assurer le déplacement d'un point bleu sur une carte géolocalisée, il faut le meilleur accès au capteur GPS de la machine.

Enfin, l'intégration du système d'exploitation et de sa machine hôte est l'ultime garantie du meilleur service. En conséquence, le résogiciel

fabrique ou contrôle ses propres terminaux, c'est-à-dire toutes les machines. Le système d'exploitation ne se cantonne pas à la machine de bureau traditionnelle ou au terminal mobile. Il se retrouvera partout dans la voiture, sur soi, dans tout l'électroménager et dans tout l'audiovisuel, jusque dans les équipements urbains et tous échangeront entre eux pour un meilleur service global. L'effet réseau est également valable pour les systèmes d'exploitation. La valeur d'un système d'exploitation est proportionnelle au nombre de systèmes d'exploitation de même famille auxquels il est connecté. Là aussi, la dynamique est sans rivale.

Ainsi les résogiciels investissent dans les services, dans les infrastructures de télécommunications, dans les satellites, dans les systèmes d'exploitation, dans les mobiles, dans les robots, dans les automobiles, dans les montres, dans les drones, jusque dans les thermostats connectés d'appartement.

Enfin, l'effet réseau est aussi valable pour les données.

La valeur d'une donnée est proportionnelle au nombre de données auxquelles elle est reliée. Cela s'appelle la contextualisation. La mise en relation des informations entre elles accroît la pertinence de chacune et par conséquent leur valeur.

Si le mot « jumelles » est repéré dans mes échanges, il faudra l'assortir d'autres informations pour savoir s'il s'agit d'un heureux événement ou de binoculaires, et par conséquent, donner de la valeur à l'information.

Ainsi plus un acteur a de données, plus les nouvelles données ont plus de valeur pour lui que pour les autres acteurs. Là encore la logique conduit à un monopole invincible de l'information par le seul effet réseau.

Services, systèmes d'exploitation, données conjuguent leurs effets réseau au sommet de la double exponentielle d'Internet. La puissance qui en résulte est sans équivalent dans l'histoire économique. Rien ne nous a préparés à l'emprise et à la puissance de ces résogiciels. Rien ne nous a préparés à la domination du réseau.

Il faut remonter au XVII^{e} siècle pour retrouver un double évènement d'une telle ampleur. Au XVII^{e}, l'océan devient un enjeu capital de pouvoir entre les nations. Comme Internet, il n'est pas un territoire traditionnel

mais un lien entre eux. Sa domination par l'Angleterre, voulue par Elisabeth I[ère], changera l'histoire du monde.

Au XVII[e], apparaissent de nouvelles formes d'entreprise : les compagnies des Indes. Elles sont révolutionnaires car elles préfigurent les sociétés anonymes par actions, ce qui leur donne accès à des ressources illimitées. Elles sont multinationales, implantées dans plusieurs pays. Elles sont les pionnières du nouveau modèle capitaliste. Enfin elles administreront des colonies et iront jusqu'à lever des armées.

Peu imaginaient alors la portée de cette nouvelle forme d'organisation économique. Aujourd'hui, sur les 100 premières entités économiques mondiales, 70 sont des sociétés privées et 30 des États.

Les résogiciels sont en ce siècle, ce qu'étaient jadis les Compagnies des Indes. Ils vont changer le monde. Les Compagnies étaient des créatures hybrides tout à la fois privées mais profondément intégrées à leurs États respectifs. Cette symbiose et cette logique sont celles qui unissent aujourd'hui les résogiciels et leurs États d'origine respectifs.

Et au premier chef, les résogiciels américains puisque, de surcroît, l'Internet, d'initiative américaine, est sous contrôle du *State Department of Commerce*. Ce dernier ne fait que déléguer la gestion du protocole, des noms de domaine et des serveurs racines, ceux-là mêmes qui déterminent toutes les adresses des machines connectées…

L'Internet est aujourd'hui une extension informatique des États-Unis sous leur domination absolue : la loi régit le comportement dans le monde physique ; le code, dans le monde immatériel, détermine l'existence même. Cette symbiose implique tout l'appareil d'État, y compris ses services de renseignement. Lorsque je publiais cela pour la première fois, en 2011, ce rapprochement paru exagéré. Les révélations d'Edgar Snowden, ancien employé du renseignement américain, en apporteront la confirmation deux ans plus tard.

Aux États-Unis, il n'y a pas de distinction véritable entre intérêts politiques et économiques, intelligence industrielle et renseignement. Les intersections sont multiples. C'est un réseau d'échanges, parfois concurrents et conflictuels, mais en dernier ressort, et c'est légitime, répondant de la souveraineté de l'État américain.

Le budget fédéral consacré au renseignement atteindrait, une centaine de milliards de dollars annuels dont plus de dix pour cent consacré à l'informatique. Des fonds de recherche, des fonds d'investissements bienveillants qui garantissent les autres investisseurs, appuient généreusement les entreprises qui auraient un quelconque intérêt stratégique. Le fonds de la CIA, In-Q-Tel, a déjà apporté son concours à plus d'une centaine de nouvelles entreprises de technologies.

Un réseau social nominatif mondial, arme de numérisation massive, va ainsi pouvoir brûler un milliard de dollars avant même d'avoir un plan d'affaires solide. Le Département de la Défense, quant à lui, est, depuis la Guerre Froide, le principal investisseur dans l'innovation aux États-Unis. C'est le support financier et logistique de toute la croissance de l'industrie informatique américaine.

Le Pentagone dépense environ 60 milliards d'euros annuels en recherche et développement, irriguant un écosystème de milliers de sociétés informatiques de toute taille.

La fameuse Silicon Valley est la partie émergée d'un véritable complexe militaro-numérique dans lequel l'administration, l'armée et le renseignement ont investi plusieurs centaines de milliards de dollars.

Identification biométrique, robotique, drones, réalité virtuelle, simulation de combat, intelligence artificielle, géolocalisation, cartographie satellitaire, reconnaissance vocale, informatique distribuée, modélisation du cerveau, capteurs, données massives, cybersécurité, détection des fraudes, chiffrement, tous ces secteurs et bien d'autres font l'objet de financement et de recherche croisés entre l'armée et les entreprises.

Sans rien enlever au fabuleux talent des entrepreneurs américains de l'informatique et d'Internet, leur garage mythique se trouve sur le pont d'envol d'un porte-avion.

Faut-il en faire le reproche aux Américains ?

Certainement pas. Ils ont raison. Et à leur place, nous ferions, à notre manière, la même chose. Car, pour les Américains, l'heure est à l'urgence et à la survie. Internet ne vient pas s'ajouter au monde que nous connais-

sons, il le remplace. Toute l'économie se reconfigure autour du réseau. La transition est terrible. Internet détruit quatre emplois quand il en crée un. Et seul un sur dix de ces emplois créés est qualifié. 20 % des tâches seraient automatisées d'ici 2025 et 47 % des emplois seraient remplacés par les machines en réseau d'ici 2035. C'est un séisme.

Ce que la mondialisation a fait aux classes populaires, Internet va le faire aux classes moyennes. Il leur est donc impératif d'orienter tout l'appareil productif vers la maîtrise du réseau et de ses technologies afin de s'en garantir les bénéfices et d'en externaliser les pertes.

Ici les compétences, les idées, les capitaux et la valeur rapatriés de partout. Là-bas, le chômage et l'appauvrissement. Chez eux, les concepteurs d'applis, chez nous les chauffeurs de taxi. Il leur faut importer les emplois qualifiés et exporter les emplois détruits. En Californie, les réseaux sociaux, en Picardie, les plans sociaux.

En second lieu, les Américains sont la première puissance du réseau mais ils ne sont plus seuls. S'ils ont réussi l'alliance organique avec le réseau offrant au monde sa dynamique ouverte, impériale et mercantile. Ils font désormais face à un géant qui lui aussi a accompli cette alliance : la Chine.

La Chine a traité l'Internet comme les invasions mongoles. En se protégeant par une muraille - une membrane filtrante peu soucieuse des libertés publiques - puis ensuite, en développant ses propres résogiciels, nouveaux géants, nés en serre et se destinant à l'hégémonie mondiale.

La Chine s'attend à un choc démographique violent. Il lui faut aller le plus vite possible pour s'y préparer. Le pillage de la propriété intellectuelle, la taille de son marché et la soumission de sa population n'y suffisent plus. Il lui faut la vitesse du réseau. La Chine n'est plus première puissance mondiale depuis 1840. Après une parenthèse de deux siècles, son expansion sur le réseau signera son retour.

Si donc le principal de l'Asie est fermé aux Américains, reste l'Europe. Elle représente un quart du PNB mondial, comme les États-Unis. Pour tenir le front Pacifique, l'arrière-cour atlantique tiendra lieu de garde-manger. L'Europe servira d'amortisseur du choc numérique sur l'économie américaine.

Là encore, les États-Unis n'agissent pas différemment de nous. Lors de la première guerre mondiale, notre empire colonial ne joua-t-il pas le même rôle ?

Enfin, l'Amérique, comme les autres nations, affronte désormais une menace dispersée, changeante, rapide, redoutable, tout à la fois autonome et en réseau. La détection anticipée du danger devient une priorité. La maîtrise du réseau est la réponse.

Seul Internet est capable de fournir en masse des données mises à jour à chaque instant. On ne gagne pas contre un réseau sans être un réseau soi-même. Seul le réseau donne une nouvelle capacité d'action inimaginable auparavant. Le réseau devient une priorité de sécurité nationale.

Les résogiciels américains, quelles que soient leurs protestations de façade, intègrent cette démarche. La défense du pays, le souci des siens, la rivalité chinoise et la menace terroriste font de la souveraineté un impératif naturel. La législation du *Patriot Act* en est la matérialisation juridique. Parallèlement, les résogiciels montent en puissance. Ils en viennent à garantir l'identité. Certains loueurs de voiture américains vérifient le profil de réseau social jugé plus fiable que des papiers aisément contrefaits. Les plateformes de commerce en ligne prélèvent une commission sur chaque transaction. Comme un impôt. Certaines alliances de services testent leur propre monnaie électronique, appuyée sur des trésoreries souvent supérieures à celles de nombreux pays. Ces services disposent enfin de leurs propres lois appelées conditions générales d'utilisation.

L'éviction d'une plate-forme, le passage en seconde page d'un classement ou la radiation d'un réseau social sont l'équivalent numérique de l'extradition, de la saisie des biens, de la prison ou de la peine de mort. Identité, impôt, monnaie, lois, prison et peine de mort. Voilà des prérogatives de l'État reprises par le réseau. D'ailleurs, avec 65 milliards de dollars de chiffre d'affaires, un résogiciel comme Amazon a un revenu supérieur au PNB de la moitié des pays du monde.

En fait, c'est la prochaine étape, les réseaux deviennent des États. L'État américain, et ses résogiciels devenus États, formeront ainsi un nouvel État fédéral multidimensionnel, physique et immatériel. Il y avait déjà cinquante états, attendez-vous à ce qu'il y en ait demain quelques-uns de plus.

Et les autres pays ?

La stratégie d'alliance ouverte État-réseau n'est pas suivie que par les États-Unis : la Corée du Sud et Israël la partagent à leur façon et avec d'exceptionnels succès. La stratégie d'alliance fermée État-réseau, incarnée par la Chine, est aussi celle de la Russie mais sans, à ce jour, la ressource d'une dynamique impériale.

Le reste du monde, le Tiers-Internet, n'a pas réalisé l'alliance entre le réseau et l'État. Le Sud-Est asiatique, le Japon, l'Australie, le Canada, l'Inde, l'Orient, l'Afrique, l'Amérique latine et l'Europe sont à la traîne. Des entreprises d'exception y réussissent pourtant malgré les handicaps. Mais leur vulnérabilité est grande, tant elles dépendent des résogiciels.

Voilà la réalité de notre situation.

Nous ne l'avons pas jusqu'à présent compris et par conséquent nos efforts ont été mal orientés. Tandis que les résogiciels devenaient des puissances soutenues par leurs États, nous avons accepté la mythologie dépassée de la start-up, petite boîte prometteuse.

Et donc, alors que la Sixième flotte se met en mouvement, nous nous extasions en organisant des concours de dériveurs… C'est une caricature, mais malheureusement pas si éloignée de notre politique industrielle.

En second lieu, alors que les résogiciels sont les moteurs de la valeur, nos investissements publics vont prioritairement aux infrastructures. La fibre sera partout. C'est bien, mais à condition que les services qui y transitent soient aussi nôtres et qui restituent une part de la valeur provenant de cette innervation du territoire. À moins d'avoir des accords avec les îles Caïmans, cela ne sera pas le cas.

Ces initiatives en décalage ne nous éviterons pas le futur le plus sombre. Voici ce qui nous attend :

La productivité du réel français et européen n'est plus concurrentielle par rapport à l'ultra-compétitivité immatérielle des réseaux américains. En conséquence, le réseau remplace le réel. L'ensemble de la société, son économie, ses ressources, ses emplois et ses données migrent sur le réseau.

Les résogiciels ne sont arrêtés par aucun obstacle. Leur seule limite est une coalition rivale. Ainsi, leurs systèmes d'exploitation se retrouvent dans toutes les machines et intelligences disséminées. Ils forment un réseau de myriades de variations du même noyau logiciel présent dans chaque terminaison du réseau, captant, calculant et communiquant sans cesse.

Ce réseau périphérique d'intelligences est, de fait, le système d'exploitation du réseau lui-même. Son rôle est l'équivalent du subconscient. L'essentiel de nos fonctions cérébrales sont sous le radar de notre perception et de notre rationalisation. Notre système nerveux capte et traite sans cesse des informations à notre insu. Le réseau est le nouveau subconscient toujours en action.

Et ce subconscient génèrera un nouveau conscient, à l'échelle d'un pays, nous donnant les moyens et la visibilité de piloter et d'orienter le destin national. C'est le pays conscient. Le réseau sera la prochaine étape de la souveraineté, mais nous ne le comprendrons que trop tard.

Quelles en seront les premières conséquences ?

Demain, tous les objets sont reliés au résogiciel et ne se conçoivent plus sans l'interconnexion et les services associés qui fondent leur valeur. Faisons un tour de quelques secteurs.

L'automobile : La valeur passe de la voiture au logiciel de la voiture. On change facilement de carrosserie, pas de résogiciel. L'industrie automobile dépendante de la licence du résogiciel la paye de sa marge. C'est ainsi que l'industrie du PC vit ses profits transférés à Microsoft. Sans marge, l'industrie n'innove plus et ne résiste pas à la compétition des véhicules automatiques du résogiciel qui bénéficient d'investissements considérables. Enfin, le résogiciel supervise le trafic qu'il sait anticiper, connaissant les trajets habituels de chaque conducteur. Il prend donc naturellement le contrôle de la signalisation urbaine.

Les télécommunications : Les opérateurs de télécommunications d'aujourd'hui sont les résogiciels. Les sociétés actuelles qui portent encore ce nom sont remplacées et deviennent, dans les zones peu denses, des fournisseurs de bande passante et d'interconnexion à faible valeur ajoutée.

La robotique et les objets connectés : Ce ne sont pas un nouveau territoire vierge pour une éventuelle revanche des perdants des résogiciels. C'est le même résogiciel déjà gagnant qui se retrouvera partout. Pas un objet, pas un robot n'y échapperont.

Le bâtiment : Pas de maison connectée sans résogiciel qui coordonne en temps réel les achats d'énergie, la consommation d'eau de l'habitat ainsi que les relations avec tous les objets intelligents du foyer.

Les médias : Difficile de concurrencer la pertinence des publicités du résogiciel, leurs moyens de production et la puissance de leurs plate-formes audiovisuelles. Quelques regroupements émergent et résistent par la taille. La plupart des marques sont absorbées par les alliances de service en quête de différenciation entre elles.

La banque : Les résogiciels accumulent de telles quantités de données identifiées qu'ils détectent les profils les moins risqués. Ils leur proposent des prêts à des taux inaccessibles pour leur concurrence et écrèment le marché des meilleurs débiteurs. Ce faisant, ils achèvent la démutualisation du risque bancaire et ne laissent aux banques traditionnelles que les clients incertains pour lesquels les taux d'intérêt explosent. Enfin, les résogiciels intègrent les paiements qu'ils associent à leurs plates-formes commerciales pour des avantages uniques et personnalisés intégrant ou remplaçant les caisses de la distribution. Le système bancaire actuel est dépassé.

L'assurance : La même logique de démutualisation est à l'œuvre. Le résogiciel dispose des données pour assurer les profils les moins risqués à des tarifs exceptionnels. À partir de quel pourcentage de démutualisation tout notre système d'assurance s'effondre-t-il ?

La santé : Les capteurs nous quantifient et nous connaissent mieux que quiconque et même que nous-mêmes. Les données de santé deviennent une clef de toute procédure de soin. Le dossier médical est absorbé par le résogiciel. L'assurance santé, fragilisée de toute part, sera démutualisée.

Les services : Les services deviennent des applications utilisant des indépendants ou des entreprises sélectionnées sur la base du prix le plus bas. L'acheteur de la prestation ne sait pas ce que reçoit le prestataire et réciproquement. La marge est dans l'intermédiation. La marge est dans

l'application. Bien des métiers se désintègrent et sont mis en compétition avec toutes les volontés de travailler, de louer, de loger, de transporter. Va naître un applitariat, nouveau prolétariat précaire des applications.

Si le résogiciel est étranger, il prendra à chaque nation tout ce qu'il peut, avec le moins de contrepartie possible. La saignée sera portée jusqu'à son terme. Plus de prêt, d'assurance, d'éducation, de syndication, de sécurité sociale. Le réseau désagrègera tout l'édifice de solidarité.

En amont du réseau, ici - mais surtout ailleurs -, les gagnants constituent une élite à la valeur démultipliée et dont la richesse explose. En aval, ici, une majorité concurrencée par les automates forme une sous-société de subsistance s'enfonçant dans la misère.

Il y a plus dramatique encore. Notre pays n'a plus de secret. Nous avons un beau défilé le 14 juillet mais notre fière nation est incapable de garantir le secret de la correspondance. Toutes nos informations sont créées, stockées, traitées et transitent par des machines, des systèmes, des programmes et des réseaux sous souveraineté étrangère.

Il n'y a pas de vie privée sans secret. Il n'y a pas de propriété intellectuelle, de concurrence sans secret. Il n'y a pas de diplomatie sans secret. Il n'y a plus de stratégie, ni de défense sans secret.

Si nous avions accès à l'ensemble des informations et des échanges d'un autre pays. Qui hésiterait à s'en servir pour faire gagner ses entreprises et pour sauver des emplois ? Qui hésiterait à s'en servir pour mieux se défendre et pour sauver des vies ?

Puisqu'il est possible d'utiliser nos secrets. Ils sont utilisés. Pour en tirer avantage et donc pour nous affaiblir. C'est une partie de poker et un des joueurs voit les cartes de tous les autres.

Cette transparence forcée est un drame absolu.

Mais ce n'est pas fini. Ces réseaux qui répondent de leurs propres règles peuvent aussi chiffrer, c'est-à-dire rendre secret leur trafic et leurs informations. Et voici que les échanges sur le territoire national deviennent opaques aux interceptions de sécurité les plus légitimes.

Mais ce n'est pas tout. L'information est manipulable à distance. Une feuille de calcul peut être altérée de manière aléatoire faisant perdre des mois de recherche. Un projet d'ingénierie peut être faussé de quelques centièmes de degrés, juste suffisamment pour le faire échouer. Des messages, des photos peuvent apparaître et disparaître. De fausses alertes peuvent être lancées sur mobile. Des informations malveillantes propagées intentionnellement à grande échelle sur les réseaux sociaux et moteurs de recherche.

D'un point de vue militaire, il faut voir le terrain comme un maillage de millions de micro-intelligences en réseau. Il sera impossible d'agir sans dialoguer constamment en profondeur et en confiance avec ce réseau. Si ce réseau joue contre nous. Nous serons bloqués, sans ressources, sans visibilité, perdus dans un état hallucinatoire. Que faire quand son propre système nerveux devient son ennemi ?

Enfin, la vitesse est ici capitale. L'accès à toutes les machines et à toutes les puissances de calcul est déterminant. Plus on a de données et de capacités à les analyser, plus on va vite et plus on ralentit le temps.

L'œil d'une mouche gère 200 images par seconde, huit fois plus vite qu'un humain. Lorsqu'il pleut, les gouttes descendent huit fois moins vite relativement pour une mouche que pour humain. La mouche se faufile entre les gouttes. L'acquisition et la vitesse de traitement des données ralentissent le monde.

Seule cette capacité de ralentir le monde par le traitement sera en mesure de compenser l'afflux d'informations au cours d'une action d'envergure et donc de donner les moyens de l'anticipation et de la décision. Sans maîtrise du réseau, l'initiative sera adverse et le brouillard de la bataille ne sera que de notre côté.

La population, quant à elle, doit être comprise, grâce aux téléphones mobiles, comme un réseau dynamique de dizaines de millions de superordinateurs de poche. Ils sont sous le contrôle d'une puissance étrangère et nous ne pourrons échanger avec nos propres citoyens qu'avec son aval.

Toute la société peut être désorganisée à partir d'un clavier et d'un écran. Les couloirs aériens, les distributeurs de billets, le réseau électrique, les feux de circulation, l'accès à Internet, les télécommunications, les sites

et les applications d'information sont des cibles. Des drones peuvent semer la panique et mille autres disruptions que nous n'imaginons même pas peuvent être déclenchées de partout par des acteurs mal identifiés et ce d'autant plus facilement que nous n'avons plus prise sur nos réseaux.

Enfin les soldats. Chaque soldat aura sur le réseau, comme chacun d'entre nous, un double numérique fait de toutes les informations collectées sur lui. Ce soi immatériel et intime sera otage soudain d'une autre puissance. Cette vulnérabilité exploitée par des algorithmes de masse peut désorganiser des unités entières.

Dans ce contexte, la confrontation militaire conventionnelle ne sera pas le premier coup mais le coup de grâce. Nous sommes à genoux. Il faut maintenant se relever.

Commençons par la déclaration du Président Obama de Février 2015 : « *Nous avons possédé Internet. Nos entreprises l'ont créé, l'on fait grandir, l'ont perfectionné, de sorte que leur large domination sur le Web ne serait qu'un juste retour des choses*. »

C'est là où il faut être clair et revenir à la boussole initiale : ne pas subir. Nous n'avons rien contre nos frères américains, alliés des périodes les plus héroïques, grande démocratie innovante et pionnière conquérante de ce monde nouveau. Simplement, nous voulons notre liberté de destin sans avoir à la demander à quiconque, y compris à nos amis.

En second lieu, nous ne nous battons pas contre le futur. Nous nous battons pour le choisir. Notre ennemi n'est pas le monde qui arrive mais notre faiblesse à le faire nôtre. Reconnaissons aussi avec admiration le génie de ces entreprises américaines, les services et produits merveilleux qu'ils proposent et qui changent positivement nos vies.

Le fond du débat n'est pas la puissance numérique des États-Unis mais notre démission sans précédent.

Est-il encore temps d'agir ?

La réponse est oui. Notre ancienne souveraineté est mise en cause par les réseaux qui deviennent des états. La nation eut déjà un défi équivalent

au Moyen-Âge avec l'essor des villes. Il fallut redéfinir le royaume. Ce que firent les Capétiens. La logique de territorialité, de droit, de citoyenneté et de coopération économique de la ville devint celle du pays entier.

Cela guide notre réponse. Nous devons en tant que nation intégrer organiquement la dynamique du réseau. Nous devons être le premier état qui devient un réseau.

Quelle est la nature de cet État-réseau ?

La question du territoire est immédiatement posée. Qu'est-ce que le territoire dans un univers immatériel et mondial ? Dans le cyberespace, l'État c'est le système d'exploitation et le territoire c'est le chiffrement. Bref, la souveraineté, c'est le code. Expliquons-nous.

Qui contrôle le réseau des systèmes d'exploitation interconnectés contrôle le réseau global, son accès, ses règles et son usage. Rien ne se fait sans lui. Il est la nouvelle incarnation de l'État. Son code informatique est l'équivalent de la Constitution : toutes les lois, comme tous les programmes, en dépendent et en proviennent.

Pour notre pays, la continuation de la République dans le cyberespace, c'est le système d'exploitation souverain. Nous y reviendrons. Le chiffrement ensuite.

Dans le cyberespace, le territoire immatériel est constitué de l'ensemble des informations générées sur le territoire physique et par les citoyens. La collection de ces données forme une totalité intègre et cohérente. La souveraineté sur cet ensemble est garantie par son chiffrement parce qu'il donne le contrôle de son accès et de son usage. Le chiffrement fait de la collectivité des données un territoire souverain.

Le territoire, ce sont les données chiffrées. Et chaque donnée ainsi chiffrée est une partie de notre souveraineté. C'est déjà le cas du dollar qui demeure, où qu'il se trouve et quel qu'en soit le détenteur, sous contrôle juridique américain.

Ainsi, une nation ne se définit plus seulement par son territoire physique mais par l'ensemble de ses données chiffrées en circulation sur la planète. Cette extension de souveraineté sur d'autres pays est une définition

même de l'empire. Sur Internet, il n'y a plus de nations physiques mais des empires immatériels en concurrence. Contre la servitude, il y a désormais un devoir d'empire.

La souveraineté c'est le code. Code du système d'exploitation qui fonde l'État et sa constitution. Code du chiffrement des données qui définit le territoire. Nous avons à nouveau un État et un territoire. Les fondamentaux de la souveraineté sont de retour.

À partir de là, tout change. Le système d'exploitation souverain est un socle public et positif de toutes les activités numériques. Il n'est ni dictateur, ni prédateur, ni concurrent de l'écosystème de milliers de sociétés, de services et d'industries privées qui s'appuieront sur lui. Quant aux données, elles sont collectées et gérées sous notre contrôle démocratique et la valeur issue de leur traitement est réinjectée dans l'économie.

La transformation sociale engendrée par le numérique trouvera la direction et les ressources pour s'orienter vers un scénario positif et pour supporter la transition. La confiance sera retrouvée dans le réseau et ses usages.

Enfin, notre sécurité et notre défense retrouveront les bases et les moyens de leurs missions. Que cela soit dans l'amical rapport de force avec nos alliés ou dans la capacité d'agir contre nos adversaires, nous ne serons rien si nous ne sommes pas une puissance numérique.

Comment devenir une puissance numérique souveraine ?

Voici un plan en trois points :

- Tout d'abord, il sera créé un Commissariat à la souveraineté numérique.

Le gouvernement a déjà pris en compte le numérique par un secrétariat d'État, des politiques d'investissement, des postes cyber dans plusieurs ministères régaliens, ainsi que par le renforcement de la sécurité des systèmes d'information des opérateurs les plus critiques. Mais ces efforts sont entravés par une absence de coordination et, par ailleurs, aucune administration n'est en charge spécifiquement de promouvoir la souveraineté numérique.

Le Commissariat à la souveraineté numérique prend appui sur l'exemple du Commissariat à l'énergie atomique, créé par l'ordonnance du 18 octobre 1945. Sa mission est de préparer les politiques garantes de notre souveraineté numérique et de suivre leur mise en œuvre. Sous l'autorité du Premier ministre, il est, pour le numérique, le pendant civil et le partenaire du secrétariat général de la Défense et de la Sécurité nationale. Il propose en interministériel d'instruire les projets susceptibles de favoriser notre souveraineté numérique. Il est en lien avec la délégation interministérielle à l'intelligence économique et le secrétariat général aux Affaires européennes afin d'étudier les textes internationaux susceptibles d'avoir un impact sur notre compétitivité ou sur notre sécurité numérique. Il pilote enfin la création du système d'exploitation souverain et l'élaboration des protocoles souverains de chiffrement des données.

➤ En second lieu, le système d'exploitation souverain.

Comme on l'a vu, le système d'exploitation souverain ou SESO, est le cœur de notre République numérique. Ce système d'exploitation est qualifié de souverain en ce qu'il est sur le réseau la continuation de la République, de ses valeurs, de ses droits et de ses devoirs. Ici la loi et le code informatique ne font qu'un. Il est le structurant de notre transformation en état-réseau. Il n'est pas question de restreindre la présence des résogiciels existants, ni de contraindre le public. Il s'agit d'être meilleur. Meilleur pour les entreprises de services et fabricants de machines qui l'utiliseront, meilleur pour les utilisateurs. Il n'est pas question non plus d'imiter les résogiciels actuels. Leur avance, leur poids, l'appui et les ressources dont ils disposent rendent la partie impossible. Nous n'avons droit qu'au coup d'après. Les résogiciels d'aujourd'hui taxent, précarisent et dévorent les entreprises tierces qu'ils hébergent. Leur logique est celle de l'exclusive et de l'exclusion. Les services essentiels sont leur propriété. Toutes les activités qui ne tombent pas sous leur contrôle sont vassalisées et leur valeur transférée. Le résogiciel remplace Internet, c'est sa logique. Le système d'exploitation souverain est le coup d'après car il est l'inverse de cette démarche et c'est ce qui fera son succès.

Tout d'abord, c'est une propriété publique et un service public. Il n'a aucune vocation à entrer en concurrence avec l'écosystème numérique qui le choisira. Les services qui l'utilisent sont protégés par le droit national, ce qui garantit leur sécurité économique.

Et le SESO est garant de la confidentialité des données des utilisateurs ce qui permet de mutualiser ces données entre les services qui le rejoignent. Ces services pourront par ailleurs se servir de briques logicielles mises en commun et de la capacité de s'intégrer réciproquement en réseau. Ce système coopératif est capital car il est la réponse à l'effet réseau des résogiciels.

Tout adhérent au SESO bénéficie de la force de tous les autres. Et cet effet réseau est mutualisé à l'échelle d'une nation. C'est pour les entreprises numériques, la plupart déjà existantes, l'accès à une dynamique exceptionnelle et massive qui les rend plus compétitives et qui les valorise pour l'avenir.

Un service de cartographie sur le SESO mutualisera ses données et se liera avec un service de réservation d'hôtels comme avec l'informatique embarquée d'une automobile. Aucune des trois entreprises ne risquera d'être remplacée par un résogiciel puisqu'elles seront elles-mêmes désormais une alliance de services et qu'elles en conserveront ainsi la valeur.

La seule économie numérique représente en France déjà plus de 5 % du PIB, soit plus d'une centaine de milliards d'euros. S'y trouve, sans conteste, la base du déploiement du SESO.

Pour les citoyens apparaît un nouvel Internet. Un Internet de confiance qu'on ne paye pas d'abord avec sa vie privée et ensuite avec son emploi. Le SESO est le garant de la sûreté et des libertés constitutionnelles. Mais c'est surtout un Internet extrêmement utile et riche d'une diversité de services que les résogiciels privatifs auront de plus en plus de mal à suivre.

Le SESO est le nouveau centre de gravité qui accélère et qui renforce les initiatives d'ores et déjà entreprises par les pouvoirs publics dans le numérique. C'est le partenaire de la mutation numérique de l'administration. Il met également à contribution l'université et le logiciel libre.

Le SESO doit être la base de l'identité numérique, du dossier médical et de la carte vitale. Il doit être recommandé pour toutes les infrastructures et pour tous les réseaux.

C'est pourquoi le SESO est conçu en collaboration avec les autorités militaires et de sécurité informatique afin d'être le plus résistant et le plus réactif aux intrusions.

Pour la société, le SESO est le support et la garantie de toutes les nouvelles activités qui vont naître avec le réseau. Demain, pour s'en sortir, chacun disposera, pour le prix d'une voiture, de plus de puissance de calcul, de performance robotique, de capacité logistique et de sources d'informations qu'une entreprise du CAC 40 d'aujourd'hui.

Chacun pourra satisfaire nombre de ses besoins par ses robots mais aussi produire en quantité ce qu'il proposera d'unique pour le vendre par le réseau. L'artisan, la famille, l'entrepreneur, l'artiste n'auront plus de limites. De nouveaux produits, services, idées et créations, monnaies, modalités d'échanges, solidarités et alliances en réseau surgiront en abondance. Grâce au SESO, ils seront libres.

À la différence des autres systèmes répondant du droit américain, le SESO est sous notre contrôle démocratique et s'incline devant notre droit de vote.

Ajoutons aussi que cette conscience du système d'exploitation est partagée. La Chine a annoncé en août dernier le lancement prochain de son COS, le *China Operating System*.

➤ Troisième point : <u>les données sont un bien commun souverain</u>

Comment nous imaginons-nous les données ? Comme un sac de billes. Chaque donnée est une bille que l'on peut prendre dans le sac et mettre dans un autre. Ce n'est plus la réalité aujourd'hui. Les données sont une pelote de laine. Chaque donnée est liée aux autres soit par nature comme un carnet d'adresses ou un rendez-vous, soit par corrélation : les données des uns servant à prédire le comportement des autres. Les données ne sont plus solitaires, c'est-à-dire ne renseignant que sur leur source, mais solidaires, c'est-à-dire renseignant également sur autrui.

Le réseau de données n'est ni dissociable, ni individualisable car chaque donnée personnelle renseigne sur les autres. C'est une indivision qui concerne toute la population.

Par ailleurs, ce réseau de données est d'un intérêt général majeur pour la collectivité en matière de santé, de transports, de consommation, d'environnement ou encore de compétitivité économique.

Le réseau des données est donc un bien commun : un bien qui appartient à tous mais qui ne peut appartenir à personne en particulier. C'est un bien commun comme la santé publique. Chacun est responsable de sa santé, pour lui-même, mais aussi pour les autres. La gestion de ce bien commun doit revenir à une Agence des données, garante des droits individuels et collectifs, garante du contrôle démocratique et souverain et seule à même d'en permettre l'accès et l'usage.

Ainsi, tout programme ou tout dispositif, collectant ou traitant des données de citoyens doit disposer de l'agrément de l'Agence des données. Cet agrément définit les protocoles de chiffrement, la localisation physique ou juridique des serveurs, la domiciliation fiscale et la mutualisation non identifiante des données collectées.

Chacun pourra, comme à l'accoutumée, utiliser le service ou l'application de son choix mais désormais en confiance, puisqu'il sera agréé. On opposera que les sociétés américaines n'accepteront jamais ces règles. Leur attitude générale en Chine tend à démontrer le contraire.

Et si, d'aventure, nous allions vers une confrontation. Mieux vaut qu'elle ait lieu maintenant. Nous nous en remettons aujourd'hui au bon vouloir de ces services pour obtenir le retrait de vidéos d'assassinat ou de décapitation.

Qu'en sera-t-il demain ?

On opposera également à cette démarche, la défiance à l'égard de l'État. Mais qu'est-ce qui n'est pas garanti par un État ? Nous ferions confiance à l'État pour notre santé et pour notre école mais pas pour Internet ? D'ailleurs, c'est la règle naturelle de nos sociétés évoluées que l'ensemble des services et produits mis à notre disposition répondent de normes et d'agréments spécifiques.

Mais, ce qui est clair, c'est qu'il n'y a pas de démocratie sans contre-pouvoirs. Il faut un contrôle parlementaire, une Cour des Codes, comme il y a une Cour des Comptes, et une ouverture vers cette nouvelle composante de la démocratie numérique, les communautés du logiciel libre. Au final, au lieu que nos données disparaissent comme un oxygène aspiré molécule par molécule par le consentement individuel de particuliers pressés,

elles seront désormais reconnues solidaires, indivisibles et arrimées à notre souveraineté.

Nous l'avons vu le chiffrement des données est capital. Le protocole de chiffrement dissociera le chiffrement des identités et des informations. Cela permettra la mutualisation des informations sans mettre en danger les identités. En garantie supplémentaire, le système des bases de données décentralisées utilisé pour les monnaies virtuelles comme Bitcoin s'appliquera à nos données. Enfin, la clef de déchiffrement des identités n'est détenue que par la Justice ou accessible au motif de la sécurité nationale.

Ajoutons ensuite que la catégorisation des données est désormais un mythe. À partir de la consommation en supermarché, on prédit des pathologies. Un profil de crédit bancaire est défini à partir des échanges sur les réseaux sociaux. De même, les données sensibles de sécurité peuvent être déduites d'autres données sans rapport apparent et nullement protégées. Par conséquent, le réseau des données solidaires et son chiffrement répondent en totalité de la sécurité nationale. Nous devons concevoir nos données comme un bien commun souverain.

Voilà ces trois directions qui s'articulent entre elles : Commissariat à la souveraineté numérique, système d'exploitation souverain et les données solidaires devenues bien commun souverain.

Nous ne pourrons pas, par ailleurs, nous voir opposer d'obstacle de droit international, dès lors que la défense de nos intérêts vitaux est ici en jeu. Il n'y a pas de lutte contre le terrorisme sans souveraineté numérique.

Nous sommes sur le réseau dans une situation nouvelle. L'atome a conduit au concept de guerre impossible par la probable destruction mutuelle des belligérants. Le réseau engendre celui de paix impossible. L'augmentation constante du nombre de connectés et la croissance exponentielle du pouvoir de nuire de chacun rend la paix statistiquement impossible. Nous sommes en état de paix impossible.

Et l'Europe ? L'Europe, et d'abord l'Allemagne, pourront nous rejoindre. La condition du succès est de n'attendre personne, de commencer et d'être rallié ensuite.

La dimension européenne sera, en effet, l'étape suivante. Le G29, groupe de travail rassemblant les autorités de protection des données nationales, a lancé la coordination des souverainetés en ce domaine. Nous pourrons ainsi nous appuyer sur la première économie mondiale.

Cette démarche sera suivie du monde entier, suivie par les pays, qui sautant l'âge industriel traditionnel, font des réseaux mobiles, leur source de croissance et de progrès, suivie aussi par les défenseurs des droits civiques, y compris et surtout aux États-Unis, qui attendent de nous la République numérique.

Mon point de départ était la liberté défendue par nos parents. Mon point d'arrivée est la liberté que nous devons à nos enfants. Ne pas subir. C'est entre nos mains.

Je vous remercie.

Les enjeux du cyber pour les armées françaises

Vice-Amiral Arnaud Coustillière
Officier général cyberdéfense, État-major des armées

« **Le cyberespace est donc désormais un champ de confrontation à part entière** »[1]. Le Livre Blanc pour la défense et la sécurité nationale de 2013 annonce clairement la perception politique des enjeux stratégiques de la dépendance de notre société aux systèmes d'information et à leurs supports. Pour autant, la compréhension et la définition des concepts liés au « cyberespace » est en soi un enjeu stratégique pour adapter la défense de la France et pour ne pas avoir une « guerre de retard ».

La révolution du cyber

Penser le cyberespace doit en effet échapper à la facilité d'ajouter cyber devant les termes pour s'inspirer des modes de pensée classique. Parler de « cyberguerre », de « cybercombattant » ou de « cyberarme », c'est prendre le risque d'enfermer sa réflexion dans le cadre rassurant des conflits connus et de manquer le développement d'une analyse audacieuse qui tirerait pleinement parti des nouvelles opportunités. Il s'agit cependant bien de l'introduction rapide dans le champ stratégique d'un nouvel espace, intimement lié à la mondialisation et au développement des sociétés modernes, qu'il serait plus précis de baptiser « espace numérique », et qui, source de richesses et d'échanges, est devenu un enjeu de pouvoir et un nouvel espace de confrontation par la volonté et par les intérêts de ses différents acteurs. Ce nouvel espace vient bouleverser nos approches classiques, issues des confrontations du vingtième siècle.

Car le cyber n'est pas une simple évolution qui permettrait de conduire les mêmes opérations avec un peu plus d'efficacité, comme l'arrivée d'un nouveau type de canon à la précision accrue. Le cyber n'est pas non plus seulement une innovation qui permettrait de conduire les mêmes opéra-

1. Livre blanc pour la défense et la sécurité nationale, 2014, p 45.

tions d'une manière différente, quand on a considéré à l'origine la bombe atomique comme un substitut à des raids massifs de bombardiers conventionnels[2]. Le cyber est une véritable révolution qui permet d'envisager un nouveau spectre d'opérations potentiellement illimité contre un adversaire « *informatiquement développé* ».

L'irruption du cyberespace dans les questions de défense ressemble par certains côtés à l'arrivée de l'aviation aux côtés des domaines séculaires des combats terrestres et maritimes. Certains affichent, tel Foch en 1910, un scepticisme trop prudent : « *L'aviation, c'est du sport, pour l'armée, c'est zéro.* ». D'autres, au contraire, s'enthousiasment pour la nouveauté, au risque d'y voir l'arme ultime comme Douhet[3]. Dans tous les cas, le nouveau phénomène a eu des conséquences irréversibles sur les questions internationales, juridiques, militaires, qui ont d'ailleurs évolué avec les progrès techniques, le contexte lui-même mouvant des sociétés humaines et l'expérience. Mais même s'inspirer de l'aviation pour penser le cyber serait une facilité intellectuelle . Le cyber est en effet bien différent dans ses implications et imprègne toutes les activités humaines et par répercussions militaires.

Pour rester une puissance à vocation mondiale, la France doit donc investir pleinement ce nouveau domaine stratégique, qui mêle civils, militaires, États, entreprises, groupes d'intérêt et individus. Si les forces armées n'y sont pas toujours en première ligne, le ministère de la Défense doit l'intégrer à son champ d'action et peut également participer au développement de la communauté nationale de cyberdéfense.

Le cyber, un défi global

Le Livre blanc pour la défense et la sécurité nationale de 2013 déclare sans ambiguïté que les cyberattaques en tant que telles sont une des menaces stratégiques pour la France[4]. Mais l'utilisation du cyberespace est par ailleurs un des moyens possibles, si ce n'est parfois le plus efficace, par lequel les autres menaces stratégiques se concrétisent.

2. Le bombardement d'Hiroshima inflige les mêmes dommages qu'un raid de 220 bombardiers B29.
3. Général Guilio Douhet, *Il dominio dell'aria*, 1921, paru sous le titre *La guerre de l'air* en 1932.
4. *Ibid*, p 47.

Le cyber est aussi l'illustration de la complexification du monde et du brouillage des repères traditionnels sur lesquels l'ordre mondial Westphalien s'est peu à peu construit. Si le cyberespace est devenu indispensable au fonctionnement des sociétés modernes, il présente par là même des fortes vulnérabilités qui sont autant d'opportunités pour tous les acteurs. Il a de plus un coût d'accès relativement faible. Les cybermenaces sont ainsi à la portée de tous (États, entreprises, groupes, individus), instituant une forme de « pouvoir égalisateur du cyber » qui multiplie les opportunités de conflits, qui met à mal le monopole étatique de la violence légitime et qui permet la « guerre de tous contre tous »[5]. Cette interaction entre civils et militaires, public et privé, États et organisations ou individus, a lieu en permanence, indépendamment d'un temps de paix ou de guerre, déjà assez indistinct dans les domaines conventionnels[6].

Le cyberespace est donc paradoxalement très conflictuel, bien que peu militarisé, et permet une « *guerre autre que les opérations militaires* »[7]. Les cadres juridiques qui ont été définis par des siècles d'expérience de la guerre sont donc ici singulièrement remis en cause. Les définitions du droit des conflits armés en particulier doivent être revisitées pour y intégrer les cybermenaces : seuil de l'agression armée, statut du combattant, cibles légitimes, notions de proportionnalité,...

Le ministère de la Défense, acteur au service de la cyberdéfense française

Organiser ce nouveau champ opérationnel et développer ses capacités de combat, non seulement les ressources techniques mais surtout les ressources humaines, c'est un chantier ambitieux. En effet, plus que le volet technique, ce sont elles qui en sont le principal enjeu. Fort paradoxalement, la cyberdéfense est avant tout une « force humaine », quantitativement et qualitativement pour participer à la bataille des volontés et des innovations, qui seule confèrera l'avantage stratégique. Plus encore que dans les autres composantes, il faut développer le concept des « ingénieurs combattants », maîtrisant à la fois la science du combat et celle de la numérisation au sein d'équipes pluridisciplinaires.

---

5. Thomas Hobbes, *Le Léviathan*, 1651.

6. Selon l'Institut pour l'Économie et la Paix, seuls 11 États dans le monde ne sont pas engagés dans un conflit. http://www.economicsandpeace.org/ consulté le 5 mai 2015.

7. Concept inverse des « *opérations militaires autres que la guerre* », popularisé aux États-Unis dans le cadre de l'approche globale.

MINISTÈRE
DE LA DÉFENSE

Pacte Défense Cyber
50 mesures pour changer d'échelle

DGA

DR

Pour donner plus de cohérence et une nouvelle impulsion au développement de la cyberdéfense, le ministre de la Défense a décidé de lancer le 7 février 2014 le Pacte Défense Cyber[8]. Ce pacte regroupe 50 mesures en 6 axes qui couvrent tous les domaines d'action du ministère et représente au total sur la période 2014-2019 un effort budgétaire d'un milliard d'euros. Dans le cadre des travaux de suivi de cette loi de programmation militaire, et suite aux orientations données par le président de la République, les investissements notamment humains affectés à cette capacité de combat vont d'ailleurs encore augmenter de façon significative. Ce pacte soulève la nécessité d'une communauté de cyberdéfense qui transcende les intérêts catégoriels au bénéfice mutuel de tous. C'est finalement une réponse collective au défi cyber hobbesien évoqué précédemment.

Le ministère de la Défense a ainsi mis en place un pôle d'excellence en cyberdéfense en Bretagne, afin d'en faire avec la région parisienne, la seconde zone de concentration des compétences techniques et opérationnelles, et de pouvoir y envisager des parcours de carrière attractifs. Outre les nombreuses implantations militaires liées au cyber (Écoles d'officiers de l'armée de terre et de la marine, école des transmissions, centre d'expertise de la DGA, écoles d'ingénieurs du ministère de la Défense, unités opérationnelles), d'autres acteurs (universités, collectivités locales, grandes entreprises, PME/PMI) sont investis dans la cybersécurité. Cette densité naturelle est favorable à la conduite de nombreux projets communs au bénéfice de tous. Les rapprochements des entreprises et des universités permettent l'émergence de projets innovants et l'enrichissement des enseignements tandis que les experts du ministère de la Défense et le soutien financier apporté par ce même ministère, appuient la recherche et le développement et qu'ils accélèrent les projets transverses. La connaissance mutuelle favorisée par ces projets transverses et la mobilité des spécialistes deviennent des atouts inestimables pour la confiance réciproque et pour la communication en temps de crise.

La réserve cyber citoyenne est un autre cadre qui favorise les échanges entre les forces armées et la nation. Les réservistes citoyens contribuent à la réflexion, diffusent les bonnes pratiques voire, dans le cadre de la nouvelle réserve à vocation opérationnelle, soutiennent le ministère en cas de crise cyber.

8. Pacte Défense Cyber, ministère de la Défense, février 2014 (http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber)

À l'international, le ministère de la Défense est moteur des indispensables discussions à différents niveaux et dans différentes enceintes internationales (ONU, OSCE) pour définir un comportement responsable des États et pour promouvoir la stabilité du cyberespace, notamment en limitant la dissémination des menaces et en évitant une escalade non maîtrisée. Il s'agit aussi de trouver, notamment dans la zone euro-atlantique (OTAN, UE) mais pas seulement, des alliés aux intérêts communs et suffisamment dignes de confiance pour partager informations et solutions et pour opérer ensemble en coalition. Il s'agit enfin d'ouvrir des canaux de discussion avec les autres pays pour faire connaître sa vision et pour mieux comprendre leurs intentions et ainsi pour éviter les malentendus et les erreurs de calculs dans le dialogue stratégique.

Le cyber : nouveau domaine de combat

Sur le plan opérationnel, la première responsabilité du ministère de la Défense est d'ajouter le cyberespace à ses environnements de combat classiques (terre, mer, air et espace). Il doit garantir l'efficacité opérationnelle des forces militaires pour accomplir les missions ordonnées par les décideurs politiques malgré les cybermenaces, et inclure les moyens cyber dans le spectre des capacités militaires. La cyberdéfense est, de ce point de vue, « *le cyber dans la défense* ».

Le Livre blanc de 2013 définit très clairement une « *organisation de cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires* »[9]. Un commandement opérationnel de cyberdéfense est en place depuis 2011, intégré au centre de planification et de conduite des opérations militaires à tous les processus de préparation et de conduite des opérations militaires. La nouvelle doctrine militaire de cyberdéfense parue en mars 2014[10] permet de franchir une nouvelle étape en plaçant résolument le cyber comme une fonction opérationnelle plutôt que purement technique, et organise les relations complexes mais nécessaires entre tous les acteurs du ministère et au-delà. Notre doctrine d'action dans le domaine cyber s'organise désormais autour de quatre grandes fonctions, qui visent à nous protéger, à nous défendre, à agir, et à se renseigner.

9. *Livre blanc pour la défense et la sécurité nationale*, 2014, p94.

10. *Doctrine Inter Armées de cyberdéfense 3.40* du 28 mars 2014.

La protection suppose des produits et des services de confiance, mais aussi une conception rigoureuse des systèmes. C'est tout particulièrement le rôle des experts de la DGA que d'y veiller, en lien avec la base industrielle et technologique de cybersécurité. La défense repose quant à elle sur la chaîne opérationnelle de cyberdéfense, qui agit en temps réel pour la sécurité de nos systèmes, et en particulier sur le centre d'analyse en informatique défensive (CALID) et les équipes de cyberdéfense projetées avec les forces. Le renseignement, obtenu par les services *via* des moyens cyber et non cyber, nous permet d'anticiper les menaces, d'adapter nos systèmes de défense et de caractériser l'adversaire. L'action, enfin, avec la « *lutte informatique offensive* » et les « *opérations d'influence* », viennent en appui des opérations militaires, dans un cadre juridique qui a été clarifié par la loi de programmation militaire.

Le théâtre d'opération cyber est vaste : il s'agit bien sûr de défendre les forces armées sur le territoire métropolitain et dans les territoires d'outre-mer mais aussi dans les pays dans lesquels nos forces sont déployées au titre d'accord de défense ou en opération. Ce grand nombre de déploiements et d'engagements en opération dans le monde entier augmente notre surface d'exposition, le nombre d'agresseurs potentiels et la variété de leurs méthodes. Il accroît également la difficulté à surveiller l'ensemble des systèmes, y compris les systèmes d'armes, à construire une vision globale de leur état et à agir si besoin pour les défendre.

Conclusion

Le cyber est ainsi pleinement intégré à toutes les étapes des opérations militaires, que ce soit en anticipation, en planification ou en conduite. La posture cyber et les moyens d'actions sont donc adaptés à chaque théâtre d'opérations, ainsi qu'aux forces et aux faiblesses de nos forces et à celles de nos adversaires. Chaque armée, service et direction contribue à cette posture en assurant une surveillance de proximité et surtout en développant une expertise de ses systèmes spécifiques et une expertise « métier ». L'armée de l'air, traditionnellement intiment liée à la technologie, peut apporter, au-delà de son expertise technique reconnue, sa vision stratégique et sa maîtrise opérationnelle des domaines spatial, aérien et nucléaire pour faire face à ces nouvelles menaces.

Recognized Cyber Picture de l'armée de l'air (RCP Air) la RAP[1] cyber des aviateurs

Colonel Christophe Vilchenon
Général des systèmes d'information et de communication
de l'armée de l'air

Introduction

Les opérations aériennes actuelles, en métropole (PPS[2], dissuasion et MISSINT[3]) comme à l'extérieur du territoire national (OPEX[4]), mettent en évidence la nécessité de fournir au Commandement Air (CDAOA[5], CFAS[6] ou commandement de la composante air de théâtre) une représentation « pertinente » de la situation opérationnelle d'intérêt air[7].

Celle-ci doit apparaître sous la forme d'une visualisation synthétique des informations strictement nécessaires à la compréhension de la situation, présente mais surtout future. De plus, cette représentation doit être partagée avec les autres composantes et avec les niveaux stratégiques (CPCO[8]) et tactiques, français ou alliés.

S'agissant de la situation dans l'espace aérien (et, depuis quelques années, dans l'espace extra-atmosphérique) et de l'état de disponibilité des moyens, l'armée de l'air dispose d'une culture et de moyens de synthèse issus de plus de soixante-dix années de pratique (des tables de situation de la bataille d'Angleterre aux écrans du SCCOA[9]).

1. *Recognized air picture* = situation d'intérêt air.
2. Posture Permanente de sûreté = défense de l'espace aérien national.
3. Mission intérieure.
4. Opération extérieure.
5. Commandement de la défense aérienne et des opérations aériennes.
6. Commandement des forces aériennes stratégiques.
7. Cf. article du GCA (2S) GAVIARD, sur la représentation opérationnelle partagée et pertinente ou « ROPP », dont est inspiré cet article.
8. Centre de planification et de conduite des opérations du chef d'état-major des armées.
9. Système de commandement et de conduite des opérations aériennes.

L'utilisation massive, ces dernières années, des nouvelles technologies de l'information et de la communication dans les systèmes d'information classiques comme dans les systèmes d'armes, ainsi que la montée en puissance rapide de menaces importantes dans l'espace numérique, imposent désormais aux aviateurs de réfléchir à la prise en compte de ce nouvel espace de confrontation dans leur représentation de la situation opérationnelle d'intérêt air.

Pourquoi une RCP Air ?

Le commandement air doit disposer, en permanence, de toutes les informations ayant un impact direct ou indirect, immédiat ou à plus long terme, sur sa capacité à assurer ses missions (évolution de la situation aérienne, apparition de menaces, disponibilité des moyens). De plus, il doit pouvoir, à partir de ces éléments, se projeter dans le temps et planifier les actions « à venir » mais aussi anticiper les conséquences stratégiques et politiques des actions menées.

Une attaque (ou une menace d'attaque) cyber, par les dégâts qu'elle peut causer sur les moyens de l'armée de l'air (perte ou divulgation de données, blocage de réseaux, arrêt de systèmes…), pendant une durée indéterminée, avec des effets de bord non négligeables (contagion à d'autres systèmes), est donc un élément essentiel à porter à la connaissance du commandement.

La partie cyber de la représentation d'intérêt air (appelée dans ce document RCP Air) doit donc permettre de faciliter la connaissance et l'appréciation de la situation dans l'espace numérique utilisé par l'armée de l'air, d'aider à la prise de décision en cas de crise cyber et de faciliter le contrôle des actions décidées.

De même, si le rôle principal du Commandement Air n'est pas uniquement de se focaliser sur la conduite en temps réel des opérations (responsabilité déléguée à un niveau subordonné ou local), il doit cependant pouvoir, si des événements d'importance surgissent et qu'ils relèvent de son niveau, voire du niveau stratégique ou politique, être capable d'effectuer un « zoom » de cet événement, et de rafraîchir des informations au bon tempo.

Dans le domaine particulier du cyber, ce zoom est en effet indispensable au Commandement Air pour qu'il puisse apprécier l'événement à sa juste valeur et répondre à ce type de questions

- quels sont les systèmes impactés ?
- quelles sont les conséquences opérationnelles, dans l'absolu ou dans le cadre de la situation ou de l'opération en cours ?
- quelles sont les actions pouvant être prises pour atténuer ou pour résoudre la crise et leurs conséquences sur l'opération en cours ?
- quel est le délai de retour à la normale ?
- …

Il s'agit, pour le Commandement Air, d'adapter sa posture dans un délai très restreint et de pouvoir résoudre des situations « soudaines » relevant de son niveau, voire même, dans certains cas, de se focaliser sur les systèmes d'information touchés. Ce cas d'intervention très ponctuel du Commandement Air au niveau d'exécution correspond bien à un événement majeur pour lequel ce niveau local n'a pas reçu de délégation d'action (cela concerne, par exemple, les systèmes d'information d'importance vitale de l'armée de l'air).

Comment construire une RCP Air ?

Il est indéniable que la représentation de la situation cyber d'intérêt air est destinée au commandement opérationnel et non à des techniciens, spécialistes des systèmes d'information ou des cyberattaques. Ces derniers doivent bien sûr disposer de systèmes adaptés à leur mission et à leur expertise (moyen technique de commandement et de conduite de la LID[10], moyens de supervision des centres d'exploitation de type *Security Operating Center*…) mais il s'agit alors d'outils avec des finalités différentes.

En revanche, les informations affichées dans la RCP Air doivent impérativement provenir d'une base de données commune avec les techniciens pour que cette représentation, appréciation synthétique de la situation présente et future, soit une vision partagée. Il s'agit ainsi de transformer des données brutes en informations directement utilisables pour le Commandement Air (savoir qu'un routeur est hors service est une chose,

10. Lutte informatique défensive.

DR

comprendre le déficit d'activités aériennes sur un site isolé à cause de ce problème en est une autre).

La définition de l'information « pertinente » relève donc du Commandement Air car elle dépend de l'événement cyber considéré, de la situation ou de l'opération elle-même et des effets possibles ou probables sur cette situation ou sur cette opération.

Cette pertinence dépend aussi de l'appréciation personnelle du commandeur, et constitue donc un véritable choix de commandement. Ce choix se fonde sur des analyses opérationnelles et techniques, de niveaux stratégique, opératif et tactique, d'origines civile et militaire. L'expérience du commandeur, comme celle de son équipe, ne peut être construite qu'à travers des exercices de crise et des réflexions « à froid » sur les plans de continuité des activités et des missions de l'armée de l'air.

À côté de problèmes cyber « très visibles » (déni de service pour un système ou destruction de données), les attaques cyber sont essentiellement « discrètes ». Ainsi, leur découverte est souvent le fait d'éléments convergents qui, pris individuellement, seraient considérés comme sans importance. Les informations, qui constituent pour le décideur des éléments synthétiques et objectifs qui facilitent la décision, nécessitent cependant d'être recoupées par d'autres moyens à fournir en temps contraint.

Le domaine du renseignement (menace cyber) doit être aussi une des priorités du Commandement Air, qui doit s'appuyer sur l'ensemble des sources d'information disponibles et orienter auprès des organismes *ad hoc* la recherche du renseignement cyber sur les pays, groupes non étatiques ou pratiques pouvant menacer son action.

Des représentations adaptées doivent être également développées afin d'offrir la visualisation d'informations non techniques comme les informations d'ambiance. Toute information politico-militaire intéressante dans ce domaine devra être signalée, voire visualisée.

Au global, il s'agit de disposer d'une « image » adaptée au Commandement Air, qui fait apparaître l'état de l'espace numérique concerné par la mission, les menaces sur cet espace de bataille et, le cas échéant, les effets attendus des actions menées pour résoudre la crise cyber.

Quelques réflexions générales autour de la RCP Air

Il sera nécessaire de coupler ce système de représentation avec un système d'archivage des données, afin de pouvoir réaliser une formation réaliste et analyser « à froid » des crises passées (prise en compte du retour d'expérience en particulier). En outre, dans le domaine juridique, cette base de données contenant l'historique des actions sera déterminante, notamment dans le cadre des enquêtes sur l'imputabilité des décisions.

Des outils de simulation connectés à cette base de données peuvent enrichir et faciliter le travail, à plus ou moins long terme, au moyen d'analyses prospectives, de comparaisons de modes d'action et d'évolutions d'effets, afin de faciliter le choix des options optimales pour la poursuite de l'opération en fonction des évolutions prévues ou constatées dans le cyberespace.

Les opérations aériennes sont par essence interarmées, interministérielles et multinationales. Il importe donc que tous les participants à une même opération puissent partager et échanger l'ensemble des données nécessaires à l'appréhension de la situation cyber (par exemple, le CDAOA, au titre de la PPS air, doit pouvoir disposer d'informations sur l'intégrité des systèmes d'information de l'aviation civile et les intégrer en temps réel dans sa RCP Air… et réciproquement).

Cette condition très exigeante implique donc une forte interopérabilité entre les systèmes de recueil des données cyber des composantes terre, air, mer et avec le niveau interarmées, mais aussi au niveau interministériel français, voire dans l'avenir avec les armées étrangères.

Dans un autre registre, la structure de l'état-major du Commandement Air doit non seulement lui permettre d'anticiper et de conduire l'opération aérienne, mais aussi de gérer la crise cyber. La RCP Air doit ainsi offrir une meilleure connaissance des enjeux et lui permettre de connaître, de planifier, de conduire et de communiquer dans ce domaine. Ces caractéristiques constituent les responsabilités majeures de l'état-major qui doit travailler dans un seul sens, en partageant toutes les fonctionnalités.

En effet, une crise cyber n'est pas seulement l'affaire de spécialistes techniques et constitue bien un problème qui a des impacts multiples,

non seulement opérationnels mais aussi en termes de communication. Il revient donc au Commandement Air d'assurer la gestion haute de la crise en s'appuyant sur cette représentation.

Une RCP Air, prémices d'une RCP pour les organismes du ministère ?

Le « cyberespace de l'armée de l'air » est constitué, grossièrement, des systèmes d'information (matériels et logiciels) utilisés par l'armée de l'air (au sens large du terme systèmes, donc en prenant en compte les systèmes d'armes), des réseaux d'échange de données ainsi que des données elles-mêmes et de leur interprétation[11].

Tout d'abord, la responsabilité des échanges de données entre systèmes basés à terre a été confiée à la DIRISI[12]. Dans l'avenir, de plus en plus de systèmes d'information vont être hébergés sur des structures communes de la DIRISI, conformément à la politique ministérielle. La responsabilité de surveiller l'état « cyber » des réseaux et des structures d'hébergement appartient donc à l'opérateur DIRISI mais il serait aberrant de prétendre surveiller l'espace numérique de l'armée de l'air sans disposer de données sur les réseaux ni sur les structures d'hébergement des systèmes d'information.

Ensuite, pour assurer ses missions, l'armée de l'air utilise des informations produites par les autres armées, directions et services du ministère de la Défense et par certains organismes hors défense (comme l'aviation civile), voire internationaux (comme cela est le cas pour les échanges de données avec les responsables de la défense aérienne des pays limitrophes). Cela implique que l'armée de l'air dispose, *a minima*, de toutes les données pertinentes de ses principaux interlocuteurs. Cette condition doit être réciproque car les systèmes air peuvent impacter les cyberespaces terre et marine, civil et alliés.

Cette constatation implique la réalisation d'une unique base de données cyber de niveau ministérielle, chaque armée venant « piocher » les données dont elle a besoin pour réaliser sa propre RCP, adaptée à ses spécificités et à son activité.

11. Cyberespace constitué en trois couches : matérielle, logique et sociétale

12. Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense

Comme évoqué en introduction, l'armée de l'air dispose néanmoins d'une culture ancienne de la représentation partagée de situation rapidement évolutive (RAP). Or, construire une RCP consiste d'abord à imaginer une représentation synthétique de la situation qui soit adaptée au niveau d'un commandeur.

En ce sens, le travail d'approfondissement de la RCP Air, lancée par l'armée de l'air en capitalisant sur son expérience, doit pouvoir profiter aux autres armées et au niveau interarmées. L'armée de l'air dispose en effet des compétences et de la culture pour spécifier à la DGA[13] le besoin d'un outil qui soit paramétrable en fonction des besoins de chacun et utilisable par tous.

Conclusion

Nos adversaires disposent d'une bonne connaissance de notre sensibilité dans le domaine des techniques de l'information et ont facilement accès à des moyens d'attaque peu coûteux.

Un instrument de visualisation de la situation cyber adaptée aux opérationnels, apporte une plus-value indispensable pour accélérer le processus décisionnel et permettre la coordination des actions dans un domaine où le temps est une contrainte forte et les effets collatéraux importants. La réaction face à une attaque cyber nécessite des capacités de commandement, en plus des capacités d'investigation, pour permettre au Commandement Air de continuer à opérer.

Un outil permettant « *une représentation opérationnelle partagée et pertinente* » s'inscrit ainsi totalement dans cette évolution au caractère irréversible et marquera bientôt le seuil à partir duquel une nation pourra prétendre aux responsabilités de « Nation-cadre » au sein d'une coalition[14].

L'armée de l'air disposant déjà de la culture et de l'expérience nécessaire, il paraît ainsi naturel de s'inspirer de cette expertise et de s'en servir comme socle pour préparer l'avenir.

---

13. Direction générale de l'armement.

14. Cf. article du GCA (2S) GAVIARD déjà cité.

Dans le cyberespace, la distinction entre civils et militaires a-t-elle encore un sens ?

Monsieur Nicolas Arpagian
Directeur scientifique du cycle « Sécurité Numérique » à l'Institut National des hautes Études de la Sécurité et de la Justice (INHESJ).

La Convention de Genève du 12 août 1949[1] consacrée à la Protection des populations civiles et des personnes civiles en temps de guerre l'affirme sans détours : « *L'interdiction d'attaque des personnes civiles et des biens civils implique celle de tous actes de violence, qu'ils soient commis à titre offensif ou défensif* ». À la sortie du second conflit mondial, le droit vient renforcer la distinction faite entre le sort réservé aux simples citoyens et aux forces armées en cas de conflit. Et les décennies suivantes, tenteront – avec un succès tout relatif – de faire vivre cette différence de traitement. Dès lors qu'il s'agit de l'engagement de troupes sur un théâtre d'opérations ce distinguo peut s'envisager selon des critères matériels : s'agit-il du personnel travaillant sous un uniforme ? Avec une formation spécifique ? Répondant à des ordres émanant d'une autorité hiérarchique ? En échange d'une rémunération d'origine étatique ? Avec des moyens et ressources fournis par un service gouvernemental ? Les équipements utilisés par les armées professionnelles (systèmes de communication, armement, moyens de transport, habillements adaptés) ont depuis longtemps des caractéristiques techniques adaptées à un environnement hostile. Même si nombre d'achats des formes armées – restrictions budgétaires obligent – se font de plus en plus chez des fournisseurs civils.

L'affrontement dans le cyberespace tend à reconsidérer cette approche. En effet, le principe même de l'attaque informatique consacre la logique du conflit asymétrique, où un individu isolé, voire un petit nombre de personnes qui n'ont pas besoin de se connaître personnellement ni de se trou-

1. https://www.icrc.org/fre/resources/documents/misc/5fzfmt.htm

ver réunis dans un même lieu, peuvent conduire des opérations offensives à l'encontre d'une administration, d'un état-major ou d'une entreprise. Qu'il s'agisse de pénétrer un système d'information pour l'espionner ou pour le dérégler, ou de conduire des campagnes de communication visant à discréditer un pouvoir politique ou à promouvoir une cause particulière. Soit une capacité de nuisance sans équivalent dans le monde physique où il faudrait rassembler des ressources humaines, financières et logistiques en nombre conséquent pour espérer atteindre des résultats équivalents. Ici ce sont l'agilité, l'opportunisme et la créativité qui priment. La connaissance informatique et la maîtrise de l'ingénierie sociale sont des disciplines plus utiles que la maîtrise des plans-reliefs.

La Défense a en outre l'habitude de traiter avec des fournisseurs de confiance pour mener à bien ses missions (Dassault, DCNS, Nexter, MBDA, Thalès…). Leurs cadres dirigeants étant souvent passés par les états-majors et l'État exerçant une tutelle plus ou moins directe sur leurs activités, les relations se déroulent dans un climat plutôt confortable. Or, quand il s'agit d'aborder le cyberespace, les militaires sont amenés à devoir traiter avec des firmes avec lesquelles elles sont loin de partager la même intimité historique (Microsoft). Surtout, comme l'a confirmé Edward Snowden en juin 2013, que les compagnies étatsuniennes doivent – selon le dispositif PRISM – répondre aux sollicitations techniques des autorités de Washington sans en avertir leurs clients. Et les géants de l'économie numérique (comme Facebook, Google, IBM, Linkedin, Microsoft) s'insèrent de plus en plus profondément dans les processus de production. Les uns collectent et analysent des données, les autres les transportent ou les stockent. Et ces entreprises, de culture éminemment civiles, soignent particulièrement leurs relations politiques. Ainsi en mars 2015, *The Wall Street Journal*[2] révélait que Google avait été reçu une fois par semaine à la Maison Blanche par l'équipe de Barack Obama depuis sa première élection. Idem pour Microsoft. Et Éric Schmidt, *chairman* de Google après en avoir été le CEO siège officiellement aux côtés de Craig Mundie (jusqu'à très récemment en charge de la direction de la stratégie de Microsoft) comme conseiller du Président Obama au sein de *l'Office of Science and Technology Policy*[3]. Un cénacle *ad hoc* pour échanger sur les enjeux stra-

2. http://www.wsj.com/articles/google-makes-most-of-close-ties-to-white-house-1427242076 "Google Makes Most of Close Ties to White House", *The Wall Street Journal*, Brody Mullins, 24 mars 2015.

3. https://www.whitehouse.gov/administration/eop/ostp/pcast/about/members

tégiques, économiques et militaires des États-Unis. Une proximité sans équivalent de notre côté de l'Atlantique, d'autant plus que cette imbrication, concerne des sociétés déjà établies, mais également tout un écosystème de jeunes pousses qui se lancent sur des technologies ou des services en devenir. Notamment dans le domaine du *big data,* ce traitement intelligent de quantités massives de données. Qui connaît des déclinaisons tant civiles que militaires pour des services marketing désireux de cerner le profil de leurs clients que de la part d'agences gouvernementales chargées de la lutte contre le terrorisme. Une stratégie résumée par le quotidien *Les Echos* le 16 avril 2015 sous le titre : « *La high tech américaine, arme de domination massive* »[4]. La *Defense Advanced Research Projets Agency* (DARPA) spécialisée dans le repérage et dans le financement de technologies exploitables par les forces armées travaillent en étroite collaboration avec les poids lourds de la Silicon Valley. La *Google Car* est ainsi née d'un concours de la DARPA visant à créer un véhicule autonome. Et les mouvements de personnel dans la fleur de l'âge entre la NSA, la DARPA et les fleurons de l'économie numérique se banalisent. On est loin des transferts en fin de carrière d'officiers généraux en mal de reconversion pour assurer leur train de vie familial.

Parfois, une gestion fine de profils sur des réseaux sociaux grand public vaut bien des actions d'infiltration sur le terrain. Ainsi, la séduisante Reut Zuckerman qui avait convaincu quelque deux cents soldats ou réservistes israéliens de devenir son amie sur Facebook n'a pas eu de difficultés à les interroger sur leurs prochains déplacements[5]. À peu de frais, le Hezbollah a ainsi disposé d'informations à jour concernant les opérations et les mouvements de troupes à venir de Tsahal. De même, quand on souhaite pirater le système d'informations de la présidence de la République française en 2012, il est plus simple de passer *via* le compte Facebook d'un collaborateur du chef de l'État[6]. Un canal très grand public pour une intervention que l'on peut attribuer à un État.

4. http://www.lesechos.fr/idees-debats/editos-analyses/0212346322-la-high-tech-americaine-arme-de-domination-massive-1111709.php *Les Échos*, Benoît Georges, 16 avril 2015.

5. http://www.spiegel.de/politik/ausland/online-spionage-die-schoene-facebook-freundin-der-elitesoldaten-a-694582.html «Online-Spionage: Die schöne Facebook-Freundin der Elitesoldaten», *Der Spiegel*, Sarah Stricker, 17 mai 2010.

6. http://www.letelegramme.fr/ig/generales/france-monde/france/cyber-attaques-l-elysee-pirate-a-deux-reprises-avant-l-intronisation-de-hollande-11-07-2012-1769862.php *Le Télégramme de Brest*, Jean Guisnel, 12 juillet 2012.

Les frontières civilo-militaires s'estompent sur le Net. Au point de rendre problématiques des éléments fondamentaux enseignés de longue date dans les amphithéâtres militaires. Qu'est-ce que l'état de paix, quand des assauts numériques peuvent intervenir sans que soit formellement déclarée une entrée en guerre. La notion de victoire a-t-elle encore un sens ? Quand sait-on que l'on a gagné quand il ne s'agit plus de prendre le contrôle d'un territoire ? Comment riposte-t-on quand l'émetteur de l'attaque n'est pas une force armée étatique ? Comment établir avec certitude que l'entité suspectée est bel et bien à l'origine de l'offensive numérique ? Quelles politiques de gestion de ressources humaines doivent être envisagées quand le savoir-faire ès cybersécurité ne se trouve pas forcément dans les enceintes académiques conventionnelles ? Cette remise à plat des notions civiles et militaires oblige à revoir les cursus de formation, le recours effectif à des corps de réserve qui ne soient pas considérés comme de simples supplétifs et les relations entretenues avec le tissu économique. Les grands industriels de la défense ont tous vu dans les perspectives des marchés de cybersécurité la planche de salut qui leur permettrait de faire face à la réduction des budgets purement militaires. Il n'en est rien. Car ce ne sont pas les mêmes sommes qui sont en cause et parce que ces conglomérats ont été conçus pour fonctionner sur des cycles longs, qui ne correspondent pas du tout à la volatilité et à la réactivité de l'univers numérique.

Il ne s'agit pas que d'une réflexion purement doctrinale ou académique, mais bien d'une capacité à se placer dans un avenir proche en position de faire face aux mutations technologiques et économiques qui s'opèrent avec la numérisation de notre environnement. En se plaçant en situation de dépendance numérique face à de grands équipementiers étatsuniens ou asiatiques, nous obérons durablement notre aptitude à maîtriser nos infrastructures. Si nous avons un doute quant à la fiabilité ou à la confiance que l'on peut leur accorder lors d'une opération nous fragilisons la concrétisation de notre politique. Et donc nous affaiblissons notre posture stratégique. À trop vouloir fonctionner avec une grille de lecture fondée sur les seuls modèles anciens, nous hypothéquons notre avenir commun. Dans le monde numérique, l'avenir n'est pas la continuation paisible du passé, mais se bâtit sur des ruptures successives. À l'oublier, ou à persister à ne pas le voir, nombre de prétendus stratèges formés dans un modèle de pensée aujourd'hui dépassé portent une lourde responsabilité dans la fragilité qu'ils nous préparent.

C2 et Cyber

Général (2s) Gilles Desclaux et Monsieur Bernard Claverie
expert C2, Président de RACAM / Directeur de l'ENSC

Le C2, « Command and Control » ou « Commandement et Conduite », correspond à un ensemble de théories, de moyens et de méthodes de gestion de grands systèmes complexes, notamment dans le domaine des opérations militaires. C'est un modèle théorique qui s'articule autour des trois dimensions de la programmation de l'action coordonnée des forces et de la gestion des crises : la stratégie, la tactique et l'opérationnalité.

Le C2 est constitué d'une part de grands ensembles informatiques qui sont mobilisés dans la réception des informations,dans leur analyse, dans l'aide à la décision, dans la transmission des informations et des directives, dans la commande de l'action et son contrôle pour ajuster cette action en permanence aux objectifs recherchés. Ce premier volet, instrumental, est totalement empreint des dimensions du « cyber » dont il tire l'essence même de sa structure. Le C2 est d'autre part défini comme une organisation de gestion et un ensemble de procédures. Ce second volet permet de déterminer un ensemble hiérarchique et de délégations entre commandeurs et opérateurs pour organiser l'action des forces. Ces deux dimensions complémentaires, structurelle et fonctionnelle, constitue ce que l'on désigne aujourd'hui sous l'acronyme C4ISR-TAR. Il associe aux caractéristiques du commandement et de la conduite des opérations les dimensions et les outils de Contrôle, Communication, Computers, Intelligence, Surveillance, Reconnaissance, Target Acquisition et Reconnaissance spécifique (acquisition de cibles). Le C4ISR[1] est notamment le sigle utilisé par le Département de la Défense (DoD) américain et l'OTAN comme « *ensemble des moyens et des processus militaires organisés et structurés en vue de la conduite des opérations, de leur commandement et de leur contrôle* ».

1 Collectif (2015) : C4ISR & Networks. *Managing massive data (white paper)*. Washington (DC — USA) : Air Force Cyber Initiatives. - Joint Chiefs Of Staff Dod (2008), *Department Of Defense Dictionary Of Military And Associated Terms : Joint Publication* 1-02, Washington (DC, USA) : Government Printing Office (GPO), GPO Bookstore.

Un troisième volet est celui de l'étude théorique, qui s'affranchit des dimensions techniques et managériales, pour aborder une dimension générique du C2. Ce champ d'étude spécifique du « Command and Control » s'est ainsi constitué dans la conceptualisation des systèmes complexes[2], et c'est dans cette perspective que les auteurs examinent les influences du « cyber » sur la modélisation du C2 et sur les apports potentiels du C2 dans la gestion du « cyber ».

La machine C2

Le C2 peut être conçu comme une machine théorique et sa définition systémique s'inscrit dans la cybernétique[3]. Cette machine repose sur trois piliers : les trois côtés du triangle C2 (cf. figure 1) au sein duquel s'effectuent les grandes étapes du travail : la perception et l'analyse situationnelle, l'approche compréhensive de l'environnement et des moyens dont on dispose pour le modifier, la planification opérationnelle synthétisée par l'« *operational design* » et sa construction en lignes d'effort convergeant vers des centres de gravité (alliés, adversaires), et enfin le cycle de décision contingent des trois horizons temporels : *So what* ? *What if* ? *What next* ? qui comprend la synchronisation et la programmation des actions et l'évaluation constante des effets obtenus (*feedback*). La mise en œuvre des différentes boucles de contrôle et de *feed-back* mobilise de manière coordonnée les différents acteurs, moyens et soutiens au succès de l'opération. Ces côtés du triangle sont d'égale importance, et ils permettent l'entrée, la transformation puis la sortie d'information traitée par la machine C2 pour commander l'action de modification de l'environnement. Chacun de ces piliers est complémentaire et dépendant des autres et alimente la problématique « cyber ».

Le premier côté du triangle est celui des entrées et de la maîtrise de l'information. Il a pour but la « dominance informationnelle » et lui sont relatifs les différents renseignements, humain, d'open source et technologique : satellites, drones, radars et autres senseurs qui scrutent le spectre électromagnétique (*ISR dominance*). C'est par lui que transitent les informations entrantes (*inputs*) qui sont traitées, recombinées, conceptualisées, enrichies de manière physique et sémantique. C'est aussi le domaine de la gestion

2. Alberts, D.S., Hayes, R.E. (2006), *Understanding Command and Control*. Washington (DC, USA) : US Department of Defense, CCRP Publication Series.

3. Claverie, B., Desclaux, G. (2015), « La cybernétique : commande, contrôle et comportement dans la gestion des systèmes d'information et de communication ». *Hermes*, CNRS Éditions : 71, 72-79.

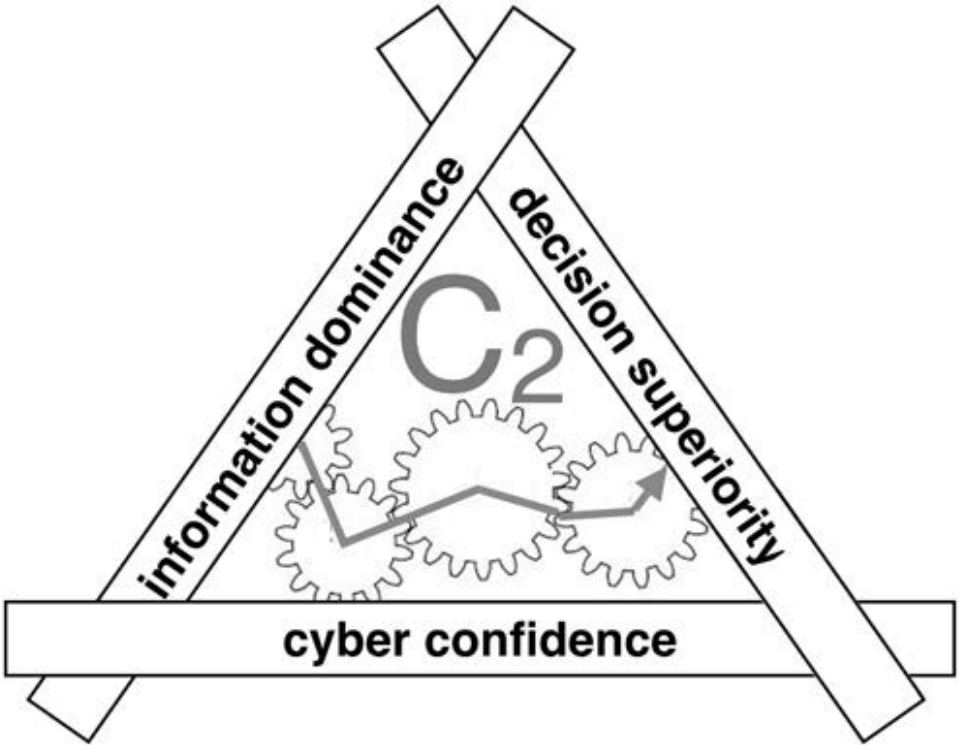


Figure 1 : la machine théorique du C2.

des connaissances, du *big data* et du *cloud computing*, de la corrélation et de la fusion des données, du ciblage intelligent (*video analytics, automated targeting workflow*)… Il permet de motiver une conscience de la situation partagée entre les différents étages du commandement et du contrôle, et d'évaluer les perspectives des réponses à l'action en fonction des moyens de recueil à programmer et à mettre en œuvre.

Le second côté est celui de la base du triangle. C'est sur lui que repose concrètement la machine avec l'ensemble des moyens matériels informatiques et des méthodes de calcul, de détection et d'imagerie. C'est sur lui que s'étaye la « *confiance informationnelle calculatoire* ». S'y rattachent les critères d'intégrité des réseaux, des calculateurs et des programmes, mais également le volet humain des relations, des interfaces et de l'intégration homme-système pour une forme de cyber résilience et de cyber agilité.

Le dernier côté est celui de la sortie de la machine C2. Il est orienté vers les effets désirés dans la constante de temps nécessaire et avec la précision temporelle souhaitée. C'est sur ce côté que s'appuient les différentes dimensions cognitives avec, notamment, l'unification et le partage des représentations, les processus de prise de décision collaborative en rapport avec les orientations du commandeur, les processus de gestion des opportunités et la programmation

critique et partagée de l'action par les différents vecteurs. Chacun de ceux-là, avion, drone, opérateur ou combattant, est lui-même soumis pour son action à une réplication de structure caractérisée par les 3 dimensions précédentes.

Cette machine C2 est inscrite dans une dynamique qui s'adapte aux demandes du pouvoir politique pour déterminer une flèche stratégique et pour produire des effets adaptés (cf. figure 2). Il est alors aisé de comprendre que dans un monde caractérisé par la convergence du « tout numérique » et par les nouveaux médias d'action de l'ennemi moderne, le « cyber » est à la fois un outil pour la théorisation du C2 et un domaine de contraintes qu'il doit prendre en compte. Sans reprendre les différentes menaces, les fragilités, les process de résilience et les moyens de correction, de protection ou d'efficacité mis en œuvre et largement développés dans le « cyber », l'évolution du domaine C2 est largement impactée par ces nouveaux paramètres. Le champ d'étude aborde aujourd'hui trois niveaux de complexité du système C2 : la complexité d'incertitude, la complexité dimensionnelle, la complexité computationnelle[4]. Chacun de ces niveaux est concerné par le « cyber ».

Les complexités « cyber » du C2

La complexité due à l'incertitude de l'information est, pour certains auteurs, le « grand défi » du C2[5]. Celui-ci est relatif à trois dimensions : l'incertitude technologique, l'incertitude de la situation et l'incertitude du facteur humain. C'est la problématique « cyber » qui permet de s'attacher à minimiser ces incertitudes et de tendre à ramener la situation à un état de relative efficience. Un premier domaine de préoccupation pour le C2 est relatif à différentes dimensions techniques, de MCO, de fusion et calcul, de limite technique... S'y ajoute la réduction pour une représentation imagée souvent immédiate et à destination d'opérateurs en situation opérationnelle complexe. La dimension « cyber » est ici celle de la réduction l'incertitude dans les deux dimensions, techniques et humaines. Si une autre voie d'incertitude est due aux activités humaines extérieures, volontaires ou

4. Cooper, C. (1994), « Complexity in C3I systems ». In D. Green et T. Bossomaier (Eds.) *Complex systems : from biology to computation*. Amsterdan (Pays Bas) : IOS Press, 223-231.

5. Levis, A. H., Athans, M. (1988), « The quest for a C3 theory : dreams and realities ». In S.E. Johnson et A.H. Levis (Eds.) *Science of Command and Control : coping with uncertainty.* Washington (DC, USA) : AFCEA International Press (Armed Forces Communications and Electronics Association), 4-9.

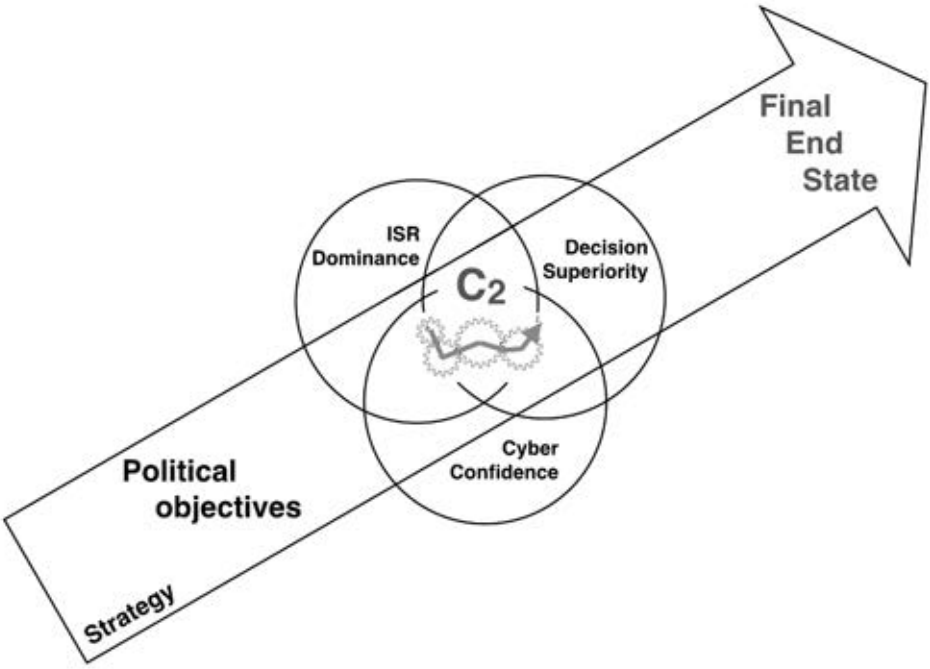


Figure 2 : le pouvoir transformateur de l'information par la machine C2.

non, la principale source est paradoxalement interne, relative aux propres faiblesses des acteurs du système. Le « facteur humain » est celui qui est le plus difficile à évaluer, comprendre, et à maîtriser. Il est cause de biais et d'erreurs qui créent cette incertitude de manière d'autant plus dangereuse qu'elle est souvent produite de bonne foi, susceptible d'être mal maîtrisée et passer inaperçue. Dans ce cadre, l'enjeu de l'ingénierie humaine est de traiter les causes de l'incertitude, en travaillant sur la robustesse des procédures, sur le partage représentationnel, sur la confiance relationnelle pour la maîtrise de l'erreur dans les systèmes complexes[6]. Ces domaines sont aujourd'hui peu étudiés dans le monde « cyber » et participent pour certains à quelques lieux de faiblesse significatifs du C2.

Un deuxième domaine d'influence « cyber » dans le C2 est relatif à la complexité dimensionnelle. Elle correspond au fait qu'un système de commande et de contrôle est structuré de manière cybernétique, en une hiérarchie de sous-systèmes en interaction mutuelle. Le nombre de cas à considérer augmente de manière exponentielle alors que chaque élément peut produire des quantités considérables d'informations dans un système fractal. Sa compréhension dépasse les capacités de compréhension et de représentation spontanée, les capacités de modélisation et surtout les moyens de leur calcul, engageant le C2 dans une véritable « malédiction de la dimensionnalité[5] ».

6. Strauch, B. (2007), *Investigagting Human Error : Incidents, Accidents, and Complex Systems*. Aldershot (UK) : Ashgate.

La complexité de calcul concerne les paramètres de rapidité, de fiabilité et de puissance de calcul. Ces dimensions classiques du monde « cyber » font entrer le C2 et son immense quantité de données dans celui du « *big data* ». Ceux qui en maîtrisent l'exploitation sont probablement les détenteurs du techno-pouvoir de demain. Son exploitation commence bien entendu par la maîtrise des capteurs mais également par le traitement des données ouvertes, de l'« open source », et de l'information « broadcast »[7] dans un monde dont la raison numérique est aujourd'hui soumise à la logique de l'exponentiel.

L'aide cognitique pour le C2

L'exploitation de l'information ouvre sur le domaine du « *data mining* » et celui de l'« intelligence artificielle ». Les techniques d'IA sont entrées depuis longtemps dans les différentes dimensions du C2[8]. L'IA et l'iconographie statistique constituent la base de la nécessaire réification des données. L'ensemble des informations est, à chaque étage de décision, le reflet plus ou moins fidèle de certaines caractéristiques physiques du milieu, de la nature d'événements qui s'y produisent, et de données artificielles surajoutées pour une forme d'« illusion du monde ». Il permet à chaque niveau d'avoir une certaine conscience du réel. Si les « *data* » sont censées en être des descriptions, elles sont transformées et interprétées, et ne parviennent au commandeur que de manière spéculaire.

Or une donnée interprétée est plus ou moins discutable, et la démarche de C2 va alors être d'en fournir un inventaire avec des algorithmes de réponse immédiate ou différée en fonction de critères de choix que supportent de nécessaires méta-systèmes d'intelligence artificielle. Elle termine avec sa synthèse par l'intelligence humaine, ainsi entraînée dans un exercice « cyber-cognitif » toujours plus difficile. Le C2 est donc un exercice hybride, inter et transdisciplinaire. Il associe aux dimensions techniques des plus grands programmes informatiques actuellement connus de ce côté de l'Atlantique pour traiter d'immenses quantités de données en perpétuelle évolution, les algorithmes de l'aide cognitive pour alimenter la gestion humaine d'opérations dont l'enjeu engage la sécurité de nos sociétés.

---

7. Alberts, D.S., Hayes, R.E. (2004), *Power to the Edge : Command, control, in the information age*. Information Age Transformation Series. Washington (DC, USA) : US Department of Defense CCRP Publication Series.

8. Taylor, E.C., Snell, D.J. (1988), « Artificial intelligence in command and control », *Signal*, 4, 25-29

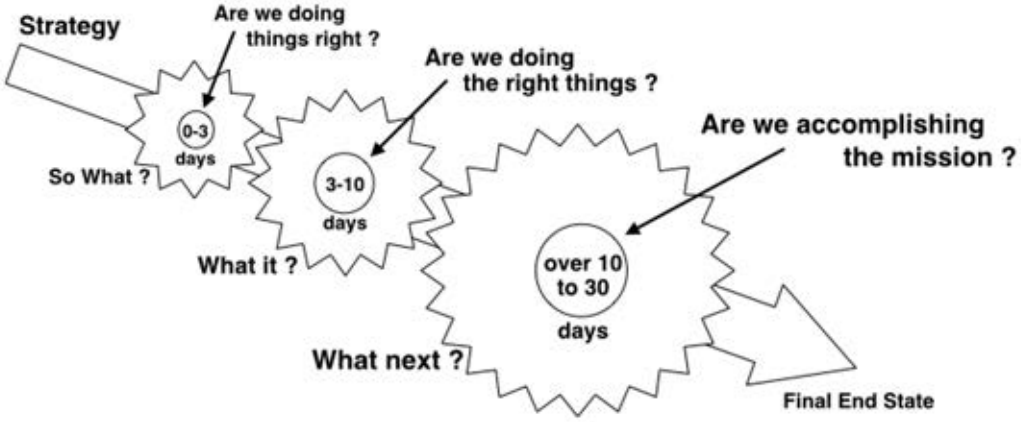
Le C2 pour gérer le « cyber »

Les dimensions de la complexité du C2 l'inscrivent dans une dynamique de création hybride, artificielle et humaine, de représentations pour la décision. C'est sur ces représentations que les acteurs fondent leur action. Le « cyber » est l'une des contraintes du C2, c'est aussi une motivation à son évolution permanente et la source de l'avancée théorique qui place l'homme dans la boucle (« *the man in the loop* ») pour la supériorité de l'action coordonnée dans un monde de plus en plus numérique. Or l'« espace cyber » semble entretenir quelques similitudes avec les domaines d'application du C2.

Le premier parallèle se fonde sur le cycle de la décision et sur les ajustements d'une boucle cybernétique associant quatre phases : la planification et la programmation (systèmes, réseaux, crypto, etc.), l'émission des ordres et des directives (cyber tasking), la supervision (situation *awareness* du cyberespace) et la conduite en temps proche du réel et, enfin, l'évaluation continue de la performance (tempo, qualité et intégrité des liaisons, pertinence des informations et des représentations). Les premiers sont du domaine du « *command* » (plan, direct) et les derniers du domaine du « *control* » (*monitor*, *assess*).

Le second parallèle est relatif à la programmation temporelle des opérations associant à la fois la performance de défense et la fiabilité des opérations. À partir d'une base théorique solide, enrichie à la fois par l'expérience et par la recherche, une doctrine permet de structurer un ensemble de procédures, maintenues actives ou « sur étagère » pour être directement disponibles dans la mise en œuvre des solutions adéquates dans les quatre phases du cycle de décision, tant pour la gestion du risque que pour le management des crises.

La culture du C2 a théorisé trois horizons temporels imbriqués qui se partagent les tâches à accomplir et la typologie de l'analyse des résultats et des effets obtenus. Le premier, à court terme, se tient prêt à réagir à l'imprévu et pose la question de la performance des actions programmées en cours : « *the things right* ». Le second envisage l'action à moyen terme et se prépare à anticiper les situations critiques ou celles qui ne sont pas conformes (« *branch plans* »). Il analyse la qualité des effets obtenus et la manière dont on y parvient : « *the right things* ». Le troisième pense les séquences opérationnelles suivantes et s'attache à évaluer la réussite de la mission.



Les 3 horizons C2 du cycle de décision.

Ces trois horizons du cycle de la décision du C2 sont applicables au « cyber » avec les objectifs généraux, avec la mise en œuvre et avec la réalisation pratique des quatre phases précédentes. Enfin, et ce n'est pas le moindre des points, le « cyber » est à la fois un espace multidimensionnel et un espace de confrontation. Naturellement inscrit dans la logique cybernétique, le « cyber » dispose des caractéristiques d'un système coordonné par le C2, dont il partage d'ailleurs les valeurs. L'hypothèse est donc celle d'un rapprochement des deux champs de la recherche et de ces deux volets complémentaires de l'exercice de Défense.

Conclusion

Les spécialistes du C2 sont chaque jour plus immergés dans le monde numérique, dans la représentation virtuelle du réel, dans la programmation et dans la gestion coordonnée pour une mobilisation de moyens au service d'une stratégie. S'ils disposent d'outils, de méthode et d'un champ pratique, ils participent à la construction d'un véritable domaine d'étude théorique, à visée applicative.

Les évolutions de ce domaine sont impactées par la préoccupation « cyber ». Mais inversement cette réflexion doit pouvoir servir au « cyber » et cela selon au moins deux pistes complémentaires : ouvrir la réflexion épistémologique du monde « cyber » sur l'opérationnel et disposer des méthodes de contrôle de l'espace virtuel du « cyber » grâce au C2, à ses principes, à ses méthodes et à ses outils.

La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine

Monsieur Danilo D'Elia
Chercheur associé à la Chaire Castex de Cyberstratégie,
doctorant au sein d'*Airbus Defence and Space*

Faire partie du club des cyber-puissances : voici l'ambition de la France en matière de cyber sécurité. Le *Military Balance 2014* de l'institut IISS[1] dresse une liste des capacités à développer pour appartenir aux Grands, parmi lesquelles une capacité devenue d'importance cruciale pour les États : la politique industrielle[2]. La cyber-puissance s'accompagne d'une capacité de décision indépendante, caractéristique indissociable du développement d'une industrie maîtrisée et souveraine. Quelles actions doivent alors être entreprises pour développer et pour maintenir une telle industrie ?

Au niveau politique, l'imbrication d'enjeux économiques (protection des citoyens et organisations contre l'escroquerie ou l'espionnage) et sécuritaires (protection des opérateurs d'importance vitale (OIV) contre le sabotage) a alimenté la représentation de la cyber sécurité comme bien public. La nécessité d'assurer la sécurité de ses propres systèmes d'information s'accompagne de la préservation de la libre utilisation des réseaux informatiques et de la garantie de protection de l'économie et du territoire nationaux[3].

La cyber sécurité est aussi devenue une opportunité économique. Le secteur génère en effet un chiffre d'affaires mondial estimé à environ 50 Md€ par an (1,3 Md€ et 40.000 emplois en France) en croissance de près de 10% par an[4].

1. ISS: International Institute for Strategic Studies.
2. The Military Balance 2014, *Possible Indicators of Cyber Capability*, pp. 19-22, 2014.
3. À ce propos, Jean-Marc Ayrault, alors Premier ministre, déclarait : la cyber sécurité est « *une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement* » (Discours du Premier ministre tenu à l'Agence nationale de la sécurité des systèmes d'information le 21 Février 2014).
4. *Visiongain, Global Cyber Security Market Report* 2013-2023.

Toutes ces raisons soulignent l'importance pour les États de se doter d'une *Base industrielle et technologique de cybersécurité (BITC*), écosystème cohérent d'entrepreneurs, de laboratoires et d'investisseurs capable d'assurer une innovation continue et un socle technologique répondant à ces enjeux.

À la suite de la publication du Livre blanc sur la défense et la sécurité nationale (2008) identifiant la cyber menace comme une des principales menaces des prochaines années, les pouvoirs publics ont lancé une politique volontariste en la matière créant dès 2009 l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

L'année 2013 peut être considérée comme un nouveau tournant: vote de la Loi de Programmation Militaire imposant des règles de cyber sécurité aux OIV et attribuant 1Md€ aux ressources techniques et humaines de l'État ; mise à disposition de 150M€ dédiés aux projets d'innovation en cyber défense; lancement d'une feuille de route de politique industrielle (*Cyber Plan)*.

L'ambition affichée est claire : développer une « offre souveraine de confiance ». Néanmoins, cette volonté soulève différentes questions : quelles sont les capacités de production autonomes dont dispose la France ? Quels sont les avantages et les limites de la coopération public-privé ?

Un marché inadapté face au périmètre redéfini de la cybersécurité

À première vue, la structure du marché national paraît atomisée, tant en terme de taille que d'offre[5], et dominée par les acteurs américains et israéliens, seuls capables d'atteindre un chiffre d'affaires dépassant la centaine de millions d'euros (FireEye, Cisco Security, etc.). Cependant, de nouvelles dynamiques se font jour suite au changement de périmètre de la SSI[6]. Celle-ci n'étant plus limitée aux réseaux étatiques mais intégrant

5. Selon l'orientation (produits/services), nous trouvons six catégories : les éditeurs de logiciels (TrendMicro, Kaspersky), les fabricants de matériels informatiques (CISCO, IBM), les fournisseurs de technologies (Qosmos), les opérateurs télécom (Orange, BT), les consultants et les prestataires de services informatiques (EMC, Sogeti), les spécialistes de la défense (Thales, Airbus Defence and Space).

6. Danilo D'Elia, La cybersécurité entre bien public et marketing de la peur, en Aude-Emmanuelle FLEURANT (dir.), Quelles stratégies face aux mutations de l'économie mondiale ?, Étude de l'IRSEM n° 38, 2015, pp 79-95.

DR

DR

désormais les systèmes industriels, l'internet mobile et le *Big Data*, nous assistons à l'émergence de nouvelles barrières à l'entrée sur le marché : la nécessité d'une vision globale et la confiance sur l'ensemble des SI. Cela a plusieurs conséquences.

D'un côté, les industriels historiques de la défense (e.g. Airbus ou Thales) ont lancé des stratégies de *démocratisation* des solutions développées jusqu'ici pour des clients étatiques (défense, renseignement, etc.) modifiant leur approche du marché. De l'autre côté, la sécurité conçue comme un millefeuille de technologies achetées sur étagère (routeurs, chiffreurs, firewall, etc.), ne semble plus adaptée. Il est désormais nécessaire d'adopter une vision globale des risques, face à une menace évolutive exigeant anticipation, détection et réaction rapide. Dans ce contexte, les éditeurs et intégrateurs ont été amenés à entreprendre des alliances afin d'élargir leur portfolio et de couvrir l'intégralité du spectre de la sécurité (e.g. Orange-Atheos ; Airbus DS-Arkoon-Netasq).

Parallèlement, la notion de prestataire de confiance s'impose comme une caractéristique structurante du marché. La sécurité des SI sensible comporte des éléments de confidentialité, d'intégrité et de continuité d'activité et impacte le fonctionnement d'une société. Dans un monde post-Snodwen, il s'agit, pour un État, de disposer de fournisseurs capables de produire des solutions maîtrisées tout en assurant une relation fondée sur la confiance.

En conclusion, les caractéristiques intrinsèques du marché (compétition mondiale et nécessité d'innovation constante) couplées avec le besoin d'une vision globale et d'une offre maîtrisée sont en train de structurer le marché. Comment ces mouvements ont-ils impacté la stratégie française de cybersécurité ?

La structuration d'un dialogue complexe

L'Alliance pour la Confiance Numérique confirme l'éclatement de l'offre française : 700 acteurs dont cinq grands groupes, une quasi absence d'entreprises de taille intermédiaire et plus de 600 PME au chiffre d'affaires souvent inférieur à 5 M€[7]. Reproduire toute la chaîne d'approvi-

7. Alliance pour la confiance numérique, http://www.confiance-numerique.fr/. Elle dénombre 700 acteurs dont 100 éditeurs, 100 équipementiers et 600 sociétés de conseil.

Tableau 1. Les initiatives de la politique industrielle en matière de cybersécurité

Initiative	Description	Impact direct / indirect	Acteurs impliqués
Réserve citoyenne cyberdéfense	Cercle de confiance composé par des personnes issues du monde industriel, de la recherche, des organismes étatiques. Deux groupes de travail sont institués pour sensibiliser les PME et les grands groupes.	indirect sur la demande	Large nombre d'acteurs privés et publics
Nouvelle France Industrielle – Plan 33	La feuille de route du *Plan Cyber* vise à : 1) Accroître la demande en solutions de confiance ; 2) Développer des offres de confiance ; 3) Soutenir l'export et 4) Renforcer les entreprises nationales.	Direct sur l'offre et sur la demande	ANSSI-DGA, OIV, Fournisseurs de sécurité
Groupe de travail sur la sécurité des systèmes industriels	Groupe de réflexion sur la cybersécurité industrielle piloté par l' ANSSI et composé d'acteurs industriels (utilisateurs, équipementiers, intégrateurs, ect.) et étatiques (ANSSI/DGA).	Indirect sur l'offre et sur la sécurité	ANSSI-DGA, OIV, Fournisseurs de sécurité
Plan Défense Cyber 2016	Plan d'action du MinDef en matière de cyber défense pour la période 2014-2016. Développé autour de 6 grands axes visant notamment à : durcir le niveau de sécurité des SI et les moyens de défense et d'intervention du ministère et de ses partenaires de confiance; intensifier l'effort de recherche; renforcer les ressources humaines dédiées à la cyberdéfense	Direct sur la demande et indirect sur l'offre	MinDef/EMA/DGA, Grands groupes, PME
Programme Investissements d'Avenir (PIA) 2013	Le ministre délégué chargé des PME, de l'Innovation et de l'Économie numérique a investi 150 millions d'euros pour la R&D des technologies « cœur de filière numérique ». Parmi elles, cinq solutions de sécurité des SI vont être développées dans ce cadre.	Direct sur l'offre	Gouvernement, ANSSI, Grands groupes, PME
Loi de programmation militaire 2014-2019	Obligation pour le OIV de déclaration immédiate de tout incident.	Indirect sur l'offre	OIV
	Imposition des règles de sécurité, organisationnelles ou techniques, comme la mise en place de systèmes de détection d'attaques par des prestataires de confiance.	Direct sur la demande	ANSSI/DGA, PME et Grands groupes
	Augmentation du financement pour les programmes d'études amont à 30 €M/an.	Indirect sur l'offre	DGA et PME
Club HexaTrust	Fédération de 19 PME dans l'objectif de promouvoir leurs technologies auprès des grands donneurs d'ordre et de gagner des marchés à l'export.	Indirect sur l'offre	PME
Pôle d'excellence en cyberdéfense-Bretagne	Il s'agit de la création d'un pôle d'excellence en cyberdéfense dédié à la formation, à l'entraînement ainsi qu'à la recherche et au développement en cyberdéfense.	Indirect sur l'offre	DGA/ANSSI, PME, Grands groupes, Laboratoires de recherche
Comité de la filière industrielle de sécurité (CoFIS)	Comité composé des principaux représentants du monde de la sécurité : fournisseurs, décideurs, investisseurs, et clients. Objectif : faire se rencontrer demande et offre et structurer l'ensemble des acteurs de la sécurité à travers un dialogue public-privé.	Indirect sur la demande et sur l'offre	Gouvernement/ANSSI, Grands groupes, PME, OIV

sionnement (systèmes d'exploitation, microprocesseurs, serveurs, etc.) au niveau national est impossible. Pour l'État il s'agit plutôt d'encourager une maîtrise nationale des technologies critiques et de s'appuyer sur des intégrateurs capables d'offrir un système sécurisé dans sa globalité.

Les caractéristiques d'une offre de confiance sont dès lors les suivantes.

Premièrement, une solution souveraine est synonyme d'intégrité, donc d'absence de moyens de contournement. Pour cela, l'État exige « *un processus d'évaluation sous le contrôle de l'autorité SSI nationale* »[8] qui se traduit par la nécessité d'un développement sur le territoire français et d'un constant niveau d'investissement. En outre, l'offre doit être simple de déploiement et d'exploitation. Ces caractéristiques de fonctionnalité et d'intégrabilité, couplées à un prix compétitif, sont un préalable indispensable au succès commercial. Tout l'enjeu de la politique industrielle consiste alors en la structuration d'une filière industrielle capable de produire une offre nationale, garantissant un niveau élevé de sécurité qui soit aussi compétitive sur le marché.

Dans le but d'atteindre cet objectif, les pouvoirs publics et le secteur privé ont mis en œuvre un ensemble d'initiatives (cf. Tableau 1) dont l'analyse fait émerger quatre piliers principaux :

- *a) Réglementation pour structurer la demande.* L'article 22 de la LPM impose aux OIV la mise en place d'équipements de détection d'attaques informatiques et leur exploitation par des prestataires labélisés par l'ANSSI. Ce recours à du *made in France* constitue un levier pour développer la demande nationale de solutions de cyber sécurité[9].

- *b) Structuration du dialogue État-Industrie.* Le lancement du CoFis, du groupe de travail sur le SCADA et de la feuille de route du *Plan*

8. Selon l'appel à projets des Programme d'Investissements d'Avenir 2013 – Développement de l'Économie Numérique, « Cœur de filière numérique-Sécurité numérique », Octobre 2013.

9. Dans le même le but de stimuler la demande et afin de montrer l'exemple à un secteur privé pas encore totalement sensibilisé aux risques informatiques, le Premier ministre a promulgué une circulaire pour obliger les ad ministrations à recourir aux produits nationaux et labélisés par l'ANSSI. Circulaire du 17 Juillet 2014, Politique globale de sécurité des systèmes d'information (PSSIE).

Cyber démontrent la volonté d'organiser la coopération entre les différentes missions de l'État (régulateur, client, investisseur) et le secteur privé (fournisseur et client). Ces initiatives ont pour but de déterminer collégialement les priorités et de concilier offre et demande.

- *c) Orientation de la R&D.* L'État a multiplié ses efforts tant dans le domaine civil que militaire. La DGA (Direction Générale de l'Armement) a triplé entre 2012 et 2014 ses crédits d'études (30M€ en 2014). En parallèle, dans le cadre du *Programme Investissements d'Avenir* (PIA) 2013, l'appel à projets « Sécurité Numérique » a fait l'objet de 18 propositions. L'ambition est d'orienter les investissements en R&D pour favoriser le développement d'une offre jusqu'à présent absente.

- *d) Certification des solutions de confiance.* Ce volet représente une forme de partenariat stratégique entre les industriels et l'État. Les industriels sont appelés à apporter une offre « valable » et l'État, dans son action de labellisation de solutions, contribue à structurer l'offre en sélectionnant les sociétés qui ont les compétences et les technologies correspondantes aux critères de sécurité requis.

Un secteur privé proche de l'État

Ces quatre piliers nous laissent percevoir la spécificité du modèle français. Tout d'abord une forte présence des pouvoirs publics, héritage du « *Colbertisme High-Tech* », c'est-à-dire de la stratégie post seconde guerre mondiale de rattrapage du retard industriel par la maîtrise technologique. Ce modèle était articulé autour de vastes projets reposant sur la commande publique, soutenus par la préférence nationale et permettant donc l'émergence de champions industriels.

Néanmoins, les contraintes de restriction budgétaire et d'internationalisation des OIV, couplées avec les caractéristiques propres à la cyber sécurité (menace évolutive, nécessité d'un temps de réaction très court) ont obligé le volontarisme politique à s'ouvrir au secteur privé. L'évolution de l'ANSSI, au sein de laquelle existe depuis 2011 un bureau de coordination avec les OIV, témoigne de cette ouverture. Un bureau dédié à la « *Politique Industrielle et Assistance* » a par ailleurs été mis en place en 2012 pour faire le lien avec le secteur privé.

Ainsi l'approche actuelle consiste-t-elle à décloisonner les secteurs civil (ANSSI) et militaire (DGA), et les domaines public et privé, chacun étant détenteur d'une partie des compétences et de la compréhension de la menace. Cette démarche structurée autour du pivot ANSSI-DGA a été rendue possible par la constitution d'une communauté réduite d'experts provenant de la sphère publique comme privée.

Ce dynamisme pourrait avoir un triple effet positif : réduire les risques, accroître le niveau de confiance et, *in fine*, structurer le marché. Mais quelles sont les possibilités de réussite d'une telle stratégie ? Au-delà de cette phase de dialogue, une analyse plus fine des actions en cours met en évidence les difficultés et les obstacles potentiels à une pleine réalisation de ce projet.

- *a) Définition d'une offre souveraine mais aussi commerciale.* Si l'État déclare avoir besoin de solutions nationales et pour cela institue des certifications françaises, les industriels réclament une clarification dans la définition de ce qui relève de l'intérêt national afin de pouvoir disposer d'une offre standardisée compatible avec celle d'autres industries européennes. Sur ce point, les intérêts des OIV (répondre à des standards communs sur les différents sites multinationaux) et ceux des fournisseurs (développer des solutions exportables) se rejoignent. Pour les fournisseurs, les certifications se traduisent par le développement de solutions adaptées à des standards nationaux pouvant limiter l'accès aux marchés extérieurs. Le marché français est trop restreint pour supporter une offre globale et compétitive vis-à-vis des géants américains dont le marché de taille suffisamment critique assure la pérennité[10].

- *b) PME-État-Grands Groupes.* Les PME sont le moteur de l'innovation dans le domaine cyber, qui se caractérise par des cycles courts, où les disruptions technologiques sont permanentes et où la réactivité est fondamentale : dès lors, la relation PME-Grands groupes est nécessaire à la construction d'un écosystème efficace[11]. En France,

10. Selon le rapport « U.S. Federal Cybersecurity Market Forecast 2015-2020 », le marché américain est estimé à 65Md$ pour la période 2015-2020.

11. Dan Senor et Saul Singer ont analysé ce dynamisme dans leur livre *Start-up Nation* : *The Story of Israel's Economic Miracle*, Twelve, 2009.

malgré les efforts récents de la sphère publique[12], le secteur privé se heurte à l'absence d'un cadre favorable aux investissements en capital. Malgré leur niveau d'innovation, les PME françaises sont peu valorisées, souvent sous-capitalisées et peinent à atteindre la taille critique pour s'ouvrir aux marchés étrangers. Après une première phase de croissance, de nombreuses PME éprouvent des difficultés à pérenniser leurs investissements : elles sont donc rachetées trop tôt par des grands groupes ou arrêtent d'investir. Une mauvaise lisibilité des programmes de financements étatiques, le contrôle des pouvoirs publics sur les investissements étrangers et une mauvaise gestion dans le relais entre PME (développement) et intégrateurs (industrialisation) expliquent les difficultés de l'attractivité du marché français.

Dans le but de favoriser l'émergence et le maintien de PME performantes, le *Plan Cyber* a proposé la création de fonds d'investissement spécialisés. Cependant, le montant des fonds (quelques millions d'euros), sa limitation à des ressources semi-publiques et focalisées sur la nationalité des entreprises concernées ont suscité des critiques[13]. Le *leitmotiv* est toujours le même : afin de disposer des fonds privés susceptibles d'investir de manière durable, le secteur privé doit s'émanciper d'une politique centrée sur la dimension nationale et sur les grands groupes.

Conclusion : À quand la crise d'adolescence du secteur privé ?

Alors que l'État régulateur espère doper la demande nationale, le marché de la cyber sécurité ne semble pas encore être l'*Eldorado* tant attendu. Les règles adoptées avec la LPM 2014-2019 sont contraignantes pour les OIV mais ne garantissent pour autant ni leur pleine applicabilité[14] ni une demande capable de satisfaire une filière nationale. La structuration de l'offre nationale est liée à l'action de l'État investisseur, tuteur et expor-

12. Parmi les initiatives : augmentation des financements DGA-RAPID à destination des PME (3M€/an), lancement du Pacte Défense PME en 2012.

13. Nous faisons référence au livre blanc rédigé par l'Association Française des Éditeurs de Logiciels et Solutions Internet, représentant 350 membres issus de grands groupes internationale, PME et Start up. Cyber-sécurité : Hisser les acteurs français au niveau de la compétition mondiale, juin 2014.

14. Le cas de l'utilisation de smartphones commerciaux par les ministres malgré une directive qui en proscrit l'utilisation illustre ces difficultés d'applicabilité. Gilbert Kallenborn, Les ministres peinent à respecter les règles élémentaires de sécurité informatique, 11/09/2013. http://www.01net.com/editorial/602914/les-ministres-peinent-a-respecter-les-regles-elementaires-de-securite-informatique/

tateur. Cependant l'État ne peut pas accompagner seul l'écosystème industriel afin de lui permettre d'atteindre une taille critique, notamment à l'échelle européenne. Au moment où la concurrence internationale capte les marchés émergents au moyen d'acquisitions milliardaires[15], organiser un écosystème à la hauteur demanderait trop de ressources.

Face à ce constat, nous pouvons ouvrir quelques pistes de réflexion pour aboutir à une situation gagnant-gagnant. En effet, la présence de grandes industries françaises (OIV et fournisseurs de sécurité) en Europe semble être un atout à exploiter. Les OIV sont à la recherche de solutions de cyber sécurité déployables dans tous leurs pays d'implantation ; les offreurs veulent être en mesure de proposer une offre à l'international donc la plus standardisée possible.

Imaginons un scénario qui prenne en considération cette dimension européenne des OIV et des fournisseurs de sécurité. Afin de développer des solutions pour des clients multidomestiques, les fournisseurs seront amenés à investir davantage en R&D et de ce fait à étendre leurs relations avec les PME innovantes. Par là même, les PME auront accès à un marché élargi ce qui leur permettra d'attirer plus d'investissements. Les OIV pourront de leur côté disposer d'une gamme de produits de confiance déployables sur l'ensemble de leurs sites.

Ce scénario pourrait constituer un élément de structuration de marché, alimentant la boucle d'amélioration continue entre pouvoirs publics et secteur privé.

NB : Les idées et les opinions exprimées dans cet article sont celles de l'auteur et ne reflètent pas nécessairement celles d'Airbus Defence and Space.

15. On peut citer ici l'acquisition de SourceFire par en 2013, évaluée à 2,7$ Mds et celle de Mandiant par FireEye en 2014 pour 1$ Md.

Vers une nouvelle lutte informatique pour l'armée de l'air

Monsieur Thierry Lemoine
Directeur de la Prospective et Product Line
Manager chez ThalesRaytheonSystems

Les systèmes d'information sont maintenant au cœur de tous les moyens techniques utilisés par l'armée de l'air : les senseurs, les effecteurs et les centres de commandement et de contrôle. La lutte informatique suit cette évolution et revêt des formes toujours plus efficaces. Il est primordial que les moyens nationaux progressent au même rythme.

La guerre électronique (GE)

Dès l'apparition de l'électronique dans les moyens de détection (radar) et de transmission (communications hertziennes), des équipements visant à perturber ou empêcher leur bon fonctionnement ont vu le jour.

Trois nouvelles disciplines ont alors fait leur apparition :

- L'exploitation des émissions de l'adversaire à des fins de renseignement. Il s'agit des ESM (*Electronic Support Measures*) qui permettent de détecter la présence de l'adversaire, de le localiser par goniométrie et d'obtenir des informations diverses par l'écoute des communications (COMINT : *Communication Intelligence*) et des émissions radars (ELINT : *Electronic Intelligence*).

- L'attaque électronique qui consiste à empêcher l'adversaire d'utiliser le spectre électromagnétique. Il s'agit pour l'essentiel de mesures de brouillage de ses émissions et de mesures de leurrage ou d'intrusion. Le brouillage rend inexploitable les émissions de l'adversaire ; le leurrage et l'intrusion lui donnent de fausses indications. L'ensemble de ces moyens est parfois appelé « contre-mesures électroniques » (ECM : *Electronic Counter Measures*).

- La protection électronique qui regroupe tous les dispositifs et toutes les procédures permettant de contrer les attaques électroniques et les moyens de renseignement électronique de l'adversaire. Ces mesures constituent les « contre contre-mesures électroniques » (ECCM : *Electronic Counter Counter Measures*).

La sécurité des systèmes d'information (SSI)

Avec l'apparition de l'informatique grand public, la sécurité des systèmes d'informations s'est focalisée sur la protection des informations : disponibilité, intégrité et respect de la confidentialité demeurent les maîtres mots en la matière.

Pour l'intégrité des données et le respect de la confidentialité, les moyens techniques utilisés se situent principalement à la périphérie des systèmes et sur les infrastructures de communication. Ils comprennent des équipements de cloisonnement des réseaux (diodes, passerelles…), de sécurisation des échanges (firewall, chiffrement,…), de détection de flux anormaux (sondes IDS : *Intrusion Detection System*), de durcissement contre les rayonnements entrants et sortants ou encore de recherche de logiciels malveillants (anti-virus).

L'amélioration de la disponibilité repose sur des architectures informatiques résilientes (il s'agit alors du domaine de la Sûreté de Fonctionnement). Elle consiste également à se protéger des attaques massives de type « déni de service » ou « force brute » en utilisant des équipements connectés en coupure sur les réseaux (IPS : *Intrusion Prevention System*).

Les mécanismes de protection sont construits sur une approche dans laquelle l'attaquant a généralement une longueur d'avance sur l'attaqué. La plupart des logiciels anti-virus par exemple ne peuvent détecter que des virus dont la signature est connue. Les logiciels malveillants qui exploitent des failles inconnues (« zéro-day ») sont indétectables par ces méthodes.

Les équipements de type IDS et IPS sont plus polyvalents puisqu'ils ne nécessitent pas de connaissance *a priori* des modes d'attaque. Ils sont cependant difficiles à paramétrer et ne constituent une réponse satisfaisante que dans certains cas d'attaque massive.

La lutte informatique « métier »

Dans le domaine cybernétique, la prise de conscience du risque est maintenant bien partagée et la révolution des moyens de lutte informatique, à la fois pour la Lutte Informatique Défensive (LID) et Offensive (LIO) est en cours.

Ainsi, la lutte informatique couvre aujourd'hui tout le spectre adressé par la guerre électronique :

- L'attaque cyber ne se limite pas aux attaques massives comparables au brouillage électromagnétique mais s'étend au leurrage et à l'intrusion destinés à fournir de fausses indications (LIO « attaques métier ») ;

- La protection cyber contre les attaques prend en compte cette nouvelle dimension et se complète de logiques de détection sophistiquées (LID « protection contre les attaques métier ») ;

- La protection cyber contre le vol d'informations est renforcée (DLP : *Data Loss Protection* étendue à l'analyse de contenu des informations échangées).

La démarche de Lutte Informatique « métier » va porter sur la détection des effets des attaques, les mécanismes de prévention et de protection n'ayant pas permis de les éviter. Elle va consister à imaginer tout ce qui permettrait de perturber le jugement de l'opérateur dans l'exercice de sa fonction.

Par exemple, si l'objectif de l'attaquant est de faire croire à un contrôleur aérien que des aéronefs se regroupent dans une zone, il va introduire des données fictives dans le système soit par leurrage électromagnétique, soit par intrusion sur les liaisons de données réelles, soit encore par le biais d'un logiciel malveillant. Quelles que soient les modalités de ce type d'attaque, une analyse de cohérence entre les différentes sources d'information va permettre de la détecter.

L'analyse va consister à définir des mécanismes d'attaque et à imaginer les moyens permettant de détecter les effets de ces attaques. Ces solutions présentent l'inconvénient de détecter les attaques lorsque les effets sont visibles. En revanche, elles ont l'avantage de couvrir tous les modes d'intrusion, y compris ceux qui n'ont jamais été observés auparavant. Elles permettent donc de rétablir une forme d'équilibre entre attaquant et attaqué.

Un large éventail de solutions complémentaires

Chacun des mécanismes couvre une partie de la menace et contribue à la sécurité de l'ensemble du système. Pour expliquer la complémentarité des différentes approches de lutte informatique défensive, on peut utiliser l'analogie avec la protection d'une succursale bancaire :

- mesures techniques « SSI » : protection physique des murs, portes et fenêtres ;
- firewall et équipement IPS : sas d'entrée surveillé par une caméra ;
- moyens de détection : caméra dans la salle des coffres ;
- moyens de surveillance du comportement des clients : c'est ici que l'on trouve les solutions « métier » les plus complètes :

- signaux forts : un client enjambe le comptoir, un client porte une cagoule…
- signaux faibles : un client entre pour la troisième fois dans la banque sur une période de 48 heures.

Pour un système de l'armée de l'air comme pour une banque, il est nécessaire d'analyser les menaces afin de déterminer la meilleure combinaison possible de solutions en maîtrisant les coûts et les risques résiduels.

De nouvelles perspectives pour l'armée de l'air

La lutte informatique est donc désormais pour l'armée de l'air comme pour beaucoup d'autres usagers du cyberespace une discipline à part entière, avec de solides expériences apportées par la GE et la SSI ainsi que de vastes domaines d'innovation.

L'identification des événements redoutés doit se faire en prenant en compte l'ensemble de la mission du système, en intégrant les senseurs, les effecteurs, les moyens de communication, les logiciels de présentation des informations et d'aide à la décision, jusqu'au décideur lui-même qui est la cible de l'attaque.

Pour la détection en temps réel des attaques sophistiquées, de nombreuses avancées doivent être faites dans le domaine de l'analyse des données présentées aux opérateurs, par exemple en vérifiant en permanence la cohérence des informations présentées avec celles reçues de tous les capteurs disponibles. Cette approche doit être complétée par une analyse continue du comportement des aéronefs.

Beaucoup de travaux restent également à faire dans le domaine de l'analyse à froid, sur de longues périodes de fonctionnement des systèmes. Toutes les analyses de cohérence des informations et de comportement des aéronefs peuvent s'effectuer sur des données enregistrées. Les données de supervision technique et opérationnelle interviennent dans ces analyses en utilisant par exemple des technologies de type « *big data* », il est souvent possible de repérer les éléments précurseurs d'une attaque.

Toutes ces avancées font appel à une compétence générale sur les différents aspects techniques de la Lutte Informatique mais aussi et surtout à une connaissance approfondie de la contribution de chaque information élémentaire à la prise de décision.

Guerre électronique et combat dans le cyber espace : quelle complémentarité ?

Lieutenant-colonel Samir Ouali-Djerbi
Chef du groupement aérien de l'informatique opérationnelle

La guerre électronique consiste à conserver la maîtrise du spectre électromagnétique à son profit tout en empêchant l'adversaire de faire de même. Offrant un panel d'actions offensives, défensives ou de surveillance, la guerre électronique est une action militaire à part entière et les opérations aériennes font depuis longtemps de la maîtrise de l'espace électromagnétique un enjeu crucial. Ce fut également la première forme de combat immatériel et technique moderne. Or ce n'est plus la seule depuis l'apparition du cyberespace en tant que nouveau milieu disposant d'un volet offensif[1] pour appuyer les opérations. Nouveau paradigme, immatériel et technique lui aussi, le cyberespace bouscule les concepts établis et, en particulier, questionne la place occupée par la guerre électronique aujourd'hui.

Le caractère englobant du cyberespace, sans préjuger des techniques de pointe employées pour transporter l'information, relie aujourd'hui des mondes identifiés jusque-là comme irrémédiablement distincts. Or la transformation technique de notre outil de combat a amené des changements majeurs. L'interpénétration et l'interconnexion entre les systèmes d'information et les systèmes d'armes est devenue un multiplicateur d'efficacité dans la planification, dans la conduite et dans l'exécution des opérations aériennes. Créant une synergie à une échelle jusque-là inégalée, le cyberespace a peu à peu émergé en tant que milieu propre qui dépasse le milieu physique sur lequel il repose. *De facto*, ce caractère englobant rendrait la dichotomie actuelle entre guerre électronique et combat dans le cyberespace aussi artificielle qu'obsolète. La guerre électronique serait-elle ainsi vouée à se dissoudre au sein de ce nouveau venu et à disparaître en tant que telle selon un schéma à l'allure darwinienne ?

1. LBDSN.

Ayant chacun la capacité de produire des effets sur des systèmes d'arme, la guerre électronique et le combat dans le cyberespace constituent des manœuvres complémentaires qui n'ont pas vocation à fusionner mais à mieux collaborer.

En effet, ces deux milieux, même s'ils sont apparentés, conservent des spécificités qui les distinguent fondamentalement. De plus, guerre électronique et combat dans le cyberespace sont également faiblement apparentés dans leurs modes d'action. En revanche, le combat dans le cyberespace constitue une réelle opportunité de prolonger les effets apportés par la guerre électronique et de diversifier ainsi les choix opérationnels offerts au chef militaire.

Des espace apparentés mais distincts

L'espace électromagnétique est avant tout un vecteur de propagation des ondes. Or cet espace est aujourd'hui pris d'assaut et encombré par un foisonnement de techniques de l'information. La confusion est aisément entretenue tant le cyberespace est lui aussi un milieu immatériel et faisant appel aux techniques de pointe mais, de surcroît, semblant pouvoir tout absorber.

Des différences fondamentales subsistent néanmoins. D'une part, ce nouvel espace ne se suffit pas d'une dimension physique pour exister. En effet, il ne devient un espace à part entière que par agrégation à cette première dimension, d'une dimension logique et d'une dimension sociale[2]. Le cyberespace est ainsi doté d'un caractère englobant qui le présente aux autres comme un méta-milieu ou milieu qui se superpose à d'autres milieux. Accessoirement, il peut utiliser l'espace électromagnétique en tant que couche physique, mais il serait faux de considérer que le cyberespace englobe totalement l'espace électromagnétique ou qu'il se substitue à lui.

Prenons une onde envoyée par un radar et réfléchie par un avion. Dans le cyberespace, l'émission de cette onde ne constitue pas une information en soi. Elle ne devient visible que lorsqu'elle est traitée en retour par un capteur et qu'elle devient ensuite une donnée. Pendant son trajet, elle peut être brouillée, redirigée ou manipulée, ce qui fausse inexorablement son

2. DIA 3.40, .109, P17.

traitement ultérieur sans qu'il y ait eu besoin d'intervenir sur le matériel devant effectuer le traitement final. Il existe donc bien un espace disjoint du cyberespace dans lequel se déplace l'onde qui n'a donné lieu à aucun traitement numérique. Le champ particulier de la guerre électronique intervient dans ce créneau précis en offrant une capacité d'altération du signal et au final du résultat du traitement sans avoir eu à altérer le fonctionnement du radar. C'est typiquement une opération irréalisable par une action de combat dans le cyberespace car tant que cette onde n'est pas traitée, elle n'existe pas en tant qu'information dans le champ du cyberespace. Pour aller plus loin, lorsqu'une onde est passée par la voie du traitement et qu'elle est devenue une information, elle disparaît à son tour du champ électromagnétique et il n'est plus possible de l'altérer avec des moyens de guerre électronique. En revanche, cette information s'est transformée et devient manipulable dans le cyberespace.

Il y a donc bien deux espaces immatériels et faisant appel aux techniques de pointe qui peuvent produire indépendamment des effets dans le même domaine d'application. En bref, s'ils sont apparentés par leurs objets, ils ne se confondent pas par leurs moyens. Mais lorsqu'on aborde la question des espaces, on aborde naturellement la question de la liberté de mouvement.

Un espace électromagnétique, des cyberespaces

Mener des actions de guerre électronique suppose une certaine facilité de déplacement entre l'espace adverse et l'espace ami ou suppose, du moins, une capacité à opérer sans contrainte depuis l'espace ami. Dans un milieu contesté, cette liberté de mouvement nécessite *a minima* l'acquisition et la conservation d'une supériorité de ce milieu. Or le cyberespace « opérationnel », différent d'Internet, est par nature discontinu, sans interconnexion entre belligérants. Première conséquence, en cas de confrontation c'est obligatoirement chez l'un ou chez l'autre des protagonistes que les opérations se dérouleront en impliquant nécessairement des difficultés de mouvement pour la partie offensive. Deuxième conséquence, il est impossible d'opérer à partir de son propre espace lorsque les espaces ne sont pas interconnectés. Finalement, il n'y a donc pas un cyberspace mais bien des cyberespaces à la différence de l'espace électromagnétique qui, lui, se présente toujours sous une forme unifiée. De cet état de fait découle sans doute la principale différence entre modes d'action propres à la guerre électronique et ceux propres au combat dans le cyberespace.

En reprenant la classification « guerre électronique », les missions caractérisant cette manœuvre sont : l'attaque électronique, la défense électronique et la surveillance électronique. Parmi ces missions, seule la posture défensive permet d'établir un rapprochement entre surveillance électronique et surveillance du cyberespace. Ayant pour objet commun de fournir une appréciation de situation, la mission de surveillance est ainsi transposable entre les deux milieux. Mais si cette action tout azimut a la particularité de rester très discrète dans le domaine électromagnétique, elle se révèle particulièrement visible dans le cyberespace. Typiquement, il sera nécessaire de disposer de capteurs, de moyens de stockage pour conserver les données puis de moyens de calculs pour les analyser. Contrairement à des moyens embarqués qui effectuent ces opérations par le biais d'une rupture de milieu, le cyberespace fournit lui-même les moyens de sa propre surveillance ce qui limite nécessairement le caractère discret de la manœuvre. Il devient alors possible de collecter des données sur une éventuelle attaque dont l'analyse nous informera, espérons-le, sur le mode opératoire et sur l'attaquant.

La discontinuité du cyberespace rend cette même manœuvre complètement contre-productive si elle est réalisée de la même manière chez l'adversaire. En effet, il n'est pas question d'écouter dans le vide et de risquer de donner l'alerte par une utilisation hors norme des ressources. Dès le franchissement de la cyber-FLOT[3], pardon pour le néologisme, il faut donc savoir rester discret et connaître *a priori* les mesures défensives mises en place pour éviter la détection. Ceci exclut immédiatement le parallèle précédent avec la surveillance électronique. Concrètement, tant que la liberté de mouvement n'est pas garantie de manière continue ou que le transfert inter-milieu est difficile, il va falloir chercher à obtenir dans la mesure du possible un effet ciblé et discret.

Ainsi, les modes d'action de la guerre électronique ne semblent pas pouvoir s'appliquer directement au combat dans le cyberespace et accentuent le fossé entre les deux disciplines. Ce n'est évidemment pas une fatalité. Cette distinction représente au contraire une opportunité de collaboration dans le cadre d'une action combinée car l'objet des manœuvres est potentiellement commun.

3. *Forward Line of Own Troops*.

Le combat dans le cyberespace comme prolongement de la guerre électronique

En particulier, en s'attachant au même objet, la diversité des manœuvres devrait permettre une diversité d'effets et constituer de ce fait une complémentarité aujourd'hui simplement imaginée au niveau tactique. Par ailleurs, les effets proposés par la seule guerre électronique sont loin de pouvoir modifier le comportement d'un système adverse dans la profondeur. La complémentarité représente donc théoriquement une piste crédible.

Reprenons notre exemple de radar. En l'espèce, si la guerre électronique s'attache à brouiller ou modifier un signal radar pour assurer une manœuvre d'aveuglement ou de déception de l'adversaire, le combat dans le cyberespace aura, quant à lui, plutôt vocation à empêcher ou à modifier le traitement du dit radar pour obtenir le même effet. Non seulement, un nouveau mode d'action serait offert au chef militaire mais il ouvrirait un champ des possibles sans commune mesure avec les outils de guerre électronique seuls.

Avec la capacité de modifier le comportement d'un système C2 adverse, il devient possible d'obtenir des effets allant bien au-delà du niveau tactique. On peut imaginer ralentir la boucle de décision opérative ou stratégique adverse, fausser les informations de conduite des opérations ou éventuellement en exfiltrer, toute opération constituant des effets dans la profondeur ne pouvant être atteints par une action sur le signal seul. Bien sûr, rien ne dit que ce serait simple mais ce n'est théoriquement plus hors de portée.

Ainsi il y a une complémentarité potentielle entre guerre électronique et combat dans le cyberespace en ce sens que le volet cyber poursuivrait la manœuvre « immatérielle et technologique » au-delà du capteur, jusqu'au cœur du système adverse et qu'il apporterait au chef militaire des modes d'actions supplémentaires pour l'appuyer dans ses opérations.

Nouvelle orientation du LBDSN, l'appui aux opérations par des capacités offensives cyber fait déjà partie des choix stratégiques français. Symbole d'une évolution majeure de nos concepts et de nos moyens, le combat dans le cyberespace n'a pourtant pas vocation à remplacer la guerre électronique mais bien à appuyer, à sa manière, les opérations.

En particulier, la guerre électronique restera un mode d'action privilégié, éprouvé et efficace pour agir dans le spectre électromagnétique tandis que le combat dans le cyberespace représentera autant de nouveaux modes d'actions supplémentaires et complémentaires mis à la disposition de la conduite des opérations. Enfin, si les pistes évoquées ci-dessus concernant les opérations de combat en profondeur dans le cyberespace se montraient pertinentes, elles pourraient alimenter une réflexion plus large sur le rôle du renseignement à l'appui de cette manœuvre en ouvrant, pourquoi pas, une nouvelle voie de renseignement plus technique et tactique qu'elle ne l'est aujourd'hui.

NB : Les idées et les opinions exprimées dans cet article sont celles de l'auteur et ne reflètent pas nécessairement celles de l'armée de l'air.

Cyber-défense et cyber-sécurité du milieu aérospatial : Quelles spécificités ? Quelles ambitions ?

Monsieur Pierre Barbaroux
Centre de recherche de l'armée de l'air

L'émergence de la question « cyber »

Depuis deux décennies, le monde a vu l'émergence de nouvelles formes organisationnelles réticulées et globalisées. En complément des infrastructures physiques traditionnelles, telles que les routes, les voies ferrées et les réseaux d'énergie, une variété d'infrastructures numériques s'est développée au point de devenir une composante vitale de l'économie mondialisée. Les réseaux de fibres optiques, les réseaux sans fil, les architectures de communication à larges bandes passantes supportent aujourd'hui l'essentiel des activités de production et de distribution de biens et de services. Cette révolution numérique s'est nourrie des progrès enregistrés dans le champ des technologies de l'information et de la communication (TIC). Mais si l'introduction des TIC a transformé les modalités d'interaction entre les personnes et entre les entreprises, améliorant de façon significative l'efficacité des processus de production et de coordination économiques, elle a également créé les conditions d'une vulnérabilité accrue des organisations publiques et privées. La cyber-sécurité des organisations dont les activités reposent sur les TIC est aujourd'hui un enjeu de société[1].

1. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la cyber-sécurité désigne *un « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles »* (ANSSI 2012, *« Défense et sécurité des systèmes d'information, Stratégie de la France »*, p. 21). Disponible en ligne à l'adresse suivante : http://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/

DR


SCAN COMPLETE
PASSWORD PROTEC
1234
567
89
10
HACKING DETECTED
01010101110000101010111
01010101110000101010111

DR

La multiplication des attaques informatiques sur les systèmes d'information et, plus largement, sur les infrastructures critiques[2] des organisations privées et publiques soulèvent le problème de la mise en œuvre des dispositifs de protection appropriés. Ces dispositifs sont d'autant plus difficiles à concevoir et à déployer que les opérations réalisées par ces infrastructures critiques reposent sur un contrôle distribué des ressources à travers un entrelacement de réseaux physiques et numérisés. Dès 2002, aux États-Unis, la protection des infrastructures critiques est reconnue comme un enjeu relevant de la sécurité nationale. Pionniers de la transformation des organisations militaires sur le modèle de l'organisation « réseau centrée »[3] (*Network Centric Warfare*, NCW), les États-Unis sont particulièrement sensibles à la question de la vulnérabilité dans le cyberespace. En France, le Livre blanc sur la défense et la sécurité nationale de 2013 rappelle justement que la cyber-défense est une priorité nationale. Le Pacte Défense Cyber lancé le 7 février 2014, identifie 50 actions organisées autours de six axes d'effort[4]. L'un des axes (axe 2) est dédié à la préparation de l'avenir à travers l'approfondissement des activités de recherche théorique et appliquée en soutien de la base industrielle. Dans ce cadre, l'action 18 propose de développer dans les écoles d'officiers, en partenariat avec les industriels, des chaires de cyber-défense. Les écoles de Saint-Cyr Coëtquidan ont créé la chaire de « Cyber-défense et Cyber-sécurité Saint-Cyr » dès juillet 2012, suivie par l'école Navale avec la chaire de « Cyber-défense des systèmes navals », officiellement lancée en novembre 2014. Aujourd'hui, l'École de l'air projette de lancer une chaire de recherche et d'enseignement dédiée au développement de la connaissance dans le champ de la cyber-défense et de la cyber-sécurité en milieu aérospatial.

2. Les infrastructures critiques désignent toutes ressources physiques et numériques des organisations privées et publiques des secteurs suivants : agriculture, eau, santé, services d'urgence, gouvernement, base industrielle de défense, information et télécommunication, énergie, transport, banque et finance, chimie et matériaux, navigation (Gorman 2005, p.7). Sean P. Gorman (2005), "*Networks, Security and Complexity. The role of Public Policy in Critical Infrastructure Protection*", Edward Elgar 2005.

3. Barbaroux, P., Godé-Sanchez, C., Mérindol, V., Versailles, D.W. (2005), « Gestion des connaissances et organisations de défense : une réflexion autours du *Network Centric Warfare* », Contrat de recherche coordonné par la Délégation aux Affaires Stratégiques (DAS), ministère de la Défense, 205 pages. Disponible (sur demande) en contactant l'auteur du présent article (coordonnées accessibles à l'adresse suivante : http://www.crea.air.defense.gouv.fr/index.php/les-equipes/organisations-de-defense-et-etudes-de-securite).

4. *Pacte Défense Cyber : 50 mesures pour changer d'échelle* (2013), document de la DICOD. Disponible en ligne à l'adresse suivante : http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber.

La création de trois chaires attachées aux trois écoles d'officiers françaises présuppose l'existence d'une spécificité du « milieu » en matière de recherche et d'enseignement portant sur le thème de la cyber-sécurité des infrastructures critiques et des organisations. Comment caractériser cette spécificité ?

Cyber-sécurité et milieu aérospatial : quelles spécificités ?

Objet complexe et multiforme, la cyber-sécurité des systèmes aérospatiaux soulève un double défi pour les chercheurs : d'une part, la définition même de l'objet pose question, d'autre part, la spécificité du milieu aérospatial appelle une clarification des dimensions pertinentes qui lui sont attachées. Dans la doctrine interarmées française, le cyberespace désigne le réseau maillé des infrastructures informatiques et de télécommunications, des systèmes de contrôle et des processeurs de données, d'informations et de connaissances utilisés par les armées. On serait tenté de limiter la spécificité de la cyber-sécurité des systèmes aérospatiaux aux seules propriétés *technologiques* des ressources physiques et numériques (vecteurs, effecteurs et des systèmes de commandement de conduite (C^2)) utilisés par l'armée de l'air. Or si les propriétés technologiques des infrastructures déployées par les armées répondent aux besoins des différentes armes, elles ne sauraient justifier *à elles seules* une formulation différenciée de la problématique « cyber » en fonction du milieu. On est alors tenté de rechercher les racines d'une spécificité « milieu » en s'intéressant aux propriétés fonctionnelles et opérationnelles des organisations concernées, en insistant justement sur les divergences en matière d'*emploi* des ressources, de missions et de caractéristiques physiques des espaces de conflits[5]. Une nouvelle fois, cette approche ne nous semble pas concluante. Certes, les missions sont différentes et les contraintes qui pèsent sur leur réalisation diffèrent d'une arme à l'autre, en termes de fluidité de l'environnement physique ou de vitesse de déplacement des vecteurs par exemples (Bonnemaison et Bossé (2014, p. 68), mais ces caractéristiques ne suffisent pas à affirmer l'existence d'une spécificité du milieu en matière de définition et d'analyse des principes attachés à la cyber-sécurité dans les organisations de défense. Les processus de cyber-défense, de cyber-protection ou de

5. Bonnemaison et Bossé (2014) distinguent cinq espaces de conflits (cyber, air, terre, mer, espace), chacun possédant des caractéristiques particulières. Aymeric Bonnemaison et Stéphane Bossé (2014), *Attention Cyber ! Vers le combat cyber-électronique*, Collection Cyberstratégie, Economica.

cyber-résilience des organisations et des infrastructures critiques sont de même nature, quel que soit le milieu[6]. Les logiques sous-jacentes ainsi que l'état final recherché sont identiques. Seuls les modes opératoires diffèrent.

Nous formulons donc la proposition suivante. Qu'il s'agisse de l'armée de terre, de la marine ou de l'armée de l'air, toute organisation dont les activités reposent sur l'interdépendance de ses architectures physiques et numériques s'expose à des formes de vulnérabilités. Dès lors, la question de la vulnérabilité des organisations dans le cyberespace et, son corollaire, celle de leur cyber-sécurité, dépend de trois facteurs[7] :

- Le degré de *dépendance à l'information* des personnes, des technologies de production et des structures décisionnelles qui composent ces organisations. Le degré de dépendance à l'information peut être fort ou faible en fonction des organisations et/ou des circonstances dans lesquelles elles opèrent.

- Le degré d'*intégration* ou de *couplage de leurs infrastructures physiques et numériques*. Les organisations peuvent être fortement ou faiblement couplées en fonction de l'interdépendance plus ou moins forte qui caractérise les relations entre les ressources physiques, humaines, techniques, matérielles et immatérielles qu'elles mobilisent et qu'elles coordonnent pour produire un type de bien ou de service.

- La *variété des dimensions* pertinentes attachées à *la représentation des phénomènes cybernétiques*. Ces dimensions concernent, d'une part, la représentation des menaces et de l'état des infrastructures physiques et numériques concernées et, d'autre part, la façon de les caractériser (notamment en termes de temporalité, de vitesse ou de durée, de volumes de données collectées, traitées et fusionnées, et de topologie de l'environnement).

---

6. Pour une définition des concepts doctrinaux de cyber-défense, de cyber-protection et de cyber-résilience, voir « *Les systèmes d'information et de communication en opérations* », CICDE, Doctrine interarmées, DIA-6_SIC-OPS(2014), N°147/DEF/CICDE/NP du 24 juin 2014, p. 70-71.

7. Pour une analyse de l'interdépendance des architectures physiques et cognitives des organisations « réseaux-centrées », voir Barbaroux, P. (2011), « A design-oriented approach to organizational change: a military case study », *Journal of Organizational Change Management*, 24(5), p. 626-639.

Ainsi, la spécificité de la « question cyber » dans le milieu aérospatial résulte, non pas des propriétés techniques attachées aux vecteurs, aux effecteurs, aux liaisons de données, aux systèmes d'information et aux structures de C² utilisés dans l'armée de l'air, mais de la forte dépendance à l'information des aviateurs (officiers et sous-officiers) qui opèrent ces vecteurs et ces effecteurs et qui coordonnent leurs actions grâce à des systèmes de C² numérisés et connectés. Par ailleurs, l'emploi de l'arme aérienne repose sur une architecture organisationnelle fortement couplée, traduisant une interdépendance forte entre ses composantes humaines, techniques et numériques. Enfin la représentation des menaces cybernétiques, de l'état de vulnérabilité (ou de protection) et de la capacité de résilience de l'organisation suppose nécessairement une topologie de l'environnement en trois dimensions, la dimension temporelle étant associées à des boucles décisionnelles courtes et à une vitesse élevée des vecteurs, et la dimension informationnelle à des flux hétérogènes et à des volumes de données importants (*big data*). Pris isolément, chaque facteur peut être associé à une organisation différente de l'armée de l'air. En revanche, la combinaison de ces facteurs apparaît spécifique, justifiant en retour le développement d'une approche « aérospatiale » des phénomènes cyber.

La chaire « Cyber » de l'école de l'air

L'école de l'air travaille sur le lancement de *sa* chaire de recherche et d'enseignement sur le thème « Cyber-sécurité et cyber-défense dans le milieu aérospatial ». Bénéficiant des compétences des chercheurs du Centre de recherche de l'armée de l'air (CReA) et du soutien de grands industriels du secteur aérospatial, cette chaire se singularise par un positionnement pluridisciplinaire et sur des axes d'efforts originaux. Dans la mesure où la cyber-sécurité des organisations résulte de la gestion, efficace et efficiente, des interactions entre une variété d'infrastructures physiques et numériques, son analyse requiert l'adoption d'une vision systémique des processus de cyber-protection, de cyber-défense et de cyber-résilience. Cette vision embrasse, en les articulant, les dimensions humaines, techniques, organisationnelles et institutionnelles attachées aux phénomènes cyber. Les travaux de recherche et les actions pédagogiques qui seront soutenues par la chaire mobiliseront ainsi différentes disciplines académiques. Plus particulièrement, les activités de la chaire s'inscriront dans le champ des sciences de l'ingénieur, des sciences cognitives et des sciences de l'organisation. Ensemble, ces champs disciplinaires permettent de traiter le sujet

de la cyber-sécurité des systèmes aérospatiaux dans sa complexité et dans sa diversité. Quatre axes d'effort en matière de recherche et d'enseignement ont dores-et-déjà été identifiés par le chef d'état-major de l'armée de l'air :

- Le premier axe, à dominante sciences de l'ingénieur, traite la question de l'adaptation au juste niveau des dispositifs de cyber-protection des systèmes d'information et de communication, mais également des processus « métier » associés. Il s'agit de travailler au développement des capacités de résilience des systèmes d'information et des organisations face à des *scenarii* d'attaque réalistes à fort ou moyen impact. L'objectif consiste notamment à identifier la vraisemblance et la criticité de la menace tout en évitant les surenchères en matière de cyber-protection des systèmes d'information.

- Le deuxième axe, orienté ingénierie des systèmes complexes et gestion de programmes, concerne la maîtrise des processus d'acquisition dans une perspective *total life-cycle management* (maîtrise des chaînes de valeur, vulnérabilité et sûreté des matériels et des équipements, souveraineté). L'intégration de la problématique de la cyber-sécurité dès la phase de conception et jusqu'à la phase de retrait des systèmes utilisés par les aviateurs, doit permettre de disposer d'une confiance raisonnable (et argumentée) dans l'intégrité des produits livrés et soutenus par les industriels. L'atteinte de cet objectif engage ainsi une adaptation des processus et des pratiques des acteurs qui participent de la gestion des programmes d'acquisition.

- Le troisième axe, orienté sciences de l'ingénieur et sciences cognitives, explore la question de la construction d'une conscience de la situation cyber-spatiale et de son intégration dans la situation aérienne générale. Quel concept et quelle représentation pour une approche opérationnelle de la cyber ? Comment intégrer cette situation avec une situation aérienne générale ?

- Le quatrième et dernier axe s'inscrit dans le champ des sciences cognitives appliquées à l'étude des processus de décision. Il aborde la question de l'entraînement et de la préparation des aviateurs, officiers et sous-officiers, dans une logique de conception des systèmes d'aide à la décision en environnement cyber. La question de la crédibilité

des informations remontées par les systèmes et de la représentation de la menace cyber par les décideurs est ici centrale. Comment intégrer ce domaine dans la prise de décision opérationnelle (pilote dans son avion, contrôleur devant sa console) ? Quelle mise en situation / quel entraînement pour conditionner de nouveaux réflexes ou pour orienter une meilleure prise en compte du risque ?

Plusieurs projets de thèses de doctorat, de séminaires et de publications académiques sont dores-et-déjà envisagés. Ces projets sont tous portés par une ambition : développer des connaissances et des savoirs théoriques et pratiques qui s'avèreront utiles pour les aviateurs et pour les industriels partenaires et, au-delà, pour la communauté de défense, acteur essentiel de la cyber-sécurité des infrastructures critiques en France.

Les enjeux de la formation aux métiers cyber

Giuseppe Leo
Directeur de l'école d'ingénieur Denis Diderot
Professeur à l'université Paris Diderot – Sorbonne Paris Cité
Laboratoire matériaux et phénomènes quantiques

La cyber-défense, la cyber-offensive, le développement des cyber-armes et la protection des systèmes contre les cyber-attaques, plus généralement la maîtrise du cyber-espace – toutes ces activités jouent un rôle croissant dans le domaine industriel et militaire. Bien que des entreprises spécialisées en sécurité informatique existent depuis une vingtaine d'années, de nouveaux enjeux et de nouveaux métiers apparaissent et demandent un nouveau type d'ingénieurs.

L'EIDD, l'école d'ingénieur de l'université Paris-Diderot, forme des ingénieurs à large spectre de connaissances qui maîtrisent l'usage des technologies jusqu'à l'implémentation dans des systèmes complexes. Notre conviction est que l'ingénieur dont on a besoin aujourd'hui se rapproche de plus en plus d'un architecte. Durant ces dernières décennies, un grand nombre d'industriels européens et américains ont déporté le centre de leurs activités vers les équipements, puis vers les systèmes. Cette nouvelle orientation stratégique a pour objectif de développer de nouveaux produits, à très forte valeur ajoutée, qui ont des fonctions généralement complexes, intégrant des systèmes et des équipements. Cette mutation, liée au déplacement de la valeur ajoutée, s'est corrélativement accompagnée d'un retrait des technologies « composants » lourdes du fait de la concurrence des pays asiatiques.

Pour l'EIDD – et en particulier pour ses spécialités « Architecture des systèmes physiques » et « Informatique : logiciel embarqué » – le domaine du cyber constitue un débouché très intéressant, et nous souhaitons que nos ingénieurs diplômés soient rapidement opérationnels dans ce domaine, et qu'ils puissent évoluer dans ce domaine dynamique en y apportant des innovations importantes.

En plus de sa dimension « systèmes », notre école d'ingénieur s'appuie sur les laboratoires d'une université au potentiel de recherche mondialement reconnu. Ce dernier renforce la cohérence du projet pédagogique de l'école, dont un des objectifs est de transmettre une démarche tournée vers l'innovation. C'est le stage de deuxième année, normalement orienté vers la découverte de la recherche en laboratoire, qui représente un réel développement et une mise en pratique de cette particularité de l'école. Les élèves doivent dans ce cadre faire preuve d'initiative, d'ingéniosité et surtout de créativité, favorisant ainsi l'émergence chez eux d'une réelle capacité d'innovation. Tout en intégrant dans ses programmes pédagogiques le référentiel de la Commission de Titres d'Ingénieur, l'EIDD implique dans l'élaboration et dans la réalisation de ses enseignements des chercheurs reconnus de niveau international et des ingénieurs des entreprises les plus innovantes. Cela nous permet de former des ingénieurs polyvalents pour diverses branches d'activité, dont le cyber.

En tant que chercheurs universitaires, nous avons essayé d'identifier certaines directions de recherche susceptibles d'avoir une influence cruciale sur le domaine de cyber. Un des thèmes de recherche développés au sein des laboratoires de Paris-Diderot qui illustrent au mieux la potentialité de l'EIDD par rapport aux besoins du domaine cyber sont les sources de photons intriqués intégrées sur puces semi conductrices (Laboratoire Matériaux et Phénomènes Quantiques). C'est un terrain – l'information quantique – qui est très connecté au domaine cyber car il repose sur l'utilisation des lois de la mécanique quantique pour améliorer l'acquisition, le traitement et la transmission de l'information par rapport aux systèmes classiques. Parallèlement aux recherches fondamentales utilisant des équipements de laboratoire complexes, l'existence de corrélations quantiques fortes, impossibles à reproduire de façon classique, est à la base d'un protocole de cryptographie quantique pour l'échange totalement sécurisé d'information : deux protagonistes, Alice et Bob, échangent une clé secrète grâce aux résultats de mesure obtenus par chacun sur un des deux photons d'une paire intriquée. La récupération d'information par un éventuel espion, quelle qu'en soit la mise en œuvre expérimentale, est une modification des conditions d'observation de la paire de photons : grâce au critère de Bell une telle modification peut être repérée par l'étude des corrélations quantiques, donc on aura réalisé un canal quantique incassable.

L'école d'ingénieur de l'université Paris-Diderot :
En haut : Les grands moulins.
En bas : La halle aux farines.

DR

DR

Compétences du cyber dans une école généraliste moderne

Une formation ouverte sur le cyber doit aborder de façon intégrée des aspects concernant la psychologie, l'informatique, la physique et l'électronique (PIPE). Par sa formation, un ingénieur diplômé de l'EIDD maîtrise déjà les trois derniers aspects, et notre conseil de perfectionnement réfléchit à l'introduction d'enseignements et de projets en psychologie au sein de notre tronc commun suivi pendant les trois années d'études. Cela valorise d'ailleurs un autre point de force de notre milieu universitaire pluridisciplinaire : l'UFR d'études psychanalytiques et, plus en général, le pôle de sciences humaines et sociales (SHS). On rappellera enfin que la diversité du vivier d'élèves ingénieurs, qui alimente l'école (prépas et universités dans divers domaines scientifiques) et qui passe par un programme intensif d'harmonisation en début de formation, facilite des parcours de formation contaminés par les SHS.

En effet, la problématique du cyberespace ne peut pas être comprise comme un simple problème limité à un programme informatique. Au contraire, un système contenant des nombreux éléments (ordinateurs, programmes, réseaux, contrôleurs, systèmes physiques, et bien sûr des agents humains) doit être considéré dans sa globalité. Cet aspect système rapproche le domaine cyber aux nouveaux produits industriels, au centre de la thématique de notre école. Ainsi l'approche système que nos élèves apprennent à maîtriser à travers des enseignements méthodologiques (analyse système) et techniques (systèmes et signaux, dimensionnement) est un atout majeur pour les activités cyber.

Pouvoir sortir de son champ disciplinaire, interagir avec des spécialistes d'autres domaines, utiliser son sens commun, rechercher l'information nécessaire, être créatif – ce sont les compétences précieuses dans le travail d'ingénieur et indispensables dans les nouveaux domaines complexes, tels que cyber. Il est difficile d'acquérir ce genre de compétences en cours, pour cette raison nous utilisons la pédagogie par projet. Ainsi nos élèves en équipe inter-spécialités travaillent sur un réel problème d'ingénierie qui ne ressemble pas aux sujets vus en cours, en particulier sur la conception d'un satellite étudiant IGOSAT.

Au cœur des compétences dans des études orientées cyber il y a l'automatique, puisque des nombreux sous-systèmes digitaux (le plus souvent

microcontrôleurs, mais aussi les ordinateurs) réalisent la tâche d'asservissement dans une boucle de rétroaction (contrôle de vitesse d'un véhicule, positionnement de têtes d'un disque). Un type d'attaque, pour l'instant rare mais très dangereux, vise ces sous-systèmes : soit en les saturant, soit en faussant leurs résultat, ce qui mène à des conséquences dramatique pour le système asservi (jusqu'à sa destruction). Dans le monde actuel, des nombreux systèmes physiques sont contrôlés par des logiciels qui s'exécutent sur des dispositifs cybernétiques. L'intrication entre les aspects physique (analogique) et cybernétique (digitale) augmente chaque année. Depuis peu les dispositifs cybernétiques se connectent aux réseaux (*Internet of things*). La communauté scientifique cherche des modèles et des techniques d'analyse adéquats pour ce type de systèmes hybrides ou cyber-physiques. Les techniques issues de cette recherche permettront entre autre de trouver des attaques informatiques contre des systèmes cyber-physiques susceptibles de détruire le matériel physique, mais aussi des moyens de contrer ces attaques. Pour envisager/contrer ce type d'attaque, l'ingénieur du domaine doit bien comprendre le fonctionnement du système asservi, et des notions de base de l'automatique (stabilité, rétroaction, fonction de transfert etc.). Dans notre école un tel enseignement est suivi déjà par tous les élèves. En perspective, il faudra introduire dans nos programmes les systèmes cyber-physiques et hybrides.

Les techniques pour le cyber : développement fondé sur modèle, vérification

Pour construire dans les délais raisonnables un système critique, satisfaisant les plus stricts critères de la sûreté et de la sécurité, il est indispensable d'utiliser des bonnes méthodes de développement. Une technique très prometteuse est le *model-based design*, où le concepteur construit et valide, dans un environnement de développement dédié, un modèle très précis de son système. Une fois le modèle terminé et validé, le design concret du système est généré automatiquement grâce à un logiciel certifié. Nos élèves découvrent cette approche moderne, sûre et efficace dans un cours (accompagné d'un projet) utilisant SCADE pour la programmation temps-réel critique, mais la méthode est d'applicabilité beaucoup plus large.

Pour assurer un excellent niveau de sûreté et de sécurité du logiciel, surtout critique, les bonnes technique et méthodologie de sa conception et de sa programmation ne suffisent pas, elles doivent se compléter par la vali-

dation du programme réalisé à travers des tests et des analyses encore plus poussées tels que vérification (*model-checking* ou preuve). Il s'agit en fait de démontrer que le programme est correct, sûr, sécurisé. Le test est un métier bien établi, tandis que la vérification reste une tâche difficile, accessible aux chercheurs et aux ingénieurs du haut niveau (souvent ingénieurs docteurs). Nos ingénieurs diplômés maîtrisent le test (ce qui est normal), mais en plus ils ont de très bonnes notions de la vérification (ce qui constitue une compétence rare). Nous sommes persuadés que dans les années à venir les techniques de la vérification seront plus largement utilisées dans le domaine cyber, et nos ingénieurs pourront les utiliser.

Il s'agit de modèles, algorithmes et outils logiciels qui permettent la détection automatique des vulnérabilités des programmes ou la garantie « mathématiquement » de l'absence de vulnérabilités. Ce type de techniques a fait ses preuves, par exemple pour la validation des protocoles cryptographiques et même pour la recherche de virus, et nous prévoyons son adoption large par l'industrie dans les années à venir.

Une variante intéressante de cette technique, *runtime verification*, permettrait la détection automatique des attaques en cours en observant le comportement du système.

Conclusion

Pour conclure, il est clair que l'homme est un acteur majeur du cyberespace, et que les sciences humaines (psychologie, sociologie, droit, économie) ont un rôle important à jouer dans le domaine cyber. Donc l'exemple de l'EIDD montre que le curriculum d'une école d'ingénieurs universitaire fortement connectée aux SHS et à des laboratoires de physique et d'informatique de pointe a de grandes potentialités par rapport aux besoins d'aujourd'hui et de demain dans les domaines cyber industriel et militaire. Nous veillons à améliorer cette adéquation à travers les stages, et à travers les embauches dans ce secteur et au travers des interactions avec ses acteurs. En perspective il faudra mieux estimer les besoins en ingénieurs cyber et définir un référentiel de compétences – ce travail ambitieux et passionnant demandera la collaboration des nombreux acteurs du cyber.

"Existe-t-il un marché des cyber-armes ?" *Pour une approche critique de la notion de cyber-arme*

Aspirant Yves Auffret
Officier enseignant chercheur au Centre de Recherche de l'Armée de l'air (CReA).

Dépourvue d'une quelconque définition légale[1], ou d'un consensus de la doctrine, la notion de « cyber-arme » est difficile à définir. Ayant émergé dans le langage commun en 2010 avec l'affaire Stuxnet[2], elle demeure marginale dans la réflexion sur les cyberconflits.

Cette difficulté est accrue si on considère que la littérature scientifique se réfère au cyberespace en tant qu'arme. Les auteurs ont par ailleurs tendance à distinguer entre cyberattaque et cyberdéfense[3]. Par analogie, il est alors possible d'associer alors l'attaque à la notion d'arme. Mais c'est bien dans la littérature anglo-saxonne que la notion de cyber-arme est le plus souvent employée. Les « *cyberweapons* » y sont alors présentées comme, des outils informatiques de nature diverse opposés aux classiques *malwares*. Même présentes et identifiées, les analyses sur ces objets restent relativement rares.

Une fois ces problèmes de définition dépassés, le principe de l'existence d'un marché spécifique des cyberarmes et de sa dynamique apparaît d'autant plus problématique. Les développements suivants reprendront dès

1. La Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale fait référence à l'idée de « cybermenace » et ses apports juridiques sont dépourvus de références à des outils particuliers.
2. Marco De Falco, *Stuxnet Facts Report - A Technical and Strategic Analysis*, NATO CCD COE Publications, 2012.
3. Cf. Daniel Ventre, *Cyberattaque et cyberdéfense*. Paris, Hermès Publishing, 2011.

lors les hypothèses développées par Thomas Rid et par Peter McBurney[4]. Leur approche offre un cadre général et elle permet de traiter l'ensemble des logiciels malveillants sans établir de distinction artificielle entre la cyber-arme et le *malware*. L'enjeu de cette question n'est pas où acheter un virus informatique, mais bel et bien de savoir si ce type de logiciel dispose de caractéristiques facilitant la construction d'un cadre d'échange propice à sa prolifération en tant que cyber-arme.

D'autre part, derrière l'idée d'un marché des cyber-armes surgit l'idée de la prolifération de celles-ci. Or la définition proposée par ces deux auteurs s'avère assez restrictive. Elle conduit à conclure que le nombre des cyber-armes telles que Stuxnet auront vocation de par leurs coûts de développement et de mise en œuvre à demeurer des exceptions plutôt qu'une tendance. Ce constat tend à questionner finalement l'avenir d'un marché dédié aux cyber-armes. En outre, la confrontation de cette définition avec le concept de marché, replacé dans le contexte général du cyberconflit, viendra dévoiler un certain nombre d'interrogations et de faiblesses de la notion même de cyber-arme. De nos jours, le « marché cyber » peut tout être, sauf un marché de la cyber-arme.

La cyber-arme : de quoi s'agit-il ?

L'expression cyber-arme peut recouvrir deux logiques complémentaires : D'une part, elle peut permettre d'envisager l'outil technique et le moyen déterminant le caractère cybernétique d'une attaque. D'autre part, elle aurait vocation à englober l'ensemble des moyens techniques, matériels et humains dédiés aux cyber-attaques. C'est ainsi que la cyber-arme incarne au choix un ensemble détaillé de logiciels précis, ou le champ cyber dans son ensemble. Dans le premier cas, adopter le point de vue de la cyber-arme revient à restreindre très fortement l'analyse. Dans le second cas, la notion de cyber-arme n'a tout simplement plus aucun intérêt.

Réfutant la notion de cyber-guerre qu'ils jugent inappropriée, Thomas Rid et Peter McBurney défendent l'idée d'une cyber-arme qui dépasse la seule composante cyber d'un conflit. Ce choix les conduit à la première solution , et à une conception très restrictive : le « *weaponised software* ». Si une arme désigne tout outil conçu pour menacer ou pour causer des

4. Thomas Rid & Peter McBurney, "Cyberweapons", *The RUSI Journal*, Volume 157, Issue 1, 2012.

dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants, alors la cyber-arme est simplement le code informatique utilisé pour des objectifs identiques[5].

Le niveau technique et donc le niveau de puissance de ces « cyber-armes » fournit alors un critère pour une première typologie :

- les armes dites à faible potentiel, génériques, peu discrètes et d'acquisition facile, faciles à mettre en place et à contrer[6] ;
- les armes à fort potentiel, spécifiques, nécessitant des investissements lourds[7] ;
- les armes combinant des caractéristiques de ces deux catégories[8].

Dans la conception de ces armes, l'accroissement du potentiel destructeur induit deux efforts : d'une part, au niveau des ressources (Temps/Recherche/Investissement) ; d'autre part, au niveau du ciblage. Ces efforts participent à la réduction du nombre des dommages collatéraux potentiels de l'arme, réduisant également son pouvoir de coercition et de menace. Tout en sachant qu'une cyber-arme dispose d'une durée limitée pour agir avant que les défenses n'évoluent suffisamment pour la contrer.

L'exploitation des bugs et l'espionnage par l'intermédiaires des chevaux de Troie ne sont pas regardées comme des cyber-armes car moins dangereux[9] ; ils appelleraient des sanctions juridiques différentes.

Le coût prohibitif des cyber-armes à fort potentiel entraîne la diminution de leur risque de prolifération, comme n'importe quel autre sys-

5. "*For the purposes of this article, a cyber-weapon is seen as a subset of weapons more generally : as computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings*." *Thomas Rid & Peter McBurney*, « *Cyberweapons* », ibid.

6. Les logiciels permettant les attaques de déni de service (DDoS) par exemple ; les attaques de 2007 en Estonie sont classées dans cette catégorie.

7. Notamment Stuxnet, Flame ou Gauss.

8. Certaines intrusions particulières, par exemple avec le virus I love you.

9. L'utilisation d'un mail piégé à l'aide d'un cheval de Troie ne serait donc pas considérée comme relevant d'une cyber-arme. *A fortiori*, l'ingénierie sociale et plus généralement les outils d'acquisition d'informations semblent ici exclus des utilisations premières de la cyber-arme. Le domaine d'une cyber-arme, du point de vue de la guerre de l'information, se limiterait paradoxalement à la dégradation des systèmes avec une variation dans le potentiel de dégâts en fonction du type d'arme en cause.

tème d'arme. De plus en raison du degré de précision (penser pour une cible identifiée voire unique), la cyber-arme dans son acception la plus restrictive devient difficilement « exportable ». De manière connexe, ceci tend à remettre en cause le postulat de la prééminence de l'attaque sur la défense dans le champ cyber. La défense est davantage présentée sous un jour favorable en raison de son coût moindre, donc de sa plus grande vitesse d'évolution.

Construite notamment sur le constat d'une absence de définition dans la doctrine américaine[10], cette approche s'avère intéressante pour différentes raisons.

Premièrement, face à une définition politisée et discutée de ce qu'est et de ce que doit être le cyberespace, il faut ici saluer l'effort qui consiste à vouloir réintégrer une forme de granularité technologique dans le raisonnement. Si on doit garder une vision normative de la définition proposée ici, il faut cependant considérer que cette granularité se construit en opposition avec l'idée de neutralité technologique qui conditionne la viabilité et la durabilité d'une norme par rapport aux évolutions de l'état de la technique. Si la notion de cyber-arme reste assez floue pour permettre une certaine interopérabilité dans la désignation, il faut mettre en avant sa spécificité.

Deuxièmement, en voulant s'affranchir de la cyber-guerre, Thomas Rid et Peter McBurney excluent de leur paradigme la question de l'acteur. On retrouve bien l'intention de nuire et la perception de la menace comme conditions de l'action ou encore l'effet psychologique sur la cible. Toutefois, ce sont ici des considérations qui semblent secondaires pour les auteurs. La question de la cyber-arme ne se pose pas en vertu de l'identité ou de la nature des acteurs. Corolairement, la cyber-arme n'est donc pas obligatoirement régalienne.

Enfin, on assiste à un paradoxe : d'un côté ce renoncement à l'acteur s'inscrit théoriquement dans les conceptions stratégiques qui font de la multiplication du nombre d'attaques un produit de la densification

10. « *Remarkably, even the US Department of Defense Dictionary of Military and Associated Terms, an authoritative 550-page compendium that defines anything from abort to Zulu time, has no definition for weapon, let alone for cyber-weapon* » Thomas Rid & Peter McBurney, op-cit.

DR

DR

et de la complexification des réseaux. De l'autre côté, le recours à une cyber-arme ne peut s'inscrire que dans un intérêt bien précis. Il s'agit de l'idée d'une émergence de cyber-attaques raisonnées et pensées comme une réalité dont les objectifs peuvent être économiques, idéologiques et/ou militaires. Les intérêts conditionnent ainsi paradoxalement la cyber-arme indépendamment (semble-t-il) de leurs propriétaires réduits à des propensions marginales.

Ainsi, adopter une approche restrictive de la cyber-arme conduit à décrire un ensemble précis et déterminé de logiciels malveillants. Cependant, cet ensemble qui n'est pas neutre est incapable de traduire la cyberattaque dans toute sa complexité et dans sa variété, et ignore les questions de l'exploitation des failles, du mécanisme de défense et des acteurs. De fait, la cyber-arme est un point de vue inefficace qui conduira à exclure la prise en compte de l'intégralité des marchés les plus fleurissants du secteur, notamment le marché global des technologies de sécurité informatique ou encore le marché des failles et de leurs codes d'exploitation.

Un marché des cyber-armes au prix de nombreuses exclusions.

Cet effort de définition est parmi les plus aboutis en ce qui concerne la cyber-arme. Toutefois, il ne peut être regardé comme suffisant pour répondre à la question de savoir s'il existe un marché des cyber-armes. Plus encore, il s'avère un obstacle à cette démarche. Car si le marché se conçoit comme un cadre de rencontre entre l'offre et la demande, plusieurs interrogations demeurent en suspens quand à l'intérêt et à l'organisation d'une telle structure pour les cyber-armes ainsi désignées. La grande question que l'on peut se poser est celle du secteur à considérer et de ses subdivisions (à inclure ou à exclure). Enfin, le caractère transparent de l'acteur dans la définition de la cyber-arme ne permettra pas de trancher la question du statut légal par essence de ce type de marché. Indépendamment de la confidentialité intuitive autour de ces échanges, il est impossible de savoir si nous avons à faire à un marché gris ou noir, sans se plonger dans la question de l'acteur qui devra faire l'objet de développements à part...

Pris dans l'idée d'une arme à faible potentiel, le marché est déjà existant depuis 1986/87 puisqu'il s'agit du marché des virus (et des antivirus) ; lequel est connu de tous et facilement accessible, y compris pour n'importe quel particulier. Notre idée du marché des cyber-armes passerait donc

nécessairement par le marché du virus informatique à l'exclusion des chevaux de Troie, des spywares ainsi que des virus « zombificateurs » qui sont hors de la définition. Il faut également exclure les équipements et les logiciels destinées à la protection des systèmes d'information ; nous touchons ici également, une des limites de cette définition de la cyber-arme ; elle ne prend pas en compte les moyens de se prémunir des attaques[11].

Il nous faut exclure également les logiciels de chiffrement ainsi que des outils qui permettent de se dissimuler, au-delà du marché des logiciels viraux et des technologies de sécurité entendues globalement. Comme le bug n'est pas regardé comme une cyber-arme, un autre domaine est à exclure malgré son caractère lucratif : le marché des vulnérabilités et de leurs codes d'exploitation[12]. Des failles, comme par exemple Heartbleed, ne pourraient être incluses dans le marché de la cyber-arme. La réponse à cette première interrogation tient donc dans l'idée que si l'arme à faible potentiel peut s'inscrire dans le marché des technologies de sécurité, elle ne peut caractériser l'essence d'un marché spécifique des cyber-armes à elle seule à cause des nombreuses exclusions opérées. Par ailleurs, la question initiale perd ainsi totalement de son intérêt. Le phénomène cyber ne serait porteur d'aucune originalité.

Pour répondre à cette question de l'existence d'un marché des cyber-armes de manière utile, il faudrait que la définition permette de dégager un nouveau marché uniquement dédié aux armes à fort potentiel. Et si un marché des cyber-armes existe avec toutes les restrictions évoquées, d'autres interrogations émergent notamment sur l'objet et sur le moment de l'échange. L'échange entre les acteurs de ce marché intervient-il au moment de la création de la cyber-arme ou de sa mise en œuvre ? Autrement dit, le marché de la cyber-arme est-il un marché de services ou un marché de biens ? Dans le premier cas, l'acheteur cherche des compétences afin de bâtir une cyber-arme qui serve ses objectifs tandis que le vendeur dispose de ces compétences. Dans le second cas, l'acheteur recherche une solution « clef-en-main » tandis que le vendeur propose des cyber-armes prêtes à l'emploi. Ce second cas correspondrait davantage au logiques d'une arme à faible po-

11. Le marché global des technologies de sécurité informatique était de 14,8 milliards d'euros en 2013,

12. Le marché des failles inconnues et des codes permettant de les exploiter (0-day exploit) produit environ 85 failles inconnues par jour, une faille Windows inédite pourrait ainsi se vendre jusqu'à 250.000 $ voir notamment : Pierluigi Paganini, « Zero-Day Exploits in the Dark », *Infosec Institute*, 21 avril 2015. http://resources.infosecinstitute.com/zero-day-exploits-in-the-dark/

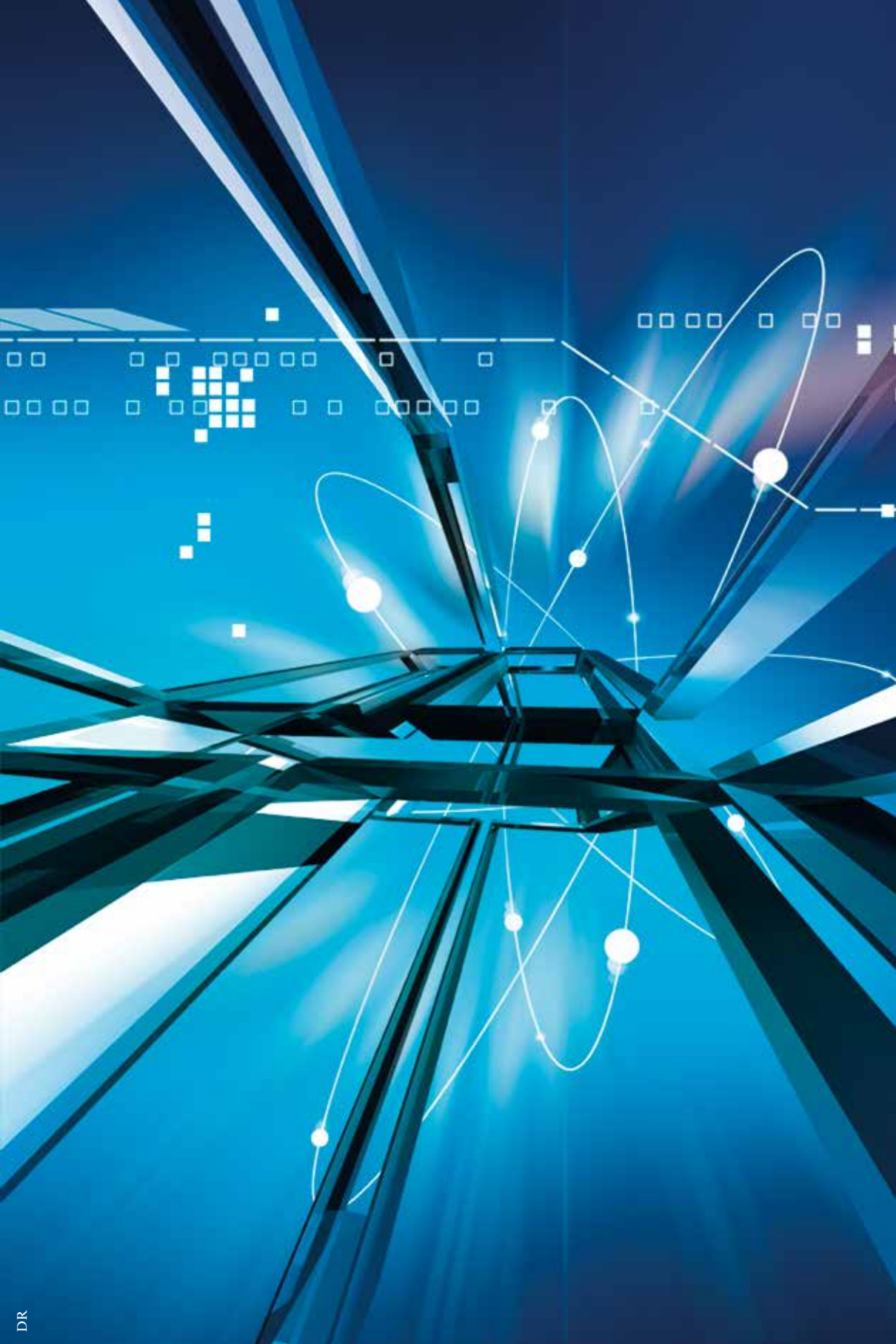
tentiel. Autrement-dit, compte-tenu des contraintes d'élaboration de l'arme, l'hypothèse d'un marché uniquement dédié aux cyber-armes à fort potentiel ne peut être qu'un cadre d'échange pour les compétences utiles ou/et des services entre un vendeur dépositaire de savoir-faire et un acheteur animé par un intérêt extrêmement précis (au sens qu'il ne peut trouver satisfaction sur les autres marchés du secteur). Le marché du travail existe bel et bien dans le champ cyber, seulement ce n'est pas un marché spécifiquement dédié à la conception de cyber-armes à haut potentiel...

Conclusion

Le marché de la cyber-arme ne peut ainsi exister sans englober le marché cyber dans son ensemble. Le risque de prolifération de la cyber-arme est limité par les importantes contraintes qu'elle impose à son utilisateur en matière de conception et d'emploi. En l'effet, les cyber-armes à faible potentiel disposent de marchés déjà connus. La question de l'existence d'un marché de cyber-arme trouve alors un intérêt inexistant. L'hypothèse d'un marché des cyber-armes à haut potentiel fondé sur l'échange de savoir faire destiné à la construction de ces mêmes armes ne peut se réaliser qu'au travers d'un ensemble plus vaste qui n'est pas spécifique en incluant des produits, et des services qui ne peuvent être regardés comme des cyber-armes.

Ainsi, bien qu'elle ne soit pas sans intérêt, la notion de cyber-arme ne peut servir à justifier de l'existence d'un seul et unique marché dédié. La prise en compte de la définition de la cyber-arme, ainsi que des exclusions auxquelles elle conduit, amène par ailleurs à replacer le risque par rapport aux autres risques du secteur. Car, il existe enfin plusieurs marchés sur lesquels ne s'échangent pas de cyber-armes mais des produits qui peuvent s'avérer tout aussi dangereux, voire causer bien plus de dommages (vulnérabilités, trojans...). Cette question conduit donc à nuancer le caractère terrifiant d'une cyber-arme à haut potentiel.

Au-delà de la question du marché, penser la question du risque au travers de la notion de cyber-arme est de nature à induire une erreur dans l'évaluation de ce dernier. Cette hypothèse pose tout simplement la question de l'utilité de cette notion. Une défense efficace ne peut se concevoir sous l'angle de la cyber-arme.



DR

La Cyberdéfense aux États-Unis : entre enjeux stratégiques et compétitions institutionnelles

Lieutenant Tony Morin
Officier doctorant au Centre d'études stratégiques aérospatiales

Le Pentagone et le cyberespace : une place centrale, acquise difficilement

La nouvelle stratégie du Pentagone dans le cyberespace : réaffirmer le rôle de des forces armées au sein de la Défense

Le 23 avril 2015, le secrétaire à la Défense américain Ashton Carter a dévoilé la nouvelle stratégie du Pentagone pour le Cyberespace. Le dernier document officiel relatif à ce sujet datait de mai 2011, mais n'a été rendu public qu'en 2013. Aux États-Unis, les opérations dans le cyberspace[1] sont en principe assurées par un commandement interarmées : l'*US Cyber Command* (*CYBERCOM*). Il assure principalement trois grandes missions : la défense de l'intégralité du réseau informatique du *Department of Defense* (*DoD*), la défense du territoire national contre toute attaque cyber et, sous la direction du Président ou du Secrétaire d'État à la Défense, le soutien aux opérations cyber conduites par d'autres entités ou agences. Le document ne propose pas de nouvelle définition pour le cyberespace, qui reste donc celle établie par la version précédente : « [cyberspace is] *a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*[2]. » Le Pentagone considère le cyberespace comme un milieu au même titre que la terre, la mer l'air et l'espace.

1. Le terme de « cyberdéfense » n'existe pas dans la documentation officielle américaine.
2. *Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms.*

Contrairement à la version précédente, cette dernière a été publiée immédiatement après son annonce. Cette démarche répond à une volonté de clarifier les missions relatives au cyberespace, dont le périmètre s'avère généralement flou. Toutefois, ce document est en grande partie tourné vers l'extérieur, que ce soit vers les partenaires industriels et vers les alliés, mais également vers les adversaires. Le vocabulaire sur la dichotomie offensive/défensive a quasiment disparu pour être remplacé par un principe de dissuasion (*Cyber Deterrence*), une initiative faisant suite à l'attaque informatique massive subie par Sony en décembre 2014 et dont le document désigne la Corée du Nord comme responsable. Bien que les contours de ce principe de dissuasion restent flous, il s'agit surtout de « connecter » les actions dans le cyberespace avec des manœuvres plus classiques ; à une attaque cyber, les États-Unis s'autorisent ainsi à répondre par des mesures diplomatiques, militaires, économique, etc.

De manière générale, le Pentagone adopte une stratégie déclaratoire spécifique au cyberespace en appelant d'un côté les alliés des Américains à une plus forte collaboration et de l'autre défini un ensemble de mesures de répression contre ses adversaires[3].

L'ouverture au monde civil constitue sans doute le volet le plus important et le plus concret de ce document. Le Pentagone met en place une vaste politique de partenariat avec les grands acteurs de l'informatique et du cyberespace. Le fait qu'Ashton Carter ait présenté cette nouvelle politique à la Silicon Valley, creuset de l'industrie numérique, symbolise cette volonté. Sa présentation s'insérait ainsi dans un ensemble de rencontres, notamment avec de hauts responsables de *Facebook*. Dans cette logique de partenariats, la politique de recrutement du *CYBERCOM* (et de ses structures subordonnées) s'appuie en grande partie sur une force de réservistes. L'objectif est de disposer d'une force de 6 000 personnes (militaires et réservistes) à l'horizon 2016. *In* fine, il s'agit de mettre en place une *Cyber Mission Force*, constituée de 133 équipes, réparties selon les missions du *CYBERCOM*. Au-delà, l'objectif est de disposer d'un vivier de spécialistes cyber déployable rapidement pour soutenir toute agence gouvernementale en formulant la demande. Toutefois, la

3. À plusieurs reprises, le document désigne explicitement la Chine, la Russie, la Corée du Nord et l'Iran comme les principaux États susceptible de menacer les États-Unis d'une attaque cyber.

faible attractivité du secteur militaire par rapport au secteur civil et la forte concurrence entre les branches du *CYBERCOM*[4] pour capter ces ressources humaines[5] risquent de rendre cet objectif difficilement atteignable. À l'heure actuelle, le *CYBERCOM* compte environ 2 500 personnes. En outre, son budget a été quasi doublé entre 2014 et 2015 en passant de 190 millions de dollars à 364 millions.

De manière générale, ce document et cette nouvelle politique peuvent s'interpréter comme une volonté du Pentagone de réaffirmer son rôle dans le cyberespace aux États-Unis. Ce secteur apparait en effet comme l'un des plus stratégiques de la Défense[6]. Néanmoins, la nature fondamentalement transversale de ce « milieu » rend les zones de responsabilité et les prérogatives de chaque service difficiles à définir. Par cette publication, le *DoD* cherche d'une part à réaffirmer son leadership sur les différentes branches des armées et d'autre part à devenir un interlocuteur incontournable pour les autres agences gouvernementales. Cette démarche atteste de la complexité de l'institutionnalisation de la cyberdéfense aux États-Unis, qui a été l'objet de plusieurs tentatives.

La création d'un commandement cyber unifié : un processus disjoint

Le *Cyber Command* n'est pas la première organisation à tenter d'institutionnaliser la fonction cyber au Pentagone. En 1998, le *Joint Task Force–Computer Network Defense* (JTF-CND), fort de 24 personnes[7], est créé. Cependant, en 2004, il est écartelé entre la *National Security Agency* et la *Defense Information Systems Agency* (qui dépend du DoD). Le *Cyber Command* a également absorbé plusieurs services déjà existants : le *Joint Task Force for Global Network Operations* (JTF-GNO)

4. À l'instar des forces armées américaines, le CYBERCOM est divisé en branches par armée : Air Force Cyber, Army Cyber Command, Fleet Cyber Command, Marine Corp Cyberspace Command.

5. John Edwards and Eve Keiser, Cyber commands coordinate strategies, C4ISR & Networks, 4 mar 2015, http://www.c4isrnet.com/story/military-tech/cyber/2015/03/04/cyber-commands-coordinate-strategies/24373109/

6. Un sondage mené auprès de hauts responsables de la Défense et de membres du congrès révèle que le Cyber est perçu par ces derniers comme la principale menace pour les États-Unis, devant le terrorisme. http://www.nationaljournal.com/defense/defense-leaders-say-cyber-is-top-terror-threat-20140106

7. Jason Healey, *The Future of U.S. Cyber Command*, The National Interest, 2013, http://nationalinterest.org/commentary/the-future-us-cyber-command-8688

Réunion du 13 mars 2015, au quartier général de la *National Security Agency,* sur l'actualité de la cybersécurité.


© Petty Officer 2nd Class Sean Hurt

et le J*oint Functional Component Command for Network Warfare* (JFCC-NW), tous deux dépendant du *Strategic Command*. Ces « aller-retour » organisationnels peuvent s'expliquer d'une part du fait de la difficulté à définir les missions et les responsabilités en matière d'opération cyber et d'autre part du fait des rivalités et des tractations internes que peuvent susciter la mise en place d'une telle structure. En outre, ces changements organisationnels ont rendu difficile le processus de retour d'expérience, d'identification de spécialistes et plus largement, d'une vraie mémoire des opérations cyber.

Finalement en juin 2009, le secrétaire à la Défense décide de mettre en place un nouveau sous-commandement unifié (dépendant du *Strategic Command*) chargé du cyberespace. Le nouveau *United States Cyber Command* (*CYBERCOM*) est opérationnel le 31 octobre 2010. Il dépend du Strategic Command et se compose d'une branche par armée : *US Air Force* (*Air Force Cyber Command*), *US Army* (*Army Cyber Command*), *US Navy* (*Fleet Cyber Command*) et *US Marines* (*Marine Corps Cyberspace Command*). Son chef, l'amiral Michael Rogers, est également le directeur de la NSA. Cette association a pour but de faire monter rapidement en puissance la structure militaire qui, à terme, pourrait être distinctement séparée. En parallèle de cette structure, chaque commandement interarmées régional (*CENTCOM*, *PACOM*, etc.) dispose de sa propre unité opérationnelle cyber, qui ne dépend donc pas directement du *Cyber Command*. La création d'un commandement unifié ne résout donc pas les problèmes d'organisation au sein de la communauté de la cyberdéfense. Cet éclatement des structures qui perdure rend la définition des missions et le contour des périmètres de responsabilité toujours complexes à évaluer. Par exemple, *AFCYBER* dépend du *CYBERCOM*, qui est rattaché à l'US Strategic Command, mais la 24th Air Force, qui arme l'*AFCYBER*, dépend de l'Air Force Space Command, également rattaché au Strategic Command, mais sans lien avec le *CYBERCOM*.

Cette complexité semble indiquer que les forces centrifuges au sein du Pentagone restent très vivaces sur ce sujet. En effet, les initiatives visant à créer une structure cyber centralisée n'ont pas eu toutes pour origine l'administration centrale du Pentagone et la plus concrète d'entre-elles fut probablement celle de l'*US Air Force*, dans la deuxième partie des années 2000.

Le projet trop ambitieux de l'*US Air Force*

L'USAF en pointe dans le cyberespace

En 2003, la Maison blanche publie une feuille de route intitulée « *The National Strategy to Secure Cyberspace* », qui prévoit toute une série d'actions destinées à protéger les intérêts américains en lien avec le cyberespace. Il s'agit du premier document institutionnel américain consacré au sujet. Ces mesures relèvent essentiellement du *Department of Homeland Security*, créé suite aux attentats du 11 septembre 2001. Néanmoins, l'un des points du document appelle à améliorer la coordination interservices dans ce domaine en faisant appel à l'ensemble de l'*US national security community*[8]. À la fin de l'année 2005, l'*US Air Force (USAF)* s'empare du sujet en publiant une nouvelle devise :

"To deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in air, space ***and cyberspace***[9]*."*

La majorité des historiens militaires s'accordent sur le fait que l'*USAF*, à la suite de la première guerre du Golfe, fût la principale armée à bénéficier de ce que l'on appelle la *Revolution in Military Affairs*. Cela s'est traduit par la mise en place de programme et l'acquisition de matériels reposant en grande partie sur les nouvelles technologies de l'information et de la communication (les satellites, les systèmes de commandement et de contrôle, etc.). Elle est en outre la première branche à se doter d'un *Information Warfare Center* en 1993. En se fondant sur cette base technologique, l'*USAF* s'expose mécaniquement à de nouvelles vulnérabilités qui portent sur ses moyens de communication. Elle considère ainsi le cyberespace comme un domaine hautement sensible pour son activité et pour sa légitimité. Son objectif est double : il s'agit autant de se protéger militairement contre les agressions ennemies que de défendre ses intérêts au sein du *Department of Defense*.

En effet, à la même époque, d'autres services tels que l'*US Navy*, l'*US Army* et la *NSA* développent aussi des projets dans le domaine du cybe-

8. Un terme qui désigne donc plusieurs services et ministères.

9. Air Force Cyber Command AFCYBER (P), http://www.globalsecurity.org/military/agency/usaf/afcyber.htm.

respace. Ces initiatives sont véritablement perçues comme menaçantes par l'*USAF*, qui cultive toujours un certain complexe existentiel vis-à-vis des autres composantes. Ainsi, la très rapide dissémination des drones aériens au début des années 2000, qu'elle perd au détriment d'autres services, la conduit à adopter un réflexe très conservateur et d'appropriation à l'égard du cyberespace afin de préserver ses capacités dans ce milieu.

Lors d'une conférence de presse en décembre 2006, le secrétaire à l'*Air Force* Michael Wynne annonce la création du l'*US Air Force Cyber Command* (*AFCYBER*). Il doit être mis en œuvre par la *8th Air Force.* Michael Wynne décrit ses missions de la manière suivante :

"The aim was to develop a major command that stands alongside Air Force Space Command and Air Combat Command as the provider of forces that the President, combatant commanders and the American people can rely on for preserving the freedom of access and commerce, in air, space and now cyberspace[10]*."*

La mise en place chaotique d'un projet aux contours mal définis

Les prétentions de l'*AFCYBER* sont donc vastes et ne relèvent pas que du domaine de l'emploi de la puissance aérospatiale. Il s'agit d'un projet aux ambitions stratégiques puisqu'il prétend traiter de l'ensemble du cyberespace et se pose comme référence directe auprès du président des États-Unis. Avec *AFCYBER*, l'*USAF* tente de reproduire un nouveau *Strategic Air Command* (l'insigne de l'*AFCYBER* est d'ailleurs identique à celle du *SAC*) avec tout ce que cela représente en terme d'influence institutionnelle. La grammaire qu'elle développe autour de cette nouvelle structure est à ce titre révélatrice de cette volonté. L'*USAF* développe un discours à la fois très alarmiste et très volontariste. Dans ses publications officielles[11], elle insiste sur l'impact du cyberespace sur la sécurité nationale des États-Unis, son influence, voire même sa politique commerciale. Ainsi, le cyberespace est présenté comme concomitant des intérêts vitaux de la nation. De ce fait, le champ d'action de l'*AFCYBER* est voulu comme tout aussi large et le vocabulaire employé est le même que celui que l'on retrouve

10. Todd Lopez, SSgt, USAF, "8th Air Force to become new cyber command". Air Force Link. United States Air Force, 3 November 2006.

11. Voire entre autre : Air Force Cyber Command : Strategic Vision, Air Force. Air Force Cyber Command, Barksdale AFB, LA, 2008.

pour ses missions classiques (on y parle de dissuasion, de boucle OODA et même de forces expéditionnaires cyber). À l'image du domaine aérospatial, l'*USAF* évoque la notion de « *cyber dominance* », ce qui illustre clairement ses ambitions (le terme est également repris par les partenaires commerciaux du projet).

Pour la mise en place du projet, plusieurs appels d'offres sont lancés, des salons sont organisés, des offres d'emploi (avec une campagne de recrutement remarquée) sont publiées, une importante campagne pour la sélection du site devant accueillir l'*AFCYBER* est initiée. Une vingtaine d'États répondent à cet appel, avec ce que cela implique en termes de mobilisations administratives, logistiques, etc. Les projets d'architectes fleurissent. Sa mise en service opérationnel initiale (*initial operationnal capabilities*) est prévue pour octobre 2008. Entre temps, il prend le nom de : *Air Force Cyber Command (Provisional) AFCYBER(P)*[12]. Cependant, le projet rencontre des difficultés.

La première difficulté provient des critiques que le projet essuie concernant la définition de ses missions. Elle est considérée comme trop large et surtout trop floue. Une incertitude loin d'être dissipée par les responsables de l'*USAF*, au contraire. Pour le directeur de l'*AFCYBER(P)*, le général William Lord : « *It's about* Air Force's *focus on the* Air Force's *protection and defense of the* Air Force's *command and control abilities*[13]. » Pour le général Robert Elder, qui commande alors la 8th air Force et qui est le supérieur direct du général Lord : « *Our mission is to control cyberspace both for attacks and defense*[14].» La confusion peut parfois aller encore plus loin, jusqu'à la définition même du terme « cyberespace » puisque pour le général Lord propose une interprétation très extensive qui comprend tout le spectre électromagnétique (radio, micro-ondes, rayons X, lasers et mêmes les armes à énergie dirigée). Ce flou général entourant le projet entame donc sa crédibilité et donne des arguments à ses détracteurs[15].

12. Le terme « provisional » signifie que le personnel qui le compose ne lui appartient pas directement, mais est détaché de plusieurs services.

13. Noah Shachtman, Air Force Wobbles on Plan for Cyber 'Dominance', http://www.wired.com/dangerroom/2008/06/marlborough-mas/.

14. Idem.

15. Les agences de renseignements en première instance, mais aussi l'*US Navy* et l'*US Army* qui ont-elles aussi leur programme cyber (moins ambitieux cependant).

Mais ce sont surtout les crises à répétition que connaît *l'USAF* dans les années 2007 et 2008 qui finissent par donner un coup d'arrêt au projet. Ce sont les nombreuses disputes entre les responsables de *l'USAF* et le secrétaire à la défense Robert Gates au sujet des drones et du F-22, la mauvaise gestion du contrat sur la flotte de ravitailleurs, mais surtout l'incident des armes nucléaire constaté sur la base aérienne de Barksdale, le 30 août 2007[16]. Finalement, en juin 2008, le secrétaire à l'air Michael Wynne ainsi que le chef d'état-major de *l'USAF* Michael Moseley sont contraints de démissionner. Etant donné l'importance de la crise et de la profonde réorganisation des structures de *l'USAF*, *AFCYBER(P)* est abandonné.

Des moyens en augmentation, mais un futur incertain

Depuis une dizaine d'années, on assiste à une militarisation progressive du cyberespace aux États-Unis ; processus illustré par la création de l'*US Cyber Command*[17]. Toutefois, ce dernier demeure toujours en mutation et son avenir sujet à discussions. La question de la séparation avec la *NSA* a été écartée par Barack Obama, mais pourrait ressurgir avec la future administration.

L'*USAF* quant à elle ne semble pas avoir abandonné ses ambitions pour le cyberespace. En 2009, elle publie un projet définissant ses objectifs au sein du nouveau *CYBERCOM*. Le langage employé, notamment en introduction, reste le même que lorsqu'elle affichait ses prétentions quelques années auparavant. En outre, son énoncé de mission reste le même que celui susmentionné. Après avoir échoué dans son approche « par le haut », elle tente désormais une approche « par le bas » et prévoit de recruter et de former environ 1 200 personnes. Elle renforce également sa contribution en matière de recherche et développement. Cette nouvelle démarche s'avère payante puisque, pour l'année fiscale 2015, elle a obtenu le budget le plus important des quatre armées en matière de cyberdéfense.

---

16. Des missiles nucléaires opérationnels ont été chargés par erreur sur un bombardier lourd B-52H, qui les a convoyé entre les bases aériennes de Minot et de Barksdale, du Nord au Sud du pays. Pendant tout ce temps, les armes nucléaires n'ont été soumises à aucune mesure particulière de sécurité et cela durant près de 36 heures.

17. Autre illustration de cette militarisation : le vocabulaire. L'utilisation de termes tels que « offensive », « défensive », « dissuasion », etc. est symptomatique de la volonté des militaires de s'approprier ce domaine. Le CYBERCOM lui-même est désigné comme un « commandement opérationnel ».

La « cybérie » russe à l'aune de la nouvelle doctrine militaire

Monsieur Yannick Harrel*
Professeur à l'ISEG Business & Finance School de Strasbourg

Cyberespace et souveraineté

Le cyberespace russe[1], et son pendant l'Internet russe que les initiés qualifient généralement de RuNet, est un espace désigné comme stratégique depuis l'an 2000 sur le plan civil et affirmé *crescendo* de la même manière au niveau militaire à partir de plusieurs rédactions officielles en 2009. Il ne faudrait malgré tout pas prétendre hâtivement que les théoriciens et publicistes militaires ne se sont pas préoccupés de la question avant 2009. D'une part parce que la réputation des militaires soviétiques puis russes dans le domaine de guerre électronique n'est pas surfaite[2]. D'autre part, et très vraisemblablement, la raison de ce silence tient le plus vraisemblablement à la refondation de l'armée russe : un chantier somme toute récent débuté dans les années 2000 après une décennie précédente catastrophique[3]. Refondation d'autant plus essentielle que la priorité première était surtout pour les autorités de disposer à nouveau d'un outil militaire à la qualité acceptable et au personnel disposant d'un minimum de qualification afin de peser sur le cours des événements et non d'en être simple

1. Le cyberespace est l'ensemble des procédures et moyens civils et militaires permettant l'échange de données à travers des systèmes automatisés de contrôle, de communication et d'information.

2. Les exemples récents du conflit russo-géorgien en 2008 puis russo-ukrainien en 2014 ont été l'occasion de constater que leur excellence était intacte, en dépit de quelques ratés en 2008 qui ont fait l'objet d'analyses puis de corrections lors de la grande réforme militaire amorcée par le ministre de la Défense d'alors, Anatoli Serdioukov, et ce juste après le conflit. Les Russes perçoivent la guerre électronique comme une activité relevant de la sécurité informationnelle.

3. Le colonel Michel Goya a traité en détail de cette transformation au travers d'un article : « La transformation militaire russe », *La Voie de l'Épée*, URL : http://lavoie-delepee.blogspot.fr/2014/05/la-transformation-militaire-russe.html
Pour information complémentaire, le budget 2015 alloué au secteur des forces armées devrait atteindre 50 milliards de dollars selon l'allocution du président Vladimir Poutine en décembre 2014.

spectateur[4], ce qui a entraîné par ailleurs la contractualisation au sein des forces armées russes, qui restent malgré tout composées de conscrits en très grande majorité.

Le principal mot d'ordre en matière de cyberespace est la souveraineté. Non seulement affirmée au niveau national mais aussi à un niveau international, soit auprès d'instances techniques telle que l'Union Internationale des Télécommunications soit auprès d'instances plus généralistes comme l'Organisation des Nations Unies. Et souvent la Russie trouve la Chine pour asseoir sa position et sa volonté de réguler le cyberespace. Ce sont par ailleurs aussi ces deux États que certains spécialistes aux États-Unis désignent comme menaces de premier ordre pour la sûreté de cet espace[5].

La publication en décembre 2014, et ce dans un contexte géopolitique tendu entre sanctions occidentales et chute du cours du pétrole, de la nouvelle doctrine militaire des forces armées de la Fédération de Russie a permis de confirmer une constante amorcée voici plusieurs années dans le cadre de la perception et de l'utilisation du cyberespace russe.

---

4. Les guerres de Yougoslavie entre 1991 et 2001 puis la chute du régime irakien en 2003 ont marqué durablement les esprits russes en posant crûment l'abaissement du statut de la Russie, déchue de son statut de puissance décisionnaire dans les affaires géopolitiques majeures. Si le premier mandat de Vladimir Poutine a été axé sur l'ouverture et la concertation sanctionné par une série de déceptions, le second de 2004-2008 sera ouvertement celui de l'affirmation des préoccupations russes sur les affaires du monde par la refondation de l'outil militaire et la reprise en main du secteur économique dont le géant Gazprom en est le plus éminent exemple.

5. Ainsi, le directeur du renseignement national américain, James R. Clapper n'a pas hésité en avril 2015 à désigner publiquement la Russie derrière l'intrusion d'une partie du réseau informatique de la Maison Blanche et d'insister sur celle-ci comme une cybermenace de première importance, plus que la Chine pourtant fortement suspectée d'actes réitérés de cyberespionnage. Pour plus d'informations circonstanciées, se reporter au Worldwide Threat Assessment of the U.S. Intelligence Community publié le 26 février 2015. URL : http://cdn.arstechnica.net/wp-content/uploads/2015/02/Clapper_02-26-15.pdf

Toutefois, la révélation de l'activité des virus Stuxnet comme Flame et de l'existence de l'Equation Group comme ayant des liens assez ténus avec les organes fédéraux américains tendent à relativiser cette assertion et plutôt affirmer que le cyberespace est un champ de bataille permanent où ingénierie sociale et innovation technique sont favorisées afin de prendre l'ascendant. Du moins temporairement. Ajoutons en complément que l'éditeur d'anvirus russe Kaspersky est en pointe dans la traque de menaces de ce type, et que la firme bélarusse VirusBlokAda fut la première à signaler la présence de Stuxnet.

© Daniel Marsula-Post Gazette

La nouvelle doctrine militaire de décembre 2014

Très laconiquement mais symptomatiquement est-il indiqué au point 11 que la Fédération de Russie doit faire face à un accroissement des dangers et menaces au sein de l'espace informationnel[6-7].

Le point 12 est en revanche encore plus disert sur le sujet en arguant l'utilisation potentielle par des puissances ennemies de technologies de l'information et de la communication dans un esprit politico-militaire contraire aux principes du droit international et attentatoire à l'intégrité comme souveraineté des États visés par de telles mesures[8]. Plus en avant, au point 13, l'emploi comminatoire de ces technologies est reconnu en tant que danger essentiel par leur capacité de mettre en péril les infrastructures militaires… et informationnelles[9].

De façon plus prospective sont énoncées les caractéristiques des guerres modernes, et plus particulièrement le point qui désigne une évolution qui aboutit à la centralisation et à l'automatisation des centres de commandement et de contrôles des forces armées[10]. Il n'y a pas de développement

6. L'espace informationnel est une acception large employé en russe afin de désigner le cyberespace. Il intègre les plans matériel, logiciel et informationnel. De la même manière, les textes russes n'emploient quasiment jamais le terme de cybersécurité et leur préfèrent la dénomination de sécurité informationnelle. Cette neutralité technologique cache en réalité une perception très différente de ce milieu afin de mieux en souligner les interactions avec certaines activités comme la guerre psychologique ou la guerre électronique.

7. « *Наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации.* »

8. « *использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности* ».

9. Il est loisible de remarquer en ce point 13 qu'à l'instar d'autres textes, accorde une attention remarquée des activités qui pourraient nuire au corps social. C'est là une préoccupation qui ne saurait être anodine dans le paragraphe. D'autant qu'elle n'est pas abordée de la même façon par les forces occidentales qui emploient préférentiellement le terme plus générique de population. Le texte de septembre 2000, la Doctrine de sécurité informationnelle de la Fédération de Russie, un document majeur en terme de cyberstratégie russe, est le premier à clairement prendre en grande considération cet aspect.

10. « *усиление централизации и автоматизации управления войсками и оружием в результате перехода от строго вертикальной системы управления к глобальным сетевым автоматизированным системам управления войсками (силами) и оружием;* »

sur ce point mais les autorités russes semblent considérer que ce phénomène, centralisation et automatisation, va de pair avec la transition d'une structure de direction verticale à un ensemble plus nodal (et non horizontal). Cette projection est dans la droite ligne du texte de 2012 : *les vues conceptuelles des forces armées dans l'espace informationnel*, qui énonçait la nécessité d'une meilleure coordination de ces mêmes centres afin d'améliorer la localisation d'unités, le recoupement d'informations en temps réel et la coordination d'actions.

Le point 21 mentionne derechef les dangers liés aux technologies de l'information et de la communication en désignant l'obligation de créer les conditions pour éviter que celles-ci ne mettent en péril la sécurité internationale dès lors qu'elles soient utilisées dans une optique de déstabilisation politique ou militaire à l'encontre d'un pays souverain[11].

Toutefois, il convient de ne pas se méprendre, et l'article 32 est assez clair sur le sujet : le feu nucléaire et l'effort aérien comme spatial demeurent les priorités de la stratégie militaire contemporaine. Cela ne lénifie en rien l'importance du cyberespace comme espace stratégique mais ne le place pas pour autant en tête des priorités actuelles.

Un peu plus loin, aux points 45 et 46, il est relaté un autre élément déjà aperçu dans les textes précédents : le besoin d'un système d'armement intégré et interconnecté : l'on peut penser au Ratnik, une combinaison de haute-technologie à la fois pour les matériaux employés comme pour les systèmes embarqués, limitée à un poids de 24 kilogrammes. Un équipement similaire au britannique FIST, à l'américain Land Warrior ou au français FELIN.

Un trop rapide passage évoque le déploiement de troupes et de moyens de guerre informationnelle. Le texte n'est hélas guère loquace sur le sujet[12], toutefois en concordance avec les autres documents officiels antérieurs, il s'agit bien de l'existence de forces dédiées à la surveillance et aux actions

11. « *создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности.* »

12. « *в) развитие сил и средств информационного противоборства;* »

militaires dans le cyberespace dont il est question, d'autant que peu après il est à nouveau fait mention d'un nécessaire système d'échange d'informations unifié et de qualité entre les combattants et le poste des opérations : un objectif déjà présenté comme majeur dans le texte de 2012, *Les vues conceptuelles des forces armées dans l'espace informationnel*.

Plus symptomatique est le passage suivant[13] enjoignant la mise en place de systèmes d'information dont la gestion simplifiée est susceptible d'être facilement intégrée aux systèmes de contrôle d'armes et aux autres systèmes complexes à différents niveaux d'opérations (stratégique, opératique, tactique voire mixte). Ce que l'on pourrait appeler modularité où la pièce d'un élément peut s'insérer facilement en un minimum de temps et d'effort dans un ensemble conséquent sans pour autant entraînement de dysfonctionnement.

Un élément qui est loin de n'être qu'une simple occurrence depuis plusieurs textes stratégiques, c'est l'importance accordée une fois encore à l'aspect économique. Décelable en plusieurs endroits épars du document, il est très clairement signifié au chapitre V, soit les articles 43 et 44 avec la notable mention d'une rapide adaptation d'une partie de l'activité économique civile aux besoins militaires en sus bien entendu de la sécurisation et du renforcement des ressources financières du complexe militaro-industriel. C'est, on peut le conjecturer, une approche empirique à la suite de l'échec suivi de la chute de l'Union Soviétique dont l'une des causes majeures fut le poids démesuré du complexe militaro-industriel dans le budget de l'État. Il n'est ici nullement question d'orienter la société vers ce complexe mais de faire bénéficier à ce dernier, en cas de nécessité est-il précisé, d'un afflux de ressources provenant du secteur civil. Il doit malgré tout vivre du sien et surtout favoriser les coopérations et les achats de matériel avec les pays étrangers[14]. Sur ce dernier élément, il est même rappelé expressément à l'article 55 qui insiste en complément sur les partenariats

13. *« ж) создание базовых информационно-управляющих систем и их интеграция с системами управления оружием и комплексами средств автоматизации органов управления стратегического, оперативно-стратегического, оперативного, оперативно-тактического и тактического масштаба. »*

14. Rappelons que l'autarcie en matière militaire durant l'Union Soviétique n'a été qu'une parenthèse dans le processus de l'équipement militaire russe qui a souvent été un commanditaire de matériel étranger : ainsi l'armurier américain Smith & Wesson fut le fournisseur de révolvers éponymes du régime tsariste (après modification du calibre sur demande spécifique) à partir de 1871 et ce pendant près de deux décennies.

à amorcer puis à développer. Et l'article 57 vient clore le sujet en exposant sans ambages que le président de la Fédération de Russie est seul décideur en la matière, ce qui pourrait apparaître comme une certaine défiance vis-à-vis de la frange conservatrice du milieu militaire peu encline à la sous-traitance avec des pays tiers.

Une réaffirmation du cyberespace comme espace stratégique

En définitive, un texte officiel fait suite à la doctrine militaire de 2010. S'il n'est en rien révolutionnaire, il est l'occasion de relever la persistance de certains axes d'action et l'inflexion perceptible d'autres. Il n'est pas dans le propos de la présente analyse d'aller plus en avant dans celles-ci, en revanche l'aspect cyber n'a pas été oublié et s'il n'a pas non plus été démultiplié en terme d'importance, il est confirmé dans son rôle d'espace stratégique. Un espace où la Russie entend faire respecter sa souveraineté, telle qu'elle est mentionnée de façon persistante. Et ce avec l'appoint d'alliés et de structures auxquelles la Fédération est membre[15].

*Il est l'auteur de deux ouvrages de référence : *La cyberstratégie russe* et *Cyberstratégies économiques et financières* (2e édition) aux éditions Nuvis.

15. Citons l'Organisation du traité de sécurité collective, l'OTSC, la Communauté des États Indépendants ou encore l'Organisation de coopération de Shanghai pour les plus proches. Et dans une moindre mesure, et plus civiles, l'Organisation des nations unies, le Conseil de l'Europe ou l'Organisation mondiale du commerce.

Cybersécurité et cyberdéfense chinoise : évolutions

Monsieur Daniel Ventre
Ingénieur au CNRS, chercheur au CESDIP (Centre de Recherches Sociologiques du Droit et des Institutions Pénales)[1]

L'essentiel de la connaissance qui nous parvient sur les pratiques, politiques et stratégies chinoises en matière de cybersécurité et défense trouve son origine dans un discours anglo-saxon dominé par la perspective américaine, grande productrice de rapports, études et discours sur le sujet. Les entreprises de cybersécurité (Mandiant, Novetta Solutions…), les médias, les responsables ou ex-responsables d'agences du gouvernement, mais encore le monde de la recherche académique, les think tanks, traitent de la question depuis le début des années 2000[2]. La Chine communique également, que ce soit par les médias, par des publications officielles, par des discours, sur sa vision de la cybersécurité et son analyse des défis que pose le cyberespace à la société et à la sécurité. Sur ces bases, essayons d'identifier quelles ont été au cours des deux dernières décennies les principales évolutions de la cybersécurité/cyberdéfense chinoise, ou du moins l'idée que l'on s'en fait.

Une « menace » exprimée en de nouveaux termes

La récente cyberstratégie publiée par le Département de la Défense américain (avril 2015)[3] considère la Chine comme une pièce maîtresse, si ce n'est « la » pièce maîtresse, dans l'environnement de la cybermenace. Cette considération n'a guère été modifiée au fil des ans**, la Chine constituant toujours une menace** en raison de ses développements capacitaires et de ses

1. L'auteur est également Titulaire de la Chaire Cybersécurité et Cyberdéfense (Ecoles de Saint-Cyr Coëtquidan/Sogeti/Thales), chargé de cours à Telecom ParisTech, Directeur de la collection Cybercriminalité et Cyberconflit aux éditions Hermes Lavoisier. Il a publié une dizaine d'ouvrages sur le cyberconflit et la guerre d et l'information.
2. Un recensement des sources et des diverses approches proposées par chacune d'entre elles est proposée dans : Daniel Ventre, Discourse Regarding China : Cyberspace and Cybersecurity, Chapitre 8, pp.199-282, *in* Daniel Ventre (Edit.), Chinese Cybersecurity and Defense, Wiley ISTE, juillet 2014.
3. U.S. Department of Defense, The DoD Cyber Strategy, 2015, 42 pages, Washington, http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

orientations stratégiques dans le cyberespace, lesquels sont confirmés par une démonstration d'efficacité soutenue, si l'on s'en réfère aux multiples opérations de cyberattaques dont le pays est crédité depuis les années 1990.

La manière de qualifier les hackers chinois en 2015 diffère de celle des années 1990-2000. On insistait alors davantage sur les hackers « patriotes », « nationalistes », « hacktivistes » qui, motivés par des sentiments patriotiques, agissaient soit d'initiative, soit de concert avec les acteurs étatiques. Il était fréquent d'évoquer les opérations de ces hackers (défigurations de sites massives, intrusions dans des serveurs étatiques) qui venaient s'inscrire dans des contextes de crises sino-japonaise ou sino-américaine. Désormais les hackers désignés sont avant tout ceux des services de renseignement militaires chinois. L'implication de Pékin dans les perturbations planétaires du réseau est sans détour dénoncée. Or le fait d'avoir déporté l'attention vers les pratiques étatiques, ne signifie pas que les communautés de hackers-citoyens ou cybercriminels n'existent plus ou qu'elles sont moins actives qu'auparavant.

Les États-Unis semblent avoir trouvé la grille de lecture qui leur faisait défaut dans les années 2000. Ayant jusqu'alors critiqué les stratégies chinoises de cyberdéfense pour leur opacité, hésité entre qualifier la cyber-puissance chinoise de menace guerrière/conquérante, de menace économique ou cybercriminelle, les États-Unis pointent aujourd'hui principalement le doigt sur la « menace économique » que constituent les pratiques de cyberespionnage menées par l'armée chinoise. Les autorités américaines voient essentiellement la Chine comme un voleur de propriété intellectuelle, vols commis par les renseignements militaires chinois au profit de leurs industries civiles et militaires, et bien sûr au détriment de la compétitivité américaine. Le cyberespionnage relèverait donc ainsi essentiellement de la guerre économique.

Les **menaces de conflits interétatiques** régionaux impliquant la Chine, dans lesquels on trouvera toujours désormais une dimension cybernétique, n'ont guère régressé. Si la menace d'attaque contre Taïwan, mobilisant une stratégie de guerre de l'information et de cyberdéfense, n'est pas écartée, la question apparaît cependant moins soulignée dans les analyses stratégiques américaines. Cette menace n'est plus aussi systématiquement mise en avant qu'elle l'était au cours des années 2000. D'autres crises perdurent toutefois : en attestent les récentes tensions territoriales entre la Chine et le Japon (îles …), les tensions entre la Chine et l'Inde.

Les États-Unis, mais aussi l'ensemble des pays qui s'affichent en victimes des pratiques agressives chinoises (intrusions dans les systèmes industriels et étatiques, APT), peinent à entamer un dialogue constructif avec la Chine, à **trouver de véritables mesures dissuasives**. Les poursuites engagées en mai 2014 contre quelques officiers de l'armée chinoise accusés de cyberespionnage économique, ne sont probablement pas de nature à altérer la détermination des agresseurs et à faire office de menace dissuasive. La Chine, face aux accusations répétées, maintient sa position, réfutant systématiquement son implication.

Sur le **plan intérieur,** mais avec de fortes connexions internationales, on constate que les efforts de domination de l'espace informationnel par les autorités de Pékin n'ont guère contribué à la réduction des violences et des revendications (Xinjiang, Tibet). Les opérations dans l'espace informationnel, les mesures prises dans le cyberespace (influence, contrôle, surveillance, censure, blocage d'applications, coupure des communications) n'ont pas contribué à pacifier les régions touchées par ces crises.

La cybersécurité est certainement l'un des enjeux majeurs de la société chinoise moderne. **Mais le pays doit faire face à d'autres défis sécuritaires énormes**, tout aussi urgents, voire prioritaires. Les conditions du développement économique, de la course effrénée au rendement, à la croissance, à l'enrichissement, ont eu des conséquences majeures sur la société : pollution environnementale, climat, sécurité sanitaire, sont au rang des priorités vitales. La société de l'Internet, des nouvelles technologies de l'information, aura contribué à la destruction environnementale. La Chine est parmi les nations les plus touchées par le phénomène.

La Chine, devenue un acteur global dans le cyberespace

Sur le plan industriel, la Chine a acquis des compétences dont elle ne disposait pas dans les années 1990. Elle ne se contente plus d'acquérir des technologies étrangères comme ce pouvait être le cas, elle ne se contente pas d'être l'usine du monde : elle est devenue force créatrice, a amélioré son processus de recherche et de développement, créé des *clusters* industriels partout dans le pays, et est en mesure d'exporter ses technologies, de gagner des parts de marchés importantes, de racheter des entreprises étrangères. La Chine tente d'imposer ses solutions. Sans doute pour lui barrer la route (pour des raisons évidentes de luttes pour des parts de marchés), tout autant que pour

répondre à de vrais enjeux de sécurité nationale, nombre d'États se sont opposés à l'accès à des marchés nationaux par les entreprises chinoises. À la détermination de conquête économique chinoise, les États opposent des barrières justifiées par la sécurité nationale, et la nécessité de technologies « souveraines ». De son côté la Chine impose elle aussi de fortes contraintes aux entreprises étrangères présentes sur son territoire (telle que l'obligation d'utiliser des systèmes de sécurisation – crypto – approuvés par Pékin, interdiction faite aux banques chinoises d'adopter des systèmes et applications chinois)[4] Ainsi Huawei s'est-elle vue dans de nombreux pays les portes des marchés étatiques sur des segments définis comme sensibles/vitaux. Le marché chinois lui-même s'est considérablement transformé : le web 2.0 chinois dispose désormais de ses industries nationales, avec des leaders comme Baidu (moteur de recherche), Weibo (équivalent chinois de Twitter). **La Chine est devenue un acteur global,** en ce sens qu'elle dispose désormais de capacités industrielles pour couvrir les trois couches du cyberespace (couche 1 : créer des infrastructures, développer du *hardware*, en industrialiser la production ; couche 2 : créer, développer, imposer commercialement des applications logicielles, y compris dans le web 2.0 ; couche 3 : créer, développer des plates-formes de réseaux sociaux, créer du contenu, permettre la croissance de cette couche informationnelle), et que cette maîtrise s'étend bien au-delà de son seul cadre national, en conquérant des parts de marchés jusque-là dominées par des entreprises occidentales ou japonaises. Cette force industrielle, et les perspectives ouvertes par la R&D, soutenues par une planification politique, ouvrent des perspectives pour les développements à venir : internet des objets, villes intelligentes, *big data*, mais encore renforcement du caractère « national », « souverain » des solutions adoptées par la sphère chinoise. **Le tout confère à la Chine une puissance réelle et un pouvoir d'influence sur la configuration du cyberespace** aujourd'hui déjà, et plus encore dans les prochaines années. Cette puissance contribue à l'évolution des rapports de force sur la scène internationale et à la capacité d'influence de la Chine.

La Chine a tenté d'exploiter le contexte de tensions internationales consécutif aux révélations d'E. Snowden sur les pratiques de surveillance, pour influencer les perceptions à son égard. Les révélations de Snowden ont suscité de l'indignation, des interrogations sur les pratiques des États démocratiques (surveillance), sur le sens des relations de confiance entre États. Les critiques traditionnellement formulées à l'encontre de la Chine se sont vues retournées contre le « modèle » que souhaitait représenter l'Amérique :

4. US voices concern over China's banking technology restrictions, RT.com, 27 mars 2015, http://rt.com/business/244589-usa-china-wto-cybersecurity/

responsable de cyberattaques, d'intrusions dans les serveurs étatiques des puissances étrangères y compris alliées, vols de données, espionnage politique et économique, surveillance des citoyens. Cette similitude entre les pratiques des États (même si les États-Unis légitiment leurs pratiques par des motivations se distinguant de celles de la Chine) contribue peut-être à **relativiser la nature de la « menace » chinoise.** Les autorités de Pékin en tous cas ont joué de cette situation pour se défendre des accusations portées à leur encontre par Washington et nombre d'autres puissances. Au lendemain des accusations visant ses officiers militaires pour cyberespionnage, Pékin accusait Washington d'hypocrisie, rappelant que les États-Unis maîtrisent l'essentiel des technologies et possèdent les infrastructures clefs pour conduire des opérations de cybersurveillance (espionnage) massive planétaire visant gouvernements, entreprises, populations[5].

Les enjeux du cyberespace sont devenus l'objet de **discussions officielles aux plus hauts niveaux** entre la Chine et de nombreux pays : ainsi les autorités américaines et chinoises s'entretiennent-elles sur le cyberespace (Sino-U.S. Cybersecurity Dialogue[6], Cyber Working Group), sur la nécessité de définir des règles de sécurité dans le cyberespace (visant par exemple à éviter tout risque d'erreur d'interprétation, qui pourrait déboucher sur une escalade de la violence entre les États). Ces échanges sont suspendus à la qualité des relations diplomatiques : le dialogue au sein du Cyber Working Group a été suspendu par la Chine en mai 2014. La Chine veut plus largement imposer sa voix à l'échelle internationale, se dit ouverte aux dialogues bilatéraux[7] sur les enjeux de normalisation et de gouvernance du cyberespace, l'un de ses leitmotivs étant la défense de la souveraineté. Elle est pour cela présente dans les instances de normalisation (UIT), et formalise des accords avec des partenaires étrangers (elle a par exemple signé en mai 2015 un accord avec la Russie, surnommé par les médias « Pacte Cyber »[8]).

---

5. Ben Knight, US goes after China over cyber attacks, 20 mai 2014, http://www.dw.de/us-goes-after-china-over-cyber-attacks/a-17648859

6. Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR) - Center for Strategic and International Studies (CSIS) , Juin 2012, http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf

7. China to deepen int'l cooperation on cyber security, CCTV.com, 10 février 2015, http://english.cntv.cn/2015/02/10/VIDE1423536244824155.shtml

8. Alexandra Kulikova, China-Russia cyber-security pact: should the U.S. be concerned?, Russia Direct, 21 mai 2015, http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned . Une traduction en anglais de l'accord est propose sur le site csistech.com : http://www.csistech.org/blog/2015/5/11/sino-russian-cybersecurity-agreement-2015

Conclusion

La Chine est donc désormais **l'un des acteurs majeurs** sur la scène internationale en matière d'exploitation du cyberespace à des fins politiques, stratégiques, militaires. Mais elle **reste encore en retrait par rapport à la puissance américaine**. D'autre part, le contexte mondial a lui aussi considérablement évolué depuis les années 1990 : depuis 2007, mais surtout 2010, de plus en plus d'États se sont engagés dans un processus d'élaboration de politiques de cybersécurité et de cyberdéfense, dans la mise en œuvre de capacités civiles et militaires, visant à sécuriser, et protéger leurs actifs, leurs systèmes, mais aussi envisagent le recours à des pratiques plus « agressives » dans le cyberespace, y compris en temps de paix. La Chine elle-même a reconnu l'existence de ses unités dédiées de cyberdéfense (cette reconnaissance serait contenue dans la dernière version de *The Science of Military Strategy* publiée en 2013)[9]. C'est donc le contexte mondial qui a subi de fortes évolutions en matière de cybersécurité ces dernières années. Nous pouvons **envisager quelques conséquences** pour la Chine de ces nouveaux équilibres, nouvelles politiques, institutions et pratiques :

- Le **durcissement des cibles**, rendant théoriquement la tâche plus difficile aux agresseurs, chinois ou autres et les contraignant à améliorer leur savoir-faire offensif.

- La montée en puissance de capacités agressives dans de nombreux pays **expose la Chine à davantage d'attaques**, du moins théoriquement.

- La **puissance acquise** par la Chine l'expose aussi à des cyberattaques plus nombreuses.

- La **dépendance accrue** de la Chine au cyberespace, voyant de plus en plus de composantes de sa société connectées aux réseaux publics, **l'expose à des actions agressives de puissances étrangères**, et plus largement de hackers de tout horizon, aux motivations les plus diverses.

9. Shane Harris, « China reveals its cyberwar secrets », *The Daily Beast*, 18 mars 2015, http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html

Le cyber en Israël : quelle stratégie ?

Monsieur Amer Eldebek
Diplômé de l'Institut d'études politiques de Paris
Doctorant en Études Politiques

Introduction

Repenser la guerre

Si la guerre du Golfe est la dernière guerre du XX[e] siècle à opposer des armées conventionnelles, la littérature sur la disparition de la guerre, dans sa forme classique, vers une nouvelle forme de guerre ne cesse de fleurir[1]. L'argument principal de ces analyses se fonde sur les changements qualitatifs[2] qui ont caractérisé – et qui continue à caractériser – la période post-*Cold War*. « *Les nouvelles guerres* » (Kaldor, 2001a : 6), ce terme, associé à ces changements, contraste avec les guerres précédentes à plusieurs niveaux : non seulement par leur nature et par leurs méthodes, mais aussi par leurs objectifs et par leurs financements[3].

Toutefois nous soutenons l'idée que la plupart de ces arguments ne sont pas nouveaux ; ils étaient présents – avec certaines limites – dans les guerres du siècle dernier et de l'avant-dernier siècle. Évidement des changements se sont produits, et ils nous permettent de parler d'une « évolution de la guerre » plus que toute autre chose. Certains académiques ont contesté la thèse de « nouvelles guerres » en évoquant que certainement il y a eu des fluctuations dans certains facteurs mais sans arriver à une rupture totale avec le passé.[4]

1. Ramel Frédéric, « À quoi ressemblent les nouvelles guerres ? », *Sciences humaines* 1/2015 (N° 266) p. 44
2. «The New Wars Debate»: A Historical Perspective Is Needed, Edward Newman.
3. A titre d'exemple, les guerres actuelles étant des guerres intra-étatiques plutôt que inter étatiques ; elles sont caractérisées par une transformation sociale (État faible, globalisation, etc.) et elles sont plutôt motivées par des convictions religieuses que par une idéologie politique.
4. *Idem* 2

La cyberguerre : le débat théorique

Dans un article publié par Rand Corporation en 1993, John Arquilla et David Ronfeldt[5] prédisent que la « cyberguerre est à venir ». Leur article, largement repris par l'établissement militaire américain, soutient l'idée qu'une petite armée extrêmement informée - à l'instar des Mongols du XIII^{e} siècle, - est capable de vaincre la supériorité quantitative de l'armée ennemie. Selon Arquilla et Ronfeldt, la révolution de l'information créant un décalage entre la manière dont les sociétés abordent un conflit et comment leurs armées s'engagent dans une guerre, c'est pour eux la technologie qui changera la nature de la guerre. Cette idée sur le changement de nature de la guerre à travers la cyberguerre est problématique. Thomas Rid[6] s'oppose à l'analyse d'Arquilla et de Ronfeldt en précisant que la cyberguerre n'a pas et n'aura pas lieu. Toutefois le débat sur la nature de la guerre se révèle très théorique. En affirmant que « *la guerre est un caméléon* », Clausewitz nous invite à penser que les modifications profondément incessantes de la guerre permettent de faire infiniment cet exercice de classification. Dans ce sens, la cyberguerre peut être vue comme le « dernier-né » de la révolution gigantesque de la technologie de l'information et de la communication, tout en pouvant être qualifiée de nouveau mode de guerre. Ce débat que suscite la cyberguerre nous pousse à étudier la réalité de la cyberguerre sur les champs de bataille actuels.

Le cyberespace et la sécurité nationale

La croissance rapide dans les domaines de l'informatique et de la communication, ainsi que l'amélioration continue de la performance des systèmes informatisés, ont créé un nouvel espace dans le monde : le cyberespace[7]. Contrairement à la terre, à la mer, à l'air, à l'espace ou au spectre électromagnétique, le cyberespace ne fait pas partie de la nature et n'aurait pas pu exister sans les technologies d'information qui se sont développées au cours des dernières décennies[8].

5. John Arquilla and David Ronfeldt, « Cyberwar is Coming! » *Comparative Strategy*, Vol. 12, N°. 2, spring 1993, p. 141-165.
6. Thomas Rid (2012) « Cyber War Will Not Take Place », *Journal of Strategic Studies*, 35:1,p. 5-32.
7. Lior Tabansky, « Basic Concepts in Cyber Warfare », *Military and Strategic Affairs* 3, n°.1, May 2011.
8. *Idem.*

Le cyberespace est composé de tous les réseaux informatiques dans le monde, ainsi que de tous les points finaux qui sont connectés aux réseaux et qui sont contrôlés par des commandes qui passent à travers ces réseaux. Le cyberespace comprend l'Internet, mais inclut également une gamme d'autres réseaux informatiques qui ne sont pas accessibles par Internet. La meilleure façon pour comprendre le cyberespace en général, et les cyberattaques en particulier, est de les imaginer comme un système à trois couches[9]: une couche physique (l'électricité, les circuits intégrés, les processeurs, les dispositifs de stockage, les infrastructures de communication, les câbles en cuivre, les fibres optiques, etc.), une couche syntaxique, au-dessus de la couche physique (variété de logiciels programmés par des êtres humains), et une couche sémantique, constituée des données que contient la machine.

Plus un État, une organisation ou même une personne se met à investir dans ce cyberespace, plus la notion de sécurité devient fondamentale. Tant que les nations s'appuient sur les réseaux et sur les systèmes d'information en tant que fondement de leur puissance militaire et économique – et tant que ces réseaux informatiques sont accessibles pour l'extérieur – ils subissent un risque. Ce risque peut devenir une arme puissante qui peut « théoriquement » cibler les objectifs stratégiques d'un pays (tels que les infrastructures) sans être physiquement dans le lieu où ils se trouvent, sans donc affronter les armées de défense, et sans une exposition claire[10]. Ainsi, de nombreux États ont déployé le cyberespace dans le contexte de leur sécurité nationale[11], en investissant un volume important des ressources financières et organisationnelles.

Par le fait que la cybersécurité est devenue une question importante et urgente pour les acteurs de la sécurité nationale, les missions de cybersécurité, dirigées par un État contre un autre État, sont maintenant considérées comme faisant partie de la scène de combat et de conflit[12].

---

9. Martin C. Libicki, « Cyber deterrence and Cyberwar », Santa Monica, CA: RAND Corporation, 2009.

10. Lior Tabansky, « Cyber defense Policy of Israel: Evolving Threats and Responses », January 2013, Article n° III.12

11. The United States attention to the issue of security in cyberspace has been increasing. In 2009,President Obama declared that: « *It's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country.*» (http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/).

12. The United States government declared a cyber attack similar to an act of war, punishable with conventional military means as a form of last resort (Department of Defense, 2011).

La politique cyber en Israël

La recherche sur la politique cyber en Israël est importante pour deux raisons : la première est que l'appareil israélien de cyberdéfense est de renommée mondiale et est considérée comme un des leaders dans ce domaine[13]. La deuxième est sa dominance sur le marché global des produits liés au « cyber ». En effet, selon le Bureau National du Cyber en Israël (BNC), l'exportation israélienne de produits et services liés au cyber a atteint 3 milliards de dollars l'an dernier, soit 5 % du marché mondial, et plus que toutes les autres nations réunies en dehors des États-Unis[14].

Alors qu'Israël n'a pas encore publié une stratégie nationale de cyberdéfense, nous essaierons, à travers l'analyse de la trajectoire du « cyber » israélien, en s'appuyant sur des publications et des débats, de traiter ce sujet à partir de deux angles : la menace d'un part et l'innovation et la législation d'autre part.

La menace : une obsession sans fin

Les défis sécuritaires en Israël ont toujours été au centre des préoccupations de l'État hébreu. Une analyse rapide de son histoire depuis sa création, en 1948, montre qu'Israël est l'un des rares pays à s'engager dans une activité de guerre tous les cinq ans[15]. Une sensation de menace qui se manifeste par un sentiment d'insécurité est à la base d'une logique militaire fondée sur la dissuasion, sur l'alerte précoce et sur l'intervention militaire rapide[16].

---

13. An international comparative study of 23 developed countries recently awarded Israel with a top grade on "cyberdefence", alongside Sweden and Finland. at: The Security & Defense Agenda (SDA) report, "Cyber-Security : The Vexed Question of Global Rules" (30 January 2012), at 66-67.

14. Barbara Opall-Rome, Defense News, Israel Claims $3B in Cyber Exports; 2nd Only to US (Jun. 20, 2014), at: http://www.defensenews.com/article/20140620/DEFREG04/306200018/Israel-Claims-3B-Cyber-Exports-2nd-Only-US

15. Guerre israélo-arabe en 1948, la guerre de Suez en 1956, la guerre de Six Jours en 1967, la guerre d'usure, la guerre d'octobre 1973, l'invasion du Liban en 1982, la deuxième guerre du Liban juillet 2006, la guerre de Gaza en 2008, la guerre de Gaza de 2012, la guerre de Gaza 2014, et la deuxième Intifada.

16 Michael Raska, "*Confronting Cybersecurity Challenges: Israel's evolving cyber defence strategy*", IDSS.

Dans son cercle de défense, Israël a distingué trois types d'engagements militaires : le périmètre, l'intra-frontalier et l'engagement à distance[17]. Le « périmètre » est destiné à traiter les menaces militaires conventionnelles provenant des armées arabes dans le voisinage immédiat des frontières (Egypte, Syrie, Jordanie). Le cercle « intra-frontalier » se réfère à la défense au sein du territoire d'Israël contre les attaques et contre les incursions de faible intensité, tandis que « l'engagement à distance » concerne les menaces provenant de pays très éloignés comme l'Irak et l'Iran. Pendant la période de la guerre froide, et avant de signer les accords avec les Égyptiens (Camp David), avec les Palestiniens (Oslo) et avec les Jordaniens (Wade Araba), le « périmètre » occupait la place primordiale dans les préoccupations militaires israéliennes. Après les années 90, la vision stratégique israélienne s'est concentrée sur les sphères « intra-frontalière » et « engagement à distance ».

À la lumière de ces développements, le débat conceptuel sur l'adoption et sur l'adaptation de la cybersécurité s'imprégnait progressivement dans les larges débats stratégiques en Israël. Au début des années 1990, pendant le mandat du chef d'état-major de l'armée israélienne Ehud Barak, des analystes de défense israélienne ont commencé à reconnaître la notion « cyberactivité » sous la rubrique de « futurs champs de bataille »[18]. Ils ont analysé la trajectoire émergente de la technologie d'information utilisée dans le combat, tout en observant le potentiel et les implications d'une nouvelle génération de munitions de précision guidées, des systèmes de commandement et de contrôle, de l'intelligence intégrée et de guerre électronique. À cette époque, la cybersécurité a été conceptualisée sous le parapluie de « guerre d'information » en tant que sphère d'une importance décisive, dans laquelle la supériorité du pays par rapport aux pays rivaux était la clé essentielle pour remporter les conflits militaires.

Cette menace a été également perçue dans le domaine civil. Bien avant 2002, la législation permettait à l'Agence israélienne de sécurité[19] (Shabaq) d'intervenir dans les affaires civiles au nom de la sécurité[20]. Cette focalisa-

17. *Idem.*

18. Ben Israel, Isaac. 2012, « Introductory Remarks of the Annual Cyber Security International Conference 2012 », Tel Aviv University. See also: Dima Adamsky, 2010, The Culture of Military Innovation: *The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*, p. 98.

19. *Idem 16.*

20. Au sein de *Shabaq*, une unité de sécurité de l'information était en place bien avant2002, cette unité s'occupe de la sécurité d'information dans les ambassades israéliennes et les sociétés appartenant à l'État.

tion initiale sur la protection des infrastructures et des bases de données informatisées a caractérisé la première étape de l'engagement national israélien dans la cyberdéfense. En effet, d'une part, l'expansion accélérée du cyberespace – qui a largement augmenté la dépendance politique, militaire et socio-économique[21] – et, d'autre part, l'insuffisance des politiques et des réglementations existantes pour la protection des systèmes informatiques dans les structures combinées (civiles et militaires) sont à la base de l'augmentation de débats « cyber» dans l'établissement de la défense israélienne qui voyait le cyberespace comme un nouveau milieu d'interaction stratégique, mi-civil, mi-militaire. En octobre 2013, le chef d'état-major de l'armée israélienne Benny Gantz dénonce la menace contre les structures civiles comme étant une caractéristique de la guerre du futur : « *Une vaste guerre cybernétique fera rage, va affecter non seulement les systèmes militaires, mais aussi les systèmes civils.*» Et d'ajouter que les médias des deux camps la couvriront intensivement en temps réel[22].

Innovation et législation

En automne 2010, peu de temps après les rapports de la presse sur « Stuxnet », le Centre de la cybersécurité au département américain de la Sécurité intérieure a déclaré au Congrès que « Stuxnet » était un « *game changer* »[23]. Dans le même sens, l'Agence européenne de sécurité des réseaux et d'information a caractérisé ce virus comme un « *game changer* » pour la défense contre les logiciels malveillants[24]. Selon le *New York Times*, « Stuxnet » a été développé et déployé par les États-Unis[25] et par Israël[26].

21. Les adversaires potentiels pourraient en théorie perturber, détruire ou détourner des objectifs stratégiques clés (les infrastructures critiques) sans utilisation d'armes et sans exposition claire.

22. *Idem 16.*

23. Leyden, J. « Stuxnet» a game changer for malware defense EU agency warning. *The Register*, 9 October 2010. At: http://www.theregister.co.uk/2010/10/09/"Stuxnet"_enisa_response

24. Benson, P. Computer virus « Stuxnet » a game changer' DHS official tells Senate. CNN, 17 November 2010. At: http://articles.cnn.com/2010-11-17/tech/"Stuxnet". virus_1_ "Stuxnet"-nuclear-power-plants-target?_s=PM:TECH.

25. Sanger, D.E. "Obama order sped up wave of cyber attacks against Iran". *The New York Times*, 1 June 2012. At: http://www.huffingtonpost.com/2012/06/01/new-york-times-obama-orde_n_1562102.html

26. Broad, W.J.; Markoff, J.; Sanger, D.E. Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*, 15 January 2011. At: http://www.cfr.org/iran/nyt-israeli-test-worm-called-crucial-iran-nuclear-delay/p23850

Ce qui distingue « Stuxnet » des milliers d'autres virus est qu'il a été conçu pour se déployer seulement quand il pénètre dans un système de contrôle industriel (ICS) conforme aux caractéristiques de l'usine d'enrichissement nucléaire d'Iran à Natanz. Une fois déployé, il altère le code du contrôleur logique programmable (PLC) utilisé pour contrôler les centrifugeuses à Natanz, détruisant environ un millier de centrifugeuses et perturbant ainsi le programme nucléaire iranien[27]. « Stuxnet » n'est pas la première cyber-arme connue utilisée par Israël. Avant « Stuxnet », Israël dit avoir utilisé des cyberarmes pour aveugler les défenses aériennes syriennes au moment de son raid aérien contre une installation d'armes nucléaires syrienne en 2007[28]. Bien que plusieurs débats[29] aient eu lieu sur l'avancée scientifique de « Stuxnet », il est clair qu'il représente une évolution sans précédent dans le domaine de la cyberguerre, et qu'il est en tant que cyberarme, une innovation majeure.

La stratégie d'Israël à répondre à la cybermenace réside sur le développement des méthodologies interdisciplinaires afin de créer un milieu qui intègre les laboratoires de recherche, les unités de renseignement militaire, le Bureau National de Cyber, les *startup* et les entrepreneurs. Ce faisant, Israël développe « une enveloppe nationale de cyberdéfense »[30]. L'armée israélienne est présente au centre des capacités et des cyber-innovations. Que ce soit dans le secteur commercial, civil ou militaire, l'armée se charge de la sélection et de la formation, ainsi que de la recherche et du développement. Le processus commence par identifier et par recruter – dans les meilleurs lycées – des candidats qui excellent dans les sujets qui présentent un intérêt pour la cybersécurité. Avec pour fondement une série d'examens de qualification, ces élèves sont ensuite placés dans plusieurs unités de cybersécurité de l'armée israélienne. Après l'obtention du diplôme, les recrues vont servir dans les différentes unités de l'IDF spécialisées dans la cyberguerre[31].

---

27. Broad, W.J.; Markoff, J.; Sanger, D.E. Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*, 15 January 2011. At: http://www.cfr.org/iran/nyt-israeli-test-worm-called-crucial-iran-nuclear-delay/p23850

28. Clarke, R.A.; Knake, R.K. *Cyber War*; Harper Collins: New York, NY, USA, 2010.

29. Dorothy E. Denning, ""Stuxnet": What Has Changed?", *Future Internet* 2012, 4, 672-687;

30. *Idem 16*.

31. ID F. 2013. "Hackers Beware: The IDF's Digital Battleground." at http://www.idf-blog.com/blog/2013/10/09/hackers-beware-idfs-digital-battleground/

Au niveau gouvernemental, la politique du Bureau National du Cyber israélien a été établie sur la base de l'« Initiative National de Cyber » de 2010. Sous la direction du président du Conseil national pour la recherche et le développement, le professeur Isaac Ben-Israël, les experts qui ont travaillé sur l'« Initiative National de Cyber » avaient pour but de préserver le statut international d'Israël comme centre de développement en technologie de l'information et de fournir le pays de puissantes capacités dans le cyberespace. Elle devait répondre à trois questions principales :

- Comment assurer la position d'Israël comme l'une des cinq premières superpuissances en cyber d'ici à 2015[32] ?
- Quelles infrastructures sont nécessaires à Israël pour développer une haute performance en technologies de l'information ?
- Quelles sont les dispositions nécessaires pour faire face aux défis du cyberespace ?

À la suite de cette réflexion a été mis en place le « Bureau National de Cyber » (BNC) qui dépend directement du Premier ministre[33]. Il constitue un organe consultatif pour le Premier ministre israélien, pour le gouvernement et pour ses comités. Il recommande la politique nationale dans le domaine du « cyber » et veille à son déploiement[34].

Toutefois le BNC a subi des oppositions de la part de l'Agence de sécurité interne[35] (*Shin Bet*). Cette dernière soutenait l'idée que l'action contre les pirates devait être prise de manière proactive pendant les stades d'organisation et de planification, plutôt que réactive. Le 21 septembre 2014, après presque deux ans de bataille entre le *Shin Bet* et le BNC, le Premier ministre Netanyahou a rejeté les recommandations du service de sécurité du *Shin Bet* et a annoncé la création d'une nouvelle autorité opérationnelle pour la cyberdéfense : l'Autorité opérative de cyberdéfense (AOCD)[36]

32. National Cyber Initiative - Special Report for the Prime Minister (The State of Israel, Ministry of Science and Technology, the National Council on Research and Development and the Supreme Council on Science and Technology, eds.) 2011 (Hebrew).

33. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

34. *Idem 16*.

35. *Idem 16*. see also Ravid, Barak. 2014. "Batue Move in Israel's Cyber Turf War. Shin Bet Loses Authority over Civilian Space." Haaretz (September 21)

36. Opall-Rome, Barbara, "Schedule Slips on Israeli Cyber Defense Command ", Defense News (13 December 2014).

Conclusion

La question sur la réalité de la menace que constitue la cyberguerre ne cesse de se poser dans les milieux académiques et militaires. Est-ce une menace réelle ou exagérée ? Est ce qu'une cyber attaque peut être à l'origine d'un conflit de haute intensité ? De nombreuses questions qui sont aussi bien d'ordre politique que juridique, scientifique et militaire. Plusieurs pays les ont intégrées au cœur de leur stratégie de sécurité nationale. Certains considèrent que la cyberguerre n'aura jamais lieu, d'autres estiment que c'est une guerre qui se déroule au quotidien. Si Israël, par sa politique cyber fondée sur un engagement gouvernemental d'un part et par ses capacités technologiques d'autre part, est classé parmi les premiers pays dans ce domaine, d'autres pays ne vont pas tarder à rejoindre le cercle du cyber. Une des principales caractéristiques du cyber est son fort lien avec la « connaissance » et avec le « temps ». Dans ce sens, Dr Eviatar Matania, chef du BNC au Cabinet du Premier ministre israélien, prend en considération le facteur de rapidité du développement technologique. En parlant de la façon, pour Israël, d'aborder les questions liées au cyber, il précise[37] « *qu'il est important de venir avec une stratégie nationale du cyber qui pourrait durer cinq à dix ans sans besoin qu'elle soit ajustée à chaque fois qu'il y a un changement dans la technologie, mais qui serait encore assez souple pour faire face aux nouveaux développements* ».

37. Yonah Jeremy Bob, IDF 'cyber-chief' Moscovitch : Today's online attackers are gaining on the defenders, *The Jerusalem Post*, April 9, 2014.