2015

ÉTUDES DE L'IRSEM

Numéro 38

QUELLES STRATÉGIES FACE AUX MUTATIONS DE L'ÉCONOMIE DE DÉFENSE MONDIALE ?

Sous la direction
d'Aude-Emmanuelle FLEURANT

IRSEM
Institut de Recherche Stratégique de l'Ecole Militaire

QUELLES STRATÉGIES FACE AUX MUTATIONS DE L'ÉCONOMIE DE DÉFENSE MONDIALE ?

Sous la direction d'Aude-Emmanuelle FLEURANT
Responsable du groupe de jeunes chercheurs de l'IRSEM en Armement et Économie de défense

Avril 2015

Pour citer cette étude :

Aude-Emmanuelle FLEURANT (dir.), Quelles stratégies face aux mutations de l'économie de défense mondiale ?, Étude de l'IRSEM n° 38, avril 2015.

Nota bene :
Cette étude fait suite à une conférence qui s'est tenue à l'École militaire le 20 septembre 2013.

DERNIERES ETUDES DE L'IRSEM

37- Les sanctions contre la Russie ont-elles un effet dissuasif ?
Céline MARANGÉ

36- La stratégie américaine en Afrique
Maya KANDEL (dir.)

35- Approche globale et Union européenne : le cas de la corne de l'Afrique
Général de division (2S) Maurice de LANGLOIS (dir.)

34- Opinion publique et armées à l'épreuve de la guerre en Afghanistan
Barbara JANKOWSKI

33- La puissance russe au Moyen-Orient : Retour ou déclin inéluctable ?
Clément THERME

32- Les stratégies du *smart power* américain : Redéfinir le leadership dans un monde post-américain
Maya KANDEL et Maud QUESSARD-SALVAING (dir.)

31- L'action extérieure de l'Europe à l'épreuve de l'Égypte et de l'Afrique
Chantal LAVALLEE

30- Accès aux espaces communs et grandes stratégies : vers un nouveau jeu mondial
Frédéric RAMEL

29- États-Unis : quelle transition stratégique ? La politique de défense sous Obama entre dynamiques internes et évolutions internationales
Maya KANDEL (dir.)

28- La Turquie au Moyen-Orient : l'apprentissage de la puissance
Gilles RIAUX (dir.)

27- Réflexions sur la crise libyenne
Pierre RAZOUX (dir.)

26- Francophonie et profondeur stratégique
Niagalé BAGAYOKO et Frédéric RAMEL (dir.)

25- Les défis stratégiques africains : exploration des racines de la conflictualité en Afrique centrale
Amandine GNANGUENON (dir.)

PRESENTATION DE L'IRSEM

L'Institut de recherche stratégique de l'École militaire (IRSEM) a pour mission de promouvoir la recherche sur les questions de défense et d'encourager une nouvelle génération de chercheurs. L'ensemble de ses productions et de ses activités peut être suivi sur son site :

@ : www.defense.gouv.fr/irsem

: http://tinyurl.com/ke3p8l7

: @IRSEM1

: *http://tinyurl.com/nr8qkz8*

AVERTISSEMENT
Les opinions émises dans ce document n'engagent que leurs auteurs.
Elles ne constituent en aucune manière une position officielle du ministère de la défense.

BIOGRAPHIE

Aude-Emmanuelle Fleurant est directrice du programme Armement et dépenses militaires au *Stockholm International Peace Research Institute* (SIPRI). Avant de rejoindre le SIPRI, elle a dirigé le domaine d'études Armement et économie de défense à l'Institut de recherche stratégique de l'École militaire. Elle travaille sur les enjeux d'économie et d'industrie de défense depuis 1995. Son expertise couvre notamment l'analyse des tendances budgétaires, l'étude des questions industrielles de défense, ainsi que des questions de commerce international des armes et de contrôle d'exportation.

SOMMAIRE

SYNTHESE

Quelles stratégies face aux mutations de l'économie de défense mondiale ?

Sous la direction de :

Aude-Emmanuelle FLEURANT, directrice du Programme *Arms and Military Expenditure* au SIPRI

Cette étude est le fruit d'une réflexion initiée en 2012 au sein du groupe des jeunes chercheurs en « Armement et économie de défense » associés à l'Institut de recherche stratégique de l'École militaire (IRSEM), sous la direction d'Aude-Emmanuelle Fleurant. Elle détaille les stratégies mises en place par les États et les entreprises dans le contexte des transformations qui ont affecté le marché mondial de l'armement et les budgets publics de défense depuis les années 1990.

En tant que régulateurs, clients et parfois producteurs, les États demeurent des acteurs centraux du marché de la défense. La première partie de l'étude se place de leur point de vue. S'adaptant à l'évolution du contexte international, et dans certains cas national, les pays importateurs d'armement comme les pays du Golfe ont modifié leurs sources d'approvisionnement, altérant le rapport de force entre pays producteurs et acheteurs. Conscients que cette reconfiguration exacerbe la concurrence internationale, les États disposant d'une industrie d'armement de premier rang mettent en œuvre des politiques visant à faciliter et soutenir les exportations de leurs entreprises domestiques. Leur marge de manœuvre étroite au plan budgétaire en pousse certains à se tourner vers la coopération. Néanmoins, s'accorder sur une politique industrielle bilatérale requiert de surmonter les rivalités industrielles, d'harmoniser les pratiques, et, surtout, d'accepter les interdépendances. Une autre voie consiste à en revenir aux politiques industrielles, d'autant que de nouvelles menaces, comme celles provenant du cyberespace, créent une demande totalement nouvelle en matière de défense et d'armement, et requièrent une direction et un soutien étatique. Cela ne signifie pas pour autant l'absence du secteur privé, qui joue un rôle central dans la lutte contre les cybermenaces, particulièrement lorsqu'il est question de la protection des infrastructures critiques. C'est pourquoi l'étude défend l'idée qu'une politique dans ce domaine ne saurait être efficace si elle n'inclut pas les acteurs privés.

Ce dernier exemple illustre le fait que les changements affectant la demande des États et leurs priorités ont d'importantes conséquences sur l'industrie qui dessert les besoins en matière de défense. La seconde partie de l'étude, consacrée à l'offre, montre que la combinaison des évolutions budgétaires et sécuritaires des puissances industrielles militaires européennes et des États-Unis a conduit les grands acteurs de l'industrie de défense à élargir leur champ d'action et à s'investir dans les marchés dits « adjacents », notamment celui lié à la sécurité nationale. La trajectoire des budgets d'investissement (achats et R&D) pousse également les grands maîtres d'œuvre à redoubler d'efforts pour exporter là où se trouve la croissance, et à réduire leurs coûts en s'approvisionnant auprès de fournisseurs moins chers. Cette approche a pour conséquence une internationalisation accrue de ces entreprises, notamment via le recours à des chaînes de valeurs mondiales pour les petits composants, mais aussi forcée par les demandes de compensations soutenant les ambitions de création de capacités nationales des pays importateurs.

En Europe, contribuer au développement d'industries militaires dans d'autres régions du monde, via les transferts de technologie, inquiète quant à la capacité de maintenir un avantage technologique de défense. En effet, les pays misent sur l'innovation, et si possible de rupture, pour détenir un avantage opérationnel décisif et un avantage concurrentiel sur le marché international. Ces deux postulats sont toutefois questionnés et il est montré comment ils orientent et restreignent le type d'innovation ainsi produit – innovation marchande et concurrentielle. La réflexion est affinée au niveau micro-économique pour dévoiler comment la logique de l'activité de production militaire tend à favoriser en réalité l'innovation incrémentale dans les entreprises de défense au détriment de l'innovation de rupture.

ABSTRACT

Changes in the global defence economy: strategies to adopt

Under the supervision of:

Aude-Emmanuelle Fleurant, head of the *Arms and Military Expenditure* Programme, SIPRI (Stockholm International Peace Research Institute)

This study is the result of a discussion initiated in 2012 among a group of young researchers in the field of "Arms and Defence Economics", who are associated with the Institute for Strategic Research of the Ecole Militaire (IRSEM), under the direction of Aude-Emmanuelle Fleurant. It takes a look at the strategies established by states and businesses in the context of the transformations that have affected the global arms market and national defence budgets since the 1990s.

Acting as regulators, clients and sometimes producers, states continue to play the leading roles in the defence market. The first part of the study looks at the situation from their perspective. Adapting to the changing international – and in some instances national – context, countries that import arms, such as the Gulf countries, have changed their supply sources, thus altering the balance of power between producer and purchaser countries. Countries with first class arms industries are aware that this reconfiguration exacerbates international competition, and are implementing policies that aim to facilitate and support the exports of their national companies. Due to their limited flexibility in budgetary terms, some decide to enter into cooperation initiatives. However, coming to agreement on a bilateral industrial policy requires overcoming industrial rivalry, harmonising practices and especially, accepting interdependency. Another method involves returning to industrial policies, especially as new threats, such as those posed by cyberspace, create entirely new demand in terms of defence and arms, and require state-led direction and support. This does not mean, however, that the private sector will be left out. It plays a key role in combating cyber threats, in particularly when protecting critical infrastructures. This is why this study defends the idea that a policy in this field cannot be effective if the private sector is not included.

This last example illustrates the fact that the changes affecting state demand and their priorities have significant consequences on the industry that serves defence-related needs. The second part of the study, which deals with supply, shows how the combination of budgetary and security changes among European military industry powers and the United States has caused the major players of the defence industry to expand their scope of action and invest in what are known as "adjacent" markets, namely those connected to national security. The trajectory of investment budgets (spending and R&D) also compels the major contractors to double their efforts to export to places experiencing growth, and to reduce their costs by sourcing materials from cheaper suppliers. This approach results in the increasing internationalisation of these companies, in particular by resorting to global value chains for small parts; but they are also compelled to internationalise by the demands for trade-offs that sustain the ambitions of importing countries to create their own domestic capacities.

In Europe, contributing to the development of military industries in other regions of the world through technology transfer is a cause for concern in terms of the ability to maintain a technological advantage in defence. These countries count on innovation, and if possible breakthrough innovation, to maintain a key operational advantage and a competitive advantage on the international market. These two premises are called into question, however, and we can see how they orient and restrict the type of innovation this produces – market-oriented, competitive innovation. The study takes a detailed look at the microeconomic aspect to explain how the military production process tends to encourage incremental innovation in defence industries at the expense of breakthrough innovation.

■ VERS UN CHANGEMENT STRUCTUREL DE L'ECONOMIE DE DEFENSE MONDIALE ?

Aude-Emmanuelle FLEURANT

Directrice, Arms and Military Expenditure Programme
SIPRI

L'économie de défense mondiale est en pleine transformation. Amorcé à la fin des années 1980, le processus touche l'ensemble du marché mondial des armements, que ce soit les dépenses militaires des États (la demande), l'industrie qui dessert les besoins des forces armées (l'offre). Les grandes phases d'adaptation[1] qui ont structuré les premières décennies post-Guerre froide ont ainsi considérablement modifié le profil du marché. La troisième phase, provoquée par les impacts de la crise économique et financière de 2008, est toujours en cours. Elle agit simultanément comme révélateur et accélérateur des mutations démarrées au tournant des années 1990, notamment le remodelage de l'industrie occidentale. Elle introduit également de nouvelles dynamiques, comme l'internationalisation des grands maîtres d'œuvre de la défense, dont les impacts et la pérennité restent, pour le moment, difficiles à apprécier.

Cette introduction poursuit deux objectifs. Il s'agit d'abord de présenter les grandes tendances de l'économie de défense des 25 dernières années et ensuite de fournir quelques éléments de contexte pour la collection de textes qui composent cette étude collective. Cette dernière est le fruit d'une réflexion collégiale démarrée en 2012 par le groupe des jeunes chercheurs sur les armements et l'économie de défense associés à l'Institut de recherche stratégique de l'École militaire (IRSEM). Les analyses originales proposées dans cette étude s'appuient en effet sur les travaux menés par des doctorants issus de plusieurs disciplines (management, science politique, économie, histoire, etc.) ayant choisi de consacrer leur thèse à des problématiques propres au champ de l'économie de défense.

Ce chapitre introductif procède en quatre temps. Le premier décrit l'érosion graduelle de la domination occidentale dans les dépenses militaires mondiales au profit d'autres régions du monde. Comme les ressources allouées à la défense constituent les fondations de l'économie de défense, ses principales évolutions affectent l'ensemble des facettes du marché. Le second temps s'intéresse à l'industrie et à la manière dont elle s'adapte à ces transformations. On y verra que les stratégies qu'elle met en œuvre pour ajuster ses activités à de nouveaux paramètres d'action alimentent à leur tour le processus de transformation global. Le troisième temps se consacre à la dynamique des transferts mondiaux d'armements. Ces derniers reflètent une des facettes de la dynamique des dépenses militaires – celle liée à la demande émanant d'États importateurs – et jette un éclairage révélateur sur le comportement des firmes et des États. Enfin, le quatrième et dernier temps introduit les thématiques abordées par les textes composant cette étude.

[1] Généralement, la littérature reconnait deux grandes phases d'adaptation de l'économie de défense. La première couvre les années 1990 et est généralement identifiée comme celle des « dividendes de la paix ». La seconde fait davantage référence aux années 2000 jusqu'à la crise.

Les grands paramètres 1 : la lente migration des pôles de croissance des dépenses militaires

En 2013, les États-Unis et les grands pays d'Europe occidentale[2] sont, en valeur absolue, toujours les pays consacrant le plus de ressources à leur défense[3]. Ensemble, ils représentent 54 % des dépenses militaires mondiales. Les facteurs expliquant la domination de ces États se trouvent dans leur cheminement historique, dans les choix faits au lendemain de l'effondrement du bloc communiste et dans les déploiements militaires importants des années 2010.

La majeure partie des États occidentaux a en effet hérité des années de Guerre froide d'imposants appareils militaires, résultats des investissements significatifs consentis pendant la rivalité est-ouest. Malgré un recul notable dans l'ère post-Guerre froide, notamment en Europe, l'effort de défense dans ces États s'est maintenu à un niveau relativement élevé au cours des deux dernières décennies. Plusieurs pays ont en effet continué de mobiliser une part de leur richesse nationale demeurée importante pour conserver un outil de défense — rationalisé et remodelé — venant en soutien à des politiques étrangères et de sécurité faisant encore une large place à la puissance militaire et à la capacité de projection de la force. Enfin, certains d'entre eux se sont engagés dans les opérations majeures et coûteuses des années 2000, ce qui a contribué à maintenir leurs budgets à des niveaux élevés pendant cette période.

La disparition de l'URSS et l'effondrement complet de ses dépenses militaires laissent *de facto* les États-Unis et les puissances européennes au sommet du classement mondial et ce, malgré la réduction sensible de leurs budgets dans les années 1990. Comme le montre la figure 2, la part du total mondial représentée par les dépenses militaires de l'URSS/Russie et des pays d'Europe centrale et orientale passe de 28 % en 1988 à 5 % en 2001, et malgré une augmentation majeure des budgets de défense opérée par Moscou depuis le début de la décennie 2000 (figure 3), la part de la Russie dans le total mondial a modestement augmenté (7 % en 2013).

Les États-Unis restent donc, et de loin, le pays qui attribue le plus de ressources à son outil de défense, que ce soit en valeurs relatives ou absolues. La mise en œuvre de nouvelles doctrines d'emplois des forces dans le cadre de la « révolution dans les affaires militaires », privilégiant le recours à des technologies de pointe, notamment des systèmes d'information, de communication et de guidage (précision) y introduit une nouvelle génération d'armements coûteux et fait repartir les dépenses en achat d'équipement à la hausse en 1999, après cinq années de décroissance majeure (-56 % entre 1993 et 1998). Les deux guerres menées par Washington dans les années 2000 viennent doper ces augmentations. De son côté, l'Europe de l'Ouest affiche une stabilité relative en termes de ressources consacrées à la défense. Malgré le fait que les puissances militaires du Vieux Continent adoptent elles aussi la RAM, sa doctrine d'emploi des forces et les technologies qui lui sont associées, les investissements dans de nouveaux systèmes d'armes ne se traduisent pas par des croissances particulièrement prononcées de leurs budgets de défense qui restent plutôt stables pendant la décennie 2000 (figure 3).

[2] Allemagne, France, Italie, Royaume-Uni en particulier, auxquels on peut ajouter la Suède et l'Espagne.

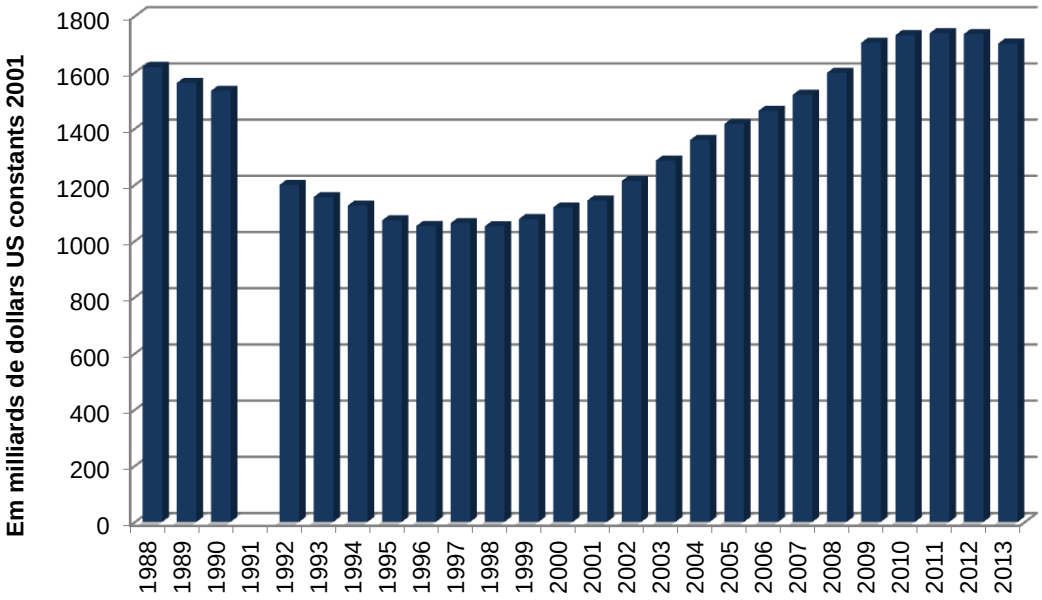
[3] Ce portrait serait sensiblement différent si d'autres indicateurs, comme la ponction des dépenses militaires dans le PIB, étaient utilisés.

On constate donc, depuis la fin de la Guerre froide, une perte de vitesse de l'Europe occidentale dans le total des dépenses militaires mondiales. Ce ralentissement se réalise au profit d'un rehaussement sensible du poids de l'Asie (de 19 % en 2001 à 24 % en 2013), une croissance ayant pour principaux moteurs les budgets conséquents de la Chine et de l'Inde pendant la période.

Tenant compte de la croissance de près de 49 % des dépenses totales entre 2001 et 2013 (figure 1), cela signifie donc un déclassement du Vieux Continent par rapport à sa position des années précédentes. On peut donc en déduire que l´érosion de la position occidentale dans le total mondial est en bonne partie imputable au dynamisme de l'Asie en matière de dépenses de défense et à la faiblesse de la croissance en Europe.

Dans pratiquement toutes les autres régions du monde (figure 3), des croissances économiques nationales appréciables pendant la décennie 2000 ainsi que les nouvelles ambitions régionales, voire globales, au plan sécuritaire de certains États mènent à des augmentations des dépenses militaires. Une partie de ces hausses soutient des programmes d'acquisition majeurs qui ciblent simultanément deux objectifs principaux à savoir : 1) le renouvellement de flottes d'armements désuètes ou en fin de vie utile; 2) la volonté d'accompagner ces politiques de puissance par des capacités nationales de production d'armements modernes susceptibles de renforcer l'autonomie stratégique par rapport aux pays technologiquement les plus avancés.

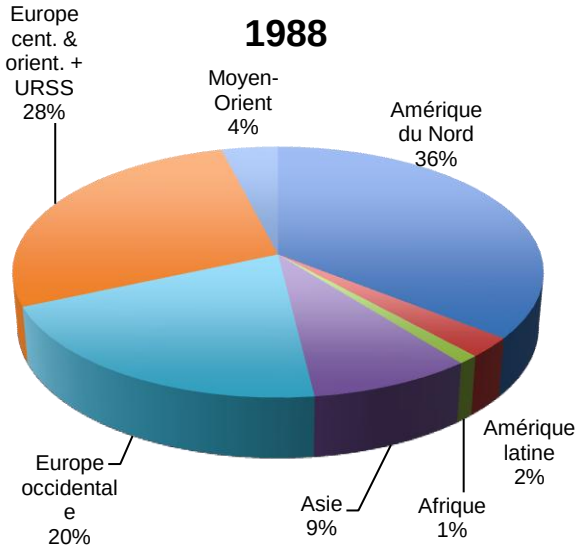
Figure 1. Évolution des dépenses militaires mondiales 1988-2013* en milliards USD de 2011



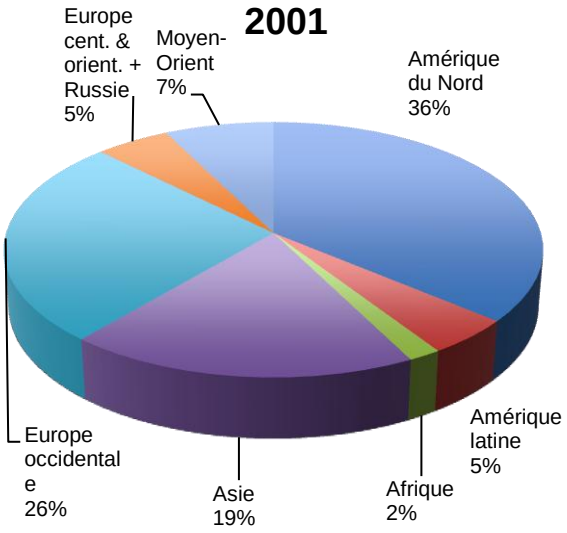
* L'absence de données pour l'ex-URSS/Russie et pour les pays membres du Pacte de Varsovie rend impossible de fournir un chiffre fiable pour 1991.

Source : SIPRI 2013.

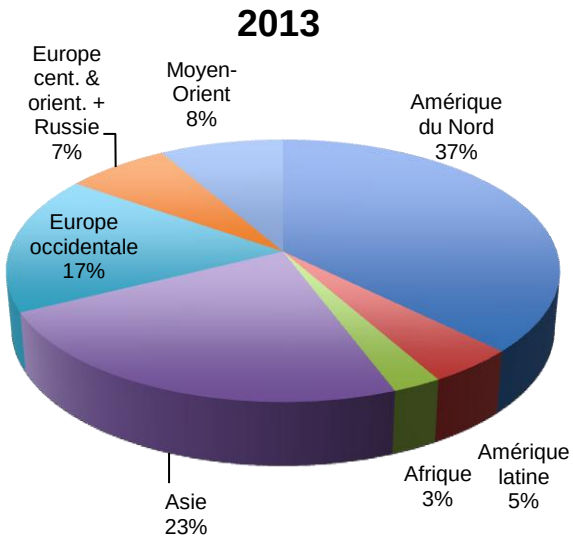
Figure 2. Comparaison de la part des grandes régions dans les dépenses militaires totales en 1988, 2001 et 2013, en pourcentages



Total mondial 1619 milliards USD



Total mondial 1144 milliards USD

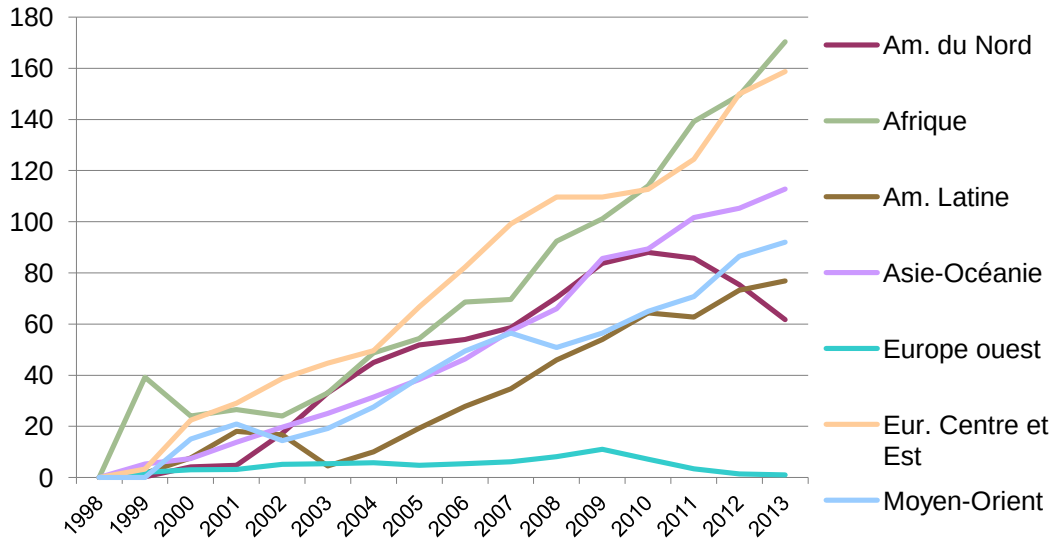


Total mondial 1702 milliards USD

*Calculs faits sur la base de dollars US constants, 2011

Source : SIPRI 2013

Figure 3. Évolution des dépenses militaires par région, 1998-2013, base 100, en pourcentages



Source : SIPRI 2013.

Les grands paramètres 2 : des stratégies d'entreprises qui modifient le profil du marché

Encore aujourd'hui, le cœur des capacités industrielles et technologiques de défense les plus avancées est concentré au sein d'une poignée d'États occidentaux. Les entreprises américaines, françaises, britanniques et italiennes (et indirectement allemande via EADS/Airbus)[4] qui forment, année après année, les dix principaux fournisseurs mondiaux d'armements n'ont pratiquement pas bougé du classement depuis 2002. Cette stabilité n'est pas réellement surprenante, ces groupes bénéficiant d'une préférence nationale et captant régulièrement les projets les plus lucratifs et les plus techniquement audacieux proposés par leurs ministères de défense. On est également en mesure d'observer qu'à valeur constante, leur chiffre d'affaires défense combiné a augmenté d'approximativement 25,3 % entre 2002 et 2013[5].

Pour les firmes américaines qui composent le top 10 (6 sur 10), cette croissance appréciable est partiellement à mettre au compte de l'impulsion donnée par les dépenses liées à l'effort de guerre. On peut également identifier comme moteur des hausses la croissance externe (fusions et acquisitions) qui a continué de caractériser la stratégie de plusieurs de ces groupes dans les années 2000. Deux des quatre firmes du Vieux Continent qui se classent parmi les dix premiers mondiaux (BAE et Finmeccanica) ont également significativement augmenté leur présence dans le marché américain pendant la décennie 2000, bénéficiant de la forte croissance du budget de défense américain en acquisition ainsi que des dépenses liées aux opérations d'Afghanistan et d'Irak.

Collectivement, les pays européens ne font pas les mêmes choix en matière budgétaire pendant cette période. Bien que certains États, notamment le Royaume-Uni, l'Espagne et l'Italie, se soient pleinement engagés dans les opérations d'Afghanistan et d'Irak, et qu'ils aient augmenté leurs dépenses militaires en conséquence, le phénomène n'est pas comparable à ce qu'on observe aux États-Unis.

De plus, à l'exception de certains segments spécifiques, notamment l'armement terrestre, cette croissance ne soutient pas les budgets d'achats. Ainsi, la faible augmentation des comptes d'investissements (achats et R&D) dans les puissances militaires européennes pendant la décennie, combinée à une forme de rigidité budgétaire créée par les opérations outre-mer, met l'industrie dans une position difficile.

Dans ce contexte, celle-ci met en œuvre des stratégies d'adaptation comportant généralement deux grands piliers. Le premier est incarné par un effort renouvelé sur les marchés d'exportation pour y remporter les gros marchés (navires, avions de combat, etc.) ; le second par une volonté de diversification vers des activités considérées comme adjacentes au cœur de métier ou vers des segments en émergence. Le domaine de la sécurité nationale devient ainsi une composante des portefeuilles de tous les grands groupes de défense[6]. Le « *continuum* défense sécurité » couvre ainsi

[4] Aude-Emmanuelle Fleurant et Sam Perlo-Freeman, "The SIPRI Top 100 Arms-Producing and Military Services Companies, 2013", *SIPRI Fact Sheet*, décembre 2014.

[5] On retrouve les mêmes compagnies dans le top 10 de 2002 et dans celui de 2013. Les chiffres d'affaires défense de celles-ci sont en dollars US constants de 2013.

[6] Vincent Boulanin, *De la défense à la sécurité: aspects économiques et enjeux politiques de la diversification des firmes européennes d'armement dans le domaine de la sécurité,* Thèse de doctorat, EHESS, Paris, non publiée, 2014.

ces activités chevauchant les besoins militaires et davantage liés à la sécurité nationale et civile, comme la cybersécurité.

Comme le montre très clairement la figure 3, la période 1998-2008 est également caractérisée par une croissance relative très appréciable des dépenses militaires dans le « reste du monde ». Cette dynamique ne passe pas inaperçue dans les puissances industrielles militaires européennes, qui voient dans ces marchés l'occasion de compenser la faiblesse des investissements nationaux. Des groupes comme TKMS, Thales et Navantia remportent d'importants contrats à l'export pendant les années 2000. Ces derniers sont cependant accompagnés de demandes de compensations industrielles – souvent appelées *offsets* - visant à soutenir la création de capacités nationales de production d'armement. Concrètement, ces demandes se traduisent par la production locale des systèmes sous licence, jusqu'à la création de co-entreprises (*joint ventures*), la transmission de savoir-faire via la formation des employés des firmes partenaires. Ainsi, plusieurs des pays qui font croître leurs dépenses de défense et qui se tournent vers l'importation disposent de capacités limitées de production d'armement et cherchent à tirer parti de ces transactions pour en créer et/ou pour moderniser celles dont ils disposent. Il faut également souligner que ces efforts d'exportation sont soutenus par les États dans lesquels ces entreprises ont leur siège social.

Selon le cabinet spécialisé IHS Jane's, les politiques de compensations tendent à « proliférer » depuis le début des années 2000. Ces demandes poussent les entreprises exportatrices à s'engager de manière durable dans les pays clients pour réaliser leurs *offsets*. Pour le moment, cette observation s'applique moins aisément aux entreprises américaines, qui bénéficient encore de commandes nationales capables de soutenir leurs activités et qui, en conséquence, peuvent se permettre d'être plus sélectives en matière d'exportation.

Cependant, plusieurs initiatives récentes, comme la réforme des règles encadrant les exportations d'armes américaines, tendent à indiquer que des changements se préparent sur le plan du commerce mondial des armes.

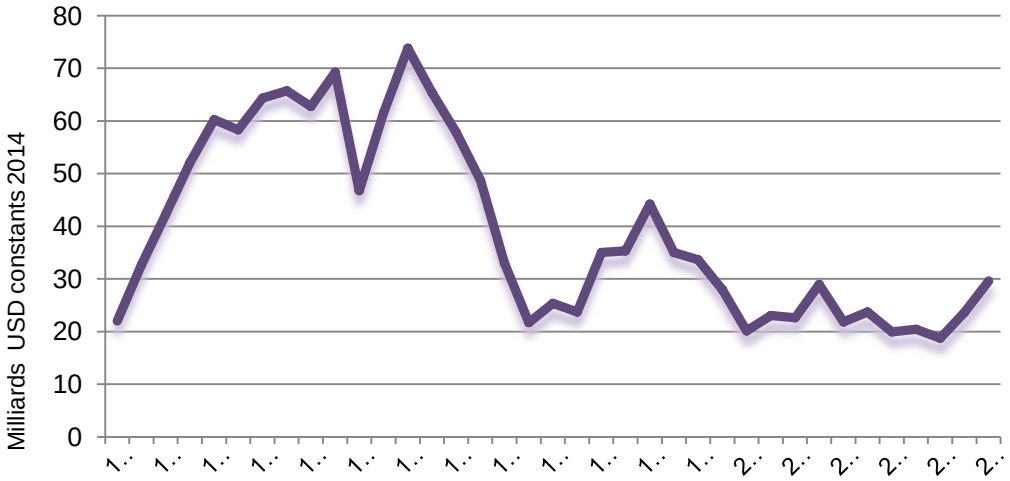
Les grands paramètres 3 : le commerce international de défense

Cette dynamique entre importateurs et exportateurs se matérialise dans un environnement où le volume du commerce mondial des équipements de défense, soit les transferts d'État à État, a reculé de manière significative depuis la Guerre froide. Comme le montre la figure 4, depuis le pic des années 1980, les transferts mondiaux d'armements ont diminué de près de la moitié de ce qu'ils représentaient dix ans plus tôt et se sont stabilisés aux niveaux de ceux de 1975[7]. Même si les données plus récentes fournies par le SIPRI indiquent des augmentations relatives très importantes (figure 5), cette évolution paraît aller à contresens de ce qui est décrit dans les sections précédentes.
Deux grands facteurs expliquent ce phénomène. D'abord, la fin de la logique de blocs mène à un effondrement de l'offre du second plus important exportateur d'armes mondial, l'URSS. En éliminant la principale menace, la fin de la bipolarité conduit aussi à une forte diminution de la demande des pays alignés, que ce soit avec les États-Unis ou avec l'Union soviétique. Par exemple, plusieurs

[7] L'importante hausse observable de 2009 à 2011 est essentiellement imputable à d'importantes livraisons faites par les entreprises américaines à l'Arabie saoudite pendant cette période.

importateurs majeurs en Occident, comme le Canada et les Pays-Bas, annulent certains programmes coûteux planifiés dans les années 1980, faisant globalement descendre le niveau des transferts mondiaux. Ensuite, malgré les croissances de dépenses militaires dans des régions encore très importatrices (figure 3), on observe que les volumes de transferts affichés pendant les années 2000 restent globalement stables, entre 20 et 30 milliards de dollars approximativement. Cela peut s'expliquer, dans un premier temps par le fait que pour certains des plus importants clients, des délais importants sont observables dans la mise en œuvre de certains projets même si des sommes ont déjà été engagées (cas de l'Inde par exemple). Dans un second temps, on peut aussi penser que la volonté de créer des capacités de production a canalisé une partie de ces dépenses vers des entreprises nationales (cas du Brésil).

Figure 4. Évolution des transferts mondiaux d'armements, 1975-2011, en milliards USD constants de 2014



Source : à partir de Grimmett 1981 à 2012 en valeur de livraisons

Il est toujours risqué de prédire l'avenir dans le champ de l'économie de défense, mais compte tenu des tendances de fond (re)façonnant l'offre et la demande exposées plus haut, on peut penser que la croissance des ventes internationales démarrée en 2009 va se poursuivre dans les prochaines années. Les données compilées par le SIPRI pour la période 2009-2013[8], indiquent d'ailleurs que les transferts d'armes ont augmenté de 14 % sur la période. Une hausse semble d'autant plus plausible que les situations sécuritaires de régions traditionnellement importatrices (Asie, Moyen-Orient) sont tendues, et qu'une partie de la réponse adoptée par les États dans ces environnements est de se procurer des armements.

Compte tenu de la situation observée dans les marchés occidentaux et particulièrement en Europe, on observe donc un durcissement de la concurrence pour l'obtention des plus importants marchés, ce qui se traduit par un rapport de force favorable aux pays importateurs, comme il a été évoqué dans la partie sur l'offre.

[8] Le SIPRI utilise un indicateur qui lui est propre – le *Trend Indicator Value* (TIV) – pour mesurer les ventes internationales de matériel de défense. Dans cette optique, les données produites par l'Institut ne sont pas comparables à celles proposées par le *Congressional Research Service* et utilisées pour la figure 4.

Conclusion : un processus multidimensionnel

Ce sont les phénomènes issus de ce processus de transformation qui font l'objet de la présente étude. Les textes qui y sont regroupés, tous produits par des candidats et des candidates au doctorat et de jeunes docteurs, jettent un éclairage précieux sur la diversité et la complexité des dynamiques à l'œuvre. La première partie s'intéresse plus particulièrement aux États qui, agissant comme régulateurs, clients et parfois producteurs, demeurent des acteurs centraux du marché de la défense et représentent donc des moteurs des changements étudiés. Par exemple, l'étude du cas des pays du golfe arabo-persique réalisée par Emma Soubrier montre que le rôle politique et sécuritaire que souhaitent aujourd'hui jouer de nombreux pays importateurs a changé de manière concomitante avec les évolutions stratégiques et géoéconomiques régionales et mondiales, ce qui conditionne des postures visant à acquérir davantage d'autonomie en matière d'approvisionnement de matériel de défense et en conséquence, des dépenses d'acquisition élevées.

Combinée à la faiblesse relative des budgets d'achats en Europe et dans une moindre mesure des États-Unis, cette configuration modifie le rapport de force entre pays exportateurs et importateurs. Les chapitres de Hugo Meijer et de Lucie Béraud-Sudreau montrent en effet que les grands exportateurs comme les États-Unis et la France, sont pleinement conscients des défis posés par cette configuration, notamment celui de l'accroissement de la concurrence. En conséquence, ils mettent en œuvre des politiques visant à faciliter (Meijer) et à soutenir (Béraud-Sudreau), le rayonnement et l'action de leurs firmes nationales pour maximiser leurs chances de remporter les marchés grand export.

D'un autre point de vue, les défis posés plus particulièrement en Europe par des budgets d'achats sous contrainte poussent les États disposant d'une industrie d'armement à mettre en place des stratégies visant à la fois à composer avec une marge de manœuvre étroite au plan budgétaire et à soutenir les capacités de production, comme le montre Alice Pannier dans son texte sur la coopération franco-britannique.

Cela se traduit notamment par un regain d'intérêt envers l'élaboration de politiques industrielles, un intérêt qui s'étend également aux besoins qui émergent de nouvelles menaces comme celles provenant du cyberespace qui, comme l'explique Alix Desforges, crée une demande totalement nouvelle en matière de défense et d'armement qui nécessite une direction et un soutien de la part de l'État. Cela ne signifie pas pour autant que le secteur privé soit complètement absent de ces discussions. Approchant la problématique de la cybersécurité sous l'angle industriel, Danilo D'Elia met en lumière le rôle central de l'entreprise privée dans la lutte contre les cybermenaces, particulièrement lorsqu'il est question de la protection des infrastructures critiques. Dans cette optique, il estime que la réflexion sur la meilleure manière d'approcher le domaine doit inclure les acteurs privés.

Ce dernier exemple illustre clairement le fait que les changements affectant la demande des États et leurs priorités ont d'importantes conséquences sur l'industrie qui dessert les besoins en matière de défense. Comme le montre Vincent Boulanin dans la seconde partie de l'étude consacrée à l'offre, la combinaison des évolutions budgétaires et sécuritaires dans les puissances industrielles militaires européennes et aux États-Unis a conduit les grands acteurs de l'industrie de défense à élargir leur champ d'action et à s'investir dans les marchés dits « adjacents », notamment celui lié à la sécurité nationale.

La trajectoire des budgets d'investissements (achats et R&D) pousse également les grands maîtres d'œuvre à redoubler d'efforts pour exporter là où se trouve la croissance, et à réduire leurs coûts en s'approvisionnant auprès de fournisseurs moins chers. Cette approche a pour conséquence, comme Paul Hérault l'explique, une internationalisation accrue de ces entreprises notamment via le recours à des chaînes de valeurs mondiales pour les petits composants, mais aussi forcée par les demandes de compensations soutenant les ambitions de création de capacités nationales des pays importateurs.

En Europe, le fait de contribuer à la création d'industries militaires plus performantes dans d'autres régions du monde inquiète quant à la capacité de maintenir un avantage technologique de défense via la réalisation de nouvelles générations d'armement conférant un avantage technique décisif à leurs forces armées.

Aujourd'hui, ce sujet donne lieu à un vaste débat auquel Sophie Lefeez contribue en explorant les principaux moteurs de l'innovation de défense par le biais d'une approche pluridisciplinaire. Elle questionne ainsi les postulats qui fondent la nécessité d'un avantage technique sur l'adversaire et propose des pistes de réflexion quant à des approches alternatives de ce dossier capital tant pour l'industrie que pour les forces armées. Jérôme Rosello, de son côté, affine la réflexion au niveau micro-économique en montrant comment la logique de l'activité de production militaire tend à soutenir une préférence pour l'innovation incrémentale dans les entreprises de défense au détriment de l'innovation de rupture.

L'ECONOMIE DE DEFENSE DES PAYS DU GOLFE, ENTRE MAINTIEN DU STATU QUO ET VOLONTE D'AFFIRMATION

Emma SOUBRIER
Doctorante en Science politique à l'université d'Auvergne[9]

Introduction

Les pays du Golfe[10] ont toujours été des clients importants d'équipements de sécurité et de défense. Ceci tient à plusieurs déterminants, tels que le fait qu'ils soient assis sur des réserves considérables de pétrole et de gaz, leur position stratégique entre l'Asie, l'Afrique et l'Europe ainsi que l'environnement régional chargé en conflictualités potentielles dans lequel ils évoluent, notamment marqué par la présence des grands voisins iranien et irakien, perçus comme des menaces plus ou moins existentielles par les États de la Péninsule arabique.

Face à ces divers paramètres, les pétromonarchies du Golfe sont mues par deux préoccupations : assurer leur sécurité nationale contre des menaces conventionnelles ou asymétriques extérieures, mais aussi et surtout préserver la stabilité de leurs régimes.

Cette réalité duale s'est, dès le début, avérée « bénéfique » pour les industries de défense occidentales, et particulièrement celles des États-Unis. Il faut cependant noter que les règles régissant les marchés de défense dans la Péninsule arabique semblent aujourd'hui en pleine mutation. Après avoir brièvement défini les dynamiques traditionnelles de ces marchés, ce chapitre examine l'évolution des déterminants internationaux et domestiques des États du Golfe, lesquels poussent ces derniers à envisager de nouvelles stratégies sécuritaires (éloignement d'une trop grande dépendance à l'égard des États-Unis, multiplication des partenariats, montage d'un système de sécurité régional intégré) et modifient les logiques de leur économie de défense.

Règles du jeu traditionnelles des marchés de défense dans la Péninsule arabique

Au sein de leur « complexe de sécurité régional »[11] consolidé dans les années 1990[12], les pays du Golfe sont confrontés à un dilemme de sécurité consistant à équilibrer les menaces venant d'Irak et

[9] La recherche doctorale de l'auteur, qui porte sur l'évolution de la politique de défense et des stratégies d'acquisitions militaires du Qatar et des Émirats arabes unis, bénéficie du soutien financier de la Direction Générale de l'Armement (DGA) et de l'entreprise Airbus Defence & Space (ex-Cassidian).

[10] Ceux que l'on désigne ici par cette appellation sont les six pays qui forment le Conseil de Coopération du Golfe (CCG), c'est-à-dire l'Arabie saoudite, le Bahreïn, les Emirats arabes unis, le Koweït, le Qatar et Oman.

[11] « *Patterns* d'amis-ennemis (…) substantiellement confinés au sein d'une aire géographique spécifique » (Barry Buzan, *People, States and Fears*, Boulder, Lynne Rienner, 1991, p. 190) régis par des interdépendances tant positives que négatives et dont les « membres » passent « le plus clair de leur temps et de leurs efforts à se préoccuper les uns des autres et non d'États extérieurs » (Gregory Gause, *The International Relations of the Persian Gulf*, Cambridge, Cambridge University Press, 2009, p. 3-4). Nous utilisons ici le cadre théorique de Gregory

d'Iran. Dans ce contexte, les États-Unis sont rapidement devenus la principale garantie de protection de l'ensemble des pays du CCG, selon une apparente stratégie coopérative. En effet, en s'associant avec la puissance américaine d'autant plus naturellement que celle-ci était devenue, après la chute de l'URSS, la seule « méga-puissance » internationale, les pétromonarchies reposaient toutes implicitement sur les arrangements sécuritaires passés entre l'Arabie saoudite et les États-Unis[13]. Il est néanmoins intéressant de souligner que cette dynamique consistant à se placer sous le parapluie militaire américain peut être lue à différents niveaux d'analyse. Ainsi, les petites monarchies du Golfe, s'en remettant en apparence à l'Arabie saoudite et à ses alliances pour assurer leur sécurité et leur stabilité, ont également mis à profit la nouvelle répartition du pouvoir international pour dépasser leur problématique sécuritaire au sein même de la Péninsule arabique. Le Qatar et les Émirats arabes unis (EAU), par exemple, en signant respectivement des accords de coopération de défense bilatéraux avec les États-Unis en 1992 et 1994, assuraient aussi un équilibre contre une autre menace perçue, venant précisément de l'Arabie saoudite[14]. Il faut noter que la volonté de ces plus petits États du Golfe de défendre leur autonomie relative en termes de sécurité et de défense est également perceptible dans leur choix d'alliance au-delà de la seule puissance américaine. Ainsi, le Qatar et les EAU ont rapidement cherché à contrebalancer une trop forte dépendance à l'endroit de l'allié américain en signant des accords bilatéraux de défense avec la France et la Grande-Bretagne[15].

Les marchés de défense associés à ces dynamiques régionales sont intéressants à observer en cela que, pour les pays du Golfe, « la finalité des achats massifs d'armement [semble] moins militaire […] que diplomatique, ces ventes entretenant une attache avec les puissances extérieures » [16]. Il est en effet possible de considérer que les marchés créés dans la région étaient en fait l'un des pans d'un « échange de bons procédés » plus large : le pacte « pétrole contre sécurité ». Selon ce dernier, la sécurité des pays du Golfe était ainsi assurée par « un flot de pétrole à moindre coût et des investissements conséquents dans leur complexe militaro-industriel »[17]. Cette réalité s'explique par la prise de conscience par ces États de leur incapacité à assurer seuls leurs propres sécurité et stabilité. Dès lors, les acquisitions militaires des pétromonarchies peuvent être vues comme un instrument de politique étrangère visant effectivement à leur assurer une plus grande sécurité, mais seulement indirectement, à travers la garantie de protection qu'elles achetaient à leurs partenaires stratégiques.

Comme pour les accords de défense mentionnés auparavant, les pays du Golfe, particulièrement le Qatar et les EAU, se ménageaient par ailleurs une autonomie relative en diversifiant leurs

---

Gause pour qui l'Iran, l'Irak, l'Arabie saoudite, les plus petites monarchies du Golfe mais aussi les États-Unis forment le « complexe de sécurité régional » du Golfe persique.

[12] L'invasion du Koweït en 1990 a représenté une dure confrontation à la réalité pour les monarchies du Golfe : il leur est apparu qu'elles ne pouvaient pas compter sur la plus puissante d'entre elles, l'Arabie saoudite, et encore moins sur elles-mêmes, pour assurer leur propre sécurité et la stabilité de la région.

[13] Particulièrement le Pacte de Quincy, signé en 1945 entre l'administration américaine et la famille al-Saoud.

[14] Entretiens de l'auteur avec différents interlocuteurs issus des milieux institutionnels, académiques et industriels français dans les pays du Golfe entre mars 2013 et juin 2014.

[15] Chronologiquement, ces accords bilatéraux de défense furent signés ainsi : Qatar/France en 1994, EAU/France en 1995, EAU/Grande-Bretagne en 1996 et Qatar/Grande-Bretagne en 2006.

[16] Jean-Loup Samaan, « Les monarchies du Golfe : un marché d'armement sans armées ? », *Moyen-Orient*, n° 17, janvier-mars 2013, p. 53.

[17] Emma Soubrier, « Vers une redéfinition du complexe de sécurité régional ? », *dans* Emma Soubrier, (coord.), *Les pays du Conseil de coopération du Golfe : Nouvelles puissances du monde arabe ?*, Paris, Éditions du Cygne, 2014, p. 41.

fournisseurs et en signant également de nombreux gros contrats de défense et de sécurité avec la France et la Grande-Bretagne.

En lien avec ces remarques, il faut souligner que les pétromonarchies exprimaient difficilement leur conception propre des enjeux sécuritaires et stratégiques auxquels elles étaient confrontées. En conséquence, les États-Unis, la France et la Grande-Bretagne avaient tendance à les analyser à travers le prisme de leurs propres enjeux stratégiques et intérêts commerciaux et il a parfois été considéré que les industriels de la défense occidentaux pouvaient ainsi vendre « tout ce qu'ils voulaient dans le Golfe, tirant avantage et profitant du manque de connaissances de leurs clients »[18] . Il est possible de suggérer qu'une certaine indifférence des États clients était plus saillante qu'un réel manque de connaissances, étant donné que leurs acquisitions militaires remplissaient en tout état de cause leur principale mission, politique, aux yeux des décideurs locaux. Soulignons enfin qu'en raison de lacunes importantes de capacités de production industrielle locales, les marchés de la défense dans le Golfe étaient caractérisés par des importations de produits « sur étagère ».

Aujourd'hui, l'onde de choc des révoltes arabes et les éventuels repositionnements stratégiques d'acteurs internationaux dans la région, États-Unis en tête, redéfinissent les enjeux sécuritaires des pays du CCG. Par ailleurs, à ces déterminants internationaux répondent des attentes et objectifs internes aux États du Golfe qui sont également en pleine mutation. De la rencontre de ces deux niveaux d'évolution naissent de nouvelles logiques de l'économie de défense de ces pays, comme il sera montré plus loin.

Nouvelle donne régionale et internationale : un ensemble de défis et d'opportunités

Le Printemps arabe est considéré comme l'un des plus grands défis jamais lancés aux pays du CCG car ses événements ont à la fois un impact sur leur sécurité nationale – en alimentant l'instabilité régionale – et sur la stabilité de leur régime – en insufflant un vent de changement dans l'ensemble de la zone. Enfin, l'Iran se trouve à la croisée de ces deux dimensions sécuritaires. En effet, « les régimes de la péninsule craignent que le tumulte régional n'offre à Téhéran l'opportunité de les déstabiliser intérieurement et d'adopter une attitude plus offensive envers elles »[19] . Le meilleur exemple de l'entremêlement de ces dynamiques sécuritaires dans la lecture que font les pays du Golfe des bouleversements régionaux a été l'intervention armée des forces saoudiennes et émiraties au Bahreïn le 14 mars 2011. La déstabilisation par un mouvement de révolte populaire d'une monarchie consœur, membre du CCG, représentait en soi la matérialisation des craintes des pays du Golfe à l'égard de l'« effet domino » potentiel du Printemps arabe. La justification avancée par le royaume saoudien et la fédération des EAU pour leur intervention, sous la bannière du « Bouclier de la Péninsule » (composante militaire unifiée du CCG), n'était néanmoins pas celle-ci : il s'agissait, selon leur discours, de contrer la tentative d'instrumentalisation des populations chiites bahreïnies par l'Iran[20].

[18] Nadim Hasbani, "The Geopolitics of Weapons Procurement in the Gulf States", *Defense & Security Analysis*, vol. 22, n° 1, mars 2006, p. 81.

[19] Emma Soubrier, « Sécurité des monarchies du Golfe : de nouvelles règles du jeu ? », *Moyen-Orient*, n° 23, juillet-septembre 2014, p. 68.

[20] Sur ces questions, voir : Toby Matthiesen, *Sectarian Gulf: Bahrain, Saudi Arabia, and the Arab Spring That Wasn't*, Stanford, Stanford University Press, 2013.

Dans le même temps, les évolutions de l'échiquier régional représentent une opportunité pour les pétromonarchies du Golfe d'affirmer leur rôle de « nouvelles puissances du monde arabe ». En effet, les situations de conflits quasi-chaotiques environnantes (Irak, Syrie, Yémen) » offrent à ces pays l'opportunité de jouer « un rôle de premier plan dans les recompositions régionales en cours, même s'il s'exerce de manière confuse et pas toujours coordonnée »[21]. Ainsi, le Printemps arabe tend à les positionner comme « centre de gravité » du monde arabe, au moins tant que l'Égypte, l'Irak et la Syrie resteront affaiblis. Venant au secours des économies nationales, au sein du CCG (Bahreïn, Oman) comme dans le reste de la région (particulièrement en Égypte), les pays du Golfe – Arabie saoudite, Qatar et EAU en tête – ont su utiliser leur puissance économique au service d'une politique étrangère plus volontariste et affirmée qu'auparavant. Traditionnellement vue comme un moyen d'influence et de rayonnement, leur manne pétrolière et gazière semble aujourd'hui être devenue un véritable outil de puissance, visant à transformer les dynamiques régionales dans le but d'y défendre leurs intérêts[22]. Ceci leur semble peut-être d'autant plus nécessaire aujourd'hui que les pétromonarchies regardent évoluer les positionnements stratégiques d'acteurs internationaux dans la région avec un intérêt parfois teinté d'une certaine appréhension.

À cet égard, l'attention des pays du Golfe est particulièrement centrée sur l'évolution potentielle de la présence américaine dans la région. Compte tenu de l'agencement traditionnel de la sécurité des pétromonarchies sous parapluie américain, ces dernières considèrent avec beaucoup de suspicion la nouvelle donne qui semble pouvoir se mettre en place aujourd'hui.

Ainsi, les États-Unis, confrontés comme la plupart des États occidentaux à des problématiques budgétaires dans le secteur de la défense, sont suspectés par les pétromonarchies de vouloir réévaluer leur engagement dans le Golfe pour se dégager de ces contraintes. L'annonce américaine d'un pivot stratégique vers l'Asie ainsi que leur volonté de devenir non seulement indépendants énergétiquement, mais exportateurs nets de gaz ajoutent aux craintes des pétromonarchies concernant un hypothétique recul des États-Unis dans le Golfe. Soulignons que ces craintes sont aussi et surtout le reflet d'une méfiance croissante envers l'allié américain[23]. Il faut également noter que les nouveaux paramètres mentionnés pourraient représenter des opportunités pour les pays du Golfe.

Si les coupes budgétaires de défense aux États-Unis et dans la plupart des pays occidentaux sont considérées comme un facteur de risque potentiel quant à la présence future des grandes puissances internationales dans la région du Golfe, elles poussent plus généralement les dirigeants et les

[21] Fatiha Dazi-Heni, « Les monarchies du Conseil de Coopération du Golfe : acteurs incontournables dans un monde arabe en manque de puissance ? », *dans* Emma Soubrier (coord.), *Ibid.*, p. 29.

[22] Sur la *riyal politik* nouvellement proactive des pays du Golfe, voir : Emma Soubrier, « La diplomatie économique des pays du Golfe à l'aune du Printemps arabe : du rayonnement à la puissance », *dans* Frédéric Charillon, et Alain Dieckhoff, *Annuaire Afrique du Nord Moyen-Orient 2014-2015*, Paris, La Documentation française, 2014, p. 123-136.

[23] En 2003, les pétromonarchies ont considéré que l'intervention américaine avait servi l'Irak à l'Iran sur un plateau. Dernièrement, leur défiance a notamment été réactivée par le soutien américain à la révolte égyptienne, tout particulièrement perçu comme une trahison par le régime saoudien : « Les États-Unis ne sont pas vraiment un dieu déchu mais ses pouvoirs divins font assurément des déçus » (David Ignatius, "Saudi Arabia Expands its Power as US Influence Diminishes", *The Washington Post*, 18 novembre 2011, disponible sur : http://www.washingtonpost.com/opinions/saudi-arabia-expands-its-power-as-us-influence-diminishes/2011/11/18/gIQAX8wwZN_story.html, dernière consultation le 12 décembre 2014).

industriels de ces États à chercher plus de débouchés à l'export pour maintenir leur base industrielle de défense.
Dès lors, les pétromonarchies, qui font partie des plus gros clients mondiaux en la matière[24], sont encore plus courtisées qu'avant à cet égard, par les puissances traditionnellement présentes dans la région ainsi que par les BRICS.

Il faut en effet citer la présence accrue de ces derniers dans la zone, défendant des objectifs et intérêts propres. Les pays du Golfe pourraient d'autant plus vouloir jouer de cette course à l'export pour réorganiser leurs stratégies, tant en termes d'alliances que de processus d'acquisition, qu'ils sont aujourd'hui mus par de nouveaux déterminants internes et notamment par une volonté d'autonomisation vis-à-vis de leurs partenaires extérieurs.

De nouvelles stratégies sécuritaires possibles

Pour comprendre l'élan de réorganisation des partenariats et des pratiques qui semble animer aujourd'hui les pays du Golfe, il est important de rappeler que certains d'entre eux ont accédé à l'indépendance assez récemment (en 1971, après le retrait britannique, pour le Qatar, les EAU et Oman). Partant, la prise d'assurance et la volonté d'autonomisation qu'ils manifestent sont fortement liées à un processus logique de construction étatique. Cette dynamique a également été favorisée par le contexte de crise économique et financière internationale, dans lequel leur manne issue des hydrocarbures leur permet de s'affirmer au concert des nations comme de nouveaux acteurs incontournables. Il s'agit d'explorer la direction nouvelle que pourraient prendre les pétromonarchies à l'avenir pour assurer leur sécurité et stabilité.

Nous l'avons vu, les partenariats stratégiques liés par les pays du Golfe depuis 1990 sont principalement avec les États-Unis, mais aussi, dans une moindre mesure, la France et la Grande-Bretagne – ceci varie d'un pays à l'autre. Ces alliances pourraient évoluer. On peut par exemple avancer que les pétromonarchies sont susceptibles de chercher à s'éloigner d'une trop grande dépendance à l'égard des États-Unis, à cause d'une défiance croissante à leur endroit ou par anticipation du désengagement qu'elles craignent. De trop nombreux intérêts sécuritaires communs subsistent pour sérieusement envisager de remettre en cause cette relation privilégiée, mais l'hypothèse d'un rapprochement à moyen ou long terme entre les États-Unis et l'Iran suffit à pousser les pays du CCG à réfléchir à d'autres options[25]. Parmi ces alternatives figure une diversification des partenariats avec un pivot vers l'est : il s'agirait de consolider des alliances sécuritaires avec l'Inde, la Chine ou la Corée du Sud. Cela serait cohérent avec l'augmentation des relations politico-économiques entre les deux régions et présenterait certains avantages qui ont pu faire défaut à leurs traditionnels alliés occidentaux. Comme il a été noté au sujet des partenariats émergents avec la

[24] Selon les données du SIPRI Yearbook 2013, les EAU et l'Arabie saoudite sont respectivement les 4e et 5e plus gros importateurs d'armements mondiaux sur la période 2009-2013.
[25] A cet égard, les pays du CCG regardent avec défiance la reprise actuelle des relations entre Washington et Téhéran – à l'exception notable du sultanat d'Oman qui l'a favorisée.

Chine, par exemple, les pays du Golfe seraient « particulièrement séduits par une politique étrangère mettant l'accent sur la non-intervention et sur la souveraineté étatique »[26].

Ainsi, depuis le début des années 2000, des accords de coopération militaire ont été signés par l'Inde avec la majorité des pays du CCG : EAU en 2003, Oman en 2005, Qatar en 2008 et Arabie saoudite en 2014. Cependant, il faut noter que l'Inde ou la Chine ne désirent *a priori* pas pour autant remplacer le rôle de garantie sécuritaire régionale que remplissent les États-Unis. Il semble d'ailleurs que les pays du Golfe cherchent aujourd'hui à s'affranchir, non du parapluie militaire américain qui leur demeure essentiel, mais au moins d'une situation où ce dernier représente le principal dispositif assurant leur sécurité.

Conscients que leur manque de moyens humains – particulièrement saillant au Qatar et aux EAU – constitue un obstacle majeur à une véritable autonomie de défense, les pays du CCG pourraient ainsi tenter de consolider un système de sécurité régional intégré.

Au niveau national, les pays du Golfe donnent également de nouvelles impulsions à leurs processus de planification et d'acquisition, qui dénotent une volonté de plus s'affirmer qu'auparavant, de diversifier leur économie et, possiblement, de prendre, à terme, un contrôle indépendant de leur propre sécurité. Ainsi, les pétromonarchies se sont progressivement éloignées de tractations dans lesquelles l'expression de besoin capacitaire était plus véritablement formulée par les fournisseurs que par les clients et où la valeur politique de l'acquisition était presque plus importante que sa finalité opérationnelle. Elles font dorénavant le choix d'acquisition et de développement de forces durables et axées sur des besoins opérationnels et non plus celui d'une compétition sur « ce qui brille le plus » consistant à acheter les systèmes d'armes les plus sophistiqués sans tenir le moindre compte de la priorité de la mission et de la capacité d'opérer et de maintenir un système agréé de forces au combat[27].

Comme nous l'avons souligné, une bonne partie des évolutions des pratiques des pays du Golfe est liée à leur processus de construction étatique. Ainsi, en termes de planification et d'acquisition, un effort de rationalisation et de transparence est à noter, les pétromonarchies s'éloignant d'un fonctionnement relativement obscur où la prise de décision semblait être le fait d'un seul homme et où les lignes entre cassette personnelle des cheikhs et budgets nationaux étaient floues[28]. Aujourd'hui, la structure décisionnelle aboutissant à la signature de contrats de sécurité et de défense ainsi que la répartition des tâches au sein des comités techniques chargés d'évaluer les réponses aux appels d'offres internationaux sont bien plus lisibles qu'auparavant. Par ailleurs, certains pays du Golfe semblent vouloir s'éloigner des logiques d'achats traditionnelles de produits sur étagère et formulent davantage de demandes de transferts de compétences et de technologies. Notons que la formation des officiers du Golfe a toujours représenté une part plus ou moins importante des marchés de défense sur place. Une augmentation de la demande à cet égard pose la question d'un intérêt des pétromonarchies pour de nouvelles stratégies de planification et d'acquisition selon l'approche capacitaire. Quant aux demandes de transfert de technologies, elles vont de pair, aux EAU particulièrement, avec la volonté de développer une industrie de défense locale notamment pensée comme un moyen de diversification économique pour préparer l'après-pétrole,

[26] Kristian C. Ulrichsen, "The GCC States and the Shifting Balance of Global Power", *Occasional Paper*, n° 6, Doha, Center for International and Regional Studies, 2010, p. 18.

[27] Anthony Cordesman, *Securing the Gulf: Key Threats and Options for Enhanced Cooperation*, Washington, Center for Strategic and International Studies (CSIS), février 2013, p. 48. Traduction de l'auteur.

[28] Entretiens de l'auteur avec différents interlocuteurs issus des milieux institutionnels, académiques et industriels dans les pays du Golfe entre mars 2013 et juin 2014.

mais également comme un moyen supplémentaire d'autonomisation. Ces dynamiques sont susceptibles d'avoir un impact sur les marchés de défense du futur dans la région.

Hypothèses quant aux redéfinitions de l'économie de défense des pays du Golfe

Un recul des États-Unis dans la zone, dû à une réévaluation de leurs priorités stratégiques ou à un choix des pétromonarchies de ne jamais reposer intégralement sur une garantie de sécurité unique, permettrait d'ouvrir plus de parts de marchés à d'autres partenaires.

Nous pensons ici aux puissances traditionnellement présentes dans la zone ainsi qu'aux BRICS, mais aussi, peut-être, à l'Union européenne (UE). Il est effectivement possible de s'interroger aujourd'hui sur la pertinence potentielle du développement de plus amples relations de région à région en matière de défense et de sécurité. Soulignons la profusion de groupes de travail et de discussion autour de ces questions et la volonté formulée par le CCG de prendre l'UE comme un modèle de la plus grande intégration institutionnelle que ses membres voudraient réaliser. Il semble par exemple que les regards du Golfe soient tournés vers l'Europe en ce qui concerne le domaine de la sécurité maritime et de la lutte anti-piraterie. Néanmoins, la mise en place de réels partenariats de région à région rencontre plusieurs obstacles. D'une part, les pays européens abordent les différents membres du CCG plus comme des compétiteurs que selon une stratégie collective en ce qui concerne les contrats de défense étant donné « la nécessité presque existentielle pour [les] complexes militaro-industriels [de ces États] d'exporter dans la région »[29]. D'autre part, les pays du Golfe eux-mêmes semblent continuer de privilégier les relations bilatérales aux relations multilatérales, que ce soit entre eux ou avec des partenaires extérieurs. Notons que le caractère stato-centré de leur cadre référentiel principal s'explique par leur statut de jeunes États et par le désir associé d'affirmer leur souveraineté nationale.

Par ailleurs, les pays du Golfe semblant être en pleine redéfinition de leurs processus de planification et d'acquisition, les États fournisseurs et les industriels de défense et de sécurité pourraient faire évoluer les offres faites à ces pays en conséquence. Cela supposerait notamment d'intégrer davantage les demandes de transferts de compétences et de technologies, de formation et d'interopérabilité des systèmes – à la fois entre eux et avec ceux de l'UE ou de l'OTAN – dans les réponses aux appels d'offre. À cet égard, une idée circule dans différents cercles institutionnels et universitaires côtoyés au cours de nos recherches, qui mérite d'être mentionnée : celle d'un passage possible du paradigme « pétrole contre sécurité » à un paradigme « démocratie contre technologie » ou, *a minima*, un paradigme « réforme contre sécurité ». Ceci permettrait notamment aux puissances occidentales de s'éloigner d'une politique du « deux poids, deux mesures » vis-à-vis du monde arabe qui est souvent décriée – soutenant les révoltes populaires et ce qui était perçu comme une « démocratisation » et une libéralisation de la politique dans la plupart des pays arabes depuis 2011, les États-Unis et les pays européens sont restés relativement silencieux sur le cas bahreïni, par exemple. Néanmoins, comme nous l'avons souligné, les pays du Golfe, individuellement et collectivement, ont régulièrement critiqué toute tentative d'ingérence extérieure dans leurs affaires intérieures, particulièrement depuis le début du « Printemps arabe ».

[29] « Ventes d'armes : la baisse des crédits de défense renforce la concurrence à l'exportation », *Le Huffington Post Québec*, 17 mars 2014, disponible sur : http://quebec.huffingtonpost.ca/2014/03/17/ventes-darmes--la-baiss_n_4980320.html, dernière consultation 12 décembre 2014.

Il est d'ailleurs intéressant de noter que ces critiques sont également formulées au sein même du CCG. C'était en effet la raison invoquée par l'Arabie saoudite, le Bahreïn et les EAU lorsqu'ils ont, d'un commun accord, retiré leurs ambassadeurs du Qatar le 5 mars 2014, arguant que la politique étrangère de ce dernier dans l'ensemble du monde arabe représentait un facteur de déstabilisation potentiel de leur propre scène nationale. De la même manière, les suspicions omanaises vis-à-vis d'une possible volonté du royaume saoudien de mettre l'ensemble des membres du CCG sous sa coupe à travers son projet d'union du Golfe ont été portées, lors du Dialogue de Manama de décembre 2013, par la voix du ministre des Affaires étrangères du sultanat, Yusuf Bin Alawi[30].

Alors que les révoltes arabes avaient dans un premier temps semblé aider la consolidation d'un système de sécurité régionale intégré, matérialisation d'une stratégie de survie collective, les dissensions internes à la Péninsule arabique semblent aujourd'hui avoir quelque peu écarté cette perspective. Cependant, il faut souligner que l'idée n'a pas été officiellement abandonnée et qu'elle continue bien au contraire d'être régulièrement défendue à la fois dans les discours des pays du Golfe et dans ceux de leurs partenaires stratégiques. Pour les États-Unis, le succès de cette initiative peut notamment être vu comme une condition *sine qua non* avant qu'ils envisagent réellement de retirer, au moins en partie, leurs propres forces armées présentes dans la région. De nombreux experts interrogés par l'auteur considèrent en effet que les États-Unis ne se désengageront pas tant que n'existera pas une base régionale solide à même d'assurer une première force de réaction rapide à tout défi sécuritaire potentiel dans cette zone qui demeure stratégique pour le monde entier.

Pour finir, soulignons que le développement des événements dans la région durant la seconde moitié de 2014 semble avoir remis à l'ordre du jour une plus grande coopération entre les pays du CCG, avec pour toile de fond l'essor de *Daech*, ou État islamique en Irak et au Levant (EIIL). Ainsi, à l'issue des travaux du 35e sommet du CCG, le 10 décembre 2014, ses pays membres ont annoncé leur engagement à combattre ensemble l'idéologie sur laquelle les groupes terroristes sont fondés, ainsi que la création d'une force navale unifiée du CCG. Le Moyen-Orient est une région qui évolue très rapidement et il serait hasardeux de vouloir prédire dès aujourd'hui les développements à attendre sur de nombreux dossiers. Dans ce climat illustrant bien le passage d'une « menace incertaine à une incertitude menaçante »[31], ce chapitre aura permis de poser des pistes de réflexion utiles à tout État ou entreprise entendant entretenir ou augmenter ses relations avec les pétromonarchies du Golfe.

[30] Le sultanat d'Oman a alors menacé de quitter le CCG si ce projet d'union était mis à exécution.

[31] Christian Bülhmann, « L'approche capacitaire: une réponse à des menaces diffuses », SOGAFLASH, 2006, p. 13.

Références

BUZAN Barry, *People, States and Fears*, Boulder, Lynne Rienner, 1991.

CORDESMAN Anthony, *Securing the Gulf: Key Threats and Options for Enhanced Cooperation*, Washington, Center for Strategic and International Studies (CSIS), février 2013.

DAZI-HENI Fatiha, « Les monarchies du Conseil de Coopération du Golfe : acteurs incontournables dans un monde arabe en manque de puissance ? », *dans* : SOUBRIER Emma (coord.), *Les pays du Conseil de coopération du Golfe : Nouvelles puissances du monde arabe ?*, Paris, Éditions du Cygne, 2014, p. 27-38.

GAUSE Gregory, *The International Relations of the Persian Gulf*, Cambridge, Cambridge University Press, 2009.

HASBANI Nadim, "The Geopolitics of Weapons Procurement in the Gulf States", *Defense & Security Analysis*, vol. 22, n° 1, mars 2006, p. 73-88.

IGNATIUS David, "Saudi Arabia Expands its Power as US Influence Diminishes", *The Washington Post*, 18 novembre 2011.

MATTHIESEN Toby, *Sectarian Gulf: Bahrain, Saudi Arabia, and the Arab Spring That Wasn't*, Stanford, Stanford University Press, 2013.

SAMAAN Jean-Loup, « Les monarchies du Golfe : un marché d'armement sans armées ? », *Moyen-Orient*, n° 17, janvier-mars 2013, p. 48-53.

SOUBRIER Emma, « La Diplomatie économique des pays du Golfe à l'aune du Printemps arabe : du rayonnement à la puissance », *dans* CHARILLON, Frédéric et DIECKHOFF, Alain, *Annuaire Afrique du Nord Moyen-Orient 2014-2015*, Paris, La Documentation française, 2014, p. 123-136.

SOUBRIER Emma, « Sécurité des monarchies du Golfe : de nouvelles règles du jeu ? », *Moyen-Orient*, n° 23, juillet-septembre 2014, p. 66-71.

ULRICHSEN Kristian C., "The GCC States and the Shifting Balance of Global Power", *Occasional Paper*, n°6 Doha, Center for International and Regional Studies, 2010.

AU-DELA DE LA « FORTERESSE AMERIQUE » : REPENSER LE CONTROLE DES EXPORTATIONS DE BIENS MILITAIRES DANS UN MONDE GLOBALISE

Hugo MEIJER
King's College London

Introduction

Depuis 2009, l'administration Obama a entrepris une réforme majeure du système américain de contrôle des exportations de matériel de guerre et de biens à double usage. *The President's Export Control Reform Initiative* a pour objectif d'adapter les contrôles à l'exportation des États-Unis aux évolutions de l'économie de défense mondiale de l'après-Guerre froide (telles que les contraintes budgétaires, la diffusion technologique, la compétition internationale accrue et la commercialisation partielle de la base industrielle de défense). Cette contribution examine les considérations politiques, militaires et industrielles sur lesquelles repose cette transformation de la politique américaine de contrôle des exportations de biens militaires. Il s'agira de montrer que la logique qui sous-tend la réforme américaine consiste à « contrôler moins pour mieux contrôler » afin de protéger la sécurité nationale des États-Unis – et notamment la capacité à maintenir leur prééminence militaire vis-à-vis de compétiteurs potentiels – ainsi que les capacités industrielles qui la sous-tendent. Afin d'étayer cet argument, après une description synthétique du système actuel de contrôle des exportations des États-Unis, ce chapitre mettra en évidence les principales préoccupations de l'administration Obama quant aux faiblesses de ce système. Enfin, nous nous pencherons sur la façon dont la réforme Obama entend répondre à ces préoccupations et adapter la politique américaine de contrôle des exportations aux transformations stratégiques, technologiques et industrielles du XXI^{e} siècle, y compris la montée en puissance militaire et économique de la République populaire de Chine[1].

Le système de contrôle des exportations américaines

Le système actuel de contrôle des exportations aux États-Unis est partagé entre le contrôle des exportations de matériel de guerre et celui des biens à double usage sous la responsabilité de deux administrations distinctes (voir le tableau ci-dessous). En d'autres termes, il s'agit d'un système « bicéphale ». Le contrôle des exportations de matériel de guerre est régi par l'*International Traffic in Arms Regulations* (ITAR) qui met en œuvre les dispositions de l'*Arms Export Control Act* de 1976. Le département d'État, et en son sein le *Directorate for Defense Trade Controls*, est responsable du contrôle des exportations de matériel de guerre figurant dans la liste de contrôle de biens militaires (*US Munitions List*, ML). La règlementation des exportations de biens à double usage, l'*Export Control Administration*, est encadrée par l'*Export Control Act* de 1979 et autorise le *Bureau of Industry and*

[1] Cette étude se base sur plusieurs dizaines d'entretiens menés aux États-Unis (Washington D.C.) et en France (Paris), entre 2010 et 2013, avec de hauts fonctionnaires des organes interministériels en charge de la sécurité nationale – respectivement le Conseil de sécurité nationale (NSC) et le Secrétariat général de la défense nationale (SGDN) – et des ministères des Affaires étrangères, de la défense et du Commerce, ainsi que des industriels de la défense.

Security (BIS) du département du Commerce à contrôler les biens à double usage énumérés dans sa liste de contrôle (la *Commerce Control List*).

Figure 1. Le système bicéphale de contrôle des exportations

	Matériel de Guerre	Biens à Double Usage
Ministère	Département d'Etat (DDTC)	Département du Commerce (BIS)
Réglementation	International Trade in Arms Regulations (ITAR)	Export Administration Regulations (EAR)
Liste	Munitions List (ML)	Commerce Control List (CCL)

Les critiques du système américain de contrôle des exportations

Ce système bicéphale de contrôle des exportations a fait l'objet de critiques croissantes dans l'après-Guerre froide pour son incapacité à s'adapter aux évolutions de l'économie de défense. En particulier, dans les débats sur la réforme du contrôle des exportations, trois grands axes de critique du système actuel peuvent être identifiés : (1) le système de contrôle des exportations, en cherchant à contrôler « trop », est non seulement inefficace, mais aussi contre-productif pour les intérêts sécuritaires et industriels américains ; (2) le labyrinthe bureaucratique en charge du contrôle des exportations défavorise l'industrie de défense américaine vis-à-vis de ses compétiteurs étrangers ; (3) les contrôles existants nuisent à l'interopérabilité au sein de l'OTAN et à la capacité de Washington de coopérer avec ses alliés.

La « Forteresse Amérique » : contrôler trop, contrôler mal

En 2009, le National Research Council a publié un rapport intitulé *Beyond Fortress America* qui a eu un impact important dans les débats initiaux sur la réforme[2]. Selon ce rapport, dirigé par l'ancien conseiller à la sécurité nationale Brent Scowcroft :

> « Conçu pendant la Guerre froide, lorsque les États-Unis dominaient la compétition internationale dans la plupart des domaines de la science et de la technologie, le système actuel de contrôle des exportations nuit à notre sécurité nationale ainsi qu'à notre capacité à faire face à la concurrence internationale »[3].

[2] Entretiens avec des fonctionnaires du Département d'État, Washington D.C., 2010. Voir National Research Council, *Beyond Fortress America: National Security Controls on Science and Technology in a Globalized World*, Washington D.C., The National Academy Press, 2009.

[3] National Research Council, *op. cit.*, p. 3. Dans ce chapitre, les documents et entretiens en anglais ont été traduits librement par l'auteur.

Selon cette première critique, la mentalité que le rapport qualifie de « Forteresse Amérique » est devenue obsolète car elle néglige le fait que trois dynamiques ont érodé la capacité des États-Unis à contrôler efficacement la diffusion technologique dans l'après-Guerre froide, rendant des contrôles excessivement stricts non seulement inefficaces, mais aussi contre-productifs. Premièrement, après la fin de la Guerre froide, les dépenses de recherche et développement (R&D) du secteur commercial ont progressivement dépassé celles du gouvernement américain et l'écart entre les deux s'est constamment élargi dans la période de l'après-Guerre froide[4]. Par conséquent, le centre de gravité dans le développement de technologies à double usage s'est déplacé de la recherche menée par l'État et le secteur militaire au secteur commercial.
Par ailleurs, la mondialisation de l'industrie des hautes technologies est allée de pair avec la diffusion à l'échelle mondiale de la capacité de produire des biens à double usage. Cette prolifération de sources d'approvisionnement a permis à des pays ciblés par des contrôles à l'exportation d'avoir accès à des biens à double usage même si ceux-ci étaient soumis à des contrôles par les États-Unis.

Deuxièmement, alors que pendant la Guerre froide les deux superpuissances et leurs blocs respectifs étaient essentiellement économiquement indépendants l'un de l'autre, les économies des États-Unis et de leurs compétiteurs sont devenues de plus en plus enchevêtrées, comme c'est le cas notamment avec la République populaire de Chine (RPC). Comme l'ont souligné deux anciens fonctionnaires du gouvernement américain en charge du contrôle des exportations « pendant la Guerre froide, les pays se divisaient de façon assez nette entre les deux blocs, et les décisions en matière de contrôle des exportations [...] étaient en large mesure basées sur cette division. Dans le marché mondialisé d'aujourd'hui, cependant, des rivaux potentiels sont également des marchés [considérables] »[5]. Dans le cas de la RPC, par exemple, l'interdépendance économique croissante entre la Chine et les États-Unis, ainsi que l'importance du marché chinois pour les exportations technologiques américaines, ont engendré une pression croissante de la part des entreprises américaines de haute technologie sur le gouvernement pour se libérer des contraintes imposées par les contrôles à l'exportation, les amenant même, dans certains cas, à accepter des transferts de technologie « forcés » en échange de l'accès au marché chinois[6].

Troisièmement, des contrôles à l'exportation unilatéraux et excessivement stricts sont non seulement inefficaces, mais ils affaiblissent la capacité de l'industrie à réinvestir les revenus des exportations en R&D de technologies de nouvelle génération. Ceci, à son tour, affaiblirait la capacité du Pentagone à avoir accès aux technologies de pointe et affecterait ainsi la capacité des États-Unis à maintenir leur prééminence militaire et technologique. C'est pourquoi, selon le rapport du *National Research Council* : « la mentalité de "Forteresse Amérique" – qui relève de la Guerre froide – entrave notre capacité de faire face aux menaces et défis de l'après-Guerre froide »[7].

---

[4] Voir à ce sujet Hugo Meijer, « Contrôler l'incontrôlable ? La politique américaine de contrôle des exportations de technologies à double usage dans l'après-Guerre froide », *Fiche de l'IRSEM*, n° 10, Institut de recherche stratégique de l'École militaire (IRSEM), 2012, p. 6-10.

[5] Mark Foulon et Christopher Padilla, « In Pursuit of Security and Prosperity: Technology Controls for a New Era», *The Washington Quarterly*, vol. 30, n° 2, 2007, p. 86.

[6] Hugo Meijer, « Globalisation, transferts technologiques américains et modernisation militaire de la République populaire de Chine », *dans* Pierre Journoud (dir.), *Stratégie, puissance et influence chinoises depuis la guerre froide*, L'Harmattan, collection Inter-National, à paraître en 2015.

[7] National Research Council, *op. cit.*, p. 2.

En d'autres termes, un système de contrôle à l'exportation excessivement contraignant n'est pas seulement inefficace, mais aussi contre-productif.

Un labyrinthe bureaucratique dysfonctionnel et le soutien de la base industrielle américaine

Une deuxième critique portée à ce système bicéphale de contrôle des exportations – avec deux bureaux et deux listes de contrôle – est qu'il engendre des luttes bureaucratiques lorsque, par exemple, il s'agit de déterminer si un bien doit être considéré et contrôlé comme un bien à double usage ou comme matériel de guerre et, par conséquent, s'il relève des compétences du département du Commerce ou du département d'État[8]. Cela entraîne de la confusion, des retards et de l'imprévisibilité dans les délivrances d'autorisations d'exportation, ce qui nuit à la capacité des entreprises à faire face à la compétition internationale. Ce d'autant plus dans un contexte de restrictions budgétaires, de processus de « séquestration » à la suite du *Budget Control Act* de 2011 et de pressions internationales croissantes pour l'industrie de défense, qui imposent de stimuler et de soutenir les exportations afin de préserver la base industrielle et technologique de défense américaine[9].

En effet, même si cette tendance est moins prononcée aux États-Unis qu'en Europe en raison de la taille du marché domestique américain (qui représente environ deux tiers des chiffres d'affaires des principales entreprises de défense américaines), « l'assaut des marchés extérieurs » n'en est pas moins devenu, par nécessité, un axe central des stratégies d'adaptation des « *super-primes* » américains[10]. Un rapport du *Government Accountability Office* évalue l'impact de la séquestration sur les ressources du Pentagone par une réduction d'environ 37 milliards de dollars en crédits (*appropriations*) discrétionnaires et environ $ 37,4 millions en dépenses directes[11]. Le contrôleur général (*comptroller general*) du Pentagone précise qu'en 2014, en raison de la séquestration, le compte d'approvisionnement du Pentagone ($ 110 milliards) sera réduit de 9,8 milliards de dollars et que son compte de recherche et développement ($ 69,6 milliards) sera réduit de 6 milliards de dollars[12]. Dans ce contexte de contraintes budgétaires importantes, les dysfonctionnements de la bureaucratie en charge du contrôle des exportations ont par conséquent des implications considérables pour l'industrie de défense américaine.

---

[8] Cf. Hugo Meijer, « The Obama Administration's Export Control Reform Effort », *Lettre de l'IRSEM – Dossier stratégique : État des lieux du marché et de l'industrie de défense mondiale*, n° 5, 2012.

[9] Pour une analyse de l'impact des contraintes budgétaires automatiques et pluriannuelles (« séquestration ») qu'impose le *Budget Control Act*, et de leur impact sur les plans d'investissements de l'industrie de défense, voir Aude-Emmanuelle Fleurant, « Budget et industrie : un nouveau cap défini dans la tourmente », *dans* Maya Kandel (dir.), Aude-Emmanuelle Fleurant, *États-Unis : quelle transformation stratégique ? La politique de défense sous Obama, entre dynamiques internes et évolutions internationales*, Études de l'IRSEM, n° 29, 2013.

[10] Aude-Emmanuelle Fleurant, « Moteurs et conséquences des mutations de l'industrie de défense américaine », *dans* Yves Bélanger, Aude-Emmanuelle Fleurant, Hélène Masson, Yanick Quéau, *Les Mutations de l'industrie de défense : regards croisés sur trois continents*, Cahier de l'IRSEM, n° 10, 2012, p. 59, 64 et 69.

[11] General Accountability Office, *Sequestration: Observations on the Department of Defense's Approach in Fiscal Year 2013*, 7 novembre 2013, p. 1.

[12] US Department of Defense, *Report on the Joint Committee Sequestration for Fiscal Year 2013*, Office of the Under Secretary of Defense (Comptroller), juin 2013.

Pour reprendre les termes de l'ancien secrétaire à la défense Robert Gates, « vieux de plusieurs décennies, ce système bureaucratique labyrinthique ne sert ni les besoins américains en matière de sécurité nationale ni nos intérêts économiques au XXI[e] siècle »[13].

Coopération et interopérabilité avec les alliés des États-Unis

Une troisième critique est, comme l'a souligné entre autres la *Quadriennal Defense Review* (QDR) du Pentagone de 2010, que le système limite la coopération, les transferts technologiques et l'interopérabilité avec les alliés des États-Unis ainsi que la contribution que les forces alliées peuvent apporter aux opérations militaires américaines[14]. Lors d'une opération militaire, par exemple, le fait que certains alliés aient reçu l'autorisation de réparer du matériel américain tandis que d'autres ne l'ont pas, peut empêcher ou compliquer la réparation des installations près du théâtre des opérations[15]. C'est entre autres pour cela qu'en 2007 les États-Unis ont signé avec le Royaume-Uni et l'Australie des traités visant à assouplir les contrôles à l'exportation afin d'accroître la capacité d'équiper et de soutenir les forces militaires américaines et celles de ces deux alliés en cas d'opérations de combat[16]. Cependant, malgré ces accords bilatéraux, le système global de contrôle des exportations américain a récemment été mis à rude épreuve en raison du volume élevé des licences requises pendant les opérations alliées en Irak et en Afghanistan. C'est pourquoi la QDR de 2010 a conclu que « le système de contrôle des exportations lui-même pose un risque potentiel pour la sécurité nationale » des États-Unis et que les carences de ce système ne peuvent « être résolues que par une réforme fondamentale »[17].

La réforme Obama ou les avatars du contrôle des exportations dans un monde globalisé

Afin de répondre à ces préoccupations, la réforme Obama vise à établir des « *higher fences around a smaller garden* », à savoir des barrières plus élevées autour d'un éventail plus restreint de biens et de technologies considérés comme étant à la base de la prééminence militaire/technologique des États-Unis[18]. Il s'agit de recentrer et de mieux focaliser les ressources humaines et financières du gouvernement sur le contrôle des « *crown jewels* » (joyaux de la couronne) de l'outil militaire américain. Cette réforme repose donc avant tout sur des considérations de sécurité nationale. À cette fin, Washington entend alléger les restrictions sur ces technologies devenues accessibles sur les marchés internationaux et ne présentant pas une menace sécuritaire majeure si elles sont acquises par les rivaux des États-Unis. Dans cette optique, l'administration américaine a proposé un nouveau

[13] Robert Gates, « Remarks by Secretary Gates to the Business Executives for National Security on the U.S. Export Control System », 20 avril 2010, disponible sur : http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4613

[14] US Department of Defense (DOD), *Quadrennial Defense Review,* 2010, p. 83-84.

[15] National Research Council, *op. cit.*, p. 18.

[16] Robert Gates, *op. cit*. Voir à ce sujet Claire Taylor, *UK-US Defence Trade Co-operation Treaty*, House of Commons Library, International Affairs and Defence Section, 17 février 2009 ; et Bruce Vaugh, "The US-Australia Treaty on Defense Trade Cooperation", *CRS Report for Congress RS22772*, Congressional Research Service, 12 décembre 2007.

[17] US Department of Defense, *op. cit.*, p. 84.

[18] Entretiens avec des responsables du Département d'État et de la Défense et des associations professionnelles de l'industrie de défense, Washington D.C., 2010.

système de contrôle des exportations qui repose sur quatre éléments : (a) l'établissement d'un bureau unique de contrôle des exportations qui serait en charge tant des exportations de matériel de guerre que des biens à double usage ; (b) la fusion des deux listes de contrôle –*l'International Traffic in Arms Regulations* (ITAR) et la *Commerce Control List* (CCL) – en une seule liste de contrôle unifiée ; (c) la création d'un organisme unique de coordination de l'application des règles de contrôle des exportations ; (d) un système informatique unifié, y compris une base de données unique sur les entités sanctionnées et les entités à qui une licence d'exportation a été refusée. Une liste et un bureau de contrôle unifiés, en particulier, permettraient de rationaliser le processus de contrôle des exportations en mettant fin aux différends bureaucratiques sur quel ministère est responsable de l'exportation d'un bien spécifique.

Cependant, jusqu'ici aucun pas n'a été fait dans la direction de la création d'un bureau et d'une liste unifiés – la réforme Obama étant à ce jour (novembre 2014) en cours de mise en œuvre. Les solutions proposées jusqu'à présent concernent essentiellement la rationalisation de la *Munitions List* – qui contrôle les exportations de matériel de guerre (ITAR) sous l'autorité du Département d'État (cf. figure 2). L'administration a notamment proposé la transition de biens et de composants de la liste de contrôle ITAR (matériel de guerre) à la liste EAR (biens à double usage) du département du Commerce et ce en vue, sur le moyen/long terme, de créer une liste de contrôle unique. Nous verrons maintenant que, ce faisant, Washington vise d'une part à resserrer l'éventail de biens contrôlés sous ITAR tout en maintenant un verrouillage sur les exportations vers la République populaire de Chine, perçue comme le principal compétiteur militaire potentiel (*near peer competitor*) des États-Unis. D'autre part, l'administration Obama entend renforcer les relations industrielles transatlantiques de défense et faciliter l'interopérabilité entre alliés de l'OTAN (ainsi que le Japon et l'Australie).

La réforme Obama, la Série 600 et l'embargo vers la Chine

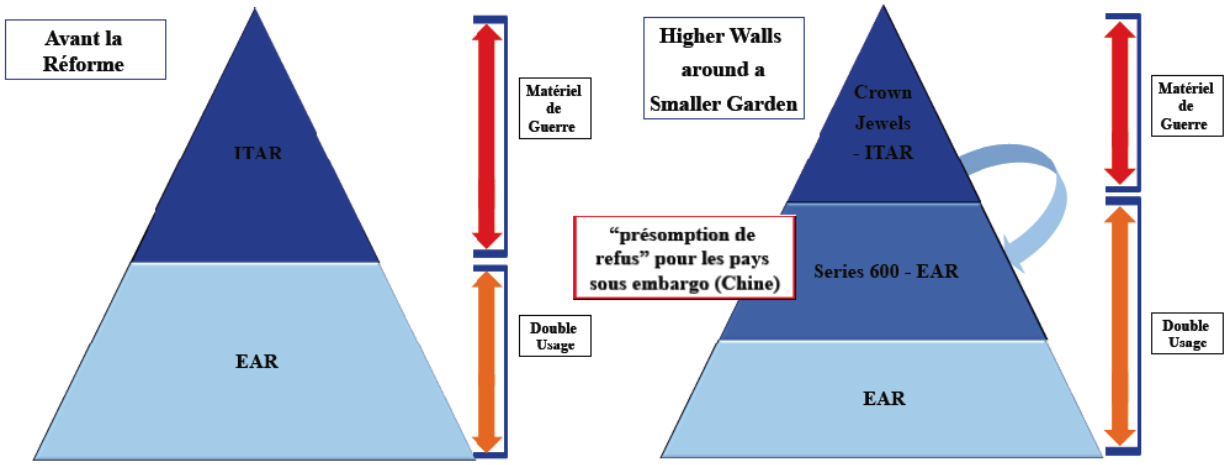
Dans le cadre de cette transition de biens et de composants du contrôle ITAR au contrôle EAR, un groupe intermédiaire de contrôle a été créé au sein de l'EAR, la Série 600, qui regroupe tous les biens et composants qui ont été déplacés de la liste des biens ITAR vers les contrôles EAR (voir la figure ci-dessous)[19]. Une spécificité de la Série 600, qui la distingue du reste des biens EAR, est le fait que les biens reclassés dans la Série 600 continuent à être sujets à une « présomption de refus » pour des pays soumis à des embargos, comme la République populaire de Chine, l'Iran ou la Corée du Nord. En d'autres termes, la Série 600 a une double finalité politique et sécuritaire. D'une part, il s'agit de tempérer les critiques potentielles, notamment au Congrès, à l'égard de ce qui peut être perçu comme un assouplissement des contrôles à l'exportation pouvant potentiellement nuire à la sécurité nationale des États-Unis. Comme le souligne un lobbyiste de l'industrie de défense américaine, « personne ne veut être dans la position d'être critiqué pour être "faible en matière de sécurité nationale" (*weak on national security*) – et c'est l'un des plus grands défis en matière de réforme des contrôles à l'exportation »[20]. L'administration Obama entend ainsi démontrer qu'il ne s'agit pas là d'une libéralisation des contrôles, mais d'une modification du type de contrôles.

[19] Pour une description détaillée de la Série 600, voir Kevin Wolf, Assistant Secretary of Commerce, « Advancing Export Control Reform: The Agenda Ahead », *Statement Before the Committee on Foreign Affairs*, U.S. House of Representatives, 24 avril 2013.

[20] Entretien avec Remy Nathan, Vice President for International Affairs, Aerospace Industry Association, 8 mars

D'autre part, la Série 600 permet de respecter l'embargo américain sur la vente d'armes à la Chine et d'éviter un accroissement des flux de technologies militaires qui pourraient contribuer à la modernisation militaire chinoise[21].

Figure 2.



L'exemple des modifications du contrôle de l'exportation du F-16 et de ses composants permet d'illustrer au concret le contenu de la réforme Obama et en particulier de la Série 600 (voir la figure 3)[22]. Le F-16 en tant que tel reste sous les contrôles ITAR (ainsi que d'autres avions qui effectuent des missions militaires ou de renseignement tels que les hélicoptères d'attaque et les avions de reconnaissance ou de surveillance). Le gouvernement a ensuite identifié les composants et technologies du F-16 donnant un avantage militaire ou de renseignement crucial aux forces armées américaines. Les systèmes d'armes et les composants les plus sensibles du F-16 sont donc restés sur la liste ITAR, y compris les lanceurs de missiles, les récepteurs d'alerte radar et les systèmes de détection des missiles[23]. D'autres éléments et composants du F-16 qui ne constituent pas une capacité militaire essentielle (*critical military capability*) ont été déplacés vers la Série 600 du département du Commerce, y compris les ailes, les gouvernes de direction, les réservoirs à carburants et le train d'atterrissage.

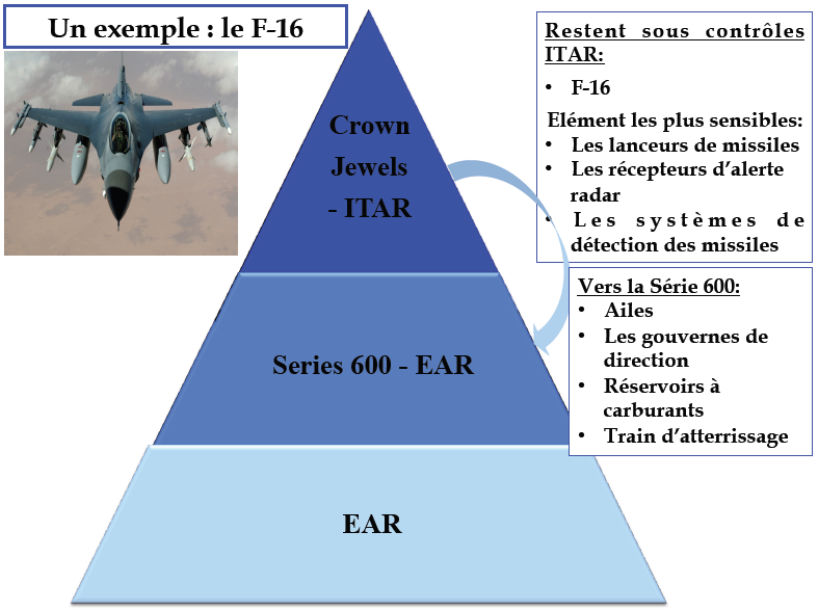
2010.

[21] Pour une comparaison des approches américaine et européennes vis-à-vis des exportations de matériel de guerre et de biens à double usage vers la Chine, voir Hugo Meijer « Transatlantic Perspectives on China's Military Modernization: the Case of Europe's Arms Embargo against the People's Republic of China », *Paris Paper,* n° 12, Institut de recherche stratégique de l'École militaire, 2014.

[22] James Hursch, Director of the Defense Technology Security Administration (DTSA), U.S. Department of Defense, *Testimony before the House Foreign Affairs Committee*, 24 avril 2013. Voir aussi Michele Flournoy, « Want to Export an F-16 Fighter Jet? », *The Wall Street Journal*, 11 mars 2013.

[23] James Hursh, *op. cit*.

Figure 3.



Le STA, la coopération transatlantique et les contrôles européens à l'exportation

Le deuxième pan de la réforme Obama vise à faciliter l'interopérabilité et le partage de technologies entre les États-Unis et leurs alliés – un souci important de l'administration, comme nous l'avons précédemment évoqué. C'est pourquoi Washington a créé une exemption de licence, le *Strategic Trade Authorization License Exception* (STA), qui permet l'exportation, la réexportation et le transfert de biens pour des exportations vers 36 pays à faible risque, y compris les membres de l'OTAN et les membres de tous les quatre régimes multilatéraux de non-prolifération (*Wassenaar Arrangement*, *Missile Technology Control Regime*, *Australia Group*, *Nuclear Suppliers Group*)[24]. L'administration américaine prévoit que les STA vont engendrer un renforcement des exportations américaines en Europe et qu'elles permettront d'assurer plus facilement le soutien de systèmes américains qui ont été vendus en Europe[25]. En même temps, certains hauts fonctionnaires européens s'interrogent sur l'impact de moyen-long terme de cette réforme pour les relations industrielles transatlantiques :

> « Les STA se traduiront en une plus grande promotion des équipements américains vers la zone Europe […]. La grande question est si ce changement d'équilibre se fera uniquement au détriment de la partie européenne. Il est possible que – puisque quand un bien américain peut être exporté les données techniques à l'achat de ces biens peuvent être aussi exportées – du coup il est plus facilement possible pour un maître d'œuvre américain de faire des appels d'offre, notamment vis-à-vis des pays européens. Cela peut apporter un certain rééquilibrage dans des secteurs dans lesquels l'industrie européenne serait plus compétitive que l'industrie américaine lorsqu'il s'agit de répondre à des besoins domestiques américains »[26].

[24] Ian Fergusson, Paul Kerr, « The US Export Control System and the President's Reform Initiative », *CRS Report for Congress R41916,* Congressional Research Service, 2014, p. 23.
[25] Entretiens avec des fonctionnaires du Département d'État et du Commerce, Washington D.C., 2013.
[26] Entretien avec un fonctionnaire du ministère de la défense, Paris, 2013.

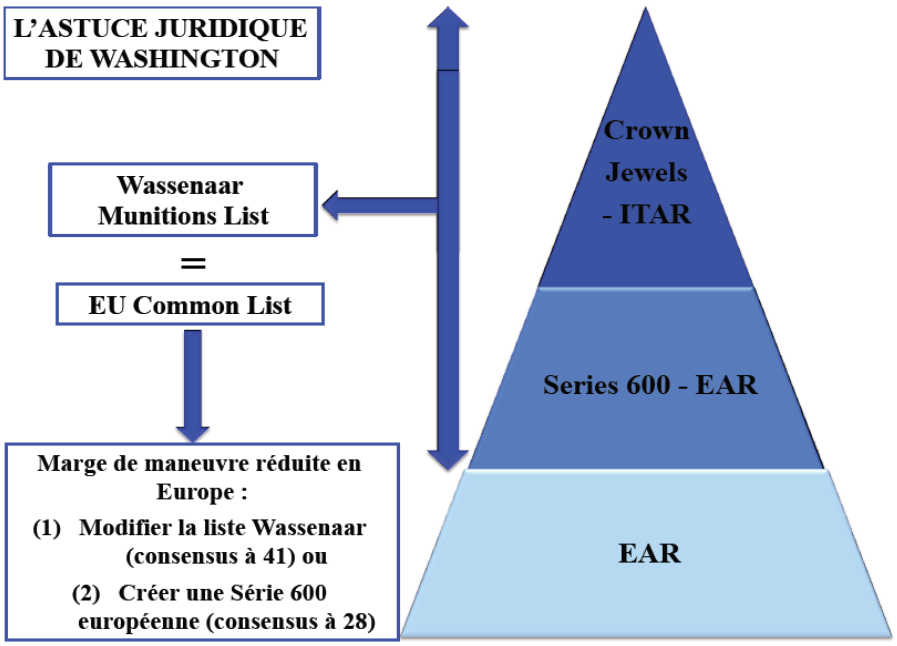
Dans ce contexte, il est intéressant de souligner les difficultés qu'impliquerait la transposition en Europe d'une réforme semblable à celle de l'administration Obama. Les listes de contrôle des États membres européens sont dérivées des listes de l'Arrangement de Wassenaar (la liste militaire et la liste industrielle/à double usage). D'une part, la liste militaire de Wassenaar est reprise dans la liste commune européenne des équipements militaires (ou matériel de guerre) dans le cadre de la Position commune 2008/944/PESC du 8 décembre 2008[27]. D'autre part, la liste Wassenaar des biens à double usage est transposée dans le règlement communautaire sur le contrôle des exportations de biens et technologies à double usage (Règlement 428/2009). Afin de modifier les listes de contrôle européennes et de transférer des biens et composants de la liste militaire vers la liste de contrôle à double usage – comme l'a fait l'administration Obama – les États membres disposent de deux options. Premièrement, ils peuvent renégocier les listes de contrôle de Wassenaar en entamant des négociations entre les 41 États membres de cette institution multilatérale. Deuxièmement, l'UE pourrait créer une « Série 600 » européenne, ce qui impliquerait des négociations et un consensus à 28. Dans les deux cas, des négociations multilatérales aboutissant à un consensus seraient requises afin de modifier les listes de contrôle. Afin de mettre en œuvre une réforme des contrôles européens à l'exportation semblable à celle de l'administration Obama, les Européens doivent donc, pour reprendre les termes d'un fonctionnaire français :

> « Se mettre d'accord au niveau international, alors que les Américains sont en mesure de mener à bien leur réforme en discutant au niveau national. […] Les Américains ne doivent consulter personne. Ils n'ont pas l'équivalent d'une directive TIC [sur les transferts intracommunautaires] qui impose d'avoir une liste commune au niveau européen. […] Nous n'avons pas les moyens au niveau européen de faire la même chose parce que pour arriver au même type de réforme il va falloir passer par Wassenaar ou créer une Série 600 européenne. […] Donc l'évolution et l'adaptation de ces listes vis-à-vis des évolutions technologiques sont nettement plus difficiles pour l'UE. […] Nous avons moins de marge de liberté que les États-Unis »[28].

Par ailleurs, afin de mener à bien la réforme Obama, le gouvernement américain a évité d'entamer une renégociation des listes de Wassenaar (reprises dans les listes de contrôle américaines) par le biais d'une « astuce juridique » (illustrée dans la figure ci-dessous)[29]. Puisque la Série 600 contient des biens précédemment classifiés comme matériel de guerre et qui ont été déplacés sous les contrôles EAR de biens à double usage tout en maintenant une procédure spécifique (y compris la présomption de refus), Washington considère que juridiquement la somme de la liste ITAR et de la Série 600-EAR est conforme à la liste militaire de Wassenaar. Par conséquent, une renégociation des listes de Wassenaar n'a pas été nécessaire, « donc l'astuce est vraiment la Série 600 »[30]. Contourner et éviter des négociations houleuses dans une enceinte multilatérale avec 41 États membres a donc permis à l'administration Obama de mener à bien ce qui s'annonçait comme une réforme majeure du système de contrôle des exportations de biens militaires – et que, à l'heure actuelle, l'Union européenne n'est pas en mesure politiquement de mettre en œuvre.

[27] La France a ajouté à ce périmètre les satellites, les lanceurs et leurs composants.
[28] Entretien avec un fonctionnaire du ministère de la défense, Paris, 2013.
[29] *Ibid*.
[30] *Ibid*.

Figure 4.



Conclusions

La réforme Obama du système américain de contrôle des exportations entamée en 2009 apparaît comme animée par une triple ambition politique, militaire et industrielle. Tout d'abord, par le biais de cette réforme, Washington entend garantir le maintien de sa prééminence militaire/technologique. Pour ce faire, le gouvernement vise à démanteler ce qui a été qualifié de « Forteresse Amérique » et à ériger des « *higher fences around a smaller garden* ». Simplifier le processus bureaucratique du contrôle des exportations (création d'une liste unique, fusion des bureaux en charge du contrôle, etc.) permet de concentrer et de focaliser les ressources humaines et financières du gouvernement sur le contrôle des « joyaux de la couronne », à savoir ces biens et technologies qui sont à la base de la supériorité militaire américaine. Washington veut contrôler moins pour contrôler mieux. L'objectif de cette réforme est donc avant tout de recentrer les contrôles à l'exportation sur « ces biens et technologies qui donnent à nos forces armées un avantage militaire. […] Nos nouveaux contrôles à l'exportation nous aideront à mieux protéger et à employer pour une plus longue période de temps ces "joyaux de la couronne" qui donnent à notre outil militaire un avantage décisif »[31]. Washington entend par ailleurs s'assurer que ces modifications n'affectent pas les exportations vers des pays sous embargo, en continuant notamment à verrouiller les exportations de biens militaires vers la République populaire de Chine – son principal compétiteur militaire potentiel – afin d'en retarder la modernisation militaire. Deuxièmement, en rationalisant les contrôles à l'exportation, l'administration Obama souhaite consolider les relations transatlantiques de défense. Il s'agit notamment de faciliter la coopération et l'interopérabilité entre les alliés de l'OTAN, mais aussi d'asseoir l'influence des entreprises américaines de défense dans le

[31] James Hursch, *op. cit*.

commerce transatlantique en soutenant leurs exportations vers le Vieux Continent – a fortiori compte tenu de l'impossibilité actuelle pour l'UE de mener à bien une réforme du même type. Troisièmement, dans un contexte de contraintes budgétaires, cette réforme a pour but de stimuler les exportations et de soutenir la base industrielle et technologique de défense américaine.

Par ailleurs, en assouplissant les contrôles aux exportations, le gouvernement américain espère inciter le secteur privé à réinvestir les profits des exportations dans la recherche et le développement de technologies de nouvelle génération. Ceci, à son tour, renforcerait la capacité du Pentagone à avoir accès aux technologies de l'état de l'art et à assurer l'avantage qualitatif de l'outil militaire des États-Unis vis-à-vis de celui de leurs compétiteurs potentiels. Force est de constater que la réforme du contrôle des exportations est perçue par Washington comme un instrument de politique étrangère, de politique de défense et de politique industrielle qui est mobilisé pour asseoir et préserver la prééminence militaire américaine dans un monde globalisé.

Références

FERGUSSON Ian, KERR Paul, « The US Export Control System and the President's Reform Initiative », *CRS Report for Congress R41916*, Congressional Research Service, 2014, p. 23.

FLEURANT Aude-Emmanuelle, « Moteurs et conséquences des mutations de l'industrie de défense américaine », *dans* BELANGER Yves, FLEURANT Aude-Emmanuelle, MASSON Hélène, QUEAU Yanick, *Les Mutations de l'industrie de défense : regards croisés sur trois continents*, Cahier de l'IRSEM, n° 10, 2012, p. 59, 64 et 69.

FLEURANT Aude-Emmanuelle, « Budget et industrie : un nouveau cap défini dans la tourmente », *dans* KANDEL Maya (dir.), FLEURANT Aude, *États-Unis : quelle transformation stratégique ? La politique de défense sous Obama, entre dynamiques internes et évolutions internationales*, Études de l'IRSEM, n° 29, 2013.

FLOURNOY Michele, « Want to Export an F-16 Fighter Jet ? », *The Wall Street Journal*, 11 mars 2013.

GATES Robert, « Remarks by Secretary Gates to the Business Executives for National Security on the U.S. Export Control System », 20 avril 2010, disponible sur : http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4613, dernière consultation le 3 mars 2015)

General Accountability Office, *Sequestration: Observations on the Department of Defense's Approach in Fiscal Year 2013*, 7 novembre 2013, p. 1.

HURSCH James, Director of the Defense Technology Security Administration (DTSA), *Testimony before the House Foreign Affairs Committee*, U.S. Department of Defense, 24 avril 2013.

FOULON Mark, PADILLA Christopher, « In Pursuit of Security and Prosperity: Technology Controls for a New Era », *The Washington Quarterly*, vol. 30, n° 2, 2007, p. 86.

MEIJER Hugo, « Contrôler l'incontrôlable ? La politique américaine de contrôle des exportations de technologies à double usage dans l'après-Guerre froide », *Fiche de l'IRSEM*, Institut de recherche stratégique de l'École militaire (IRSEM), n° 10, 2012, p. 6-10.

MEIJER Hugo, "The Obama Administration's Export Control Reform Effort", *Lettre de l'IRSEM – Dossier stratégique : État des lieux du marché et de l'industrie de défense mondiale*, n° 5, Institut de recherche stratégique de l'École militaire (IRSEM), 2012.

MEIJER Hugo, "Transatlantic Perspectives on China's Military Modernization : the Case of Europe's Arms Embargo against the People's Republic of China", *Paris Paper*, Institut de recherche stratégique de l'École militaire (IRSEM), 2014.

MEIJER Hugo, « Globalisation, transferts technologiques américains et modernisation militaire de la République populaire de Chine », *dans* JOURNOUD Pierre (dir.), *Stratégie, puissance et influence chinoises depuis la Guerre froide*, L'Harmattan, collection Inter-National, à paraître 2015.

National Research Council, *Beyond Fortress America: National Security Controls on Science and Technology in a Globalized World*, Washington D.C., The National Academy Press, 2009.

TAYLOR Claire, *UK-US Defence Trade Co-operation Treaty*, House of Commons Library, International Affairs and Defence Section, 17 février 2009.

US Department of Defense, *Quadrennial Defense Review*, 2010.

US Department of Defense, *Report on the Joint Committee Sequestration for Fiscal Year 2013*, Office of the Under Secretary of Defense (Comptroller), juin 2013.

VAUGH Bruce, "The US-Australia Treaty on Defense Trade Cooperation", *CRS Report for Congress RS22772*, Congressional Research Service, 12 décembre 2007.

WOLF Kevin, Assistant Secretary of Commerce, "Advancing Export Control Reform: The Agenda Ahead", *Statement before the Committee on Foreign Affairs,* U.S. House of Representatives, 24 avril 2013.

LA FRANCE ET LA COOPERATION EUROPEENNE SUR LE CONTROLE DES EXPORTATIONS D'ARMEMENT : L'ADAPTATION AUX MUTATIONS DE L'ECONOMIE DE DEFENSE COMME RESULTAT DE RAPPORTS DE FORCE DOMESTIQUES

Lucie BERAUD-SUDREAU
Doctorante en sciences politiques à l'université Paris 2 Panthéon-Assas

Introduction

L'approfondissement des coopérations en Europe dans le secteur de l'armement est une des évolutions marquantes de l'économie de défense post-Guerre froide, tant pour les industriels – avec des groupes européens – que pour les gouvernements – avec des institutions formalisant ces coopérations[1]. Cette dynamique de long terme s'est accompagnée d'une recherche d'harmonisation du contrôle des exportations d'armement sur cette période. Pour les industriels, les programmes en coopération ou menés au sein d'une même entreprise ont entraîné une circulation croissante de matériels entre États européens et donc une augmentation du nombre de contrôles de ces biens – engendrant coûts et délais. La facilitation de la circulation des produits de défense dans l'Union européenne (UE) représente donc un enjeu important pour les entreprises. De plus, les industriels ont aussi intérêt à l'harmonisation de la prise de décision des États européens vers des clients hors de l'UE, car celle-ci réduit les incertitudes sur les autorisations d'exportation et facilite la prise de décision dans les entreprises. Enfin, la coopération dans le secteur de l'armement a eu des répercussions en matière de contrôle des exportations pour les gouvernements eux-mêmes. En effet, les autorités en charge du contrôle des exportations se sont inquiétées des risques de « *licence-shopping* » c'est-à-dire la possibilité que les entreprises localisent leur production là où les règles de contrôle des exportations seraient les moins strictes. Pour les décideurs politiques, l'harmonisation du contrôle des exportations est donc aussi devenue un enjeu crucial, qui participe de l'adaptation des stratégies étatiques aux mutations de l'économie de défense.

Le Code de conduite sur les exportations d'armement a ainsi été adopté en 1998. Cet instrument de nature politique liste huit critères[2] que les gouvernements européens doivent respecter dans leurs évaluations des demandes d'autorisation d'exportation des industriels, et crée un mécanisme de

[1] Voir, entre autres, Jean-Paul Hébert, «La consolidation de l'Europe de l'armement face au défi transatlantique», *Cahiers d'Études stratégiques*, n° 30, 2001 ; Bastien Irondelle et Pascal Vennesson, « L'Europe de la défense : institutionnalisation, européanisation », *Politique européenne*, n° 8, 2002 ; Catherine Hoeffler, *Les politiques d'armement en Europe : l'Adieu aux armes de l'État nation ? Une comparaison entre l'Allemagne, la France, le Royaume-Uni et l'Union européenne de 1976 à 2010*, thèse doctorat: Sciences Po, Paris, Institut d'études politiques, 2011.

[2] La liste des critères est la suivante : respect des engagements internationaux des États membres de l'UE ; respect des droits de l'homme dans le pays de destination finale ; situation intérieure dans le pays de destination finale ; préservation de la paix, de la sécurité et de la stabilité régionales ; sécurité nationale des États membres et des territoires dont les relations extérieures relèvent de la responsabilité d'un État membre ainsi que celle des pays amis ou alliés ; comportement du pays acheteur à l'égard de la communauté internationale (attitude envers le terrorisme, nature de ses alliances et respect du droit international) ; existence d'un risque de détournement de l'équipement à l'intérieur du pays acheteur ou de réexportation de celui-ci dans des conditions non souhaitées ; compatibilité des exportations d'armements avec la capacité technique et économique du pays destinataire.

notification des refus et de consultations entre États membres. Ce Code est aussi le résultat de mobilisations d'ONG en faveur d'un tel accord européen[3], dans un contexte international favorable à l'émergence de normes éthiques dans le commerce des armes[4]. La même année, les six plus importants producteurs d'armement (Allemagne, Royaume-Uni, France, Italie, Espagne et Suède) ont signé la *Letter of Intent* (LoI), concrétisée en 2000 par l'accord-cadre de Farnborough. Ces traités créent six groupes de travail pour rendre le marché de l'armement européen plus efficace, dont un groupe sur le contrôle des exportations d'armement. Les objectifs dans ce domaine sont de s'accorder sur des listes de clients pour des programmes d'armement en commun et de faciliter la circulation des produits de défense entre les États parties.

Au long des années 2000, des acteurs transnationaux (ONG, Commission européenne) recherchent un approfondissement de ces premières tentatives d'harmonisation. Les ONG souhaitent que le Code de conduite devienne un instrument juridiquement contraignant, et la Commission européenne travaille pour une libéralisation des contrôles des exportations intra-européennes. Malgré les intérêts économiques (amélioration de l'environnement de travail des entreprises) et éthiques (renforcement des normes) que favorisent ces différentes propositions, la France s'est opposée à cette intensification des coopérations sur les exportations d'armement. Ce jusqu'à la fin de l'année 2008, lorsque la France modifie drastiquement ses positions de négociations, pour permettre finalement l'adoption de la transformation du Code de conduite en Position Commune[5], et la directive 2009/43/CE sur les transferts intracommunautaires (directive TIC)[6]. Comment expliquer ce changement à la fois radical (passant du refus pur et simple à l'acceptation) et brusque (courant de l'année 2008) ?

Pour les chercheurs en analyse des politiques publiques, les explications du changement se divisent généralement entre facteurs externes ou internes[7]. Dans le cas présent, les facteurs de changement externes que sont le contexte politique et économique n'évoluent guère dans les années 2000, n'apportant pas d'élément décisif pour expliquer un changement aussi rapide. En effet, la majorité politique en France reste à droite en 2007, et les exportations d'armement ne diminuent pas drastiquement dans les années précédant 2008[8]. Nous verrons dans une première partie que les mobilisations des ONG et de la Commission européenne ont été constantes dans les années 2000. Dans cette optique, le changement français ne peut s'expliquer par ces facteurs externes.

[3] Anna Stavrianakis, *Taking Aim at the Arms Trade. NGOs, Global Civil Society and the World Military Order*, Londres, Zed Books, 2010.

[4] Mark Bromley, Neil Cooper et Paul Holtom, "The UN Arms Trade Treaty: arms export controls, the human security agenda and the lessons of history", *International Affairs*, n° 88:5, 2012, p. 1029-1048.

[5] Conseil de l'Union européenne, «Code de conduite de l'Union européenne en matière d'exportation d'armements », Bruxelles, 5 juin 1998.

[6] Directive 2009/43/CE du Parlement européen et du Conseil, du 6 mai 2009, simplifiant les conditions des transferts de produits liés à la défense dans la Communauté.

[7] Pour une revue de littérature dans PPC voir « Introduction générale : L'explication du changement dans l'analyse des politiques publiques : identification, causes et mécanismes », p. 11-52, *dans* Bruno Palier et Yves Surel (dir.), *Quand les politiques changent : Temporalités et niveaux de l'action publique*, Paris, L'Harmattan, 2010.

[8] Ministère de la défense, *Rapport au Parlement sur les exportations d'armement de la France en 2007*, oct. 2008, p. 14. Les évolutions des prises de commande montrent une certaine baisse entre 2002 et 2005, mais sont de nouveau sur une pente ascendante en 2006-2007.

Nous verrons ensuite que les réticences françaises vis-à-vis de l'approfondissement des coopérations en matière de contrôle des exportations se comprennent à partir des positions d'acteurs domestiques. Ainsi, le changement de pied du gouvernement français s'expliquera dans un troisième temps par l'interaction entre facteurs internes et externes : des acteurs au sein du système politico-administratif français ont effectué un travail politique à partir de fenêtres d'opportunités ouvertes par le niveau européen, ce afin de renverser le rapport de force interne et imposer leurs préférences. C'est donc par un « usage »[9] du niveau européen qu'il y a pu avoir une modification du rapport de force entre acteurs défendant des positions adverses, et par conséquent une modification des positions de négociation de la France. Cette contribution montre *in fine* que l'adaptation d'une stratégie étatique aux mutations sur le temps long de l'économie de défense ne se fait qu'à partir de mobilisations d'acteurs du système politico-administratif domestique.

Les mobilisations d'acteurs au niveau européen

Vers une position commune : la mobilisation des ONG

Les ONG actives sur les questions de contrôle des ventes d'armes ont rapidement estimé que l'Union européenne devait se doter d'un instrument plus contraignant que le Code de conduite. Adopté sous la forme d'une déclaration du Conseil de l'UE, dans le cadre de la Politique Étrangère et de Sécurité Commune (PESC), sur la base du titre V du TUE, le Code de 1998 n'était contraignant que politiquement. Son application n'était donc pas garantie par la Cour de Justice européenne. Les critères du Code étaient vagues, entraînant des divergences d'interprétation entre États. Le Code avait donc des limites quant à une mise en œuvre harmonisée entre États, notamment en matière de restriction des ventes[10]. C'est pourquoi le Parlement européen et les ONG ont continué à demander un instrument juridiquement contraignant[11].

Un travail d'évaluation du Code de conduite et de son application a été entrepris par les États à partir de 2003, puis les ONG ont lancé leur campagne demandant le renforcement du Code à partir de 2004[12]. En juin 2005, le Comité COARM a finalisé la révision du Code et s'est accordé sur un document de travail[13].

---

[9] Sophie Jacquot et Cornélia Woll (dir.), *Les Usages de l'Europe. Acteurs et transformations européennes*, Paris, L'Harmattan, p. 18.

[10] Mark Bromley et Michael Brzoska, "Towards a Common, Restrictive EU Arms Export Policy ? The Impact of the EU Code of Conduct on Major Conventional Arms Exports", *European Foreign Affairs Review*, n° 13, 2008, p. 333-356.

[11] Sybille Bauer, "The EU Code of Conduct on Arms Exports – much accomplished, much to be done", *Arms Trade, Final Report from the 2nd Ecumenical Conference in Gothenburg*, Christian Council of Sweden, n° 7, 2004, p. 31-47; Mark, Bromley, "10 years down the track – the EU Code of Conduct on Arms Exports", *European Security Review*, n° 39, juillet 2008 ; Sylvie Matelly, "Un code de conduite européen pour sécuriser les exportations ? Le cas des exportations d'armes en Europe", *Les cahiers Irice*, vol. 2, n° 6, 2010, p. 93-110.

[12] Anna Stavrianakis, *Taking Aim at the Arms Trade. NGOs, Global Civil Society and the World Military Order*, Londres, Zed Books, 2010, p. 77.

[13] Helen Close et Roy Isbister, "*Good Conduct? Ten Years of the EU Code of Conduct on Arms Exports*, Londres, Saferworld, juin 2008.

Mais cette première proposition pour en faire une Position commune est bloquée, notamment par la France qui demandait en échange la levée de l'embargo européen à l'encontre de la Chine. La transformation du Code en Position Commune nécessitant un consensus, la France a pu bloquer les négociations, jusqu'à fin 2008[14].

On observe l'existence d'une dynamique continue entre 2003 et 2008 en faveur d'un instrument contraignant, poussée principalement par les ONG. Ce n'est donc pas un changement dans la mobilisation des acteurs favorables à une Position Commune qui explique le retournement français.

Vers le « paquet défense » de la Commission

La Commission européenne dont, à l'origine, les compétences ne concernaient pas le secteur de l'armement, s'est intéressée à la création d'un marché européen de produits de défense, sous l'angle de la politique industrielle. Le développement des entreprises européennes de défense et l'évolution des compétences communautaires en matière de concurrence et d'industrie se sont conjugués pour que la Commission se saisisse de l'enjeu des contrôles intraeuropéens en matière d'armement[15]. La mobilisation du niveau communautaire s'explique d'autant plus que les résultats de la LoI sur cette question ont été décevants[16].

C'est particulièrement le cas pour la facilitation des contrôles des exportations : seules des licences globales de projet ont été créées, d'ailleurs peu utilisées par les entreprises[17].

Une étape importante de l'action de la Commission a été une communication datant de mars 2003, intitulée « Vers une politique communautaire en matière d'équipements de défense »[18]. En 2006, la Commission a lancé une consultation publique « sur la circulation intracommunautaire des produits liés à la défense ». La consultation visait à « jeter les bases pour une initiative communautaire facilitant le mouvement des produits liés à la défense au sein de la Communauté »[19]. D'après la Commission, la disparité des procédures de contrôle entre États-membres constituait un obstacle à l'émergence d'un marché européen de l'armement. Suite à cette consultation, la Commission a présenté en décembre 2007 le « paquet défense », incluant deux directives. La première concerne la régulation des marchés publics de défense et de sécurité. La seconde directive, la directive TIC, traite l'harmonisation des procédures d'exportation d'armement entre États-membres. L'objectif mis en avant par la Commission était la réduction des coûts générés par l'existence de 27 systèmes différents de contrôle, grâce à leur remplacement par des procédures communes dans le cas des

[14] Mark Bromley, "The Impact on Domestic Policy of the EU Code of Conduct on Arms Exports. The Czech Republic, the Netherlands and Spain", *SIPRI Policy Paper*, n° 21, mai 2008, p. 9.

[15] Hélène Masson, «La consolidation des industries de défense en Europe, et après? », *Notes de la Fondation Robert Schuman*, avril 2003.

[16] Samuel Faure, « Institutionnalisation de l'Europe de l'armement. Espaces et logiques d'action », *Working Paper*, Journée d'études organisée par les doctorants pour le 60ème anniversaire du CERI, 2012.

[17] Entretien, industriel, 24 avril 2013; Yves Fromion, « Les exportations de défense et de sécurité de la France », Rapport confié par M. Dominique de Villepin, Premier ministre, 2006.

[18] Commission européenne, Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, « Vers une politique de l'Union européenne en matière d'équipements de défense », *Défense européenne – Questions liées à l'industrie et au marché*, Bruxelles, 11 mars 2003.

[19] Commission européenne, Entreprise et industrie, "Call for Comments : Consultation Paper on the Intra-Community Circulation of Defence-Related Products", échéance 30 juin 2006.

transferts intracommunautaires et un principe d'autorisation des transferts entre États-membres plutôt qu'un principe de prohibition[20]. La directive TIC ne concernait toutefois pas les procédures de contrôle vers des clients hors UE, qui restent de la responsabilité des gouvernements. Toutefois, bien que cette directive visât à améliorer les conditions économiques pour les entreprises de défense, le gouvernement français était réticent face à l'initiative de la Commission. Dans leur réponse à la consultation de 2006, les autorités françaises ont souligné l'importance de la souveraineté nationale en matière d'exportation d'armement, et formulé leur préférence quant à une approche intergouvernementale[21].

On observe donc une pression continue de la Commission européenne en faveur d'une harmonisation des procédures de contrôle intracommunautaires – là encore ce facteur externe ne peut expliquer le retournement français.

Le village gaulois résiste encore et toujours…

Afin d'étudier les raisons du changement de position français, il nous faut d'abord comprendre pourquoi la France s'est retrouvée en position de blocage sur ces deux possibles approfondissements des coopérations sur le contrôle des ventes d'armes.

Les résistances face à la TIC : rester dans l'entre soi des grands exportateurs

Entre juin 2006, moment de la consultation de la Commission européenne sur le projet de directive TIC, et le début de l'année 2008 qui marque le début des négociations, les autorités françaises, et en particulier les fonctionnaires en charge du contrôle, sont réticentes vis-à-vis de ce projet.

Tout d'abord, une large part des acteurs de la politique d'exportation d'armement partage la crainte d'une ingérence de la Commission dans les décisions de contrôle des exportations : « Le ministère des Affaires étrangères résistait face aux directives, de même que les industries de défense. Ils avaient tous peur que la Commission n'aille se mêler de leurs affaires »[22]. L'initiative de l'instance bruxelloise n'était guère appréciée : « La directive était perçue comme empiétant sur la souveraineté nationale, parce qu'elle ouvrait la voie à la contestation d'un refus d'autorisation par une juridiction supranationale »[23]. En particulier, le SGDSN « craignait que la Commission n'outrepasse son rôle dans ce domaine : il y avait la crainte d'être dessaisi du contrôle des exportations »[24].

Par ailleurs, la directive TIC venait perturber les négociations de la LoI. Au moment où la Commission faisait sa proposition de directive, « le sous-comité 2 de la LoI s'apprêtait à mettre en place d'autres licences globales et à instituer des licences générales entre les six pays concernés, quand la

[20] Parlement européen, Communiqué de presse : « Produits liés à la défense : simplification des conditions des transferts », 16 décembre 2008; voir aussi Hélène Masson, « Union européenne et Armement, des dispositions du traité de Lisbonne aux propositions de directive de la Commission européenne », *Recherches et documents*, n° 9, Fondation pour la recherche stratégique, 2008.
[21] Secrétariat général des affaires européennes, Réponses des autorités françaises aux consultations publiques de la Commission : « Circulation intracommunautaire des produits liés à la défense des États membres », 2006.
[22] Entretien, responsable politique français, juin 2013.
[23] Entretien, ministère de la défense, juin 2013.
[24] Entretien, ministère de la défense, juillet 2013.

Commission s'est aussi intéressée à cette question »[25]. Ce sous-comité 2 est piloté par la France, plus précisément par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), acteur clé du dispositif de contrôle des exportations. Le Secrétaire général de cette institution préside la Commission interministérielle pour l'étude des exportations de matériel de guerre (CIEEMG), laquelle rassemble des représentants du ministère des Affaires étrangères, de la défense et de l'Économie. Le SGDSN gère le secrétariat de la CIEEMG et présente ses avis au Premier ministre. « Pour le SGDSN le contrôle des exportations c'est une question de légitimité institutionnelle. C'est le seul champ de compétences où il peut s'imposer aux autres. Le ministère des Affaires étrangères, de la défense, ils sont obligés de passer par le SGDSN pour traiter du contrôle export. […] Sur les autres sujets de politique étrangère […] le SGDSN n'a pas de spécificité. Et pour toutes les autres décisions, les ministères des Affaires étrangères et de la défense peuvent discuter et décider entre eux, sans consulter le SGDSN. Mais pas pour les exportations »[26]. Ainsi, en tant que clé de voûte du système administratif de contrôle et responsable des discussions au sein de la LoI, le SGDSN avait des griefs contre le projet de directive TIC qui lui étaient propres, les fonctionnaires de cette institution souhaitant privilégier la LoI comme lieu des discussions sur le contrôle des exportations, dans un cadre intergouvernemental[27]. Un ancien fonctionnaire du ministère de la défense relate qu'« il y avait une lutte de vitesse, entre ceux qui depuis 10 ans n'arrivent à rien produire dans la LoI et la Commission européenne. Une partie du SGDSN s'est sentie dépossédée »[28]. Un autre acteur confirme : « Les licences globales de projet ont été mises en place sous la houlette [du SGDSN]. C'était d'une extrême complexité, ça a eu peu de succès. Ça n'a jamais fonctionné. La TIC passait dessus ces licences globales de projet et vidait de leur contenu… »[29]

Certains acteurs domestiques souhaitaient donc préserver les coopérations sur le contrôle dans un cadre intergouvernemental restreint. Plus largement il y avait un consensus national dans le secteur des exportations d'armement pour éviter l'implication du niveau communautaire. Les réticences françaises quant à la TIC s'expliquent donc plutôt par des facteurs internes.

Le refus de la Position Commune : stratégies de blocage

Les autorités françaises étaient d'autre part opposées à la transformation du Code de conduite en Position Commune. Cependant, l'avancée des négociations sur la directive TIC va pousser les autorités françaises du secteur à faire progresser l'Europe intergouvernementale contre le développement de l'Europe communautaire.

Une des premières raisons pour lesquelles la France bloquait l'adoption d'une Position Commune qui renforcerait le statut du Code de conduite était, comme indiqué précédemment, le fait que les fonctionnaires en charge du contrôle étaient très attachés à la notion de souveraineté nationale et à leurs prérogatives. Un sentiment partagé par les acteurs du secteur était qu'une telle coopération

[25] Entretien, SGDSN, mai 2013.
[26] Entretien, SGDSN, décembre 2013.
[27] Entretiens, SGDSN, juin et juillet 2013; Entretien, ministère de la défense, juillet 2013.
[28] Entretien, ministère de la défense, juillet 2013.
[29] Entretien, ministère de la défense, juillet 2013.

n'est guère faisable ni souhaitable à 15 ou à 27, les discussions étant alors plus complexes et pouvant plus régulièrement mener à des blocages[30].

Mais les négociations sur la Position Commune sont restées longtemps dans l'impasse du fait que la France les ait attachées à la levée de l'embargo sur les armes à destination de la Chine, embargo établi en 1989 après la répression de la place Tiananmen[31]. Dès le début des débats en 2004 sur la transformation du Code de conduite en instrument juridiquement contraignant, cette question est liée à la question de l'embargo sur la Chine[32]. Conséquemment, entre juin 2005 et décembre 2008, la situation du Code de conduite n'évolue guère[33]. Si en 2005 la France est à la tête d'un petit groupe d'États en faveur de la levée de l'embargo[34], elle se retrouve isolée dès 2006[35]. En 2007, des députés européens et la Présidence finlandaise de l'UE tentent de faire repartir les discussions, en vain, la France demandant toujours la levée de l'embargo chinois en échange[36].

Toutefois, le contexte international semble favoriser une évolution de la position française. En 2005, une loi anti-sécession autorise la Chine à recourir à la force armée si Taiwan souhaitait rompre le *statu quo*. De plus, les violences au Tibet et dans le Xinjiang, qui coïncident avec l'organisation des Jeux Olympiques de Pékin, reçoivent une forte attention médiatique. Le consensus sur la levée de l'embargo devient alors politiquement difficile à obtenir[37]. La question de l'embargo chinois disparaît donc de l'agenda européen. D'autre part, des discussions débutent aux Nations unies sur le Traité sur le Commerce des armes, où l'Union européenne s'engage en faveur d'un tel traité. Les ONG et le Parlement européen pointent l'incohérence qui consiste d'un côté à pousser pour un traité contraignant au niveau international, mais à refuser cette contrainte au niveau régional[38]. Ces changements de contexte suffisent-ils à expliquer que la France, qui s'opposait à l'adoption d'un instrument européen contraignant, cède finalement, ce alors qu'elle maîtrise l'agenda politique européen sous sa présidence ? Le *timing* du changement de position français, dans le courant de l'année 2008, ne semble pas valider cette hypothèse[39].

Nous proposons une explication alternative aux changements des objectifs français, liée aux rapports de force internes du système politico-administratif français, et en interaction avec les développements européens.

---

[30] Entretiens, SGDSN, juin et juillet 2013 ; Entretien, industriel, juillet 2013.

[31] Sarah Depauw, "The Common Position on arms exports in the light of the emerging European defence market", *Background note*, Flemish Peace Institute, Bruxelles, janvier 2010.

[32] *Idem*.

[33] Bastien Irondelle, "European Foreign Policy: the End of French Europe?", *European Integration*, vol. 30, n° 1, 2008, p. 153-168 et p. 158.

[34] Daniel Dombey, "EU Considers Binding Rules on Arms Sales", *Financial Times*, 18 avril 2005.

[35] Roy Isbister, "EU: Rethinking the Arms Exports Code", *International Relations and Security Network (ISN)*, juin 2008 ; Helen Close, Roy Isbister, "Good conduct? Ten years of the EU Code of Conduct on Arms Exports", Londres, Saferworld, juin 2008, p. 4.

[36] Andrew Rettman, "France Blocking Plan for EU Code on Arms Exports", EUobserver.com, 18 janvier 2007.

[37] Sarah Depauw, *op. cit*.

[38] *Idem.*

[39] Pour plus de précisions sur les débats concernant la levée de l'embargo européen, voir : Hugo Meijer, " Transatlantic Perspectives on China's Military Modernization : The case of Europe's Arms Embargo Against the People's Republic of China ", IRSEM, *Paris Paper,* n° 12, 2014.

Les revirements français : jouer l'Europe contre l'Europe

Ainsi débutent, suite à des mobilisations d'acteurs non gouvernementaux, les négociations pour de nouveaux instruments européens sur le contrôle des ventes d'armes. Dans un cas comme dans l'autre, les autorités françaises sont réticentes, voire opposées, à ces évolutions. Pourtant, et la directive TIC et la Position Commune seront adoptées sous la présidence française de l'Union européenne (PFUE) à la fin de l'année 2008. Il s'agit maintenant d'expliquer ces revirements.

Le revirement sur la TIC : un usage stratégique du niveau européen

Le revirement français sur la directive TIC s'explique par le fait que les acteurs du contrôle, et notamment le SGDSN, ont dû céder à une double pression. En premier lieu, les négociations sur le « paquet défense » ont coïncidé avec les 6 mois de présidence française de l'Union européenne (PFUE) entre juillet et décembre 2008. Des pressions de la part des acteurs politiques se sont alors exercées afin de pouvoir obtenir des résultats en fin de présidence. En effet, l'approche de la PFUE a incité les dirigeants français à mettre en avant un projet en matière de défense, les questions de sécurité et de défense ayant été placées au sommet de l'agenda[40]. L'Élysée et le ministère de la défense ont demandé aux représentants français à Bruxelles qu'un accord sur les questions de défense soit atteint avant fin 2008[41]. Or, « l'Europe de la défense » étant traditionnellement un sujet défendu par la France, le « paquet défense » de la Commission était un projet à la disposition des autorités françaises, pour que celles-ci récoltent les bénéfices politiques d'une adoption sous présidence française[42]. « La Commission a convaincu le MAE qui s'est dit : "on tient quelque chose d'emblématique pour la PFUE". Le paquet défense de la Commission permettait de mettre quelque chose à faire lors de la PFUE, de plus il était en cohérence avec l'idée d'"Europe de la défense" qu'on voulait mettre en avant. Ça a donc été le MAE qui était pour, contre le SGDSN. Ça a été tranché par un arbitrage des hautes autorités. Ça a grincé un peu. Mais les politiques ont privilégié la lecture politique de la présidence européenne, avec la volonté de faire avancer l'Union »[43]. Face à la détermination des décideurs politiques d'obtenir un accord européen sur les questions de défense, et face à la stratégie diplomatique de la Commission, les craintes des responsables du contrôle des exportations sont passées au second plan.

De plus, les fonctionnaires responsables du soutien aux exportations ont vu dans la directive TIC une opportunité pour simplifier les processus de contrôle des exportations français dans leur ensemble – basés sur un dispositif législatif quasiment inchangé depuis 1939.

---

[40] Secrétariat général des affaires européennes, Présidence française du Conseil de l'Union européenne, *Bilan et perspectives, 1er juillet – 31 décembre 2008, Une Europe qui agit pour répondre aux défis d'aujourd'hui*, 2008, p. 11.

[41] Catherine Hoeffler, L*es politiques d'armement en Europe : l'Adieu aux armes de l'État nation ? Une comparaison entre l'Allemagne, la France, le Royaume-Uni et l'Union européenne de 1976 à 2010*, thèse doctorat: Sciences Po, Paris, Institut d'études politiques, 2011, p. 518 ; p. 523-524.

[42] Catherine Hoeffler, *Idem* ; Yves Buchet de Neuilly, « Sous l'emprise de la présidence. Déplacements structurels, construction des intérêts et stratégies des diplomates au Conseil », *Politique européenne*, n° 35 (3), 2011, p. 83-113 ; Entretien, ministère de la défense, juillet 2013.

[43] Entretien, ministère de la défense, juin 2013.

Or, pour les acteurs en charge du soutien à l'export, il était devenu urgent de moderniser ces procédures perçues comme trop rigides et génératrices de coûts et d'incertitudes pour les industriels[44]. La directive TIC offre alors l'opportunité de proposer au Parlement français une réforme du contrôle des exportations et par cette occasion de simplifier l'ensemble des procédures[45].

Les acteurs qui soutenaient la relance des exportations se sont donc saisis de l'initiative de la Commission pour pousser vers une refonte complète du système de contrôle, via une simplification calquée sur les procédures développées dans la directive TIC.

Un acteur impliqué dans les négociations relate qu'« il y a eu un changement d'état d'esprit pendant les négociations en France, un changement constructif : ne pourrait-on pas en profiter pour améliorer le système ? En effet, il y avait un engorgement du système administratif et des plaintes des industriels. Au début de l'année 2008, au commencement des négociations, on s'est alors dit qu'on allait profiter de la transposition pour tout rénover, puisqu'on devait de toute façon passer par la loi et par plein de décrets d'application »[46]. Un responsable du soutien aux exportations raconte que : « Les gens ne voulaient pas réformer le système. […] Mais on leur a dit : la TIC est de toute façon contraignante, ça va arriver. Et si on n'est pas prêts à ce moment-là, le système va être complètement grippé »[47]. Ceci témoigne de luttes internes et plus largement du travail politique effectué pour simplifier les procédures de contrôle à la faveur des négociations sur la directive TIC.

Le « paquet défense » est adopté par le Parlement européen en décembre 2008, ce qui permet aux autorités françaises de le porter au bilan de la PFUE. L'adoption finale a lieu début 2009, via la directive 2009/43/CE, qui crée plusieurs mécanismes visant à simplifier les exportations d'armement entre États-membres[48]. La loi n° 2011-702 du 22 juin 2011 transpose la directive TIC, tout en appliquant les procédures prévues pour les exportations intra-UE à l'ensemble des exportations hors UE, ce en vue de simplifier le système français de contrôle des exportations[49].

Le revirement sur la Position Commune : un « consensus ambigu » ?

La reprise des discussions sur la Position Commune coïncide avec les négociations sur la directive TIC. L'arrivée désormais perçue comme inéluctable de cette dernière suscite de fortes inquiétudes quant à des ingérences futures de la Commission européenne dans les décisions des États en matière d'exportation d'armes. D'après un acteur du ministère de la défense, ces craintes s'appuyaient sur des fondements juridiques. « Des débats ont eu lieu dans les 6 mois avant la PFUE et le début des négociations. On craignait que la Commission ne finisse par avoir la compétence du commerce extérieur dans l'armement. Si elle pouvait réguler le commerce intérieur [grâce à la TIC], elle pouvait gagner des compétences externes. Via des questions de jurisprudence la Commission peut prendre

[44] Entretien, ministère de la défense, juin 2013.
[45] Entretien, ministère de la défense, juillet 2013.
[46] Entretien, ministère de la défense, juin 2013.
[47] Entretien, ministère de la défense, juillet 2013.
[48] Hélène Masson, Lucia Marta, Patrick Léger, Martin Lundmark, "The 'Transfer Directive' : Perceptions in European Countries and Recommendations", *Recherches & Documents*, n° 4, Fondation pour la recherche stratégique, 2010, p. 7.
[49] Loi n° 2011-702 du 22 juin 2011 relative au contrôle des importations et des exportations de matériels de guerre et de matériels assimilés, à la simplification des transferts des produits liés à la défense dans l'Union européenne et aux marchés de défense et de sécurité.

les mesures nécessaires dans les relations internationales, hors de l'UE. C'est le parallélisme des compétences internes/externes, cette évolution était redoutée de façon fondée. Après avoir organisé la " libre-circulation " des biens militaires au sein de l'UE, la Commission pouvait prendre des compétences sur les exportations vers le reste du monde »[50]. Ces propos font référence à l'affaire 22/70 de la Cour européenne de justice du 31 mars 1971 (arrêt AETR). Une conséquence de cet arrêt est que la mise en œuvre d'une politique par le niveau communautaire, du fait qu'elle génère la création de règles communes à caractère interne, entraîne l'impossibilité pour les États membres d'établir par eux-mêmes des accords internationaux dans le même domaine[51].

En conséquence, si le gouvernement français avait pris la décision *in fine* de ne pas s'opposer au principe d'une directive régissant les exportations d'armement au sein de l'UE, la question se posait alors d'endiguer le développement des compétences communautaires.

La solution envisagée par les services juridiques du ministère de la défense a été « d'investir la PESC, le 2ème pilier[52], où on avait déjà le Code de conduite »[53]. Plus précisément, « pour bloquer le développement d'une compétence communautaire dans les exportations hors UE, il faut un acte PESC dans le domaine des exportations, pour montrer que les gouvernements ont commencé à exercer cette compétence sur une base 2e pilier. C'est une protection, par la construction d'une base juridique. Pour qu'ensuite la Commission ne puisse pas plaider un vide juridique pour prendre cette place »[54]. Cette initiative apparaît d'ailleurs dans un rapport parlementaire analysant les possibles impacts de la directive TIC[55]. L'analyse proposée par le ministère de la défense est donc de développer la coopération intergouvernementale dans le cadre du 2e pilier, afin de freiner le développement d'une compétence communautaire, dans une logique autant politique que juridique : « La Position Commune est un geste politique visant à protéger les États dans leur rôle de contrôleurs des exportations. La liste des biens militaires est faite dans le cadre de la PESC. Chaque année la Commission doit transposer la liste qui est PESC pour le fonctionnement de la TIC. Cela montre que les États restent maîtres. La Commission peut faire les transferts [intracommunautaires], mais les États gardent la main sur le " grand export ", la politique » [56].

Avant la fin de la PFUE, le 8 décembre 2008, le Conseil de l'UE adopte donc finalement la Position Commune 2009/944/CFSP (PSDC)[57].

---

[50] Entretien, ministère de la défense, juillet 2013.

[51] Robert Kovar, « L'affaire de l'A.E.T.R. devant la Cour de Justice des Communautés Européennes et la compétence internationale de la C.E.E. », *Annuaire français de droit international,* vol. 17, n° 17, 1971, p. 386-418; « Arrêt de la Cour de justice, AETR, affaire 22-70, », *Centre Virtuel de la Connaissance sur l'Europe,* 31 mars 1971, disponible sur: http://www.cvce.eu/obj/arret_de_la_cour_de_justice_aetr_affaire_22_70_31_mars_1971-fr-0d4dae9f-514b-47e0-bd49-502318d6e798.html, dernière consultation le 5 mars 2015.

[52] Depuis le traité de Lisbonne : « compétences partagées ».

[53] Entretien, ministère de la défense, juillet 2013.

[54] Entretien, ministère de la défense, juillet 2013.

[55] Yves Fromion, « Rapport au Premier ministre. Les moyens de développer et de structurer une industrie européenne de défense », 30 juin 2008, p. 25.

[56] Entretien, ministère de la défense, juillet 2013.

[57] Conseil de l'Union européenne, « Position Commune 2008/944/PESC du Conseil du 8 décembre 2008 définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires », 8 décembre 2008.

Conclusion

Comment expliquer l'acceptation par la France de la directive TIC et de la Position Commune, alors qu'elle était au départ opposée à ces évolutions et alors même que celles-ci étaient *a priori* dans l'intérêt de ses entreprises de défense ? Au-delà des mutations au long cours de l'économie de défense, les évolutions du contexte immédiat ne suffisent pas à expliquer ces revirements : le contexte politique et économique ne connaît pas de revirement majeur dans la période précédant cette décision fin 2008, de même que les pressions des acteurs externes au système politico-administratif français (ONG, Commission européenne). Il faut plutôt rechercher l'explication du changement dans l'interaction entre facteurs internes et externes.

Ce sont les luttes domestiques internes et l'appropriation par les acteurs du soutien aux exportations d'armement des développements européens qui permettent de comprendre l'évolution des choix de négociations français, *in fine* favorables à la TIC afin de réformer dans son ensemble le système de contrôle des exportations d'armement de l'Europe. Les négociations sur la directive TIC ont ainsi enclenché la modification des intérêts français quant à la Position Commune : celle-ci est apparue alors comme un instrument permettant d'empêcher un développement de la compétence des instances communautaires en matière de contrôle des exportations d'armement hors de l'Union européenne.

Ce chapitre montre par ailleurs que l'adaptation de la stratégie étatique aux mutations de long terme de l'économie de défense, en l'occurrence l'approfondissement des coopérations européennes, ne se fait qu'à l'issue de rapports de forces internes au système politico-administratif national.

Références

BAUER Sybille, "The EU Code of Conduct on Arms Exports – Much Accomplished, Much to Be Done", *Arms Trade, Final Report from the 2nd Ecumenical Conference in Gothenburg*, Christian Council of Sweden, n° 7, 2004, p. 31-47.

BROMLEY Mark, "The Impact on Domestic Policy of the EU Code of Conduct on Arms Exports. The Czech Republic, the Netherlands and Spain", *SIPRI Policy Paper*, n° 21, mai 2008.

BROMLEY Mark, "10 Years Down the Track – the EU Code of Conduct on Arms Exports", *European Security Review*, n° 39, juillet 2008.

BROMLEY Mark, BRZOSKA Michael, "Towards a Common, Restrictive EU Arms Export Policy? The Impact of the EU Code of Conduct on Major Conventional Arms Exports", *European Foreign Affairs Review*, n° 13, 2008, p. 333-356.

BUCHET DE NEUILLY Yves, « Sous l'emprise de la présidence. Déplacements structurels, construction des intérêts et stratégies des diplomates au Conseil », *Politique européenne*, n° 35(3), 2011, p. 83-113.

CLOSE Helen, ISBISTER Roy, *Good conduct? Ten years of the EU Code of Conduct on Arms Exports*, Londres, Saferworld, juin 2008.

Conseil de l'Union européenne, « Code de conduite de l'Union européenne en matière d'exportation d'armements», Bruxelles, 5 juin 1998.

Commission européenne, Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, « Vers une politique de l'Union européenne en matière d'équipements de défense », *Défense européenne – Questions liées à l'industrie et au marché*, Bruxelles, 11 mars 2003.

Commission européenne, Entreprise et industrie, "Call for Comments : Consultation Paper on the Intra-Community Circulation of Defence-Related Products", échéance 30 juin 2006.

Conseil de l'Union européenne, « Position Commune 2008/944/PESC du Conseil du 8 décembre 2008 définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires, 8 décembre 2008.

DEPAUW Sarah , "The Common Position on Arms Exports in the Light of the Emerging European Defence Market", *Background note*, Flemish Peace Institute, Bruxelles, janvier 2010.

DOMBEY Daniel, "EU Considers Binding Rules on Arms Sales", *Financial Times*, 18 avril 2005.

FAURE Samuel, « Institutionnalisation de l'Europe de l'armement. Espaces et logiques d'action », *Working Paper*, Journée d'études organisée par les doctorants pour le 60ème anniversaire du CERI, 2012.

FROMION Yves, « Rapport au Premier ministre. Les moyens de développer et de structurer une industrie européenne de défense », 30 juin 2008.

HEBERT Jean-Paul, « La consolidation de l'Europe de l'armement face au défi transatlantique », *Cahiers d'Études stratégiques*, n° 30, 2001.

HOEFFLER Catherine, *Les politiques d'armement en Europe : l'Adieu aux armes de l'État nation ? Une comparaison entre l'Allemagne, la France, le Royaume-Uni et l'Union européenne de 1976 à 2010*, thèse doctorat : Sciences Po, Paris, Institut d'études politiques, 2011.

IRONDELLE Bastien, VENNESSON Pascal, (eds.), « L'Europe de la défense : institutionnalisation, européanisation », *Politique européenne*, 2002.

IRONDELLE Bastien, "European Foreign Policy: the End of French Europe?", *European Integration*, vol. 30, n° 1, 2008, p. 153-168 et p. 158.

ISBISTER Roy, "EU: Rethinking the Arms Exports Code", *International Relations and Security Network (ISN)*, juin 2008.

JACQUOT Sophie, WOLL Cornélia (dir.), *Les Usages de l'Europe. Acteurs et transformations européennes*, Paris, L'Harmattan, 2004.

KOVAR Robert, « L'affaire de l'A.E.T.R. devant la Cour de Justice des communautés européennes et la compétence internationale de la C.E.E. », *Annuaire français de droit international*, vol. 17, n° 17, 1971, p. 386-418.

MASSON Hélène, « La consolidation des industries de défense en Europe, et après ? », *Notes de la Fondation Robert Schuman*, avril 2003.

MASSON Hélène, « Union européenne et Armement, Des dispositions du traité de Lisbonne aux propositions de directive de la Commission européenne », Fondation pour la recherche stratégique, Recherches et documents, n° 9, 2008.

MASSON Hélène, MARTA Lucia, LÉGER Patrick, LUNDMARK Martin, "The 'Transfer Directive' : perceptions in European countries and recommendations", *Recherches & Documents*, n° 4, Fondation pour la recherche stratégique, 2010, p. 7.

MATELLY Sylvie, "Un code de conduite européen pour sécuriser les exportations ? Le cas des exportations d'armes en Europe", *Les cahiers Irice*, vol. 2, n° 6, 2010, p. 93-110

MEIJER Hugo, "Transatlantic Perspectives on China's Military Modernization : The Case of Europe's Arms Embargo Against the People's Republic of China", *Paris Paper,* n° 12, 2014.

Ministère de la défense, *Rapport au Parlement sur les exportations d'armement de la France en 2007*, octobre 2008.

PALIER Bruno, SUREL Yves (dir.), *Quand les politiques changent : Temporalités et niveaux de l'action publique*, Paris, L'Harmattan, 2010.

Parlement européen, Communiqué de presse : "Produits liés à la défense : simplification des conditions des transferts", 16 décembre 2008.

RETTMAN Andrew, "France Blocking Plan for EU Code on Arms Exports", *EUobserver.com*, 18 janvier 2007.

Secrétariat général des affaires européennes, Réponses des autorités françaises aux consultations publiques de la Commission : « Circulation intracommunautaire des produits liés à la défense des États membres », 2006.

Secrétariat général des affaires européennes, Présidence française du Conseil de l'Union européenne, *Bilan et perspectives, 1er juillet – 31 décembre 2008, Une Europe qui agit pour répondre aux défis d'aujourd'hui*, 2008.

STAVRIANAKIS Anna, *Taking Aim at the Arms Trade. NGOs, Global Civil Society and the World Military Order*, Londres, Zed Books, 2010.

LA COOPERATION FRANCO-BRITANNIQUE DANS LE SECTEUR DES ARMES COMPLEXES : VERS UNE POLITIQUE INDUSTRIELLE BILATERALE

Alice PANNIER
Doctorante en Relations internationales à Sciences Po Paris

Logiques et dilemmes de la coopération internationale dans l'armement

Depuis la deuxième moitié du 20e siècle, les besoins de défense des États occidentaux se sont sophistiqués, donnant lieu à une augmentation inexorable du coût des équipements (de l'ordre de 5 à 10 % par unité par an)[1] alors que, depuis la fin de la Guerre froide, les budgets de défense n'ont cessé de baisser. En Europe, France, Allemagne et Royaume-Uni restent les trois pays bénéficiant d'une industrie de l'armement solide et de budgets de défense significatifs et ont le désir de maintenir des compétences industrielles et technologiques militaires sur leurs territoires, malgré les pressions de la mondialisation. Dans ce contexte, la coopération interétatique apparaît alors comme le moyen de réconcilier l'augmentation des coûts des équipements, la libéralisation des marchés, la baisse des budgets de défense, et la quête de maintien des compétences nationales. Les rapprochements industriels doivent permettre de partager les coûts de R&D, de maintenir une taille critique pour faire face à la concurrence (notamment transatlantique), et les programmes menés en coopération doivent offrir des économies d'échelles et faire ainsi baisser les coûts unitaires. Ainsi, dans certains domaines industriels de défense, stratégies étatiques et stratégies industrielles ne font qu'un.

Cela étant, les difficultés économiques et les enjeux politiques de la coopération internationale dans un domaine stratégique comme l'armement ont déjà été largement démontrés, particulièrement dans le cas des programmes multilatéraux et/ou *ad hoc*[2]. Keith Hartley, économiste libéral, s'est intéressé aux « inefficiences » de la collaboration internationale qui augmentent avec le nombre de participants : complexité des accords de gouvernance, besoins multiples et divergents, le tout menant à des retards et à une augmentation des coûts, voire à des abandons de projets[3]. Face à ces difficultés, les États européens ont cherché à créer des structures de gouvernance multilatérales et ont semblé assouplir leur emprise sur ce marché. Toutefois, Catherine Hoeffler a démontré comment les stratégies industrielles des États européens, en semblant se libéraliser, se réinventent en fait au niveau de l'UE via un déplacement de l'action étatique (c'est la « montée vers l'Europe »).

---

[1] David Kirkpatrick, "Trends in the Costs of Weapon Systems and the Consequences", *Defence and Peace Economics*, vol. 15, n° 3, 2004, p. 262-263.

[2] Pour une perspective générale : Ethan Kapstein, "International Collaboration in Armament Production: the Second Best Solution", *Political science quarterly*, vol. 106, n° 4, 1991-1992, p. 567-675 ; Mark A. Lorell et Julia Lowell, *Pros and Cons of International Weapons Procurement Collaboration*, Santa Monica, RAND, 1995. Pour des cas impliquant la France : Pierre Dussauge et Christophe Cornu, *L'industrie française de l'armement : coopérations, restructurations et intégration européenne*, Paris, Economica, 1998 ; Ulrich Krotz, *Flying Tiger : International Relations Theory, and the Politics of Advanced Weapons Production*, Oxford, Oxford University Press, 2011 ; Jean Joana et Andy Smith, « Du couple franco-allemand à une nouvelle Entente cordiale : la France dans le programme A400M », *Les Champs de Mars*, n° 16, 2004, p. 133-146.

[3] Voir par exemple Keith Hartley, « White Elephants? The Political Economy of Multinational Defence Projects », *New Direction : The Foundation for European Reform*, octobre 2012.

En résulte une gouvernance « multiniveaux » de la coopération en matière d'armement, à laquelle participent les États, l'AED (UE), l'OCCAr (hors UE)[4]. Ces nouvelles structures de gouvernance facilitent-elles la coopération internationale ?

Selon Marc DeVore, elles sont un piège pour la coopération interétatique dans le secteur de l'armement, notamment parce qu'elles limitent le contrôle des États sur ce que font les firmes et contraignent leur pouvoir de rétractation, augmentant les risques de dépassement des coûts[5].

Au vu de ce bref état de l'art, on note que la littérature existante est déjà significative pour ce qui est, d'une part, de la coopération sur des programmes *ad hoc* et, d'autre part, du fonctionnement des institutions multilatérales. L'initiative franco-britannique témoigne d'une approche encore différente. D'abord, son niveau de gouvernance n'est ni simplement national ni européen, mais bien bilatéral. Mais aussi, et surtout, nous avons affaire à une réelle stratégie sectorielle de long terme, un programme de politique industrielle qui est mis en commun, et s'élabore entre les gouvernements britannique et français avec les acteurs industriels. On peut alors rapprocher la démarche franco-britannique du concept de « politique publique internationale » (PPI) développé par Frank Petiteville et Andy Smith et défini comme « l'ensemble des programmes d'action revendiqués par des autorités publiques ayant pour objet de produire des effets dépassant le cadre d'un territoire stato-national »[6]. Ce chapitre espère alors offrir de nouveaux éléments pour comprendre le fonctionnement et les enjeux d'un programme de politique industrielle bilatérale en nous intéressant à la démarche franco-britannique dans le secteur industriel des armes complexes.

Dans ce chapitre, on expliquera pourquoi et comment le niveau bilatéral, dans le cas franco-britannique, se construit comme nouvel échelon d'action dans le secteur de l'industrie missilière, principalement autour de MBDA, deuxième fabricant mondial et leader en Europe. La firme majoritairement franco-britannique MBD est née de la fusion de BAe Dynamics et Matra Défense (aujourd'hui EADS) en 1996. A l'origine de la fusion : des programmes de missile longue portée similaires lancés en parallèle par les firmes française et britannique[7]. En 1999, MBD est rejoint par l'italien Alenia Marconi (qui deviendra Finmeccanica) qui acquiert 25 % des parts, Français et Britanniques restant les principaux actionnaires avec 37,5 % chacun. MBDA est officiellement formée en 2001. Le missile air-sol Storm Shadow/SCALP-EG est en 1996 le premier – et à cette date le seul – système d'arme produit par MBDA en franco-britannique. Mais en 2008, les gouvernements français et britannique annoncent leur projet d'élaborer conjointement une « stratégie industrielle pour les armes complexes »[8].

[4] Catherine Hoeffler, *Les politiques d'armement en Europe : "l'Adieu aux armes" de l'État nation? Une comparaison entre l'Allemagne, la France, le Royaume-Uni et l'Union européenne de 1976 à 2010*, Thèse de doctorat, Sciences Po, Paris, 2011.

[5] Marc Devore, "The Arms Collaboration Dilemma: Between Principal-Agent Dynamics and Collective Action Problems", *Security Studies*, vol. 20, n° 4, 2011, p. 624-662.

[6] Frank Petiteville et Andy Smith, « Analyser les politiques publiques internationales », *Revue française de science politique*, vol. 56, n° 3, 2006, p. 362.

[7] Hélène Masson, « La réorganisation de l'industrie de défense britannique », *Recherches & Documents*, n°5, Fondation pour la recherche stratégique, 2008, p. 62.

[8] Gordon Brown et Nicolas Sarkozy, « Déclaration du Sommet franco-britannique », 27 mars 2008.

L'objectif est « [d'utiliser] de manière plus efficace nos capacités et nos compétences industrielles respectives pour tenir compte de nos besoins militaires en armes, notamment lorsque ceux-ci sont communs »[9].

Le premier contrat commun depuis le lancement de cette initiative a été signé en mars 2014 et concerne le missile antinavire FASGW/ANL[10]. Entre temps, le traité de Lancaster House a été signé. Ce dernier donne à la relation franco-britannique de défense un nouveau cadre et prévoit un renforcement des liens bilatéraux dans tous les domaines de la politique de défense[11].

Dans une première partie, on s'intéressera à la conception de cette stratégie industrielle conjointe, qui s'inspire d'une politique de partenariat public-privé instaurée au Royaume-Uni, avant de se tourner vers la mise en œuvre de cette initiative bilatérale dont on peut déjà analyser les enjeux.

" Team Complex Weapons " : la nouvelle stratégie industrielle britannique

Dans les années 1980, Margaret Thatcher lance une politique qui lui survivra : celle de la " *best value for money* ", c'est-à-dire de choix d'acquisition guidés par les offres de la libre concurrence plutôt que par un protectionnisme industriel, y compris dans le domaine de la défense. Cette politique est critiquée à partir du milieu des années 1990 au sein de la communauté de défense britannique : la concurrence entraîne les entreprises à faire des promesses irréalistes, et la concurrence internationale met en danger leur survie et la sécurité d'approvisionnement de l'État[12]. Pourtant, les publications successives post-Thatcher, telles que la *Defence Industrial Policy* en 2002, la *Defence Industrial Strategy* en 2005 et la *National Security Through Technology* en 2012 reprennent le mot d'ordre de la " *best value for money* " : « Notre politique générale… est d'utiliser la concurrence ouverte pour atteindre un bon rapport qualité-prix – obtenir les meilleurs produits et services au coût le plus bas possible pour les contribuables »[13]. Or, dans le même temps, les documents rappellent la nécessité de préserver une base industrielle de défense dans certains domaines jugés stratégiques. C'est sur cette base que se développe en Grande-Bretagne un partenariat public-privé dans le secteur stratégique des armes complexes – partenariat qui entraîne ensuite le développement d'une approche coopérative bilatérale.

Depuis le milieu des années 2000, le secteur des armes complexes[14] connaît une baisse des commandes. Or, ce secteur dépend uniquement des clients étatiques, puisqu'il ne produit pas de technologies à double usage ni de biens purement commerciaux. Ainsi, le gouvernement Blair note dans la *Defence Industrial Strategy* publiée en décembre 2005 que les investissements britanniques

[9] *Ibid*.

[10] FASGW(H)/ANL : *Fast anti-ship guided weapon (heavy)*/Antinavire léger, renommé à l'automne 2014 *Sea Venom*-ANL.

[11] *Traité de coopération en matière de défense et de sécurité entre la République française et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord*, Londres, 2 novembre 2010.

[12] Catherine Hoeffler, *Les politiques d'armement en Europe*, thèse Sciences Po, p. 193-202.

[13] "Our general policy… is to use open competition to achieve value-for-money – obtaining the best products and services at the lowest possible cost to the taxpayers", *National Security Through Technology*, Ministry of Defence, 2012, p. 13.

[14] Il s'agit, typiquement, des missiles téléguidés fixés sur des plateformes (avions, navires, chars).

dans le secteur devraient baisser de 40 % au cours des cinq années suivantes[15]. Pour préserver les capacités industrielles et technologiques nationales le gouvernement annonce une « stratégie de soutien » au secteur des armes complexes. Aussi, à partir de 2006 se met en place un nouveau type de partenariat gouvernement-industrie avec l'initiative " *Team Complex Weapons* " (TCW).

Cette stratégie consiste, en fait, à garantir à l'industrie un portefeuille de commandes par le biais d'une « filière industrielle intégrée dans une approche globale de la relation entre le ministère de la défense et l'industrie »[16]. La " *Team Complex Weapons* " est présidée par le *Ministry of Defence* (MOD) via l'agence chargée d'administrer l'acquisition militaire, DE&S (*Defence Equipment and Support*) et par MBDA UK et implique d'autres acteurs industriels britanniques : Thales UK, Roxel et QinetiQ. MBDA et le gouvernement britannique ont signé un accord pour un portefeuille de six projets d'une valeur totale prévue de 4 milliards de livres (4,85 milliards d'euros) sur 10 ans, permettant de réaliser une économie globale de 1,2 milliard de livres (1,5 milliard d'euros)[17]. Les économies seront réalisées, notamment, par le biais d'une réutilisation de certains composants sur plusieurs programmes. Au-delà de ces épargnes, l'équipe « mixte » gouvernement-industrie traduit une nouvelle « philosophie de partenariat » : « l'idée est que le gouvernement bénéficie d'une recherche dans des domaines pertinents pour ses besoins de défense, et l'industrie est assurée que son travail a des chances de donner lieu à un produit commercialisable »[18]. En principe, cela améliore le contrôle du MOD sur l'industriel, et rapproche le Royaume-Uni des pratiques en vigueur dans la filière missile française.

L'autre axe de la stratégie britannique : la coopération internationale, particulièrement bilatérale, avec les États-Unis et la France. C'est ce qui est indiqué dans le *Defence Growth Partnership*, lancé en décembre 2012 et co-présidé par le *Minister for Business* et MBDA, avec le MOD comme « client »[19]. Un document paru en septembre 2013 présente la stratégie globale du gouvernement britannique pour maintenir une industrie de défense compétitive et innovante et indique : « [les] tendances globales résultent en une concurrence accrue sur le marché de l'export, aussi bien pour les joueurs bien établis que pour les nouveaux entrants, et encourage à davantage de coopération avec tous nos alliés et partenaires de défense dans le monde, notamment les États-Unis et la France »[20]. La même logique est reprise, côté français, dans le Livre blanc de 2013, avec toutefois un regard tourné vers l'Europe, plutôt que vers les États-Unis.

Une intégration bilatérale du secteur

Dans la deuxième moitié des années 2000, les motivations pour développer la coopération franco-britannique dans le secteur des missiles sont donc nombreuses.

---

[15] Secretary of State for Defence, "Defence Industrial Strategy : Defence White paper", décembre 2005, p. 102.

[16] Assemblée nationale, Commission de la défense nationale et des forces armées, « Audition de M. Antoine Bouvier, président-directeur général de MBDA, sur la coopération franco-britannique et la filière missile », *Compte rendu n° 39*, 18 mai 2011, p. 5.

[17] Steve Wadey, "Progressing Team Complex Weapons", *RUSI Defence Systems*, juin 2010, p. 90-91.

[18] Entretien, Ministry of Defence (MOD), 2014.

[19] Defence Growth Partnership, "Securing Prosperity: A strategic vision for the UK Defence Sector", septembre 2013, p. 3.

[20] *Ibid*., p. 5. Traduction de l'auteur.

On assiste notamment à une convergence des intérêts publics et privés. En premier lieu, la firme MBDA dont « la forme juridique et l'organisation interne […] demeurent imprégnées par les logiques nationales »[21] et par les duplications offre de bonnes perspectives pour une « rationalisation » du secteur. Le mot est pris en 2008, semble-t-il sous l'impulsion du Groupe de travail de haut niveau franco-britannique (*High Level Working Group*, HLWG) qui regroupe les gouvernements et l'industrie de défense et vise à promouvoir la coopération. D'abord, les gouvernements français et britannique lancent un partenariat pour l'innovation et la technologie dans le secteur des armes complexes (*Innovation and Technology partnership*, ITP), partenariat qui implique les mêmes firmes que celles impliquées dans la TCW. Ainsi, dans la même logique que celle qui a mené à l'initiative nationale britannique, les gouvernements et l'industrie se coordonnent pour produire une recherche correspondant à des besoins capacitaires et orientée pour le long terme (il s'agit de technologies à faible niveau de maturité).

Peu de temps après la signature du partenariat ITP, lors du sommet bilatéral de mars 2008, le Président Sarkozy et le Premier ministre Brown annoncent leur volonté d'adopter une « stratégie industrielle conjointe » dans le domaine des armes complexes. En d'autres termes, il s'agit de rationaliser le secteur (principalement MBDA) en intégrant les filiales France et Royaume-Uni du groupe. Pour cela, les gouvernements français et britanniques se sont accordés, avec l'industrie, sur un portefeuille de programmes qui seront développés en commun. Cette volonté est entérinée en novembre 2010, avec la signature du Traité de coopération de défense et de sécurité (dit traité de Lancaster House) et la déclaration qui s'en est suivie :

> « Nous sommes parvenus à un accord sur un plan stratégique décennal concernant le secteur britannique et français des missiles. Nous allons travailler à la mise en place d'un maître d'œuvre industriel européen unique et à la réalisation d'économies pouvant aller jusqu'à 30 %. Cette stratégie optimisera la fourniture de capacités militaires, adaptera nos technologies plus efficacement, permettra une interdépendance accrue et consolidera notre base industrielle dans le secteur des missiles »[22].

Bien que le nom du « maître d'œuvre […] unique » ne soit pas précisé, pour des raisons liées au respect de la concurrence, l'initiative se concentre en fait autour de la rationalisation de l'industriel MBDA qui deviendrait le fournisseur missilier unique en Europe par le biais d'une intégration de ses filiales française et britannique.

Ainsi, le nom officiel de l'initiative est " *One Complex Weapons* ", mais dans les discussions informelles (et dans les déclarations de l'industriel lui-même), on fait souvent référence à "One MBDA".

La coopération franco-britannique dans le secteur des armes complexes s'est concrétisée en 2013 avec l'annonce (attendue de longue date par les Britanniques) du lancement du programme de missile antinavire FASGW/ANL. L'idée de coopérer sur le programme de missile antinavire FASGW/ANL remonte à 2008, avec une lettre d'intention des chefs d'État et de gouvernement en janvier 2009. L'initiative plus large de " *One Complex Weapons* " est venue ensuite.

[21] Hélène Masson, *op.cit.*, p. 63.

[22] David Cameron et Nicolas Sarkozy, « Déclaration franco-britannique sur la coopération de défense et de sécurité », 2 novembre 2010.

D'abord, il s'agissait d'éviter une répétition de ce qui s'était produit sur le SCALP/Storm Shadow, qui avait donné lieu à deux programmes, avec deux contrats distincts, en adoptant une approche autrement plus intégrée. Aussi, le 29 mars 2010, les gouvernements français et britannique signent avec MBDA un « mandat de gestion de portefeuille » (*Portfolio Management Agreement*) : des besoins capacitaires communs sont identifiés qui pourraient permettre de réaliser des économies de l'ordre de 30 %, à deux, d'ici à 2035 (soit 1,9 milliard d'euros)[23]. Les gains seront réalisés grâce à des économies d'échelle, à une plus grande efficacité de l'organisation et à la suppression des doublons et d'une partie des marges.

Le programme FASGW/ANL est une étape nécessaire à cette démarche d'intégration. Le traité de novembre 2010 crée une sorte de « *momentum* » politique autour de ce programme, puisqu'il fait partie des principaux projets annoncés lors du Sommet[24]. Cependant, il a fallu attendre 2013 pour que la partie française entérine ce programme. En effet, celui-ci ne constituait pas une priorité pour les forces françaises dans le contexte d'un ministère en proie à des réductions budgétaires. Plusieurs verrous au sein de l'administration et du gouvernement français se sont donc opposés à ce programme, jugé strictement politique[25]. Au final, il aura fallu trois ans et une lettre de David Cameron à François Hollande à l'hiver 2013 pour que l'Élysée confirme le financement du missile antinavire. En d'autres termes, « c'est l'intérêt de politique industrielle et l'intérêt franco-britannique […] qui ont permis à ce programme de survivre »[26]. Après la confirmation du lancement du programme au printemps 2013, un contrat conjoint de développement et de production a été signé en mars 2014 avec MBDA (UK) pour un montant de 600 millions d'euros[27].

Aujourd'hui, quatre ans après l'annonce du 2 novembre 2010, l'intégration n'en est encore qu'à ses balbutiements. La TCW et la « filière missiles » forment encore deux blocs bien distincts qui échangent de façon ponctuelle à différents niveaux : pouvoir exécutif via le *Senior Level Group*, ministères et directeurs d'industrie via le *High Level Working Group*, via la *Strategic delivery team* au niveau « 1* » et enfin au niveau des équipes de programmes. L'ambition, à terme, est d'avoir des « centres d'excellence », c'est-à-dire une spécialisation des sites en fonction de leurs compétences, avec l'acceptation de part et d'autre d'abandonner certaines capacités de production. Quatre centres spécialisés « tests » sont en train d'être mis en place en 2014-2015, deux de chaque côté de la Manche[28], formant la première étape en vue de valider des dépendances mutuelles librement consenties. Un accord intergouvernemental qui sera ratifié par les Parlements et aura donc valeur de traité doit encore être signé pour l'intégration de MBDA France et MBDA UK, c'est pourquoi le programme ANL sera géré par un comité de pilotage classique[29].

[23] Entretien, Ministry of Defence, 2014.

[24] David Cameron et Nicolas Sarkozy, « Déclaration franco-britannique », *ibid.,* paragraphe 18.

[25] Entretiens, ministère de la défense et Assemblée nationale, 2013.

[26] Entretien, ministère de la défense, 2013.

[27] Alain Ruello, « Missile franco-britannique : MBDA décroche un contrat de 600 millions d'euros », *Les Echos*, 27 mars 2014, disponible sur : http://www.lesechos.fr/27/03/2014/lesechos.fr/0203402258145_missile-franco-britannique--mbda-decroche-un-contrat-de-600-millions-d-euros.htm, dernière consultation le 4 mars 2015.

[28] Alain Ruello, *op. cit.*

[29] Entretien, Ministry of Defence, 2014.

En fait, le programme FASGW/ANL ne sera pas mené dans le cadre de l'initiative bilatérale "*One Complex Weapons* ", mais fait partie du portefeuille britannique de la TCW. Ainsi, le contrat a été passé par le biais du ministère de la défense britannique avec MBDA UK au nom des gouvernements français et britannique.

Une politique industrielle bilatérale ? Les enjeux de la mise en œuvre

À première vue, il semblerait impossible de réconcilier les approches de Londres et Paris vis-à-vis de leurs industries de défense : au tout-protectionnisme français s'opposerait l'ultra-libéralisme britannique. En réalité, les approches des deux États convergent particulièrement dans ce secteur.

Selon Catherine Hoeffler, la coopération dans les programmes d'armement constitue une forme de patriotisme économique au niveau européen[30]. Aussi, même le Royaume-Uni a jugé, depuis les années 1990, que le secteur des armes complexes, comme le secteur naval, était suffisamment stratégique pour l'avenir pour en garder le contrôle de la propriété intellectuelle. C'est ainsi que la Grande-Bretagne a choisi dans les années 1990 de collaborer avec la France sur le SCALP/Storm Shadow plutôt que d'acquérir un système américain[31]. La France, qui a traditionnellement défendu une politique industrielle en vue de préserver une BITD nationale dans tous les domaines, s'est donc retrouvée alignée avec l'approche britannique dans le secteur. En effet, selon le PDG de MBDA :

> « Nous avons en France cette culture de relations de partenariat avec l'industrie ; le Royaume-Uni, qui ne l'avait pas, s'en est doté, ce qui permet à nos deux pays d'engager un dialogue sur la base d'une compréhension commune des enjeux industriels et de défense »[32].

Dans une certaine mesure, dans ce secteur spécifique, France et Royaume-Uni partagent ainsi une même approche politique basée sur la nécessité de la préservation des technologies et capacités de production en Europe.

L'intégration de la filière missile a été présentée par les gouvernements français et britannique comme un « cas test » pour une coopération industrielle bilatérale qui doit pouvoir s'étendre à d'autres secteurs, notamment le secteur des drones, dans le contexte des traités de Lancaster[33]. Si l'on en est aux prémices de cette initiative sans précédent de par sa nature et sa temporalité, l'on voit poindre certains enjeux qui devront être surmontés pour une mise en œuvre effective de cette politique industrielle commune. Ces difficultés sont de plusieurs ordres : les différences juridiques relatives aux pratiques contractuelles État-industrie en France et au Royaume-Uni, la structure du secteur et la persistance d'une concurrence entre plusieurs entités impliquées, et enfin la non stricte « bilatéralité » du secteur.

---

[30] Catherine Hoeffler, "European Armament Co-Operation and the Renewal of Industrial Policy Motives", *Journal of European Public Policy*, vol. 19, n° 3, 2012, p. 438.

[31] Andrew James, « L'évolution de la coopération franco-britannique en matière d'armements : du Jaguar au futur porte-avions », *dans* Jean-Paul Hébert, et Jean, Hamiot, *Histoire de la coopération européenne dans l'armement*, Paris, CNRS éditions, 2004, p. 111.

[32] Assemblée nationale, « Audition de M. Antoine Bouvier », p. 5.

[33] David Cameron, et Nicolas Sarkozy, « Déclaration franco-britannique ».

Selon un officier français, du fait que MBDA ne produit pas de technologies duales ou commerciales et dépend alors entièrement de la commande publique, qui elle-même dépend de la coopération, c'est du côté des gouvernements qu'il faut chercher la responsabilité dans les blocages à la rationalisation[34]. Comme le remarque le PDG de MBDA, Antoine Bouvier, le principal blocage à une industrie intégrée est que « les deux interfaces contractuelles, agissent de manière moins coordonnée [que ne le fait l'industrie] et sur la base d'un cadre juridique non harmonisé ou incompatible »[35]. En effet, les obligations de confidentialité et de procédures de sécurité entraînent une lourdeur dans le travail du groupe : pour pouvoir échanger des informations classifiées, les équipes de programme doivent faire des demandes *ad hoc* par le biais d'un arrangement technique.

Les procédures sont complexes également pour les envois de matériels entre les deux pays qui peuvent prendre plusieurs mois[36]. Une solution à ce problème devrait être apportée par l'accord intergouvernemental qui sera signé début 2015 et permettra l'octroi d'une licence globale d'exportation entre France et Royaume-Uni.

Il existe ensuite des différences liées aux pratiques contractuelles, et plus largement aux relations État-industrie des deux côtés de la Manche. Le programme FASGW/ANL, par exemple, fait partie de l'initiative britannique TCW, et le contrat est passé au nom des deux gouvernements par le MOD. Selon un officier français, la question qui se pose alors est : « comment on fait de la coopération à partir d'un contrat global britannique ? »[37]. Ce n'est pas sans difficulté, notamment du fait que les contrats de droit britannique sont des contrats qui « ne prévoient pas d'obligation de résultat » et les caractéristiques et prix peuvent être modifiés[38], alors qu'en France, « l'ensemble des risques est supporté par les titulaires du contrat […] et les clauses de prix sont fermes dans presque tous les cas »[39]. Par ailleurs, la DGA est composée uniquement d'ingénieurs, qui ont les moyens de discuter des aspects techniques des programmes avec l'industrie, et donc d'exercer davantage de contrôle que l'administration britannique, composée à la fois d'ingénieurs, de managers civils, et de militaires[40]. Ainsi, après la décision de lancer le programme en avril 2013, il a fallu que les administrations françaises et britanniques négocient pendant un an pour s'accorder sur les termes du contrat. La négociation s'est faite par le biais de la DGA et d'une équipe de Français implantés au sein de DE&S (*Defence equipment and support*), qui ont cherché à rapprocher la position britannique des pratiques françaises. En raison des ralentissements provoqués par la démarche coopérative sur le programme – qui a failli être lancé en national faute de décision française – on évoque côté français le sentiment d'être considérés par les Britanniques comme « des empêcheurs de tourner en rond »[41].

[34] Entretien, Ministère de la défense, 2013.

[35] Cité dans François Cornut-Gentille, « Avis présenté au nom de la Commission de la Défense nationale et des forces armées sur le Projet de loi de finances pour 2012 », *Défense : équipement des forces, dissuasion,* tome VII, n° 3809, Assemblée nationale, 25 octobre 2011, p. 107.

[36] Entretien, industriel français, 2014.

[37] Entretien, ministère de la défense, 2014.

[38] Entretiens, ministère de la défense et industriels français et britannique, 2014.

[39] Jean-Michel Oudot, « Marchés d'armement : choix contractuels et performance », *Ecodef,* n° 51, Observatoire économique de la Défense, mai 2009, p. 4.

[40] Il n'existe pas d'équivalent au corps des ingénieurs de l'armement.

[41] Entretien, ministère de la défense, 2014.

En outre, malgré la volonté de créer des « interdépendances », c'est-à-dire d'accepter de ne pas avoir l'ensemble des capacités de production en national, force est de constater que les logiques nationales persistent. D'une part, il y a les problèmes liés à la concurrence passée – et persistante – entre Français et Britanniques sur le secteur. Même s'il y a une volonté d'harmoniser les besoins pour les décennies à venir (identification des menaces, compatibilité des plateformes, calendriers de remplacement), les programmes français et britanniques sont structurellement en décalage du fait d'une longue histoire de rivalité et de concurrence industrielle[42]. Les acteurs étatiques maintiennent un état d'esprit concurrentiel y compris dans le cadre de cette démarche intégrationniste. Dans le cas du contrat FASGW/ANL, les négociations ont également été prolongées en raison de désaccords sur la répartition de la production et à cause des relations entre MBDA et les autres firmes présentes dans le secteur. D'autre part, il existe un double enjeu de préservation des emplois et du savoir-faire lié aux éléments jugés « nobles » (par exemple, l'auto-directeur ou système de guidage). L'objectif de l'intégration de la filière, c'est de dépasser les difficultés liées aux exigences de « juste retour » qui peuvent créer des partages de production inefficients, et pérenniser les duplications.

Cela requiert l'établissement d'un équilibre global de la filière sur un ensemble de programmes. Or, les équipes de part et d'autre de la Manche cherchent elles aussi à préserver leur volume de commandes, leurs compétences, et leurs emplois. Aussi, lorsque l'on descend en-dessous du niveau politique, la spécialisation n'est pas toujours vue d'un très bon œil[43].

Ainsi, en pratique, les discussions sur le FASGW/ANL ont donné lieu à des échanges classiques sur le nombre de commandes, les spécifications, mais aussi la répartition des parts de travail, qui reflètent une peur de perdre au change malgré un contexte encadré politiquement et juridiquement qui doit permettre un équilibrage des gains et des pertes sur le moyen à long terme.

Pour terminer, il faut replacer l'intégration de MBDA dans le paysage industriel et politique plus large. La stratégie industrielle franco-britannique est censée s'appliquer au secteur entier des armes complexes, or peu de progrès ont pu être faits à cette échelle, notamment en raison d'une concurrence entre différents acteurs : l'État français est logiquement enclin à protéger Thales et Sagem (Safran, en concurrence avec MBDA et Selex UK), qui sont minoritaires, mais présents dans le secteur. La question se pose moins côté britannique, où il n'y a pas de concurrence directe entre les activités de MBDA et Thales UK. Ces autres acteurs ne sont pas enclins à coopérer. En outre, ils peuvent légitimement craindre que MBDA, « qui ressort gagnant » du traité de Lancaster[44] ne cherche purement et simplement à prendre le contrôle de l'ensemble du secteur. Il faut enfin souligner la difficulté de mener une politique industrielle sectorielle strictement bilatérale. L'idée de créer un maître d'œuvre unique « repose sur l'idée que MBDA a un contrôle complet de la chaîne de production […], que l'on peut isoler la France et le Royaume-Uni […], mais il y a aussi MBDA Italie, par exemple, qui participe pour certains composants des missiles »[45]. Enfin, il faut noter que la « rationalisation » franco-britannique ne pourra pas s'appliquer à l'ensemble de la filière, mais seulement à environ 80 %, soit parce que certains programmes ou composants sont jugés trop

[42] Entretien, ministry of Defence, 2014.

[43] Entretien, industriel français, 2014.

[44] Guillaume Lecompte-Boinet, « MBDA, presque un Airbus des missiles », *L'Usine Nouvelle*, 12 mai 2011, disponible sur : http://www.usinenouvelle.com/article/mbda-presque-un-airbus-des-missiles, N151762, dernière consultation le 4 mars 2015.

[45] Entretien, industriel britannique, 2014.

stratégiques pour être menés en coopération (l'armement nucléaire), soit, ou également, parce qu'ils font déjà l'objet d'une coopération internationale, transatlantique notamment, et ne peuvent être partagés avec d'autres.

Conclusion

Face, d'une part, au risque de disparition de la filière industrielle des armes complexes et, d'autre part, aux inefficiences des programmes en coopération *ad hoc*, la France et le Royaume-Uni se sont lancés dans une initiative conjointe de long terme qui prévoit d'intégrer l'ensemble de la filière, depuis la R&D jusqu'à la maintenance, en passant par la production et l'export. Le niveau bilatéral d'action doit permettre un alignement des besoins et des pratiques plus aisé et moins coûteux qu'à l'échelon multilatéral. L'approche par portefeuille, elle, doit garantir la pérennité du partenariat et suppose de repenser en bilatéral les calendriers, les spécifications et les capacités industrielles.

L'initiative franco-britannique s'est d'abord construite brique par brique, à travers des programmes d'action nationaux (*Team Complex Weapons*) et bilatéraux (*Innovation and Technology Partnership*) avant d'être promue au rang de stratégie industrielle conjointe et entérinée par le traité et la déclaration de Lancaster House signés le 2 novembre 2010. Cette politique industrielle bilatérale a été rendue possible par l'existence d'un acteur industriel déjà largement franco-britannique, qui trouve dans l'intégration bilatérale l'assurance de se maintenir à flot. En outre, l'intégration des filières française et britannique se base sur une refonte des rapports public-privé, rendue possible par une nouvelle approche britannique de certains secteurs de son industrie de défense.

Cette contribution a souligné une série d'enjeux qui se posent aux deux États qui cherchent à intégrer un secteur de leur industrie de défense : les logiques habituelles de partage des coûts et d'allocation de la production se retrouvent malgré les velléités d'interdépendance ; on fait également face à des incompatibilités juridiques en matière de gestion des programmes, à une concurrence persistante entre acteurs industriels, y compris au sein du même groupe, et à des problèmes de partage d'informations liées à certains programmes stratégiques, mais aussi aux liens industriels et technologiques très forts existant entre le Royaume-Uni et les États-Unis.
Les acteurs des deux côtés de la Manche sont conscients de ces difficultés, et travaillent quotidiennement à les surmonter. Une question qui se pose toutefois est dans quelle mesure une politique publique internationale peut-elle être décorrélée des dynamiques plus larges des politiques publiques nationales ? Comme pour les difficultés mentionnées au fil de ce chapitre, l'on constate que tout programme de politique industrielle internationale est intrinsèquement lié à des dynamiques juridiques, économiques, et politiques nationales. Pour se construire et durer, il doit notamment s'assurer qu'il repose sur des référentiels et des soutiens politiques et institutionnels plus larges que le seul secteur concerné, et que le strict niveau bilatéral de sa mise en œuvre.

Références

Assemblée Nationale, Commission de la défense nationale et des forces armées, « Audition de M. Antoine Bouvier, président-directeur général de MBDA, sur la coopération franco-britannique et la filière missile », *Compte rendu n° 39*, 18 mai 2011.

BROWN Gordon et SARKOZY Nicolas, « Déclaration du Sommet franco-britannique », 27 mars 2008.

CAMERON David et SARKOZY Nicolas, « Déclaration franco-britannique sur la coopération de défense et de sécurité », 2 novembre 2010.

CORNUT-GENTILLE François, « Avis présenté au nom de la Commission de la Défense nationale et des forces armées sur le Projet de loi de finances pour 2012 », *Défense : équipement des forces, dissuasion*, tome VII, n° 3809, Assemblée nationale, 25 octobre 2011.

Defence Growth Partnership, "Securing Prosperity: A Strategic Vision for the UK Defence Sector", septembre 2013.

DEVORE Marc, "The Arms Collaboration Dilemma: Between Principal-Agent Dynamics and Collective Action Problems", *Security Studies*, vol. 20, n° 4, 2011, p. 624-662.

DUSSAUGE Pierre et CORNU Christophe, *L'Industrie française de l'armement ; coopérations, restructurations et intégration européenne*, Paris, Economica, 1998.

HARTLEY Keith, "White Elephants? The Political Economy of Multinational Defence Projects", *New Direction: The Foundation for European Reform*, octobre 2012.

HOEFFLER Catherine, "European Armament Co-Operation and the Renewal of Industrial Policy Motives", *Journal of European Public Policy*, vol. 19, n° 3, 2012 p. 435-451.

HOEFFLER Catherine, *Les politiques d'armement en Europe : "l'Adieu aux armes" de l'État nation ? Une comparaison entre l'Allemagne, la France, le Royaume-Uni et l'Union européenne de 1976 à 2010*, Thèse de doctorat, Sciences Po, Paris, 2011.

JAMES Andrew, « L'évolution de la coopération franco-britannique en matière d'armements : du Jaguar au futur porte-avions », *dans* HEBERT Jean-Paul et HAMIOT Jean, *Histoire de la coopération européenne dans l'armement*, Paris, CNRS éditions, 2004, p. 99-121.

JOANA Jean et SMITH Andy, « Du couple franco-allemand à une nouvelle Entente cordiale : la France dans le programme A400M », *Les Champs de Mars*, n° 16, 2004, p. 133-146.

KAPSTEIN Ethan, "International Collaboration in Armament Production: the Second Best Solution", *Political science quarterly*, vol. 106, n° 4, 1991-1992, p. 567-675.

KIRKPATRICK David, "Trends in the Costs of Weapon Systems and the Consequences", *Defence and Peace Economics*, vol. 15, n° 3, 2004, p. 259-273.

KROTZ Ulrich, *Flying Tiger: International Relations Theory, and the Politics of Advanced Weapons Production*, Oxford, Oxford University Press, 2011.

LECOMPTE-BOINET Guillaume, « MBDA, presque un Airbus des missiles », *L'Usine Nouvelle*, 12 mai 2011, disponible sur : http://www.usinenouvelle.com/article/mbda-presque-un-airbus-des-missiles, N151762, dernière consultation le 4 mars 2015.

LORELL M.A. et LOWELL J., *Pros and Cons of International Weapons Procurement Collaboration*, Santa Monica, RAND, 1995.

MASSON Hélène, « La réorganisation de l'industrie de défense britannique », *Recherches & Documents*, n° 5/2008, Fondation pour la recherche stratégique, 2008.

Ministry of Defence, "National Security through Technology: Technology, Equipment, and Support for UK Defence and Security", février 2012.

OUDOT Jean-Michel, « Marchés d'armement : choix contractuels et performance », *Ecodef*, n° 51, Observatoire économique de la Défense, mai 2009.

PETITEVILLE Frank and SMITH Andy, « Analyser les politiques publiques internationales », *Revue française de science politique*, vol. 56, n° 3, 2006, p. 357-366.

RUELLO Alain, « Missile franco-britannique : MBDA décroche un contrat de 600 millions d'euros », *Les Echos*, 27 mars 2014, disponible sur : http://www.lesechos.fr/27/03/2014/lesechos.fr/0203402258145_missile-franco-britannique--mbda-decroche-un-contrat-de-600-millions-d-euros.htm, dernière consultation le 4 mars 2015.

Secretary of State for Defence, "Defence Industrial Strategy: Defence White paper", décembre 2005.

Traité de coopération en matière de défense et de sécurité entre la République française et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Londres, 2 novembre 2010.

WADEY Steve, "Progressing Team Complex Weapons", *RUSI Defence Systems*, juin 2010, p. 90-93.

CYBERSECURITE, CYBERDEFENSE : UNE NOUVELLE DEMANDE POUR UNE NOUVELLE MENACE

Alix DESFORGES
Doctorante à l'Institut français de géopolitique de l'université Paris VIII Vincennes-Saint-Denis

Introduction

Depuis quelques années, un nouveau marché émerge dans l'économie de défense : celui de la cyberdéfense[1] et plus largement de la cybersécurité[2]. Ce marché se développe en réponse à l'émergence d'une nouvelle menace qui transforme le contexte international : le recours de plus en plus systématique aux attaques informatiques comme moyen d'action dans les conflits de tout type (politiques, économiques, géopolitiques, etc.). En 2007, suite aux très médiatiques attaques informatiques qui ont touché l'Estonie pendant plusieurs jours, de nombreux États ont pris conscience des enjeux de sécurité et de défense que pose le cyberespace. Alors même que ces attaques n'étaient pas d'une grande sophistication, leurs conséquences directes (indisposition de services bancaires et étatiques dans un pays ultra-connecté) et indirectes (question de la mise en application de l'article 5 du Traité de l'Atlantique nord lors d'attaques informatiques) ont incité les États à s'interroger sur leurs enjeux et les défis que pose le cyberespace pour leur sécurité nationale. Depuis, les attaques informatiques portées à la connaissance du public n'ont cessé de s'intensifier et de se complexifier. Pour l'État, les très nombreux cas d'espionnage rapportés dans les médias ont notamment servi de catalyseur pour faire émerger une demande de plus en plus forte de produits et de services en cybersécurité et cyberdéfense. Dans ce chapitre, nous nous interrogerons d'abord sur l'émergence de cette menace qualifiée de « cybermenace »[3] afin d'en comprendre les enjeux et les représentations. Nous étudierons l'émergence de la thématique au sein des cercles militaro-stratégiques dans une perspective historique. Dans un deuxième temps, nous étudierons la fonction de cette représentation de la cybermenace, à savoir son impact sur la demande étatique dans le domaine de la sécurité et de la défense et la façon dont elle l'a structurée. Pour cela nous analyserons les évolutions des politiques et des stratégies étatiques en matière de cyberdéfense et de cybersécurité. Dans un contexte de réduction des dépenses publiques, nous verrons que les budgets alloués à ces questions ont pourtant augmenté de façon significative dans de nombreux États. Enfin, nous identifierons les grandes tendances actuelles de la demande étatique dans ce domaine. Nous verrons alors que faute de pouvoir prévenir ou stopper des attaques informatiques de plus en plus sophistiquées, les États cherchent à en limiter l'impact. La protection des réseaux à tous les niveaux et la mise en place de leur surveillance permanente afin de détecter toute activité suspecte constituent la première pierre à l'édifice d'une cybersécurité.

[1] Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels (Source : Agence nationale de la sécurité des systèmes d'information, 2011).
[2] État recherché pour un système d'information de résister à des événements 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. (Source : Agence nationale de la sécurité des systèmes d'information, 2011).
[3] Livre blanc sur la défense et la sécurité nationale, 2013, p. 7.

Mais ces seules mesures ne peuvent suffire. Les États développent ainsi d'autres stratégies pour faire face à une menace qui constitue à la fois un enjeu économique, stratégique et de souveraineté.

Une prise de conscience récente des États face à une menace toujours plus complexe

Si les premières attaques informatiques à l'encontre des États ont eu lieu dès les années 1990, leur impact et leur intensité n'étaient alors pas de nature à perturber le fonctionnement de l'État.
Les premières attaques informatiques d'envergure apparaissent au milieu des années 2000, mais le véritable tournant se situe en 2007. Certains États comme les États-Unis avaient entamé dès le début des années 1990 une réflexion sur les enjeux de ces menaces (Arquilla et Ronfeldt, 1993), mais la majorité des États en a pris conscience lorsqu'en avril 2007, des attaques en déni de service[4] ont paralysé pendant plusieurs jours, voire plusieurs semaines, de nombreux services en ligne gouvernementaux et bancaires en Estonie. L'État estonien a immédiatement accusé la Russie d'être derrière ces attaques qui ont pour point de départ l'opposition de la minorité russophone estonienne au déplacement d'une statue en mémoire des soldats soviétiques de la Seconde Guerre mondiale.

Si elles n'ont pas occasionné de gros dégâts, ces attaques ont marqué les esprits parce que l'Estonie avait fait très tôt le pari du développement numérique et de nombreux services gouvernementaux et privés ont été touchés et rendus indisponibles. Un an plus tard, les attaques informatiques contre la Géorgie précédant de quelques heures l'invasion des troupes russes sur le sol géorgien, ont confirmé que le cyberespace était devenu un nouvel outil dans l'expression de rivalités de tout type qu'il s'agisse de manifestations, de guerres ou d'espionnage. En France, la thématique apparaît pour la première fois à un niveau stratégique dans le Livre blanc sur la défense et la sécurité nationale de 2008. La sécurité des systèmes d'information est alors identifiée comme faisant partie des domaines de souveraineté de « premier cercle »[5] aux côtés de trois éléments du domaine nucléaire (la dissuasion nucléaire, le secteur des missiles balistiques et les sous-marins nucléaires d'attaque).

À partir de 2008, on observe une véritable intensification et sophistication de ce moyen d'action. Le recours de plus en plus fréquent aux attaques informatiques s'explique d'une part par la démocratisation des outils informatiques, la pénétration de ces outils dans la vie quotidienne des sociétés et par l'interconnexion croissante des réseaux informatiques. Mais leur usage s'explique également par les spécificités de ces attaques qui permettent de mener une action à distance, de façon discrète et anonyme pour celui qui en maîtrise les outils ; des caractéristiques particulièrement utiles notamment dans les cas d'espionnage. Ces attaques ont visé tant des États que des entreprises stratégiques issues du secteur de la défense (Lockheed Martin, 2009), de l'industrie ou de l'énergie (Areva, 2011).

À partir de 2010, les premières attaques d'envergure visant à saboter voire détruire des systèmes sont apparues comme Stuxnet (2010)[6] et Aramco (2012)[7].

[4] Attaque visant à saturer un serveur, un site web, de requêtes dans le but de le mettre hors service.
[5] Livre blanc sur la défense et la sécurité nationale, 2008, p. 318.
[6] Ver qui a détruit plusieurs milliers de centrifugeuses de centrales nucléaires iraniennes.
[7] Attaque informatique qui a mis hors d'usage plusieurs milliers de postes de travail de l'entreprise pétrolière Saudi Aramco.

Le Livre blanc sur la défense et la sécurité nationale de 2013 distingue trois types de menaces :

- la cybercriminalité « qui ne relève pas spécifiquement de la sécurité nationale » ;
- « les tentatives de pénétration de réseaux numériques à des fins d'espionnage » ;
- et « les attaques visant le sabotage de systèmes d'importance vitale » (LBDSN, 2013).

Patrick Pailloux, alors directeur général de l'Agence nationale de la sécurité des systèmes d'information, identifiait quant à lui en 2013 un quatrième type de menace : la déstabilisation conduite par des attaques de type défacement[8], déni de service ou publication d'informations dérobées.

Il ajoute qu'« au même titre que les manifestations de rue, les attaques informatiques sont devenues un moyen d'exprimer une protestation»[9]. Elles pourraient dès lors être susceptibles de compliquer les opérations militaires par exemple.

En termes d'impact pour la sécurité nationale d'un État, ce sont bien l'espionnage et le sabotage qui constituent certainement à la fois les menaces les plus courantes (espionnage), mais aussi les plus potentiellement destructrices (destruction physique pour le sabotage ou destruction économique pour l'espionnage). Si les attaques de sabotage peuvent se révéler particulièrement dommageables et avoir un impact important sur la vie de la société, elles requièrent toutefois d'importants investissements financiers et humains pour leur mise en œuvre ; des moyens qui ne sont pas à la portée du premier venu. Ce facteur limitant réduit ainsi le nombre d'acteurs susceptibles de mener de telles attaques et donc leur probabilité. Ainsi ce sont bien les attaques d'espionnage qui constituent certainement à l'heure actuelle la plus grande menace pour un État. Cet espionnage vise les intérêts directs des États (opération *Red October* en 2012 visant notamment les représentations diplomatiques de plus d'une trentaine de pays ou encore l'espionnage de l'Élysée lors de la passation de pouvoir entre Nicolas Sarkozy et François Hollande en mai 2012), mais également leurs intérêts indirects et tout aussi stratégiques comme des entreprises du secteur de la défense, de l'énergie ou encore de l'industrie. Le pillage de la propriété intellectuelle et industrielle de ces entreprises affecte alors la compétitivité et la croissance potentielle de ces dernières. C'est encore plus vrai dans un contexte de mondialisation et de crise économique où la compétition entre entreprises est particulièrement forte.

Ainsi si leur impact est moins perceptible (notamment parce qu'aujourd'hui il n'existe pas d'outils fiables pour en évaluer le coût), les attaques d'espionnage ne menacent pas moins la sécurité des États soit directement par la perte d'information diplomatique et/ou politique soit indirectement par la perte économique et de compétitivité présente et à venir, thème particulièrement prégnant dans le débat politique alors que l'Europe peine à sortir d'une crise économique. D'attaques opportunistes et principalement motivées par l'appât du gain financier, les États doivent faire face à la multiplication des attaques concernant désormais la sécurité de la nation.

[8] Un défacement ou défiguration consiste à modifier l'apparence d'une ou plusieurs pages web sans le consentement de son titulaire. Généralement, ce type d'attaque est utilisé pour faire valoir une revendication politique.

[9] Audition de M. Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information devant la Commission de la défense nationale et des forces armées de l'Assemblée nationale, le 16 juillet 2013.

En les liant aux questions de sécurité nationale, de nombreux États ont ainsi placé les questions de cybersécurité et de cyberdéfense au premier plan de leur agenda politique (Dunn Cavelty, 2008). Certes, les États se sont préoccupés dès les années 1980 de sécurité informatique, mais elle concernait essentiellement les experts de culture scientifique. La deuxième moitié des années 2000 a été marquée par l'entrée de ces questions dans le champ politique. C'est une véritable prise de conscience politique qui a amené les États à se saisir au plus haut niveau de la question et à élaborer une stratégie à une échelle plus globale.

Ces mises en place de stratégies se sont accompagnées de la montée en puissance de discours étatiques concernant ces menaces, popularisant le terme de « cybermenace ». Pourtant, tout comme celui de cyberespace, le terme cybermenace demeure relativement flou et semble désigner tout type de menace dont le véhicule est le cyberespace. Myriam Dunn Cavelty note à ce titre que l'utilisation du préfixe cyber- (qui devient même parfois un adjectif en soi) consiste avant tout à désigner une action qui se fait par l'utilisation d'ordinateurs. Ainsi, concomitamment à l'explosion des attaques informatiques, on assiste à la prolifération d'une sémantique « cyber » particulièrement anxiogène. Associée à des références historiques fortes ("*Cyber Pearl Harbor*", « 11 septembre numérique »), elle tend à produire un discours aux accents catastrophistes. Il existe pourtant de nombreux désaccords et de vifs débats parmi les spécialistes sur les définitions (comme c'est le cas pour cyberguerre ou encore cyberterrorisme) ainsi que sur la portée et l'impact des attaques informatiques sur la sécurité nationale.

Ainsi en quelques années, cette « cybermenace » a fait l'objet d'une attention, d'un intérêt et de craintes de plus en plus vives pour les États même si l'évaluation de cette menace comporte de nombreuses difficultés, notamment celle de sa perception, de sa représentation. On assiste à des discours contradictoires sur l'état de la menace[10], à la prolifération d'une sémantique anxiogène et finalement à l'émergence d'un sentiment global d'insécurité (Desforges, 2014).

Des stratégies issues de la défense

Dès 2008, de nombreux États ont réagi en adoptant des politiques et des stratégies fortes visant à réduire les risques inhérents à ces « cybermenaces ». Ils ont développé et mis en place des stratégies principalement issues de la doctrine militaire. On observe à ce titre un glissement de la thématique de la sécurité à celle de la défense reflétant l'importance stratégique de cette question ainsi que la proximité des enjeux. C'est ainsi que pour évoquer les différents types de stratégies mis en place pour faire face aux attaques informatiques (y compris pour parler des stratégies mises en place par des acteurs non étatiques), on parle davantage de stratégie de défense et non de sécurité.

La première réponse apportée par les États a été de penser la protection des systèmes d'information et des réseaux en termes de défense dite périmétrique. Cette stratégie s'appuie sur le développement d'une meilleure sécurité des systèmes d'information à ses bordures. Elle s'apparente à une défense de type « ligne Maginot » comportant une seule ligne de protection. Mais comme la ligne Maginot en son temps, ce type de défense peut être aisément contournable.

[10] Alors même que de nombreuses attaques ne sont pas portées à la connaissance du public ou ne sont pas (encore) détectées.

D'abord parce que la menace ne vient pas uniquement de l'extérieur du système d'information à protéger, mais aussi parce qu'il existe de nombreuses possibilités pour l'attaquant de franchir cette ligne de défense[11]. Et si elle constitue une base nécessaire pour mettre en place une défense robuste, elle s'avère, seule, largement insuffisante pour faire face aux attaques qui s'avèrent être de plus en plus ciblées. Alors pour pallier les manques de la défense périmétrique, le concept de défense en profondeur a été repris des doctrines militaires (notamment dans les travaux de Vauban)[12] pour l'appliquer aux enjeux de la cybersécurité et de la cyberdéfense.

La logique de la défense en profondeur est de multiplier les lignes de défense (à l'inverse de la défense périmétrique constituée d'une seule ligne). Chaque ligne est conçue et gérée de manière indépendante et c'est leur accumulation qui contribue à construire une défense solide. Le but de cette stratégie est d'augmenter le rapport coût/investissement de l'attaquant en le ralentissant et en l'affaiblissant. L'objectif principal de cette stratégie est de redonner l'avantage à la défense dans un domaine où l'attaque, de par son immédiateté, sa discrétion et ses larges possibilités, est considérée comme étant supérieure. La mise en œuvre d'une stratégie de défense en profondeur répond également à l'élaboration d'une conception plus globale et systémique de la cybersécurité et de la cyberdéfense.

Plus récemment a émergé le concept de cyberdéfense active. Il s'agit ici de valoriser une approche beaucoup plus proactive que dans les deux stratégies précédemment évoquées. La cyberdéfense active, c'est la possibilité de mettre fin à une attaque au moment où celle-ci se produit en répondant par d'autres attaques informatiques. Cette stratégie est notamment évoquée par le ministère de la défense américain concernant ses actions dans le cyberespace en 2011, mais n'est pas clairement définie. De fait, il existe peu ou pas de définitions de cette stratégie dont les contours restent à préciser. En effet, elle pose à ce jour de nombreuses questions notamment en termes d'escalade du conflit, mais pas seulement. Elle suppose également de disposer de capacités efficaces de détection en temps réel des attaques ainsi que de capacités d'identification de la source de l'attaque de façon quasi instantanée : deux conditions particulièrement difficiles à réunir, en tout cas pour le moment. La cyberdéfense active semble en fait davantage servir des objectifs politiques (pouvoir répondre à une agression) et de puissance (démonstration de capacités qui sont à ce jour non matures).

On notera qu'aucune de ces stratégies ne remplace l'autre. Elles sont davantage destinées à se cumuler et à se compléter pour faire face à des menaces toujours plus complexes. De plus, les stratégies évoquées (y compris pour la cyberdéfense active) ne concernent pas uniquement celles mises en place par des États, mais également celles relevant d'acteurs privés comme les entreprises. La combinaison défense périmétrique et défense en profondeur est également appliquée au sein des entreprises. Ainsi si certains chercheurs observent que la défense est devenue une « composante de la sécurité elle-même »[13], on peut ici noter que les logiques et concepts issus de la défense pénètrent le monde de l'entreprise et la sécurité des systèmes d'information devient alors une composante de la défense de celui-ci.

Les attaques informatiques toujours plus nombreuses et plus complexes ont montré combien les réseaux pouvaient être vulnérables. La multiplication d'attaques ciblées a fait prendre conscience aux États de l'importance de la maîtrise des technologies utilisées et a fait émerger l'idée de la

[11] Les logiciels et les applications sont particulièrement vulnérables et constituent le vecteur de la majorité des attaques informatiques.

[12] Direction centrale de la sécurité des systèmes d'information, « La défense en profondeur appliquée aux systèmes d'information - Mémento », juillet 2004.

[13] Jean Porcher, « Défense versus sécurité nationale », *Revue de Défense Nationale*, n° 711, août-septembre 2008.

constitution d'une stratégie que l'on pourrait qualifier de « maîtrisée » voire « souveraine ». Le principe de cette stratégie est de maîtriser certains composants, outils ou services de bout en bout afin d'en garantir la sécurité. En France, cette inquiétude est par exemple exprimée dans un rapport du Sénat sur la cyberdéfense en 2012.

Dans ce rapport le Sénateur Jean-Marie Bockel recommande de ne plus avoir recours à « des routeurs ou d'autres équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les routeurs et certains équipements d'origine chinoise »[14]. Cette préconisation reflète l'inquiétude que ces équipements particulièrement stratégiques en termes de surveillance et d'interception des données et des flux puissent être utilisés par la Chine pour servir ses intérêts. Cette inquiétude s'est également exprimée dans d'autres pays (Allemagne, Australie ou États-Unis par exemple).

Depuis juin 2013, les révélations faites par l'ancien consultant de la *National Security Agency* (NSA), Edward Snowden, ont montré combien certains États, au premier rang desquels les États-Unis, s'étaient engagés dans le développement de capacités d'interception et de surveillance des réseaux notamment en s'appuyant sur le positionnement des entreprises américaines souvent *leaders* du marché en informatique. Il a été notamment révélé que la NSA avait intercepté des routeurs d'entreprises américaines afin d'y introduire des mouchards[15]. Ces révélations ont sans doute permis de contribuer à accentuer les efforts de mise en œuvre de cette stratégie.

Vers des marchés « souverains » ?

Comme évoqué, le marché de la cybersécurité et de la cyberdéfense s'est développé pour permettre aux États (mais pas seulement) de faire face au développement d'un nouveau type de menace. Nous allons voir maintenant comment les stratégies mises en place par les États impactent ce marché.

D'abord en termes budgétaires, de nombreux États ont dédié une part croissante de ressources (financières et humaines) à la cybersécurité et à la cyberdéfense. Dans un contexte budgétaire particulièrement tendu, les budgets dévolus à la cybersécurité et à la cyberdéfense sont en constante évolution. Le plan Défense Cyber porté par le ministère de la défense français, présenté en 2014, prévoit un financement d'un milliard d'euros[16]. En 2013, l'État annonçait que le budget R&D de la DGA sur la cybersécurité serait multiplié par trois passant de 10 millions à 30 millions d'euros[17].

Aux États-Unis, le constat est le même. En 2015, le budget du *Department of Defense* consacré aux opérations dans le cyberespace serait augmenté de 8,5 % par rapport à 2014 et passera de 4,7 à 5,1

[14] Rapport d'information du Sénat sur la cyberdéfense, 2012, p. 5.
[15] Sean Gallagher, "Photos of an NSA "upgrade" factory show Cisco router getting implant", Arstechnica, 14 mai 2014, disponible sur: http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/, dernière consultation le 1er juillet 2014.
[16] Alain Ruello, « La France met la défense à l'heure des cyberattaques », *Les Echos*, 21 janvier 2014, disponible sur: http://www.lesechos.fr/21/01/2014/LesEchos/21609-092-ECH_la-france-met-la-defense-a-l-heure-des-cyberattaques.htm, dernière consultation le 1er juillet 2014.
[17] Loukil R., « Le budget R&D cybersécurité de la DGA multiplié par trois », *L'Usine Nouvelle*, 29 janvier 2013, disponible sur: http://www.usinenouvelle.com/article/le-budget-r-d-cybersecurite-de-la-dga-multiplie-par-trois.N190482, dernière consultation le 1er juillet 2014.

milliards de dollars[18]. Les mêmes efforts sont observés dans les différents pays européens laissant penser que le marché public de cybersécurité et cyberdéfense devrait croître de façon importante.

On l'a vu, la cybersécurité passe d'abord par la mise en place et le perfectionnement de systèmes de surveillance des réseaux, des outils de détection de toute activité suspecte (flux de données trop important à l'entrée ou à la sortie du système d'information), mais aussi des outils de protection des données en elles-mêmes comme le chiffrement. Ces outils sont mobilisables dans le cadre d'une défense périmétrique et d'une défense en profondeur et sont déjà disponibles sur le marché (éditeurs de solutions de sécurité comme McAfee, Kaspersky ou Symantec). L'expérience tirée des attaques passées a révélé la nécessité de développer des outils qui permettent notamment la rétro-ingénierie afin de comprendre comment sont élaborées les charges actives (virus, vers et autres) utilisées dans les attaques.

À ce titre, la dernière Loi de Programmation militaire votée fin 2013 vise notamment à permettre aux équipes de l'Agence nationale de la sécurité des systèmes d'information d'utiliser de tels moyens, ce qui leur était jusque-là interdit. Si on se situe ici dans une optique défensive (même si le procédé est de nature offensive), le développement d'outils dédiés à l'offensive pure n'est pas à exclure. On sait qu'il existe déjà un marché que l'on peut qualifier de « gris » dédié à l'achat par les États de failles "*zero-day*", c'est-à-dire des failles qui n'ont pas encore été révélées publiquement. Ces failles sont par la suite utilisées dans la conception de vers et virus sophistiqués comme cela a été le cas avec Stuxnet en 2010 qui à lui seul utilisait cinq failles *"zero-day"*. Edward Snowden a d'ailleurs révélé que la *National Security Agency* américaine avait déjà eu recours à ce type de failles pour mener des attaques d'espionnage et qu'elle se fournissait notamment auprès d'une société française, Vupen[19]. Si les États sont des acteurs majeurs de ce marché, ils ne sont pas les seuls acteurs à la recherche de ce type de produits. Les criminels, terroristes, mafias, et même les entreprises sont intéressés par ce marché qui semble florissant. Peu d'études existent sur ce marché pour lequel on manque de visibilité. Le magazine Forbes publiait en 2012 un portrait de Vupen qui présentait la société française comme étant une entreprise « rentable »[20]. En 2007, Charlie Miller[21], chercheur en sécurité informatique, avait estimé le prix de ces failles en fonction de leur support.

[18] IHS Jane's, « Pentagon Budget 2015 : DOD cyberspace operations would get 8.5% boost », 16 mars 2014, disponible sur: http://www.janes.com/article/35427/pentagon-budget-2015-dod-cyberspace-operations-would-get-8-5-boost?from_rss=1, dernière consultation le 1er juillet 2014.

[19] Yves Eudes, « Vupen, la PME française qui a travaillé pour la NSA », *Le Monde.fr,* 29 novembre 2013, disponible sur : http://www.lemonde.fr/international/article/2013/11/29/vupen-la-pme-francaise-qui-a-travaille-pour-la-nsa_3522578_3210.html, dernière consultation le 1er juillet 2014.

[20] « Meet the Hackers who Sell Spies the Tools to Crack your PC (and Get Paid Six-Figure Fees) », *Forbes Magazine*, 9 avril 2012.

[21] Il travaille actuellement chez Apple pour détecter les failles "*zero-day*" mais a également travaillé chez Twitter et à la NSA.

Tableau 1.

Vulnerability/Exploit	Value	Source
"Some exploits"	$200,000 - $250,000	Gov't official referring to what "some people" pay [9]
Significant, reliable exploit	$125,000	Adriel Desautels, SNOSoft [11, 22, 13]
Internet Explorer	$60,000 - $120,000	H.D. Moore [22]
Vista exploit	$50,000	Raimund Genes, Trend Micro [24]
"Weaponized exploit"	$20,000-$30,000	David Maynor, SecureWorks [18]
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks [18]
WMF exploit	$4000	Alexander Gostev, Kaspersky [26]
Microsoft Excel	$\geq$ $1200	Ebay auction site [21, 25]
Mozilla	$500	Mozilla bug bounty program [4]

Table 1: Estimates on exploit values.

Source : Charlie Miller, 2007, " The Legitimate Vulnerability Market, Inside the Secretive World of 0-day Exploit Sales ", Independent Security Evaluators.

Mais le principal impact des stratégies étatiques sur le marché est la demande de la constitution d'outils maîtrisés voire « souverains » car pour disposer de tels outils et équipements, les États cherchent à dynamiser et à structurer un marché actuellement dominé par quelques grandes entreprises principalement américaines. Cette thématique a émergé à la fin des années 2000, mais se formalise au début des années 2010 avec la mise en œuvre de projets spécifiques.

En France, la réflexion sur le sujet est entamée dans le Livre blanc de 2008 en désignant la sécurité des systèmes d'information comme une capacité de « premier cercle », c'est-à-dire une capacité « nécessaire au maintien de l'autonomie stratégique et politique de la nation »[22].

Puis elle est réaffirmée dans le Livre blanc de 2013 puisqu'il précise qu'« un effort budgétaire annuel en faveur de l'investissement permettra la conception et le développement de produits de sécurité maîtrisés »[23] et qu'« une attention particulière sera portée à la sécurité des réseaux de communication électroniques et aux équipements qui les composent »[24]. Elle est ensuite mise en œuvre dans le plan 33 de la « Nouvelle France industrielle » porté par le ministère de l'Économie et le « Pacte Défense Cyber » du ministère de la défense en 2014. L'objectif du plan 33 « Cybersécurité » est de construire « la France de la sécurité et de la confiance numérique » et de « mieux structurer la demande nationale afin d'orienter la R&D publique et privée sur le marché national, puis partir à la conquête des marchés internationaux, mettre en place des projets vitrines de déploiement de solutions de cybersécurité, développer nos entreprises françaises sur les nouvelles technologies de souveraineté »[25]. Afin de mettre en place un marché de confiance, ce plan prévoit notamment la création d'un « label France » pour favoriser les produits et services des entreprises françaises sur les marchés publics[26].

[22] Livre blanc sur la défense et la sécurité nationale, 2008, p. 318.
[23] Livre blanc sur la défense et la sécurité nationale, 2013, p. 106.
[24] *Ibid.*
[25] Plan Cybersécurité, La Nouvelle France Industrielle.
[26] Sandrine Cassini, « Un plan Cybersécurité pour aider les industriels français », *Les Echos,* 10 juin 2014, disponible sur: http://business.lesechos.fr/directions-juridiques/0203548960886-un-plan-cybersecurite-pour-aider-les-industriels-francais-100513.php, dernière consultation le 4 juillet 2014.

À l'appui de cette politique le Pacte Défense Cyber poursuit en expliquant que « pour maintenir et étendre notre capacité souveraine d'action dans le cyberespace, il est indispensable de renforcer une véritable base industrielle et technologique de défense en cybersécurité, capable notamment d'offrir une nouvelle génération d'équipements et de logiciels, fortement maîtrisés, soutenue en premier lieu par les Projets d'Étude Amont (PEA) et les programmes d'équipement des forces, à côté d'autres modes de financements publics et en cohérence avec le Comité de la Filière des Industries de la Sécurité (COFIS) et en appui des plans de reconquête de la Nouvelle France Industrielle »[27].

Certains acteurs du marché ont d'ailleurs déjà commencé à se structurer en ce sens. C'est le cas de l'association Hexatrust « née de la volonté commune de PE et ETI françaises, acteurs complémentaires experts de la sécurité des systèmes d'information, de la cybersécurité et de la confiance numérique »[28]. L'État français a par ailleurs déjà lancé plusieurs initiatives « souveraines » sur la question du *cloud computing* et des anti-virus. La question de la confiance est l'une des thématiques essentielles à la compréhension des questions de cybersécurité et de cyberdéfense alors même que les spécialistes reconnaissent volontiers qu'il n'y a pas d'alliés dans le cyberespace.

Les difficultés à construire des coopérations internationales sur ce sujet (y compris au sein d'un groupe d'alliés comme l'OTAN) témoignent de la réserve des États quant au partage de leurs informations, leurs stratégies et outils alors même que tous reconnaissent un besoin de coopération afin de réguler et réglementer les actions des États dans le cyberespace.

Conclusion

Si les États constituent un acteur du marché important et ayant potentiellement un rôle structurant, les entreprises (et notamment les entreprises stratégiques) doivent faire face aux mêmes types de menaces et ont, en conséquence, le même type de besoins et pas seulement en termes d'équipements, mais également en termes d'audit, de conseils et de formations. D'ailleurs l'étude de l'évolution du marché de la cybersécurité et de cyberdéfense (fusions et acquisitions) montre que celui-ci a entamé sa recomposition avant même la formalisation des stratégies étatiques pour répondre avant tout aux demandes d'acteurs privés.

[27] Ministère de la défense, « Pacte Défense Cyber, 50 mesures pour changer d'échelle », p. 11.
[28] Site internet www.hexatrust.com, dernière consultation le 7 juillet 2014.

Références

ARQUILLA John et RONFELDT David, " Cyberwar is coming ! ", *Comparative Strategy*, vol. 12, n° 2, 1993, p. 141-165.

BOYER Bertrand, *Cyberstratégie : l'art de la guerre numérique*, Nuvis, Paris, 2012.

DESFORGES Alix, « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, n° 152-153, Paris, La Découverte, 2014, p. 67-81.

DUNN CAVELTY Myriam, *Cybersecurity and Threat Politics- US efforts to secure the information age*, Abingdon, Routledge, 2008.

DUNN CAVELTY Myriam, *The militarization of Cyber Security as a Source of Global Tension*, Strategic Trends-Center for Security Studies, février 2012.

MILLER Charlie, "The Legitimate Vulnerability Market, Inside the Secretive World of 0-day Exploit Sales", *Independent Security Evaluators*, 2007.

RID Thomas, *Cyber War Will Not Take Place*, Oxford, Oxford University Press, 2013.

SAMAAN Jean-Loup, *La menace chinoise, une invention du Pentagone ?*, Paris, Vendémiaire, 2012.

LA CYBERSECURITE ENTRE BIEN PUBLIC ET MARKETING DE LA PEUR

Danilo D'ELIA[1]
Doctorant à l'Institut français de géopolitique de l'université Paris VIII Vincennes-Saint-Denis

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

Les réseaux informatiques et les technologies de l'information se sont imposés en peu de temps comme un élément essentiel des économies développées. En partant des robots médicaux jusqu'à la production d'électricité, désormais tous les services indispensables au bon fonctionnement de notre quotidien dépendent de ces technologies.

Toutefois, la pénétration de l'informatique dans les secteurs industriels et notamment l'interconnexion et l'interdépendance entre les réseaux des infrastructures critiques, a entraîné de nouveaux risques. Aux débuts de l'informatique, la sécurité ne figurait pas parmi les priorités des développeurs. Le résultat a alors été la forte présence de vulnérabilités et donc l'élargissement de la surface d'attaque potentielle par des agents malveillants.

Depuis les événements de 2007 en Estonie, nous avons assisté à une multiplication et à un impact grandissant des attaques informatiques[2]. Au-delà de celles ayant pour but l'escroquerie et l'atteinte à la réputation, le risque de piratage de secrets industriels (*Night Dragon*, 2011) et étatiques (Bercy, 2011), ainsi que celui de sabotage des Opérateurs d'Importance Vitale - OIV (Stuxnet, 2010) a marqué un changement dans le périmètre de la sécurité des systèmes d'information (SI). À cet égard, le terme cybersécurité a pris de plus en plus de place pour définir « l'état recherché (…) permettant de résister à des attaques visant la disponibilité, l'intégrité et la confidentialité des données »[3] et la capacité de réaction, de riposte et de remédiation suite à une attaque informatique.

Au niveau politique, l'intrication des enjeux économiques et sécuritaires correspond à la représentation de la cybersécurité comme un bien public, comme étant l'affaire de tous[4]. On retrouve dans les discours politiques l'idée que l'État doit aller au-delà de la protection de ses propres systèmes pour assurer à tous les citoyens la liberté d'utiliser les réseaux informatiques, et en

---

[1] Le projet de recherche de l'auteur, qui porte sur les dynamiques public-privé de la mise en place de la stratégie française de cybersécurité, bénéficie du soutien financier de l'entreprise Airbus Defence & Space Cybersecurity. Les idées et opinions exprimées dans ce document sont celles de l'auteur et ne reflètent pas nécessairement celles d'Airbus Group.

[2] En France le CERT de l'ANSSI a reçu plus de 700 signalements et a pu traiter directement environ 70 incidents en 2012 alors que le Centre d'analyse de lutte informatique défensive a traité plus de 500 remontées d'incidents en 2013 contre 196 en 2011.

[3] Agence Nationale de la Sécurité des Systèmes d'Information, Défense et sécurité des systèmes d'information – Stratégie de la France, 2011.

[4] Selon la théorie économique, la notion de bien public ou collectif répond aux deux critères de non-rivalité (la consommation de ce bien par un usager n'entraîne aucune réduction de la consommation des autres usagers) et de non-exclusion (il est impossible d'exclure quiconque de la consommation de ce bien ; il est, par conséquent, impossible de faire payer l'usage de ce bien). Paul A. Samuelson, "The Pure Theory of Public Expenditures", *Review of Economics and Statistic*, vol. 36, n° 4, novembre 1954, p. 387-389.

même temps doit garantir la protection de son économie et de son territoire. À ce propos, Jean-Marc Ayrault, alors Premier ministre, déclarait en février 2014: la cybersécurité « 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 »[5].

Alors que le statut de bien public de la cybersécurité est discuté par les économistes et les politologues[6], la géopolitique s'intéresse plutôt aux conséquences de l'utilisation de la représentation de la cybersécurité comme bien public dans les rapports de force entre acteurs. Selon l'École française de géopolitique, une représentation est « un ensemble d'idées cohérentes qui expriment la réalité, se nourrissent d'objectivité, mais gardent tout de même un caractère subjectif »[7]. Elles ne sont donc pas neutres, mais elles peuvent influencer les stratégies des acteurs.

C'est ainsi que la représentation d'un risque collectif s'est traduite par une implication majeure des pouvoirs publics dans les affaires de cybersécurité. Compte tenu de l'impact potentiel sur la compétitivité et la sécurité d'une nation à partir de la seconde moitié des années 2000, de nombreux pays ont élaboré des documents stratégiques déclarant la protection des SI priorité de sécurité nationale[8]. Il s'ensuit que cette volonté s'est déclinée par le biais de politiques publiques visant des dispositions réglementaires, le contrôle des données personnelles et des technologies[9].

En outre, au-delà des enjeux sécuritaires (protection des OIV) et de souveraineté (être indépendant dans l'atteinte de cet objectif), la cybersécurité est aussi devenue une source d'opportunités économiques au moment de la crise financière. L'industrie du secteur génère un chiffre d'affaires global de 50 milliards d'euro (1,3 milliard d'euros en France, soit 40 000 emplois) et les prévisions de croissance sont de 10 % par an[10]. Toutes ces raisons convergent et contribuent à la montée du discours sur l'importance pour les États de se doter d'une « Base industrielle et technologique de cybersécurité » (BITC), c'est-à-dire d'un écosystème cohérent d'entrepreneurs (grands groupes et PME), laboratoires et investisseurs capable d'assurer une innovation continue et un socle technologique répondant aux enjeux sécuritaires et économiques.

C'est sur ce dernier point que nous allons focaliser notre recherche. En effet, comme cela a été mis en évidence par l'affaire Snowden, la domination commerciale d'un pays, à savoir les États-Unis, à travers ses entreprises dans la chaîne d'approvisionnement du cyberespace, constitue un avantage informationnel sans comparaison aucune. Cet avantage est déjà exploité à des fins d'espionnage et de renseignement, tant économiques que politiques[11].

---

[5] Discours du Premier ministre tenu à l'Agence nationale de la sécurité des systèmes d'information, le 21 février 2014.

[6] Dave Clemente, *Cyber Security and Global Interdependence: What Is Critical?,* Chatham House, février 2013.

[7] Yves Lacoste (dir.), *Dictionnaire de géopolitique*, Flammarion, Paris, 1993.

[8] Stefano Mele, *I principi strategici delle politiche di cyber security*, 2014, disponible sur: http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html, dernière consultation 10 avril 2014.

[9] Frederick Douzet, « La Géopolitique pour comprendre le cyberespace », *Hérodote*, n° 152-153, p. 3-21, 2014.

[10] Visiongain, Global Cyber Security Market Report 2013-2023.

[11] Danilo D'Elia, «La Guerre économique à l'ère du cyberespace », *Hérodote*, n° 152-153, p. 240-260.

De cette façon, la révélation de PRISM a alimenté les discours autour de la souveraineté selon lesquels la puissance d'une nation passerait par la maîtrise des technologies nécessaires à la sécurité des systèmes d'informations les plus sensibles. La problématique pour l'État est alors d'initier une offre efficace pour répondre aux enjeux de souveraineté qui sont perçus. L'État, dans des secteurs tels que l'armement ou la santé, trouve ici une fonction indéniable de fournisseur de la cybersécurité perçue comme un bien collectif et ceci conduit à analyser la manière dont ce bien peut être produit, c'est-à-dire la politique industrielle[12].

La France depuis le Livre blanc sur la défense et la sécurité nationale de 2008 a identifié la cybersécurité comme un enjeu majeur pour sa sécurité nationale et vise à devenir une puissance mondiale dans le domaine. Une politique volontariste a suivi sur le sujet, notamment avec la transformation de la Direction centrale de la sécurité des systèmes d'information (DCSSI) en Agence nationale (ANSSI). Dans ce contexte, l'année 2013 peut être considérée comme un tournant historique.

Parallèlement au vote de la Loi de Programmation militaire – LPM 2014-2019 – qui impose des règles de cybersécurité aux OIV et finance 1 milliard d'euros en ressources techniques et humaines pour l'État, la sphère publique a lancé un vaste chantier de politique industrielle : des investissements en R&D pour 150 millions d'euros ont été mis à disposition, une feuille de route de la politique industrielle (*Cyber Plan)* a été lancée et la constitution d'un pôle d'excellence est en cours.

L'ambition affichée est claire : développer une « offre souveraine de confiance ». Mais il est pour l'instant difficile d'établir le bilan de ces initiatives récentes. Néanmoins, cette volonté soulève différentes questions : quelles sont les capacités de production autonome dont dispose la France ? Quels sont les avantages et les limites de la coopération public-privé ?

Malgré les enjeux importants, l'État doit faire face à la spécificité de la cybersécurité qui lui impose certaines limites. Premièrement, parce que les OIV sont gérés par le secteur privé (50 % dans le cas de la France). Deuxièmement, parce que l'État ne possède ni les compétences nécessaires (laboratoires en R&D et experts) ni les moyens financiers, notamment dans une période de crise économique, pour défendre à lui seul le périmètre complet des infrastructures critiques. Pour ces raisons, une coopération avec le monde privé est donc indispensable. Ainsi les dynamiques État-Industrie constituent l'objet principal des recherches menées pour cet article.

Pour répondre aux questions posées, il est nécessaire d'expliquer dans un premier temps pourquoi le marché et notamment l'offre ne sont pas suffisamment matures et en quoi consiste une « offre souveraine ». Une fois ce constat établi, on se penchera sur la structuration du dialogue entre les acteurs de la cybersécurité par une analyse des rapports de force.

[12] Il est nécessaire de rappeler la définition de l'économiste Elie Cohen selon laquelle la politique industrielle est une politique sectorielle visant « à promouvoir des secteurs qui, pour des raisons d'indépendance nationale, d'autonomie technologique, de faillite de l'initiative privée, d'équilibre territorial ou politique méritent une intervention » Elie Cohen, *Que reste-t-il des politiques industrielles ?*, L'Industria, Paris, 21 mai 2007.

Un marché inadapté face au périmètre redéfini de la cybersécurité

Le marché de la cybersécurité est un marché de produits et services de forte innovation. Il nécessite des investissements constants en R&D (en moyenne autour de 20 % du chiffre d'affaires d'une entreprise) pour faire face à l'évolution rapide et la complexification des menaces et des technologies. En outre les cycles de développement et de déploiement sont très courts (entre trois mois et trois ans) pour une diffusion à l'échelle mondiale. Au cours des six dernières années, le marché a été profondément bouleversé en termes d'offre (longue série d'acquisition et formation de *pure players*) et de demande (+20 % pour la période 2011-2014). Cette partie tentera d'apporter un éclairage sur les dynamiques sous-jacentes.

Les dynamiques industrielles en cours

La demande se structure d'une façon générale autour de trois piliers :

a) *Business to Government* : il s'agit du marché *"high grade"* correspondant à la cyberprotection où les mécanismes cryptographiques souverains sont au cœur des SI de l'État et des systèmes d'armes. À l'exception des États-Unis, ce marché est estimé entre 50 et 100 millions d'euros par an et par pays. Les intégrateurs issus du secteur de la défense comme Lockheed Martin et Thales dominent ce marché ;

b) *Business to Business* : segment qualifié de *"mid grade"* où la demande est constituée par les grands opérateurs économiques avec de forts besoins de sécurité et de défense qui n'ont pas accès au premier niveau parce que trop cher ou avec des standards inadaptés aux SI commerciaux ;

c) *Business to Customer* : ici la demande de sécurité est "*low level*" et l'achat est plutôt guidé par le rapport prix/performance et la réputation du fournisseur. Ce segment correspond en grande partie au marché des antivirus et des *firewalls* pour la plupart des entreprises. Les géants américains comme McAfee (1,3 milliard d'euros de chiffre d'affaires en 2012) et Symantec (2,7 milliards d'euros de chiffre d'affaires en 2012) en sont les acteurs les plus importants.

La demande est répartie entre trois grands blocs : les États-Unis (45 %), l'Europe incluant Israël (25 %) et le reste du monde (30 %).

La structure du marché est fortement atomisée. Les entreprises sont de taille très hétérogène et celles qui totalisent plus d'un milliard d'euros de chiffre d'affaires sont américaines. Selon leur spécialisation et leur orientation (produits/services), nous proposons la typologie suivante : 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), et les spécialistes de la défense (Thales, Airbus Defence and Space).

La structure du marché a fortement évolué depuis la moitié des années 2000. Sur la base d'une rétrospective des mouvements du secteur menée pour cet article, nous observons depuis 2008 une accélération nette des acquisitions, des fusions et partenariats stratégiques[13]. Cette dynamique démarre suite aux grandes vagues d'attaques de 2005 qui ont touché le secteur privé aux États-Unis (demande privée) puis se consolide avec la prise de conscience des questions de cybersécurité par les États suite à l'attaque en Estonie en 2007 (demande étatique).

Deux catégories d'acteurs sont principalement impliquées. Premièrement les entreprises de défense, qui dans un contexte de restriction des dépenses publiques de défense, cherchent à diversifier leurs revenus à travers des partenariats avec des sociétés, souvent des PME, spécialisées dans un segment de la sécurité informatique tel que la détection ou le conseil[14]. En 2008 par exemple, BAE Systems a fait l'acquisition de Detica, société de conseil spécialisée dans la fraude et la sécurité des marchés financiers.

Dans un second temps, ce sont les grands éditeurs et intégrateurs qui se sont fortement lancés dans des fusions et alliances afin d'élargir leur portfolio. On peut citer comme exemple, l'acquisition de SecureWorks – spécialiste dans la prévention et détection d'intrusion – par le constructeur d'ordinateurs Dell en 2011. Cette dynamique d'alliances et de fusions connaît aujourd'hui un deuxième essor comme le démontrent les acquisitions, CISCO-Sourcefire (2013), FireEye-Mandiant (2014), Orange-Atheos (2014).

Le chemin difficile vers une offre sur mesure

Le dynamisme du marché peut être expliqué par le changement de périmètre de la cybersécurité qui n'est plus limité aux systèmes étatiques, mais qui englobe désormais les systèmes industriels, l'internet mobile et le *Big Data*. Cela s'est traduit par la constitution de deux nouvelles barrières à l'entrée sur le marché : la nécessité d'une vision à la fois globale et maîtrisée sur l'ensemble des SI.

D'un côté, les fournisseurs classiques de la défense, issus notamment du monde C4ISR[15], mettent en place des stratégies de « démocratisation » des solutions développées jusqu'ici pour des clients étatiques (défense, renseignements, etc.). Il s'agit pour ces industriels de la défense de diversifier leur marché en temps de restrictions budgétaires grâce à l'élaboration d'une nouvelle offre commerciale, notamment en direction des OIV. Pour cela, il leur faut disposer de solutions de bout en bout, aux prix attractifs et ayant une vision globale sur les fonctions métiers, les nouvelles menaces et l'évolution des usages.

De l'autre côté, la sécurité conçue comme une superposition de technologies achetées sur étagère (routeurs, chiffreurs, firewall, etc.), malgré leur faible coût, n'est plus adaptée aux besoins de sécurité permettant d'anticiper, de détecter et de réagir à une menace évolutive et techniquement sophistiquée qui nécessite une vision globale des risques. La consolidation du marché est ainsi l'illustration d'une offre pas encore mature face au changement d'une menace perçue comme étant de plus en plus complexe et qui aujourd'hui touche aussi l'informatique en nuage et l'internet des objets.

[13] Sur la base des cinquante acquisitions et alliances les plus importantes en terme de capital (> 100 millions d'euros) entre 2008 et 2014.

[14] Vincent Boulanin, "Cybersecurity and the Arms Industry", *SIPRI Yearbook 2013: Armaments, Disarmament and International Security* Oxford University Press, 2013, p. 218-226.

[15] Ce sigle représente l'ensemble des fonctions militaires définies dans la doctrine comme *Command, Control, Communications, Computers, Intelligence, Surveillance* et *Reconnaissance.*

Parallèlement, la notion de prestataire de confiance s'impose comme une caractéristique structurante du marché. La sécurité des SI sensibles tant pour l'administration que pour les OIV comporte des éléments de confidentialité, d'intégrité et de continuité des opérations qui impactent les activités au cœur du fonctionnement d'une société. Comme démontré par les révélations sur le programme de la NSA, PRISM, les pays concepteurs et producteurs de *hardwares* et de *softwares* et encore plus de solutions de sécurité profitent d'un avantage informationnel sur les pays consommateurs qui peut être exploité à des fins stratégiques. Comme cela fut souligné par le journal britannique *The Economist*[16], PRISM a eu un impact important sur la confiance placée dans les entreprises américaines.

Afin de répondre à ces préoccupations sécuritaires et stratégiques et à la suite du scandale PRISM, plusieurs hommes politiques ont manifesté dans leurs déclarations la volonté de disposer de solutions dites « de confiance ». Il s'agit, pour un État, de disposer de fournisseurs capables à la fois de produire des solutions maîtrisées et d'assurer une relation de confiance avec le client.

Dans ce contexte, le travail des intégrateurs devient fondamental car ils ont une fonction de maîtres d'œuvre industriels dont l'objectif est d'intégrer plusieurs briques technologiques (développées en *open source*, achetées sur étagère, ou conçues sous contrôle des autorités nationales). Ils sont dès lors les plus à même de définir des architectures dont la sécurité globale est maîtrisée. De leur côté, les grandes entreprises de la défense (Airbus, Thales) avec les géants de l'IT (Atos) ont une vision d'ensemble sur les « systèmes de systèmes » et donc un avantage dans la compréhension de la complexité de la protection des réseaux informatiques.

En conclusion, les caractéristiques intrinsèques du marché (compétition mondiale et nécessité d'innovation constante) avec le besoin nouveau d'une vision globale tout en gardant un aspect de confiance, sont en train de le structurer vers l'émergence de ce qu'on pourrait appeler des *pure players* de la cybersécurité. Mais comment ce contexte et 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[17] : 700 acteurs (100 éditeurs, 100 équipementiers et 600 sociétés de conseil), dont cinq grands groupes, une quasi-absence d'entreprises de taille intermédiaire, à l'exception de Bertin Technologies, et plus de 600 PME ayant un chiffre d'affaires souvent inférieur à 5 millions d'euros.
Reproduire toute la chaîne d'approvisionnement (systèmes d'exploitation, microprocesseurs, serveurs, etc.) au niveau national est donc impossible : pour l'État il s'agit plutôt de développer une maîtrise nationale autour de quelques technologies critiques et de s'appuyer sur des intégrateurs capables d'offrir un système sécurisé dans sa globalité.

[16] "The NSA and Cryptography, Cracked Credibility", *The Economist*, 4 septembre 2013.
[17] Alliance pour la Confiance Numérique, *Observatoire de la confiance numérique,* 2013.

La boucle d'amélioration continue du trinôme État-OIV-fournisseur de sécurité

Se doter d'une offre de solutions souveraines et « valables » est devenu une priorité nationale pour la France. À partir de la lecture croisée des documents officiels, nous pouvons mettre en exergue ses caractéristiques principales[18].

Premièrement, une solution souveraine est synonyme d'intégrité : c'est-à-dire avoir l'assurance de l'absence de moyens de contournement garantissant ainsi « la protection d'informations et de systèmes sensibles ». Pour cela, l'État exige « un processus d'évaluation sous le contrôle de l'autorité SSI nationale »[19] qui se traduit pour de nombreux industriels par un prérequis de développement sur le territoire français[20] et qui nécessite un niveau d'investissement fort et constant.

Au-delà du critère de l'intégrité, l'offre pour être « valable » doit être simple à déployer, à exploiter, et disposer d'une bonne ergonomie. Ces caractéristiques de fonctionnalité et intégrabilité, couplées à un prix compétitif, sont un préalable afin de permettre une bonne acceptation par le marché et ainsi faciliter un succès commercial. Tout l'enjeu de la politique industrielle consiste alors à structurer 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 synthétisées dans le tableau 1. La combinaison de ces mesures constitue la politique industrielle française en matière de cybersécurité.

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, etc.) et	Indirect sur l'offre et sur la demande	ANSSI-DGA, OIV, Fournisseurs de sécurité

[18] Trois documents sont indispensables à ce propos : la Loi de Programmation militaire 2014-2019, art. 22 ; l'appel d'offre pour octobre 2013 ; le guide pour la qualification de prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés par l'ANSSI.

[19] Selon l'appel à projets des Programmes d'Investissements d'Avenir 2013 – Développement de l'Économie numérique, « Cœur de filière numérique-Sécurité numérique », octobre 2013.

[20] Entretiens recueillis à l'occasion du Forum International de la Cybersécurité, Lille 21-22 janvier 2014.

	étatiques (ANSSI/DGA).		
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 les 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 12 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 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

L'analyse des processus et du contenu de telles initiatives fait émerger quatre piliers principaux autour desquels la politique industrielle s'articule : la règlementation visant les OIV, l'organisation structurelle du dialogue État-Industrie, la campagne de financement en R&D et la politique de certification des solutions de confiance.

Règlementation pour doper la demande

Le tournant dans la stratégie de cybersécurité des OIV a été l'adoption par le Parlement de la LPM 2014-2019 (Chapitre IV, art. 21-25). Ce dispositif législatif donne à l'État les moyens d'imposer aux OIV des mesures de sécurité. Notamment l'article 22 impose aux OIV la mise en place d'équipements de détection d'attaques informatiques et leur exploitation par un prestataire labélisé par l'ANSSI et localisé sur le territoire national. Les OIV seront ainsi obligés de renforcer la protection des SI sensibles en ayant recours à un prestataire "*Made in France*". Du point de vue du marché, ces mesures contraignantes sont alors un levier économique pour développer la demande en faveur d'une solution nationale de cybersécurité et pour dynamiser l'apparition de solutions différenciées afin de viser les marchés à l'export. 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 administrations à recourir aux produits nationaux et labélisés par l'ANSSI[21].

Organisation formelle du dialogue État-Industrie

Le lancement du CoFis, du groupe de travail sur le SCADA et de l'équipe projet en charge de l'élaboration de la feuille de route du Plan Cyber sont la démonstration de la volonté d'organiser formellement 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 faire se rencontrer les acteurs opérationnels de la cybersécurité, les acteurs de la recherche et les pouvoirs publics afin de déterminer les priorités, d'éviter des redondances et de concilier offre et demande.

Ce dialogue, associé à la nouvelle règlementation, apporte une dimension stratégique à la structuration d'une offre « valable ». Pour les industriels de la sécurité, il est indispensable de disposer d'un modèle économique viable pour lancer des projets complexes comme celui du développement de nouvelles sondes de détection des attaques. Pour faire face aux difficultés d'évaluation du marché, le secteur public, par son action de règlementation, offre aux industriels des tendances sur le volume du marché afin d'avoir des coûts annoncés plus proches de la réalité.

En effet, un industriel qui manque de visibilité sur la demande provisionnera ses risques et les répercutera sur le prix final. Ainsi, la structuration du dialogue État-Industrie, couplée avec la règlementation, contribue à la compréhension du marché qui de son côté donne de la confiance aux acteurs de l'écosystème et aide à définir les priorités.

[21] Circulaire du 17 juillet 2014, Politique globale de sécurité des systèmes d'information (PSSIE).

Le groupe de travail sur la sécurité des SCADA, par sa composition, est l'exemple à citer d'une e-participation à la décision du trinôme État-OIV-fournisseur de sécurité. Il est important de rappeler ici que l'ANSSI n'est pas le seul représentant de l'État dans les enjeux industriels. Comme montré par le tableau 1, le ministère de la défense, via la DGA, occupe aussi une place importante dans le dialogue avec le secteur privé. Grâce à son expertise historique dans la protection de la confidentialité et de l'intégrité des données classifiées (les SI du ministère, les systèmes d'armes, etc.), la DGA partage avec l'ANSSI le rôle d'acteur déterminant de la politique industrielle.

Orientation de la R&D

Afin de garantir des investissements constants en R&D, l'État a multiplié ses efforts tant dans le domaine civil que militaire. La DGA a triplé en deux ans les crédits d'études (30 millions d'euros en 2014). En parallèle, dans le cadre du Programme Investissements d'Avenir 2013, un appel à projets intitulé « Sécurité numérique » a fait l'objet de 18 propositions. À travers un fonds de 20 millions d'euros, cette initiative ambitionne d'orienter les investissements en R&D et ainsi de favoriser le développement d'une offre jusqu'à présent absente. Cela permettra notamment la mise en œuvre des capacités demandées par la LPM 2014-2019[22]. Dans la continuité de cette stratégie de pilotage de la R&D, le « Plan Cyber » envisage une nouvelle vague d'appel à projets pour 2015, dans le but de développer deux à trois nouvelles gammes d'offres par an.

Certification et label France

Ce volet représente une autre forme de partenariat stratégique. Les industriels et l'État, notamment l'ANSSI et la DGA, jouent un rôle fondamental pour réduire les risques et accroître le niveau de confiance. Il s'agit de l'expression plus concrète de la boucle d'amélioration continue entre État, OIV et fournisseurs de solutions de sécurité. 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 technologies correspondant aux critères de sécurité requis. En outre, l'État, en remontant les retours d'expérience des utilisateurs finaux aux industriels, assure une fonction d'intermédiaire entre les consommateurs et les fournisseurs qui développeront dans le bon sens les solutions de sécurité pouvant ensuite être commercialisées.

Une fois le processus de labellisation des prestataires terminé, l'ANSSI, considérée en l'état actuel par certaines sociétés comme un concurrent sur le marché de l'audit, pourra se retirer et laisser la place aux prestataires de confiance[23]. Néanmoins, le catalogue des solutions et sociétés labélisées souffre en l'état actuel d'une méconnaissance générale parmi les acteurs français surtout face aux géants américains et israéliens qui proposent des solutions souvent plus performantes en termes de coût-efficacité. Pour remédier à cela, le « Plan Cyber » propose de promouvoir un « Label France » afin de valoriser les produits certifiés ANSSI et ainsi augmenter leur visibilité, notamment à l'export.

[22] Cinq projets sont financés dans le cadre du PIA « Sécurité Numérique »: 1) terminaux mobiles sécurisés et applications de confiance ; 2) Solutions de protection des infrastructures et dispositifs voix/visiophonie sur IP ; 3) Outils passifs de détection et de corrélation à haut débit, outils d'investigation après incidents ; 4) Solutions de protection des dispositifs SCADA ; 5) Solutions de supervision de la sécurité (SIEM) maîtrisées.

[23] Cependant des réseaux hautement sensibles de l'administration ou des OIV resteront la prérogative de l'ANSSI.

Un secteur privé encore trop proche de l'État

Ces quatre piliers de la politique industrielle nous laissent percevoir la spécificité du modèle français. Tout d'abord une forte présence des pouvoirs publics, via le pilotage bicéphale ANSSI-DGA. Il s'agit de ce qu'on pourrait qualifier d'héritage du « Colbertisme *High-Tech* : »[24] c'est-à-dire la stratégie post Seconde Guerre mondiale de rattrapage du retard industriel fondée sur l'idée de maîtrise des grandes technologies (défense, télécommunication, énergie). Ce modèle, développé pendant trente ans, était articulé autour de vastes projets reposant fondamentalement sur la commande publique. Celle-ci était elle-même soutenue par la préférence nationale permettant l'émergence de champions nationaux bénéficiant de la recherche publique. Comme montré par notre analyse, les mêmes dynamiques réapparaissent à l'heure de la construction d'une BITC.

Néanmoins, les contraintes déjà mentionnées (restrictions budgétaires, libéralisation des OIV), couplées avec les caractéristiques propres à la cybersécurité (une menace évolutive et complexe touchant tant le civil que la défense, la nécessité d'un temps de réaction très court) ont obligé le volontarisme politique à s'ouvrir au secteur privé afin de trouver de nouveaux modèles de coopération. L'évolution interne et l'adaptation de l'ANSSI depuis son institution en 2009 sont un exemple de cette ouverture. Parallèlement à sa montée en puissance[25], à partir de 2011 un bureau de coordination avec les OIV a été instauré afin de permettre une meilleure connaissance des spécificités de chacun des douze secteurs d'importance vitale. De plus, un bureau entièrement dédié à la « Politique Industrielle et Assistance » a été mis en place en 2012 dans le but d'accompagner et faire le lien avec le secteur privé. À travers ces initiatives d'animation de l'écosystème industriel, l'ANSSI se positionne comme un acteur structurant du marché.

Ainsi l'approche actuelle consiste à décloisonner les secteurs civils (ANSSI) et militaires (DGA-MI), et les domaines publics et privés, chacun de ces acteurs étant détenteur d'une partie des compétences et de la compréhension de la menace. Cette démarche synchronisée et structurée surtout autour du pivot ANSSI-DGA a été rendue possible par la constitution d'une communauté réduite d'experts, opérationnels et techniques, provenant de la sphère publique aussi bien que du secteur privé[26]. Une telle coopération permet aux différents acteurs d'échanger en permanence et constitue ainsi la base du cercle vertueux entre règlementation, certification et financement public.

Ces dynamiques de la politique industrielle conçue par les pouvoirs publics pourraient avoir un triple effet positif : réduire les risques, accroître le niveau de confiance mutuelle et, *in fine*, structurer le marché. Mais quelles sont les possibilités de réussite d'une telle stratégie ? Au-delà de cette importante phase de dialogue, une analyse plus fine des actions en cours met en évidence comment les politiques publiques ont surtout bénéficié aux services publics (augmentation des effectifs de l'État) alors que le dialogue État-Industrie se fonde avant tout sur un rapport de force et des intérêts divergents.

[24] Elie Cohen, *Le colbertisme high-tech. Économie du grand projet*, Paris, Hachette Pluriel, 1992.

[25] Les effectifs ont été augmentés de 170 % (350 agents) par rapport à la date de lancement de l'ANSSI en 2009 (132) et le budget a été augmenté de 80 % (80 millions d'euros en 2014 contre 45 millions d'euros en 2009).

[26] Selon l'IGA Denis Plane, dans les départs des ingénieurs d'armement vers l'industrie, la cyberdéfense est depuis 5 ans la deuxième spécialité après le nucléaire. Voir Denis Plane, "Ce que ce cybernuméro n'a pas dit", *Le Magazine des Ingénieurs de l'Armement*, n° 102, mars 2014.

Définition d'une offre souveraine, mais aussi commerciale

La première de ces rivalités concerne la définition d'une offre souveraine. Si d'un côté 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, et cela afin de pouvoir disposer d'une offre la plus standardisée possible avec 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 ANSSI se traduisent par le développement de solutions spécifiques à des standards nationaux pouvant limiter l'accès aux marchés extérieurs s'ils ne sont pas partagés. En fait, le marché national français, évalué autour de 1,5 milliard d'euros ne permet pas d'atteindre la taille critique pour pérenniser les investissements en R&D et développer une offre compétitive vis-à-vis des géants américains. Ceux-ci sont souvent soutenus par leur gouvernement et le marché intérieur permet d'assurer un certain niveau de rentabilité des investissements[27]. Ainsi, si le Label France n'est pas accompagné d'un effort de standardisation international, le marché « de confiance » ne sera pas compétitif et donc pas rentable pour les fournisseurs français.

Du côté des OIV, leur présence à l'international nécessite une « offre valable » qui puisse être utilisée sur les territoires des différents sites de production ainsi que sur ceux de leurs filiales sans devoir multiplier les investissements. Par exemple, Total, qui constitue sûrement un OIV, aurait un intérêt économique à déployer des solutions de cybersécurité similaires sur ses cent six sites de raffinage.

Dans la même logique d'équilibre entre demande de souveraineté et offre commerciale, se pose la question de la définition des cahiers des charges. Du point de vue industriel, les marchés aux enjeux de souveraineté ont besoin d'être conçus avec des clauses de sécurité, réalisés de préférence par des experts de l'administration connaissant d'une part l'état de l'art de la menace, mais également les éventuels métiers associés. Pour cela, selon le privé, ces cahiers des charges doivent être développés sur la base d'une coopération avec les industriels. En effet, les contraintes de prix et de sécurité minimale nécessitent une vision claire des capacités actuellement disponibles dans le secteur privé. Du côté de l'administration, la rédaction d'un cahier des charges avec des niveaux de sécurité élevés est considérée comme un moyen de tirer l'offre vers le haut et d'en contrôler les spécifications à des fins de sécurité. Il s'agit donc ici encore de trouver le bon équilibre entre offre commerciale et demande de souveraineté.

De l'opacité de la définition de l'offre souveraine, découle aussi la question du financement de la R&D. Selon les acteurs privés, l'État doit assumer un rôle central dans le soutien à la R&D pour assurer les intérêts technologiques de souveraineté nécessaires à l'industrie nationale. Un financement public de la R&D permettrait de développer une solution dont le coût final serait adapté au marché permettant alors sa commercialisation tout en étant en conformité avec la règlementation. Du point de vue du secteur privé, chaque utilisateur *in fine* pourrait bénéficier des gains de mutualisation, plutôt que de devoir développer ses propres solutions, et par conséquent obtenir de meilleurs effets d'échelle, et une réduction significative des coûts. Cependant, cette vision d'une R&D soutenue par l'État nécessite un investissement conséquent dans un moment où les finances publiques font face au défi du redressement des comptes publics.

[27] Selon le rapport "U.S. Federal Cybersecurity Market Forecast 2015-2020", le marché américain est estimé à 65 milliards de dollars pour la période 2015-2020.

PME-État-Grands Groupes

Les PME sont le moteur de l'innovation dans le domaine cyber : c'est pour cela que la relation PME-Grands groupes est nécessaire à la construction de l'écosystème de la cybersécurité. Bien que ce ne soit pas une spécificité de la cybersécurité, cette relation prend toute son importance dans le cas français en raison de l'urgence actuelle et de la concurrence âpre subie sur les marchés internationaux.

Si le système français n'est pas comparable à la très enviée Silicon Valley, un rapprochement avec Israël nous apporte en revanche des éléments de réflexions. Bien que les dimensions de cet État soient proches de celles d'un département français, Israël est parmi les pays dominant le marché de la cybersécurité. Une première clé de son succès est un écosystème riche et bien rôdé : en Israël il existe une relation historique de proximité entre agences gouvernementales – civiles et militaires – et secteur privé favorisant l'innovation en coopération avec les laboratoires de recherche. Le *CyberSpark*, *cluster* sur la cybersécurité basé à Beersheva, offre un bon exemple du bénéfice d'un partenariat entre PME locales, grands groupes (souvent internationaux) et acteurs publics[28]. Sans avoir les moyens colossaux de la fameuse DARPA américaine, l'*Israel Defence Forces* finance le développement privé de solutions innovantes et apporte un soutien technique grâce à l'expertise de l'armée, notamment sa branche spécialisée dans le renseignement d'origine électromagnétique, et des laboratoires de l'université Ben-Gourion.

Les solutions développées sont, dans un premier temps, utilisées de façon exclusive par l'armée. Cependant, à cause de la faible importance du marché national, les PME israéliennes, souvent lancées par d'anciens officiers, utilisent l'innovation ainsi financée pour exporter vers de nouveaux marchés. Cette logique de domination commerciale fonctionne : 5 % du marché mondial en 2013 a été généré par des firmes basées en Israël. En conséquence, ce dynamisme attire les investisseurs privés nationaux ou étrangers, ce qui permet aux PME israéliennes de croître, soit grâce au capital-risque, soit en étant rachetées par les grands groupes. Les PME israéliennes génèrent ainsi des profits et pérennisent la R&D de manière indépendante : 165 millions de dollars ont été investis en 2013 par ces sociétés, soit 11 % des investissements globaux en cybersécurité[29].

Cette double capacité à favoriser le soutien public comme incubateur et la mobilisation de l'argent privé permet à la "*Nation Start-up"* de financer l'innovation de façon continue. Les grands groupes finissent par prendre la relève de l'État et des PME, tout en bénéficiant d'une R&D financée.

En France, malgré les efforts récents de la sphère publique[30], le secteur privé se heurte à une difficulté dans ce deuxième volet : l'absence d'un cadre favorable aux investissements en capital.

En France, la présence d'un tissu dynamique de pépites technologiques est incontestable, pourtant les taux de survie et les rythmes de croissance sont différents de ceux des États-Unis ou même

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

[29] Niv Elis, "Israel Raised 11 % of all Global Cyber Defense Investments in 2013", *The Jerusalem Post*, 23 février 2014, article disponible sur: http://www.jpost.com/Business/Business-News/Israel-raised-11-percent-of-all-global-cyber-defense-investments-in-2013-342312, dernière consultation 10 avril 2014.

[30] Parmi les initiatives, nous retrouvons l'augmentation des financements DGA-RAPID à destination des PME (3 millions d'euros par an), la demande de participation coopérative PME-Grands groupes dans les appels d'offres et le lancement du Pacte Défense PME en novembre 2012.

d'Israël. Malgré leur 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 soit rachetées trop tôt par de grands groupes, parfois étrangers, soit elles arrêtent d'investir. Dans tous les cas, elles cessent d'être innovantes au détriment d'un écosystème compétitif.

Une mauvaise lisibilité des différents programmes de financement 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. Sur ce point en particulier, État et industrie partagent le même diagnostic quant à la difficulté des grands groupes industriels, issus de la défense, à gérer les relations de coopération avec les PME. Tout d'abord, le manque d'une culture adaptée au nouveau marché est au cœur des difficultés de coordination pour répondre aux appels d'offres d'une façon conjointe : les temps et les méthodes de développement, les canaux de vente et la culture du management ne sont plus les mêmes pour le marché de la cybersécurité. En outre, des complexités s'ajoutent en cas d'acquisition ou de fusion d'une PME : les grands industriels ayant des difficultés à gérer l'intégration des effectifs et à maintenir les technologies innovantes des PME.

Dans le but de favoriser l'émergence de PME performantes, le Plan Cyber a proposé la création de fonds d'investissement spécialisés en matière de cybersécurité pour la fin 2014. Cependant, le montant des fonds correspondant à quelques millions d'euros, la limitation de celui-ci à des ressources semi-publiques et focalisées sur la nationalité des entreprises concernées ont suscité de vives critiques par de nombreuses sociétés du secteur[31]. Le *leitmotiv* est toujours le même : afin de disposer des fonds susceptibles d'investir de manière durable dans les PME, le secteur privé doit s'émanciper d'une politique jusqu'ici trop centrée sur la dimension nationale.

Finalement, l'opacité de la définition de l'offre souveraine et l'absence d'un tissu de PME performant déclenchent de plus en plus de critiques du secteur privé sur les initiatives lancées. Bien que ces positions soient récentes, elles ont l'avantage d'ouvrir le débat sur le rôle de l'État qui, encore prisonnier de l'héritage du « Colbertisme *High-Tech* », est toujours à la recherche de son rôle définitif vis-à-vis du secteur privé.

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

L'analyse de la politique industrielle française en matière de cybersécurité a montré deux tendances. Tout d'abord, la volonté des États de réaffirmer leur souveraineté sur les questions de cybersécurité se traduit par la nécessité de disposer d'une offre nationale : c'est-à-dire une offre développée sur le territoire national et contrôlée par les autorités étatiques compétentes.

[31] Nous faisons notamment référence au Livre blanc rédigé par l'Association française des éditeurs de logiciels et solutions internet, composée de 350 membres de grands groupes internationaux, PME et *Start up*. *Cyber-sécurité : Hisser les acteurs français au niveau de la compétition mondiale*, juin 2014.

Malgré les déclarations politiques au sujet d'une plus forte coopération internationale, la protection des SI stratégiques reste un domaine sensible. Ainsi, les initiatives en matière de politique industrielle ne font que confirmer la tendance à la fragmentation des politiques de cybersécurité qui se traduit par la définition d'une zone de confiance limitée à un périmètre national.

Le deuxième aspect à retenir porte sur les relations État-Industrie. De nombreuses initiatives pour améliorer le dialogue Public-Privé ont été lancées dans le but de structurer l'offre et la demande, toutefois cette coopération s'articule sur des rapports de force qui profitent actuellement aux pouvoirs publics.

Alors que l'État régulateur espère doper la demande nationale, le marché de la cybersécurité ne semble pas encore être l'*Eldorado* tant attendu en France. Les règles adoptées avec la LPM 2014-2019, issues de deux années de tractations, sont certes contraignantes pour les OIV, mais ne garantissent pas pour autant leur pleine applicabilité[32]. De plus, cette règlementation établissant un niveau de sécurité *à minima* est souvent déjà dépassée en raison de l'évolution toujours plus rapide de la menace. De ce fait, la règlementation exigerait un renouvellement régulier et rapide.

La structuration de l'offre paraît, quant à elle, encore dépendante de l'action de l'État investisseur, tuteur et exportateur. Des investissements publics insuffisants par rapport aux objectifs fixés, le retour décevant sur l'appel d'offres Programme Investissements d'Avenir 2013[33], l'absence d'investissements dans les PME, montrent que l'État ne peut pas accompagner seul l'industrie pour lui permettre d'atteindre une taille critique. Au moment où la concurrence internationale capte les marchés émergents au moyen d'acquisitions milliardaires, organiser un écosystème à la hauteur demanderait trop de ressources. De ce point de vue, les initiatives lancées, malgré tout décisives, ne nous semblent pas complètement adaptées à l'objectif d'un écosystème compétitif.

Face à cette situation insatisfaisante, nous pouvons ouvrir quelques pistes de réflexion pour une situation gagnant-gagnant pour tous. À cet égard, la présence sur le territoire européen, de grandes industries françaises tant dans les OIV que parmi les fournisseurs, semble être un atout insuffisamment exploité. Ces firmes, par leur configuration internationale, partagent les mêmes risques, mais également les mêmes intérêts économiques : être globalement protégées à moindre coût et vendre au plus large nombre de clients.

Imaginons donc un scénario qui prenne en considération et mette en valeur cette dimension européenne des OIV et des fournisseurs de sécurité. Afin de développer des solutions pour des clients multidomestiques, les fournisseurs sont incités à payer leur R&D et de ce fait à étendre leurs relations avec les PME les plus innovantes sur le territoire européen.

---

[32] Le récent cas de l'usage de smartphones commerciaux par les ministres malgré une directive qui en proscrit l'utilisation illustre la difficulté de donner du bâton. Gilbert Kallenborn, « Les Ministres peinent à respecter les règles élémentaires de sécurité informatique », 11 septembre 2013, disponible sur : http://www.01net.com/editorial/602914/les-ministres-peinent-a-respecter-les-regles-elementaires-de-securite-informatique/, dernière consultation 15 avril 2014.

[33] A l'occasion de la présentation du Plan Cyber en mai 2014, l'ANSSI lamente que dans le cadre du PIA 2013 aucun projet n'ait été soumis concernant la mobilité sécurisée tandis qu'au moins huit le furent sur la sécurité des infrastructures et dispositifs voix/visiophonie sur IP. Toujours selon l'ANSSI, en mai 2014, l'offre en matière de SIEM (*Security information and event management*) n'était pas assez mature pour rivaliser avec le marché et celle en matière de sécurité industrielle est complètement absente. Notre source est le débat qui s'est tenu à l'occasion du petit-déjeuner organisé par le Cyber Cercle mercredi 7 mai 2014 à Paris.

D'une part, les grands groupes seront ainsi affranchis des spécifications nationales, mais pourront toutefois exporter ces solutions, vers l'Europe d'abord, puis conquérir des marchés internationaux. D'autre part, les PME auront accès à un marché élargi ce qui leur permettra d'attirer plus d'investissements.

Les OIV pourront ainsi disposer d'une gamme de produits de confiance déployable à l'ensemble de leurs sites. En revanche, l'État se limitera à financer la R&D pour les solutions les plus sensibles à ses réseaux, à fixer aux OIV un cadre de règles minimales, et à soutenir les PME sans imposer de spécifications supplémentaires pour l'offre commerciale. Parallèlement, les OIV et les fournisseurs européens devraient organiser leur lobbying afin d'établir une préférence européenne, ce qui aurait pour double effet de favoriser la structuration du marché et d'assurer la résilience des OIV en Europe.

Le scénario ci-dessus, initié par les grandes firmes, pourrait constituer un élément de structuration de marché, alimentant la boucle d'amélioration continue entre pouvoirs publics et secteur privé.

Au secteur privé de se détacher des jupons de Colbert !

Références

CLEMENTE Dave, *Cyber Security and Global Interdependence: What Is Critical?,* Chatham House, février 2013.

COHEN Élie, *Le colbertisme high-tech. Économie du grand projet*, Paris, Hachette Pluriel, 1992.

D'ELIA Danilo, « La Guerre économique à l'ère du cyberspace », *Hérodote*, n° 152-153, 2014, p. 240-260.

DOUZET Frédérick, « La Géopolitique pour comprendre le cyberspace », *Hérodote*, n° 152-153, 2014, p. 3-21.

DUNN Myriam et MAUER Victor, *Towards a Global Culture of Cybersecurity*, International CIIP Handbook, 2006, p. 196-206.

MEYNET Stéphane et FEUILLET Mathieu, "SCADA/ICS Security ANSSI Working Group", présentation faite à l'occasion du Computer & Electronics Security Applications Rendez-vous 2013, 20 novembre 2013.

MOORE Tyler et ANDERSON Ross, "Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research, 2011 Internet Security", *In*: PEITZ Martin, WALDFOGEL Joel (eds.), *The Oxford Handbook of the Digital Economy*, Oxford, Oxford University Press, 2011.

DE LA DEFENSE A LA SECURITE : LA DIVERSIFICATION DES FIRMES D'ARMEMENT EUROPEENNES DANS LE DOMAINE DE LA SECURITE

Vincent BOULANIN
Chercheur au SIPRI

Introduction

La diversification est une thématique qui a été largement traitée en économie de défense notamment au début des années 1990 en raison des attentes portées par la chute de l'Empire soviétique en matière de désarmement. L'essentiel des travaux s'est intéressé à la conversion et la diversification des firmes de défense dans le secteur commercial civil[1]. Le sujet est progressivement tombé en désuétude à la fin des années 1990 à la fois du fait du bilan mitigé des tentatives de conversion et de diversification des firmes dans le civil et surtout du fait de la reprise de la conjoncture américaine et mondiale sur le marché de l'armement[2]. Il n'en reste pas moins une actualité saillante, surtout en Europe. La diversification des firmes dans le domaine de la sécurité est un phénomène qui n'a d'ailleurs pas reçu l'attention qu'il mérite dans le champ de la production d'armement.

Depuis maintenant plus d'une décennie, « la sécurité » est régulièrement présentée dans la presse spécialisée comme un relais de croissance potentiellement important pour les firmes de défense européennes dans un contexte marqué par une atonie de la demande sur le marché de l'armement[3]. Cette remarque fait écho aux attentats terroristes du 11 septembre 2001 ainsi qu'à ceux de Madrid en 2004 et de Londres en 2005, qui ont amené les États européens à délaisser (partiellement) la grande stratégie et les questions de défense au profit de problématiques de « sécurité » qui ne relèvent plus seulement du domaine militaire comme en témoignent par exemple les Livres blancs britanniques et français publiés au cours des années 2000[4].

---

[1] Roland de Penanros (dir.), *Reconversion des industries d'armement*, Paris, La documentation française, 1995 ; Steven Schofield, "Defence Technology, Industrial Structure and Arms Conversion", *In* : Richard Coopey, Matthew Uttley et Graham Spinardi, *Defense Science and Technology : Adjusting to Change*, Hardwood, Hardwood Reading, 1993 ; Jurgen Brauer et John Tepper Marlin (dir.), "Converting Resources from Military to Non-Military Use", *Journal Of Economic Perspectives*, vol. 6, n° 4, Automne 1992 ; Jacques Fontanel, *La conversation économique du secteur militaire*, Paris, Economica, 1994.

[2] Michael Brzoska, "Success and failure in defence conversion in the long decade of disarmament", *In*: Keith Hartley et Todd Sandler (dir.), *Handbook of Defense Economics, Defense in a Globalized World*, Amsterdam, Elsevier B.V., 2007 ; Michael Brzoska, "Military Conversion: The Balance Sheet", *Journal of Peace Research*, vol. 36, n° 2, Londres, Sage Publications, mars 1999 ; Paul J. Dunne et Eamon Surry , "Arms Production", *SIPRI Yearbook 2006,* Oxford, Oxford University Press, 2006, p. 408.

[3] Michael Oborne (dir.), *The Security Economy*, Paris, OCDE, 2004 ; David Mulholland, "US Homeland Security Unlikely to Provide Industry Bonanza", *Jane's defence Weekly*, p. 18 ; James Murphy, "Diversification, a Key as Defense Contractors Seek New Markets », *Jane's defence Industry*, 1er septembre 2006 ; « Marché de la sécurité en France : Un dynamisme réel, tous secteurs confondus », *L'info expoprotection*, 13 novembre 2009.

[4] Le recours à la notion de sécurité s'expliquerait selon ces Livres blancs par le besoin d'une approche globale, les menaces qui pèseraient aujourd'hui sur la sécurité des États appelleraient à une réponse qui transcenderait les champs de la défense et de la sécurité intérieure. La sécurité est un concept intemporel autour duquel

Le phénomène terroriste tout particulièrement a été élevé au rang de menace stratégique ultime pour la paix et la sécurité collective. Comme l'explique Colombe Camus, ces attentats « auraient ainsi entériné un retournement dans l'univers des évidences occidentales post-1990 et seraient venus consacrer un nouveau paradigme de la violence suscitant l'idée d'un nécessaire renouvellement des pratiques et des dispositifs de sécurité »[5]. Les menaces contemporaines seraient ainsi « multiples et diffuses », le monde serait exposé à des « vulnérabilités nouvelles » (terrorisme, mais aussi prolifération nucléaire, contamination chimique ou biologique, cybercriminalité, catastrophes naturelles) qui transcenderaient les frontières traditionnelles entre les mondes de la sécurité intérieure et de la sécurité extérieure. Ces nouveaux enjeux sécuritaires conduiraient les forces armées et forces de police à collaborer davantage et à confondre leurs pratiques. Didier Bigo parle à ce titre de « dé-différentiation » entre les métiers militaires et les métiers de la sécurité civile et intérieure[6]. On observerait une « policiarisation » des affaires militaires d'un côté et une militarisation de la police de l'autre.

Rares sont les travaux universitaires qui ont cherché à saisir les implications économiques et industrielles du « *continuum* » qui semble ainsi s'établir entre la défense et la sécurité dans les affaires stratégiques. C'est ce que propose de faire ce chapitre. Il présente une étude de cas portant sur plusieurs grandes firmes d'armement européennes qui se sont diversifiées dans le domaine dit de la « sécurité » : BAE Systems (Royaume-Uni), Cobham (Royaume-Uni), Ultra Electronics (Royaume-Uni), Thales (France), Safran (France), Diehl (Allemagne), SAAB (Suède) et Airbus group (Europe). À partir des rapports annuels, brochures et sites internet de ces firmes, cette contribution propose d'explorer les questions suivantes : 1) en quoi consiste l'offre de sécurité des firmes sur un plan technologique ; 2) quand et comment les firmes se sont-elles diversifiées ; 3) que représente économiquement l'activité « sécurité » dans le chiffre d'affaires des firmes ; 4) qui sont les principaux clients visés par l'offre ; 5) à quels usages sont destinées les solutions de sécurité.

L'enjeu de ce questionnement sera de mieux comprendre dans quelle mesure, en se diversifiant dans le domaine de la sécurité, les firmes d'armement se sont éloignées ou non de leur cœur d'activité. Il s'agira aussi de montrer qu'il est réducteur de lire la diversification des entreprises d'armement dans le domaine de la sécurité uniquement sous l'angle de l'expansion de leur activité sur le marché de la sécurité civile[7].

---

s'agrège un ensemble de politiques, de moyens et d'acteurs (voir le débat sur l'élargissement du concept de sécurité dans les années 1980-1990 dans le champs des études stratégiques) tandis que le concept de défense renvoie à un champ d'action politique spécifique bien délimité et clairement identifiable en matière de missions, moyens et acteurs : aux activités militaires de l'État visant à protéger le territoire national contre une agression extérieure. Voir *Livre blanc sur la défense et la sécurité nationale*, Préface de Nicolas Sarkozy, Paris, Odile Jacob / La documentation française, 2008; *Livre blanc sur la défense et la sécurité nationale*, Préface de François Hollande, Paris, Ministère de la défense, 2013 ; Ministry Of Defence, *Delivering Security in a Changing World, Defence White Paper*, Cm 60- 41.I, Norwich, The Stationary Office Limited, 2003 ; Hm Office, *Securing Britain in an Age of Uncertainty, The Strategic Defence and Security Review*, Cm 7948, Norwich, The Stationary Office Limited, 2010.

[5] Colombe Camus, *La Lutte contre le terrorisme dans les démocraties occidentales: État de droit et exceptionnalisme*, Paris, Dalloz/IRIS, 2007, p. 9.

[6] Didier Bigo, "When Two Become One: Internal and External Securitisations in Europe", *In:* Morten Kelstrup, et Michael Charles Williams, *International Relations Theory and the Politics of European Integration, Power, Security and Community*, Londres, Routledge, 2000, p. 171-204.

[7] Sur le rapport entre industrie de la défense et industrie de la sécurité voir aussi : Vincent Boulanin, *Defense and Security Industry : Which Industry are you Talking About ?,* Paris Paper, n° 6, IRSEM, 2012.

L'offre de sécurité : entre exploitation de synergies industrielles et acquisitions de nouvelles compétences

Les biens et services de sécurité des firmes d'armement étudiées peuvent être répartis en neuf catégories différentes (tableau 1) : 1) solutions de surveillance géospatiale ; 2) solutions de surveillance statique ; 3) solutions de communication et de commandement ; 4) solutions de déminage et de détection d'explosifs ; 5) solutions biométriques ; 6) solutions de paiement sécurisé ; 7) solutions pour la sécurité du trafic aérien ; 8) solutions pour la sécurité routière. Comme l'indique le tableau 1, les firmes étudiées sont pour la plupart présentes sur quatre créneaux : la surveillance du périmètre (géospatiale et statique), la communication et le commandement, la cybersécurité et la biométrie.

Tableau 1. Typologie de l'offre de sécurité sur un plan technologique

CATÉGORIE	FIRMES
Solutions de surveillance géospatiale (drones, systèmes de géolocalisation)	BAE Systems ; Cobham ; SAFRAN ; Airbus Group ; Diehl ; SAAB
Solutions de surveillance statique (caméras, radar)	BAE Systems ; Cobham ; Ultra Electronics ; SAFRAN ; Airbus group ; Diehl ; SAAB
Solutions de communications et commandement	BAE Systems ; Cobham ; Ultra Electronics ; Thales; AIRBUS GROUP ; SAAB
Solutions de déminage et détection d'explosifs	Cobham ; SAFRAN ; Airbus group
Solutions biométriques	BAE Systems ; Thales ; SAFRAN ; Airbus group
Solutions de cybersécurité et cyberrenseignement	BAE Systems ; Cobham ; Ultra Electronics ; Thales ; Airbus group ; Diehl
Solutions de paiement sécurisé	Thales ; SAFRAN
Solutions pour la sécurité du trafic aérien	Thales ; SAFRAN ; SAAB
Solutions pour la sécurité routière	SAFRAN

Source : Rapports annuels

Pour reprendre des termes d'économie industrielle, la diversification de l'offre des entreprises dans le domaine sécurité semble avoir suivi à la fois une trajectoire concentrique et une trajectoire conglomérale[8]. La diversification concentrique consiste pour une firme à diversifier son offre tout en gardant des liens étroits avec son périmètre d'activité d'un point de vue productif.

[8] Yves Morvan, *Fondement d'économie industrielle*, Paris, Economica, 1991, p. 210.

Dans notre cas, cela veut dire que les firmes se sont appuyées sur leurs compétences techniques dans le domaine de la défense, pour proposer une offre de sécurité. Ce fut clairement le cas pour l'offre de solutions de surveillance du périmètre et de communication et de commandement. L'essentiel de ces produits et ces services a été développé pour une utilisation militaire. Les firmes cherchent désormais à justifier leur utilité pour la sécurité des frontières, la sécurité maritime ou la sécurité des infrastructures critiques. Ces domaines ont l'avantage de constituer des marchés qui partagent un certain nombre de caractéristiques avec le marché de la défense (taille des contrats et procédure contractuelle) qui permettent aux firmes de se positionner facilement. Les firmes parlent elles-mêmes de « marchés parallèles ».

La biométrie et la cybersécurité sont en revanche des domaines émergents et représentent à ce titre de parfaits exemples de diversification conglomérale. Celle-ci consiste pour une firme à diversifier son offre dans un domaine sans aucun lien avec la base initiale d'activité. La plupart des firmes n'avaient aucune compétence dans ces deux domaines. Comme nous allons le voir dans la section suivante, elles ont dû avoir recours à des partenariats stratégiques ou à des acquisitions.

Genèse de l'activité de sécurité

La consultation des rapports annuels sur les 15 dernières années indique que l'intérêt affiché des entreprises pour la sécurité est globalement récent et a été progressif, à l'exception de quelques sociétés qui historiquement ont toujours été engagées dans l'offre de solutions de sécurité à destination du monde civil (tableau 2).

SAAB a fait de la diversification dans le domaine de la sécurité civile une priorité stratégique en 2005. Pour BAE System, la diversification dans le domaine sécurité n'est devenue une stratégie vraiment visible qu'en 2007-2008. Cela coïncide avec une période durant laquelle le gouvernement britannique s'est officiellement engagé à accroître ses dépenses dans les domaines du renseignement et de la sécurité publique. Cobham a exprimé sa volonté de développer son offre de sécurité encore plus récemment avec l'acquisition en 2010 et 2011 de trois firmes engagées spécifiquement dans le secteur de la sécurité intérieure. La firme délivrait cependant depuis longtemps des solutions de surveillance et de communication aux forces de sécurité civile. Ultra Electronics avait quant à elle identifié la sécurité comme secteur d'activité crucial dès 2003, mais il aura fallu attendre 2011 pour que cette résolution s'exprime sous forme de stratégie assumée dans les rapports annuels. Thales Airbus group, et SAFRAN sont tous les trois des acteurs historiques dans le domaine de la sécurité. Thales dispose depuis plusieurs décennies d'une activité de sécurité. SAFRAN a hérité des activités du groupe Sagem qui s'était lancé dans le business de l'identification biométrique dès 1993 avec l'acquisition de Morpho. Airbus group était présent sur le marché de la sécurité civile depuis sa création via son activité de radio mobile professionnelle (héritée du groupe MATRA) et via son offre d'hélicoptères. Ces trois firmes ont cependant toutes affiché une volonté croissante de renforcer leur activité sécurité sur la dernière décennie.

Tableau 2. Date du tournant « sécurité » dans les rapports annuels des firmes

FIRMES	TOURNANT SÉCURITÉ
BAE Systems	2008
Cobham	2011
Ultra Electronics	2003 /2011
Thales	Acteur historique
SAFRAN	Acteur historique
Airbus group	Acteur historique
Diehl	NC
SAAB	2005

Source : Rapports annuels

Pour diversifier leur offre, les firmes ont pu choisir entre trois options. S'appuyer sur des compétences internes, recourir à des acquisitions ou signer des partenariats. Lorsqu'il s'est s'agit de développer des compétences nouvelles notamment en matière cyber, les firmes ont privilégié le recours aux acquisitions et aux partenariats.

BAE Systems a par exemple multiplié les acquisitions d'entreprises travaillant dans la cybersécurité et le renseignement : Detica en 2008, Stratsec et L1 Identity Solutions Inc.'s Intelligence Services Group en 2010, ainsi que ETI et Norkom en 2011 (tableau 3). Le groupe SAFRAN via sa filiale SAGEM a développé ses activités pour la sécurité routière en signant un partenariat avec Selex Elsag une filiale du groupe Finmeccanicca et ses activités de paiement électronique sécurisé en signant un partenariat avec Ingenico. Thales en revanche s'est largement reposé sur ses compétences internes. Il n'a eu recours qu'à un nombre très limité d'acquisitions ces dernières années.

Dans la plupart des cas, la diversification dans le domaine de la sécurité s'est traduite sur un plan institutionnel par la création d'une nouvelle division, une filiale ou une marque dédiée. Airbus group avait par exemple créé une filiale dédiée à la cybersécurité, Cassidian Cybersécurité en 2012 (depuis fondue dans la filiale Airbus Defence and Space).

Tableau 3. Principales acquisitions liées à la sécurité depuis 2000

FIRMES	ACQUISITION	SPÉCIALITÉ	ANNÉE
BAE Systems	Detica (UK)	Cybersécurité	2008
	Stratsec (AUS)	Cybersécurité	2010
	ETI (DK)	Cybersécurité	2011
	L-1 Identity Solutions Intelligence Service Group (USA)	Renseignement	2010
	Norkom (UK)	Renseignement, criminalité financière	2011
Cobham	RVision (UK)	Surveillance vidéo	2010
	Corp Ten Inc (US)	Surveillance et géolocalisation	2011
	Telerob (ALL)	Robot terrestre télécommandé	2011
Ultra Electronics	SML Technologies (UK)	Surveillance et commandement	2003
	Audiopack Inc (US)	Système de communication et solution respiratoire	2005
	Atkins et Partners (US)	Gestion de crise	2007
	Telemus Inc (CA)	Guerre électronique et cybersurveillance	2007
	Audiosoft (UK)	Gestion de l'information	2008
	Dascam (EAU)	Services de formation et conseil	2008
	ProLogic (US)	Renseignement	2008
	Radmon (UK)	Détection de radioactivité	2008
	Scytale (US)	Cybersécurité	2009

	3eTI (US)	Cybersécurité	2011
	AEP Networks (UK)	Communications sécurisées	2011
	Zu (US)	Cybersécurité	2011
	Sotech (US)	Cybersécurité Cybersurveillance	2011
Thales	SVS (FR)	Surveillance video	2006
	Activités Sécurité et transport d'Alcatel (FR)		
	Alcatel Cybersecurity business (FR)	Cybersécurité	2014
	N –Cipher	Cybersécurité	2008
SAFRAN	Orga Karten /(FIN)	Cartes à puce	2005
	SDU Identification (NL)	Documents d'identité sécurisés	2008
	Printrak (US)	Biométrie	2009
	GE Homeland Protection (US)	Détection d'explosifs	2010
	L-1 Identity solutions	Documents d'identité sécurisés ; Biométrie	2011
Airbus group	Cogent (UK)	Cybersécurité	2003
	Activité PMR de Nokia (FIN)	Communication	2005
	Altas Elektronik (ALL)	Electronique navale	2005
	Regency IT (UK)	Cybersécurité	2010
SAAB	Cold Cut System (UK)	Systèmes anti-incendies et solutions de secours	2005
	Sensis International US	Trafic aérien	2011

Sources : Rapports annuels

Une importance économique encore relative

À la question de savoir si le secteur de la sécurité civile offre des opportunités commerciales suffisantes pour amortir, voire supplanter les revenus dégagés sur le marché de l'armement, les chiffres disponibles invitent à répondre par la négative.

Les firmes n'indiquent pas toujours leur chiffre d'affaires de sécurité dans leurs rapports annuels. Sur la liste des cas étudiés, seuls BAE Systems, Ultra Electronics, Thales et SAAB ont détaillé les revenus tirés de la vente de biens et de services de sécurité civile. Ces chiffres indiquent que les montants générés restent relativement mineurs à l'échelle du chiffre d'affaires total de ces entreprises (tableau 4).

Tableau 4. Chiffre d'affaires de sécurité en pourcentage du chiffre d'affaires total des firmes en 2011

	% du CA total en 2011
BAE Systems	7 %[9]
Cobham	NC
Ultra Electronics	17 %
Thales	23 %[10]
SAFRAN	11 %
Airbus group	NC
Diehl	NC
SAAB	6 %

Source : Rapports annuels

Lorsqu'il été possible de comparer les chiffres sur plusieurs années, comme dans le cas de Thales (jusqu'en 2009) et de Saab, ces derniers indiquaient une croissance rapide des revenus issus de la vente de solutions de sécurité. SAAB a doublé ses revenus de sécurité civile en part du chiffre d'affaires total entre 2006 et 2011.

Le marché de la sécurité civil n'est ainsi pas près d'offrir une alternative significative au marché de la défense pour les firmes d'armement. Il n'en reste pas moins un relais de croissance qui permet de compenser partiellement l'atonie des ventes sur le marché de l'armement en Europe.

[9] Civil et militaire.

[10] Chiffre pour 2009. Thales a cessé de publier son chiffre d'affaire de sécurité en 2009.

Une clientèle mixte, mais haut de gamme

Avec leur offre de sécurité, les firmes visent une clientèle mixte d'acteurs militaires et civils, privés et publics. Côté clientèle publique, lorsqu'il s'agit de promouvoir des solutions pour la surveillance du périmètre et la communication, les firmes s'adressent en priorité aux « forces en bleu » (police, douanes, garde-côtes) et « forces en rouge » (premiers secours : pompiers, ambulanciers). Leur offre de sécurité virtuelle (cyber et biométrie) est quant à elle plus transversale : elle s'adresse tout autant aux militaires (responsable de la cyberdéfense) qu'aux forces de sécurité publique. Elle s'adresse également aux agences étatiques soucieuses de protéger leurs infrastructures contre les cyberattaques.

Côté clientèle privée, les entreprises ciblent essentiellement les clients à fort potentiel commercial : les opérateurs d'infrastructures critiques ou les grandes entreprises que ce soit pour fournir des solutions de sécurité physique, de biométrie ou de cybersécurité. L'offre des entreprises ne s'adresse pas à des clients individuels. Les sociétés restent sur le créneau de la haute sécurité, c'est-à-dire l'apport de sécurité à des fins publiques. Même quand elle s'adresse à des clients privés, l'offre de sécurité se consomme comme un bien public[11]. L'exemple type est la sécurité des infrastructures aéroportuaires. Si l'enjeu premier est de sécuriser un espace restreint, la sécurité de cet espace est d'intérêt public.

Usage : de la défense à la sécurisation

Dans leur rapport annuel, des entreprises comme Airbus group ou SAAB reprennent largement l'idée selon laquelle les besoins des forces de la sécurité intérieure et de la sécurité extérieure seraient de plus en plus proches, que ce soit pour des missions de protection physique ou des missions virtuelles. Leur offre permettrait de répondre au *continuum* de risques et de menaces qui concerne la société dans son ensemble : le terrorisme, le crime organisé, les catastrophes naturelles, la cybercriminalité et les cybersabotage, ou encore l'immigration illégale.

Pour faire face à ces menaces et risques, les sociétés proposent d'adopter des capacités intégrées de sécurisation proactive : surveillance, détection, communication, commandement ou protection. Ces solutions apporteraient aux professionnels de la sécurité les moyens de se prémunir contre l'incertitude stratégique.

En ce sens, la diversification des entreprises en matière de sécurité ne peut se résumer au simple développement d'une offre en direction des acteurs de la sécurité civile. Certaines d'entre elles, comme BAE Systems, ne font d'ailleurs pas nécessairement la différence entre civil et militaire quand elles évoquent leur activité sécurité.

[11] Un bien public se distingue des biens privés par deux critères principaux : la non-rivalité et la non-exclusion. Un bien est dit « rival » quand son achat ou son utilisation par une personne exclut définitivement toute consommation par une autre personne. Un bien public comme la sécurité extérieure peut, au contraire, être consommé par autant de personnes qu'il y a d'utilisateurs potentiels sans coût supplémentaire. Un bien est dit « non-exclusif » quand son détenteur n'est pas en mesure d'en empêcher l'accès à toute personne qui refuserait d'en payer le prix qu'il demande. Paul A. Samuelson, « The Pure Theory or Public Expenditures », *Review of Economics and Statistics,* vol. 36, n° 4, 1954, p. 387-89.

Si certaines sociétés d'armement se présentent en fournisseurs de solutions de sécurité, cela reflète le fait qu'elles ont intégré le basculement de rationalité qui s'est opéré dans les affaires stratégiques et qui ajoute à la logique défense une logique sécurisation proactive et gestion du risque. L'offre n'est plus seulement destinée à la « défense » face à des menaces, mais aussi à la gestion des menaces de manière prédictive et proactive.

Conclusion

Ce chapitre a exploré la diversification des firmes d'armement dans le domaine de la sécurité au travers d'une étude de cas portant sur BAE Systems, Cobham, Ultra Electronics, SAAB, Diehl, SAFRAN, Thales et Airbus Group. Celle-ci nous a révélé que la diversification dans le domaine de la sécurité était tout d'abord un phénomène récent dont les modalités sur un plan industriel ont également été variables en fonction des domaines de sécurité visés par les firmes. Dans la plupart des cas, la diversification a été « concentrique ». Elle a consisté pour les firmes à s'appuyer sur des compétences industrielles et technologiques existantes dans le domaine de la défense pour fournir des solutions sur des marchés de sécurité civils ou paramilitaires dont les caractéristiques étaient proches du marché militaire : sécurité des frontières, sécurité des espaces maritimes et portuaires, sécurité des infrastructures critiques. Les seuls domaines où les firmes ont dû acquérir ou développer des compétences nouvelles sont la biométrie et la cybersécurité. Dans ce cas, on a pu parler de diversification « conglomérale ». Les rares données disponibles semblent indiquer que l'importance des activités de sécurité reste faible au niveau du chiffre d'affaires des firmes, en particulier en comparaison avec les revenus générés par les grands systèmes intégrés de défense. On a ainsi pu mettre en évidence que les modalités économiques et industrielles de la diversification dans le domaine de la sécurité ne sont pas différentes de celles identifiées dans la littérature sur la vague de diversification dans le civil qui a eu lieu dans les années 1990. Elles ne s'éloignent pas fondamentalement de leur cœur d'activité.

Les firmes d'armement proposent par ailleurs une vision assez restreinte et homogène de ce que pourrait être selon elles l'industrie de la sécurité, vision qui rappelle fortement l'industrie de la défense. Les solutions proposées sont essentiellement destinées à des formes de sécurité « dures » et des usages de « haute » sécurité. Elles servent principalement à garantir la sécurité de l'État ou de la collectivité face à des risques du type terrorisme, immigration illégale ou criminalité organisée. Elles se caractérisent aussi par une technicité qui est typique du monde de l'armement et qui tend à répondre à chaque menace par une technologie adaptée. Elles sont destinées pour une large part aux professionnels de la sécurité, qu'ils soient publics ou privés, civils comme militaires. Au travers d'un discours à forte résonance capacitaire, les firmes insistent à ce titre largement sur le caractère à double usage de leurs solutions. L'offre de sécurité n'est ainsi pas nécessairement « civile ». Les biens et services sont souvent présentés comme des outils de gestion et de prévention des risques qui peuvent servir à des missions de sécurité civile, de sécurité intérieure tout autant qu'à des opérations militaires.

Notre principale contribution par rapport aux travaux existants aura ainsi été de montrer qu'il est réducteur de lire la diversification des entreprises d'armement dans le domaine de la sécurité uniquement sous l'angle de l'expansion de leur activité sur le marché de la sécurité civile.

Ce phénomène repose aussi sur une évolution dans le discours sur l'utilité et la rationalité des biens et services proposés. Lorsque les entreprises présentent leur offre de sécurité, elles présentent une offre destinée à gérer une multitude de risques et de menaces par le recours à des moyens de sécurisation prédictifs et proactifs.

L'INTERNATIONALISATION DES CHAINES DE VALEUR DANS L'INDUSTRIE DE DEFENSE : « LA BANALISATION » D'UN SECTEUR STRATEGIQUE ?

Paul HERAULT[12]
Doctorant en Sciences économiques à l'université Paris-Dauphine

Une évolution profonde des processus productifs…

Depuis plusieurs années, l'internationalisation des chaînes de valeur fait l'objet de nombreux travaux de recherche afin de mieux décrire et quantifier ce processus[13]. Un des enjeux majeurs consiste à améliorer la mesure du commerce international en fonction de la valeur ajoutée créée dans chaque pays, et non en fonction de la valeur brute de ses échanges puisqu'ils incorporent des intrants étrangers. La part importante des consommations intermédiaires tend en effet à surestimer le volume des exportations des pays en fin de chaîne, notamment les pays où sont réalisées des tâches d'assemblage final, comme la Chine[14].

Ces recherches ont révélé une importante évolution des processus productifs, caractérisée par une désintégration verticale, une spécialisation des territoires, une augmentation du commerce international de biens (et services) intermédiaires ainsi qu'une part croissante des services incorporés dans la production de biens manufacturés[15]. Cette division internationale des processus productifs a été illustrée par plusieurs études de cas, notamment sur les produits de la firme Apple. Ainsi, de plus en plus de produits peuvent être qualifiés de " made in the world "[16].

… qui va à l'encontre des ambitions d'autonomie des BITD nationales.

Ces tendances semblent a priori très éloignées de l'industrie de défense dans la mesure où de nombreux États affichent leur ambition de maintenir ou acquérir une certaine autonomie d'approvisionnement à travers une base industrielle et technologique de défense (BITD)[17] nationale.

---

[12] Doctorant en Thèse CIFRE (Convention Industrielle de Formation par la Recherche) DCNS – Université Paris-Dauphine.

[13] Une chaîne de valeur peut-être définie comme un ensemble d'activités interdépendantes, créatrices de valeur ajoutée et qui aboutissent à la réalisation d'un produit ou service donné. L'internationalisation de cette chaîne implique que les différentes activités constitutives du processus de production soient localisées dans différents pays.

[14] Pour plus de précisions sur la notion de commerce en valeur ajoutée et pour accéder aux études et à la base de données de l'OCDE et de l'OMC : http://www.oecd.org/sti/ind/measuringtradeinvalue-addedanoecd-wtojointinitiative.htm, dernière consultation le 22 juillet 2014. Voir à cet égard notamment : http://www.oecd.org/fr/sti/ind/38558122.pdf.

[15] Cette tendance est qualifiée de « servicification » par plusieurs auteurs.

[16] Expression employée pour un programme de l'OMC traitant de l'internationalisation des chaînes de valeur.

[17] Cette notion de BITD reste relativement imprécise et son périmètre est difficile à délimiter. La notion de chaîne de valeur qui permet de reconstituer les filières permet d'intégrer l'ensemble des acteurs intervenant dans la conception, l'industrialisation, la fabrication, l'intégration et le maintien en condition opérationnelle des systèmes militaires et de leurs composants. Au-delà des principaux intégrateurs ou grands systémiers et équipementiers, cette approche favorise l'inclusion des ETI, PME ainsi que des prestataires de services (R&D,

Au vu de ces ambitions, l'internationalisation des chaînes de valeur devrait être moins importante dans le secteur de la défense où les clients finaux, les États, ne souhaitent pas dépendre de l'autorisation d'exportation d'un État tiers.
Pourtant, d'autres tendances structurantes favorisent l'internationalisation des chaînes de valeur de matériels de guerre. En premier lieu, la complexité et le niveau d'exigence technique des systèmes et équipements militaires rendent *a priori* particulièrement avantageuse une forte spécialisation des acteurs afin de bénéficier d'avantages comparatifs. Par conséquent, la complexification des matériels de guerre pourrait s'accompagner d'une fragmentation des chaînes de valeur et donc potentiellement, de leur internationalisation en fonction d'avantages comparatifs.

De plus, les contraintes budgétaires des États entraînent des pressions accrues sur les coûts de production des programmes d'armement et renforcent l'intérêt d'intégrer des équipements et composants civils achetés sur étagère (COTS, *commercial off-the-shelf*) dont les chaînes de valeurs sont elles-mêmes de plus en plus internationalisées. C'est particulièrement le cas de l'électronique et des nouvelles technologies de l'information et de la communication (NTIC) dont les innovations sont aujourd'hui davantage portées par les marchés civils que militaires. Or, l'intégration de plus en plus fréquente de ces technologies dans des systèmes militaires dits « réseaux-centrés » (*network-centric*) renforce la probabilité d'une internationalisation des approvisionnements[18].

Outre l'évolution des besoins des armées et les innovations technologiques apportées aux équipements militaires, de nombreux éléments concourent à cette internationalisation des approvisionnements. Les accords internationaux peuvent y contribuer en facilitant les échanges transnationaux : accords entre les États-Unis et le Royaume-Uni (traité de coopération sur les échanges de matériels de guerre), au sein de l'Union européenne (directives 2009/43/CE sur les transferts intracommunautaires et 2009/81/CE sur les marchés publics de défense et sécurité) ou entre l'UE et les États-Unis[19]. De plus, les processus de fusion-acquisition et les restructurations industrielles, qui ont été particulièrement importants aux États-Unis et en Europe, ont conduit à l'émergence de firmes multinationales dont les chaînes de valeur se déploient au-delà des frontières (BAE Systems, EADS, etc.)[20].

---

assurance, financement, …) dont l'activité ne relève pas toujours majoritairement du secteur défense mais n'en reste pas moins essentielle au bon déroulement des activités défense.

[18] Pour plus d'exemples sur l'internationalisation des approvisionnements d'équipements militaires américains :
http://americanmanufacturing.org/press-releases/report-says-us-military-dangerously-dependent-foreign-suppliers.

[19] C'est notamment le cas avec les accords ACSA (*Acquisition and Cross Servicing Agreement*) qui facilitent les échanges logistiques et les approvisionnements entre les États-Unis et leurs alliés soit sur la base d'accords avec des États soit avec des organisations comme l'OTAN, voire l'Union européenne :
http://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cooperation-common-security-and-defense-policy.

[20] On pourrait également s'interroger sur les conséquences industrielles des évolutions doctrinales intervenues post-2001 avec la mise en avant des concepts de sécurité et de sécurité nationale. La croissance du marché de la sécurité alors que les budgets défense étaient en contraction n'a-t-elle pas modifié l'offre et l'organisation des industries de défense, notamment via la dualité des technologies mobilisées et des processus de R&D ? Sur ce sujet, on pourra consulter la note de Daniel Fiott, "The Three Effects of Dual-Use: Firms, Capabilities, and Governance", *ISS Brief*, n° 21, 2014, disponible en ligne :
http://www.iss.europa.eu/fr/publications/detail-page/article/the-three-effects-of-dual-use-firms-capabilities-and-governance/.

Enfin, les stratégies d'indigénisation mises en œuvre par les États importateurs ont une influence majeure sur l'organisation industrielle des programmes « export ». Les compensations (*offsets*) exigées par ces clients accroissent la part de valeur ajoutée générée localement à travers les transferts de technologies, de savoir-faire, de production, et l'intégration de fournisseurs locaux dans la chaîne d'approvisionnement.

Entre ambitions d'autonomie des États et nouvelles dynamiques technologiques, industrielles et commerciales, la spécificité des industries de défense face à l'internationalisation des chaînes de valeur est-elle en régression ? Assiste-t-on à une forme de « banalisation » des industries de défense ?

Une réponse générale pour l'ensemble du secteur défense est difficile à apporter dans la mesure où ce secteur ne forme pas un agrégat statistique. Par conséquent, il est difficile d'appliquer à l'industrie de défense dans son ensemble des méthodes statistiques employées par les macro-économistes, notamment au travers des tableaux d'entrées-sorties.

Quant aux différents secteurs aéronautique, naval, terrestre ou électronique, ils ne permettent pas facilement de distinguer la part d'activité civile et militaire.

Malgré ces obstacles méthodologiques, des éléments de réponse peuvent être apportés sur la base d'études de cas. Ces données illustrent l'internationalisation des chaînes de valeur, dont deux tendances majeures citées ci-dessus seront approfondies : l'internationalisation des approvisionnements en composants électroniques, dans un premier temps, puis le rôle des politiques d'indigénisation. Ces éléments permettront de montrer que si une forme de banalisation de l'industrie de défense est bien à l'œuvre, elle se heurte à de fortes spécificités (cycles de vie, cadre réglementaire, sécurité d'approvisionnement notamment).

Une internationalisation des chaînes de valeur via les approvisionnements de composants électroniques

Les matériels de guerre intègrent de plus en plus d'équipements et de composants électroniques. Or, de nombreuses études montrent que les chaînes de valeur de produits informatiques et électroniques sont assez largement internationalisées[21]. Ainsi, les consommations intermédiaires en composants électroniques concourent à l'internationalisation des chaînes de valeur de matériels militaires. C'est ce dont témoignent plusieurs cas analysés en détail par le Sénat américain dans le cadre d'une enquête sur les origines de pièces suspectées de contrefaçon[22].

Si l'objectif ici n'est pas de traiter de la contrefaçon, le périmètre de l'enquête et les données publiées offrent des informations précieuses permettant à la fois d'illustrer l'ampleur du phénomène et de retracer des chaînes d'approvisionnement précises. Les 1 800 cas recensés en deux ans (2009 et 2010) représentent plus d'un million de pièces suspectes.

[21] Cf. notamment les intéressantes études de cas réalisées par le *Personal Computing Industry Center* : http://pcic.merage.uci.edu/papers.htm

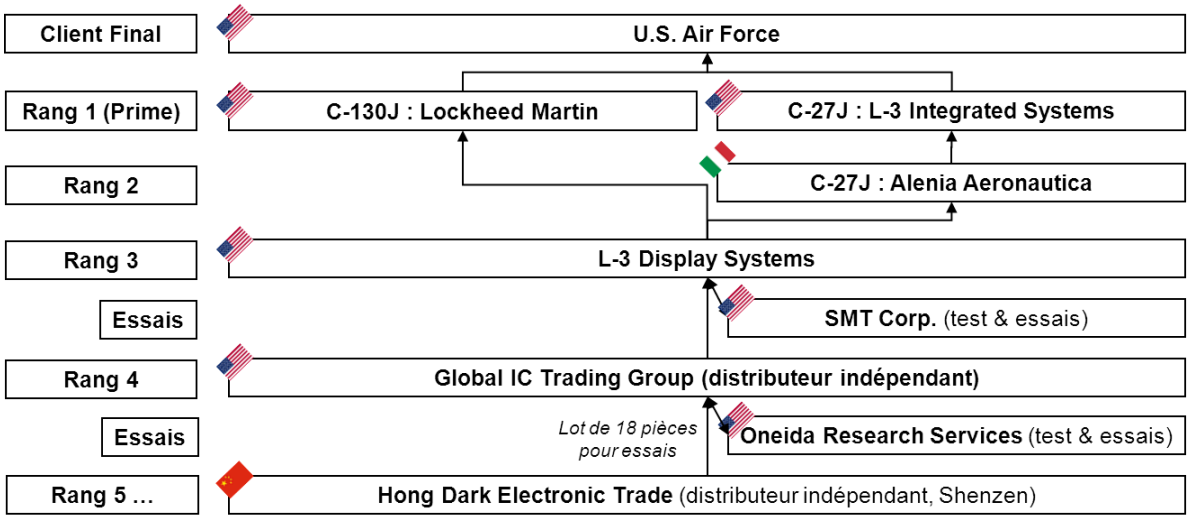
[22] United States Senate, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain", *Report of the Committee on Armed Services*, mai 2012.

Sur les 126 cas étudiés de manière plus approfondie, plus de 70 % des cas remontent à une source localisée en Chine avec parfois des intermédiaires au Canada et au Royaume-Uni.

L'exemple de cartes électroniques Samsung (cf. schéma ci-dessous) a permis de révéler l'existence de 28 000 composants achetés par L-3 à *Hong Dark Electronic Trade* en Chine (Shenzen) via un distributeur américain, *Global IC Trading Group*, en 2009 et 2010. Ces composants ont été intégrés à de nombreux systèmes différents : systèmes d'alerte anti-collision d'avions de l'*US Air Force*, systèmes de guerre électronique, hélicoptères des forces spéciales, système ISIS (*Integrated Submarine Imaging System*) destinés aux sous-marins nucléaires américains, etc. Au total, ce sont environ 84 000 pièces achetées à *Hong Dark Electronic Trade* via *Global IC Trading Group* qui auraient alimenté les chaînes d'approvisionnement du ministère de la défense américain.

Au vu de ces données et des quantités considérées, l'internationalisation des chaînes d'approvisionnement à l'œuvre dans l'électronique de défense ne se limite pas à quelques cas isolés. Elle concerne même des systèmes d'armes ou d'information sensibles, y compris au sein du plus important marché de défense, les États-Unis.

Figure 1. Chaîne d'approvisionnement de cartes Samsung contrefaites intégrées aux systèmes de visualisation d'avions C-130J et C-27J



Reconstitution d'après le rapport : United States Senate, Inquiry into counterfeit electronic parts in the Department of Defense Supply Chain, Report of the Committee on Armed Services, Mai 2012.

Des politiques d'acquisition qui conduisent à une internationalisation des chaînes de valeur

Une logique d'exportation remise en cause par l'« indigénisation » des programmes

Si à l'échelle mondiale, les budgets de défense ont eu tendance à stagner autour de 1 700 milliards de dollars (2011) sur la période 2010-2013[23], le volume des marchés ouverts à des offres internationales a crû de 38 %[24]. Cette évolution s'explique notamment par la part croissante des États émergents dont les bases industrielles et technologiques de défense ne sont pas encore suffisamment autonomes pour pouvoir se passer de fournisseurs étrangers.
Cette croissance des marchés « export » n'est pas sans contrainte pour autant car leur accessibilité est de plus en plus encadrée par des stratégies d'indigénisation. Celles-ci se traduisent par des exigences de compensations (*offsets*) indirectes (hors programme militaire) et surtout directes, qui se concrétisent par une part de réalisation locale et/ou des transferts de technologie ou de savoir-faire.

Ainsi, d'après certaines estimations, le montant global de ces compensations s'élèverait à près de 100 milliards de dollars sur la période 2012-2022 pour 25 États, hors États-Unis et États membres de l'Union européenne[25]. Au total, environ 80 États imposent des formes de compensations à leurs fournisseurs étrangers de matériels militaires[26].

Par conséquent, si les opportunités de marchés restent importantes, elles se traduisent de moins en moins par l'exportation d'un produit fini conçu, développé, réalisé, intégré et testé dans un seul et même pays et s'accompagnent d'une internationalisation accrue de la chaîne de valeur, i.e. la localisation de certaines activités auprès du pays client. Le cas du programme australien de destroyers anti-aériens de la classe Hobart illustre cette tendance.

Exemple : le cas des destroyers anti-aériens australiens de la classe Hobart

Le Programme SEA 4000 vise à remplacer six frégates de la classe *Adélaïde* (dont deux ont déjà été retirées du service actif) par trois destroyers assemblés en Australie. Outre l'acquisition de ces navires et de leur système de soutien associé, l'objectif du programme est également de renforcer l'industrie navale australienne. Il s'agit de recréer des compétences à la fois en réalisation de navires et en conception, ne serait-ce que pour assurer l'entretien et les évolutions des navires tout au long de leur cycle de vie.

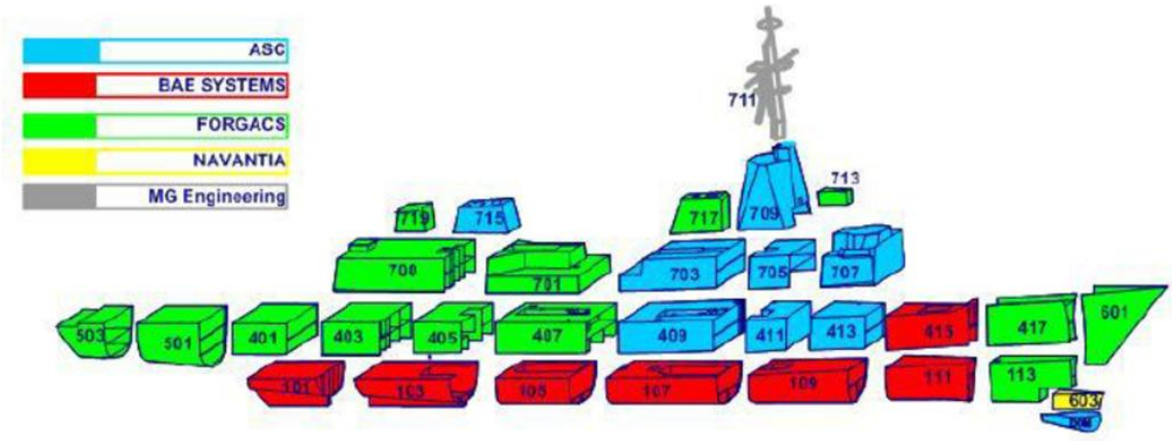
L'organisation contractuelle et industrielle fait intervenir plusieurs acteurs dont certains sont regroupés au sein d'une alliance, l'*Air Warfare Destroyer Alliance* (AWD Alliance). Celle-ci réunit la *Defence Materiel Organisation* (DMO), qui est l'agence d'acquisition du département de la Défense australien, ASC qui est le chantier naval d'assemblage, ainsi que Raytheon, l'intégrateur de systèmes. D'autres acteurs importants participent au programme sans pour autant faire partie de l'Alliance : Navantia, Forgacs, BAE Systems Australia (ex-Tenix), et Lockheed Martin.

[23] SIPRI, SIPRI Military Expenditure Database, 2013.
[24] Guy Anderson et Ben Moores, "The Growing Burden of Offsets", *Jane's Defence Weekly*, 25 octobre 2013.
[25] *Idem*.
[26] *Idem*.

L'industriel européen, Navantia fournit un concept sur la base de celui des frégates espagnoles F-104 et F-105 adapté aux normes et exigences australiennes ainsi qu'au système de combat dont la responsabilité incombe principalement à Raytheon. Si Navantia fournit le concept, la société n'est pas membre de l'Alliance AWD et agit en tant que sous-traitant pour un contrat de 300 millions de dollars australiens (2007) sur un programme global évalué à plus de 8 milliards[27]. En tant que concepteur de la plateforme, Navantia ne capte donc qu'une faible part de marché (inférieure à 5 %). L'industriel espagnol fournit également quelques blocs de la plateforme à ASC, le chantier d'intégration de la plateforme. Initialement très limité (cf. schéma ci-dessous), le nombre de blocs fournis par le chantier espagnol est actuellement d'une dizaine sur 93 (31 par destroyer), contre moins de 5 prévus en 2009.

L'Alliance AWD coordonne et capte l'essentiel du programme : sur les 4,7 milliards de dollars australiens attribués en 2007 au titre de la phase 3 du programme, l'Alliance AWD en a perçu 4,4 milliards, bien plus que le concepteur de la plateforme, Navantia (300 millions). Le chantier public ASC réalise de nombreux blocs qu'il assemble avec ceux sous-traités à Forgacs, Navantia et BAE. Raytheon joue le rôle de concepteur-intégrateur du système de combat, en dehors du système Aegis approvisionné par la DMO auprès de l'*US Navy* et Lockheed Martin dans le cadre de *Foreign Military Sales* (FMS).

Figure 2. Schéma d'allocation des blocs[28]



NB : le schéma d'allocation des blocs entre chantiers a été modifié à plusieurs reprises

La chaîne de valeur qui résulte de cette organisation contractuelle et industrielle est à la fois très fragmentée et très internationalisée.

[27] ANAO, Australian National Audit Office, "Air Warfare Destroyer Program", *Audit Report,* n° 22, 2013-14.
[28] Site de l'*Air Warfare Destroyer Alliance* : http://www.ausawd.com/library/How%20do%20you%20build%20an%20AWD_0.pdf, dernière consultation le 21 juillet 2014.

Elle est fragmentée car :

- le concepteur de la plateforme (Navantia) est différent de l'intégrateur de la plateforme (ASC) ;
- le concepteur de la plateforme (Navantia) est différent du concepteur-intégrateur du système de combat (Raytheon) ;
- il n'y a pas un, mais quatre chantiers navals (ASC, Forgacs, Navantia, BAE Australia) ;
- la conception et l'intégration du système de combat sont partagées par Raytheon sur le Système Aegis avec deux partenaires : Lockheed Martin et l'US Navy ; sans compter les nombreux fournisseurs d'équipements et sous-systèmes (sonars Ultra, torpilles légères Eurotorp).

Cette chaîne de valeur est internationalisée car une part importante de la valeur ajoutée est créée dans plusieurs États (au moins aux premiers rangs de la chaîne) :

- en Australie : réalisation de blocs, intégration physique du navire, gestion du programme ;
- aux États-Unis : système de combat Aegis, radar et autres équipements, assistance technique ;
- en Espagne : conception de la plateforme, réalisation de blocs.

En 2013, la cour des comptes australienne, l'ANAO (*Australian National Audit Office*), estimait que la part des dépenses allouées à des acteurs australiens dépassait l'objectif de 50 % du coût estimé pour l'ensemble des contrats passés à l'Alliance AWD[29]. Même si cette part importante n'est pas assimilable directement à de la valeur ajoutée locale, elle illustre clairement l'impact d'une politique d'acquisition sur l'internationalisation des chaînes de valeur, et sur la stratégie de déploiement des groupes puisqu'une part de l'activité locale est générée par des groupes étrangers : BAE Australia et Raytheon Australia, notamment[30].

Banalisation et spécificités des industries de défense

Une certaine forme de banalisation des industries de défense…

Les différents éléments évoqués tant sur les chaînes d'approvisionnement d'équipements et composants électroniques que sur la chaîne de valeur globale de grands programmes internationaux comme l'AWD australien témoignent d'une forme de banalisation des chaînes de valeur dans l'industrie de défense, dans la mesure où les caractéristiques observées au niveau macro-économique sont également visibles dans l'industrie de défense à travers :

- **une importante fragmentation des processus productifs** : cette fragmentation s'observe à travers les nombreux niveaux de sous-traitance (plusieurs intermédiaires et prestataires de services pour l'approvisionnement de composants) et l'importante segmentation des responsabilités tant entre les différentes phases du programme (concepteur, réalisateurs de blocs, intégrateurs des blocs, intégrateur des systèmes de plateforme) qu'entre les différents systèmes et sous-systèmes du navire (plateforme, système de combat, *combat management system*, équipements) ;

[29] Australian National Audit Office, "Air Warfare Destroyer Program", *Audit Report*, n° 22, 2013-14.

[30] À titre d'exemple, Raytheon Australia compte plus de 1 300 collaborateurs (source : Alliance AWD http://www.ausawd.com/).

- **une forte dispersion géographique** : certains composants traversent (au moins virtuellement[31]) plusieurs États entre leur réalisation en Asie, leur expédition par des distributeurs chinois et leur approvisionnement par plusieurs intermédiaires européens et américains. De même, le cas australien illustre la répartition des activités sur plusieurs États (Espagne, Australie, États-Unis) ;
- **une incorporation significative de services** : avec l'exemple des nombreux distributeurs, centrales d'achats, laboratoires de test qui participent aux chaînes d'approvisionnement de composants et équipements ;
- de nombreux **échanges de biens intermédiaires** (composants, équipements, blocs de plateformes) et du **commerce intra-firme** : avec l'exemple de L-3 pour l'avion C-27J sur lequel interviennent à la fois *L-3 Integrated systems* et *L-3 Display Systems*.

Ainsi, ces dynamiques couramment observées dans l'industrie civile tendent à s'appliquer de manière croissante aux programmes militaires (domestiques et internationaux).

… qui se heurte néanmoins à de réelles spécificités…

Cette tendance à la banalisation va néanmoins à l'encontre de caractéristiques structurantes de la plupart des programmes d'armement.
En premier lieu, la complexité technique des systèmes à concevoir et réaliser renforce l'intérêt d'une certaine proximité géographique entre acteurs pour gérer les risques aux interfaces entre systèmes et sous-systèmes et entre phases du programme, notamment lors de l'industrialisation. La communication d'informations implicites ou de savoir-faire difficilement codifiables, les échanges entre ingénierie de conception et chantier de réalisation sont fortement facilités par la proximité géographique, le recours à des processus communs, l'utilisation de systèmes d'information partagés. *A contrario*, la distribution des activités entre plusieurs acteurs industriels et entre plusieurs États renforce les risques au niveau des interfaces entre acteurs.

En outre, les matériels de guerre et les entreprises qui les conçoivent, les réalisent et les commercialisent sont soumis à des règlementations spécifiques (licences de production, autorisations d'exportation, protection de données classifiées).

Ces spécificités réglementaires accroissent les coûts de transaction liés aux échanges transfrontaliers par rapport aux échanges civils. Une chaîne de valeur plus fragmentée et plus internationalisée accroît ces coûts de transaction et peut nuire à la performance de l'organisation industrielle si ces coûts ne sont pas compensés par des gains de compétitivité sur les activités localisées à l'étranger.

Par ailleurs, les matériels militaires intègrent de nombreux équipements, matériaux, composants spécifiquement militaires, voire développés pour un programme ou client précis. Ainsi, les sources uniques sont fréquentes, ce qui limite la possibilité et l'intérêt d'une mise en concurrence systématique à l'échelle internationale, d'autant plus que les États clients recherchent une sécurité d'approvisionnement tout au long du cycle de vie des matériels.

[31] La cartographie des chaînes de sous-traitance ne correspond pas nécessairement à celle des flux physiques de marchandises dans la mesure où certains intermédiaires peuvent réaliser des commandes au profit de leur client sans que les marchandises transitent physiquement par eux.

Maintenir la disponibilité de systèmes intégrés comptant parfois près d'un million de pièces (sous-marins nucléaires) pendant plusieurs décennies impose une grande fiabilité et une certaine permanence des chaînes d'approvisionnement qui n'a aucune commune mesure avec l'approvisionnement de composants électroniques standardisés sur des marchés internationaux hautement concurrentiels, pour des produits civils dont la durée de vie et la disponibilité des pièces de rechange, excèdent rarement quelques années. L'importance de la sécurité et de la pérennité des approvisionnements justifie le maintien et le développement de filières nationales.

In fine, ces spécificités se traduisent par des organisations industrielles requérant davantage de stabilité et de résilience que les filières couramment étudiées (électronique, automobile, notamment)[32]. Par conséquent, il s'agit moins d'une banalisation des chaînes de valeur de l'industrie de défense que de leur hybridation, autrement dit, la coexistence de segments plus intégrés verticalement, plus concentrés géographiquement lorsqu'il s'agit de biens ou activités spécifiques, complexes et stratégiques, avec des segments beaucoup plus fragmentés lorsqu'il s'agit de biens ou activités relevant de standards civils et pour lesquels la diversité des sources disponibles limite les risques de rupture d'approvisionnement.

La coexistence d'organisations industrielles aux logiques si différentes n'est ni évidente, ni immuable. Il n'est pas impossible que la banalisation l'emporte si les contraintes de coûts, les réductions de cibles, l'allongement des cadences de livraison d'une part continuent de fragiliser les filières nationales, leurs écosystèmes régionaux et que les exigences d'*offsets* d'autre part renforcent la dynamique d'internationalisation des chaînes de valeur. Cette hybridation en cours n'est pas un état stable, mais un équilibre en tension : un défi pour les industriels comme pour les États désireux de maintenir une forme d'autonomie technologique et industrielle.

… et pose de nouveaux défis en matière de politique industrielle

Les éléments présentés jusqu'ici démontrent une certaine forme d'hybridation de l'industrie de défense qui connaît des évolutions similaires à l'industrie civile (fragmentation et internationalisation des chaînes de valeur, part croissante des services, etc.), tout en conservant des spécificités propres (durée des cycles de vie, nécessité de pérenniser les organisations industrielles et les savoir-faire sur le long terme). Par ailleurs, ces données permettent d'apporter d'autres éléments de réflexion.

D'abord, l'idée que les marchés export peuvent compenser la baisse de marchés domestiques est en partie fausse dans la mesure où les exigences d'*offsets* tendent à réduire la part de valeur ajoutée captée par le pays exportateur (même lorsque le montant du contrat peut paraître très élevé). Pour la BITD française, la baisse d'un milliard d'euros de commandes nationales n'est pas mécaniquement compensée par un milliard de commandes à l'international au vu de la part de valeur ajoutée captée.

De plus, il arrive que le marché soit attribué à un acteur local et que l'industriel du pays « exportateur » se trouve en position de sous-traitant. Dans ce cas, même si la part de valeur ajoutée peut rester importante, elle s'applique à un volume bien moindre.

[32] Même dans ces filières, il semble que l'importante fragmentation et internationalisation des chaînes de valeur entraîne une vulnérabilité parfois coûteuse si l'on considère l'impact de catastrophes naturelles en Asie sur la production de sites européens et américains.

En outre, si l'on tient compte de l'importante pression concurrentielle qui s'exerce en Europe et à l'international, on peut penser que la solution n'est pas tant d'exporter pour maintenir à flot des BITD européennes affaiblies par la contraction des marchés domestiques, que de renforcer la compétitivité de ces BITD nationales et européennes afin de gagner des marchés internationaux.

Par ailleurs, l'accès à ces marchés requiert souvent une adaptation de l'offre : autant pour des contraintes d'exportation (contrôle export), que pour s'adapter aux besoins du client local. Plus les groupes nationaux doivent trouver des débouchés internationaux, plus leurs portefeuilles-produits doivent intégrer ces besoins et pas uniquement les besoins nationaux. Ainsi, « l'exportabilité » des programmes nationaux devrait de plus en plus influencer le succès commercial des industries nationales sur les marchés internationaux[33].

En définitive, l'ambition des États de développer ou maintenir des BITD pleinement autonomes se heurte à la réalité des dynamiques économiques et industrielles[34]. Du fait de l'internationalisation des chaînes de valeur, l'industrie de défense est de moins en moins un secteur à part, et de plus en plus influencée par les dynamiques à l'œuvre dans le civil, alors même qu'elle conserve certaines spécificités (durée des cycles de vie, sécurité d'approvisionnement, performances spécifiques, etc.).

Dès lors, toute règlementation ayant trait au commerce international, à la libéralisation des échanges de capitaux, de biens, mais aussi de services peut impacter au moins indirectement les industries de défense, quand bien même celles-ci ne seraient pas explicitement visées.

[33] Cet enjeu est d'autant plus important que les financements nationaux en matière de R&D de défense sont contraints et que le développement complet de produits dédiés à l'export se heurte à la capacité des entreprise à autofinancer des projets risqués et très coûteux. Ceci incite les entreprises du secteur à rechercher de nouvelles sources de financement, notamment dans le cadre de l'Union européenne, y compris sur les segments en amont de leur chaîne de valeur (R&T-D).

[34] Même pour le premier marché mondial, les États-Unis, si l'on en croit les problèmes soulevés par le rapport du Sénat américain cité précédemment.

Références

Alliance for American Manufacturing, *Supply Chain Vulnerabilities and National Security Risks across the U.S. Defense Industrial Base*, Rapport complet, 2013. "*Executive Summary*", disponible en ligne : http://www.americanmanufacturing.org/research/entry/remaking-american-security, dernière consultation le 22 juillet 2014.

Australian National Audit Office (2013), "Air Warfare Destroyer Program", *Audit Report*, n° 22, 2013-2014.

ANDERSON Guy et MOORES Ben, "The Growing Burden of Offsets", in *Jane's Defence Weekly*, 25 octobre 2013.

FIOTT Daniel, "The Three Effects of Dual-Use: Firms, Capabilities, and Governance", *ISS Brief*, n° 21, 2014, disponible en ligne : http://www.iss.europa.eu/fr/publications/detail-page/article/the-three-effects-of-dual-use-firms-capabilities-and-governance/, dernière consultation le 22 juillet 2014.

SIPRI, SIPRI Military Expenditure Database, 2013, disponible sur : http://www.sipri.org/research/armaments/milex/milex_database.

United States Senate, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain"*, Report of the Committee on Armed Services*, 2012.

Air Warfare Destroyer Alliance, disponible en ligne : http://www.ausawd.com/, dernière consultation le 22 juillet 2014.

OCDE, *Trade in Value Added*, disponible sur : http://www.oecd.org/sti/ind/measuringtradeinvalue-addedanoecd-wtojointinitiative.htm, dernière consultation le 22 juillet 2014.

Personal Computing Industry Center, disponible en ligne : http://escholarship.org/uc/search?entity=pcic_rw, dernière consultation le 04 mars 2015.

■ LES MOTEURS DE L'INNOVATION AUJOURD'HUI

Sophie LEFEEZ
Docteur en sociologie des techniques au Centre d'études des techniques, des connaissances et des pratiques (CETCOPRA)

L'innovation, prise au sens d'avancées techniques, est un point fort de la politique industrielle européenne. S'il existe de nombreuses études sur les moteurs de l'innovation pour le milieu civil, rien ne dit *a priori* que ces derniers s'appliquent de la même façon au milieu militaire, ni qu'ils sont suffisants pour expliquer l'innovation militaire. Nous présenterons ici trois moteurs de l'innovation en milieu militaire en ce qui concerne la France : un moteur économique, un moteur opérationnel et un moteur socio-anthropologique.

L'innovation comme moteur de croissance

L'innovation est aujourd'hui considérée comme un élément de la croissance économique du pays, ce qui fait d'elle un élément de politique industrielle. Pour comprendre ce passage, nous allons donner un rapide descriptif historique de la politique industrielle française depuis l'après-guerre. Puis nous verrons que, toujours pour des raisons économiques, le champ d'appréhension de l'innovation s'est restreint au cours de ces trente dernières années.

Une politique industrielle tournée vers l'innovation

Après la Deuxième Guerre mondiale, l'État français mit en œuvre une politique industrielle ambitieuse, dont l'exemple emblématique dans le milieu de la défense fut la conception d'armes nucléaires, alors même que la France était loin de disposer des mêmes moyens que les États-Unis et l'Union soviétique. Au cours des années 1980, le libéralisme, alors puissamment en vogue sous la houlette de Reagan et Thatcher, influença le personnel politique français au point de l'inciter à délaisser toute action en matière industrielle. Il fallut attendre le tournant de la décennie 2000-2010 pour que l'État se sente de nouveau légitime à intervenir, quoique indirectement, dans le domaine industriel. Au plan théorique, la reconnaissance de défaillances de marché, en particulier l'existence d'externalités et d'une information imparfaite asymétrique, justifie que l'État vienne en quelque sorte « compenser » ces imperfections tout en se maintenant dans un cadre économique libéral.

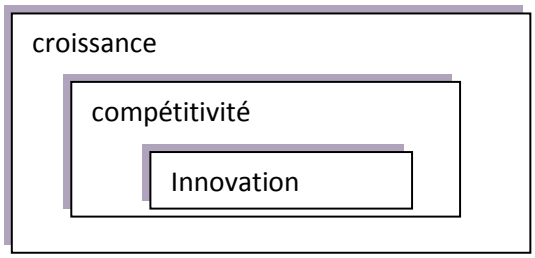
Par ailleurs, l'enlisement dans une période économique morne à la suite des Trente Glorieuses[1] poussa les politiques et les économistes à réfléchir aux moyens de doper la croissance. Le raisonnement adopté est le suivant : pour jouir d'une croissance économique, il faut être compétitif, et la clé de la compétitivité réside dans l'innovation (cf. figure 1). Chaque passage d'une proposition à l'autre constitue une réduction dans la mesure où la croissance repose sur d'autres piliers que la compétitivité, même si celle-ci joue un rôle majeur, de même que cette dernière s'obtient par d'autres facteurs que la seule innovation, même si dans la situation actuelle l'innovation en est un

[1] Période allant de la fin de la Seconde Guerre mondiale jusqu'aux années 1970 et caractérisée par une forte croissance économique.

élément clé. Dès le milieu des années 1990, le spécialiste en management Garry Hamel, également professeur invité à la *London Business School*, préconisait de miser sur l'innovation car « l'innovation sera le premier voire le seul avantage concurrentiel du nouveau millénaire »[2] pour les États avancés.

La politique européenne procède de la même intention : le processus de Lisbonne de mars 2000 vise à faire de l'Europe un lieu d'investissement attirant, en créant un environnement productif favorable à l'innovation, afin de favoriser la croissance ; les programmes lancés depuis s'inscrivent dans la même ligne[3].

Figure 1. Chaîne d'équivalences qui réduit la croissance à une question d'innovation



Pour les entreprises, le raisonnement est identique. En outre, subissant « l'accélération du temps », ces dernières se sentent contraintes à innover pour accroître ou au minimum sauver leurs parts de marché, renforçant encore l'accélération du rythme. Ainsi, comme l'a très bien décrit le philosophe Harmut Rosa, parce que tout va très vite, il faut encore accélérer : c'est le piège de l'accélération du temps[4]. Ce faisant, l'accent entrepreneurial s'est déplacé de ce que l'entreprise connaît, et qui existe donc déjà, vers ce qu'elle peut créer – et qui n'existe donc pas encore.

L'innovation vise donc à donner aux entreprises un avantage par rapport à leurs concurrentes sur le marché international. Séduire de nouveaux clients se traduit par un surplus d'exportations pour le pays producteur, puisque les clients sont des États dans le domaine militaire. En outre, par effet de contamination, une partie des découvertes réalisées dans le domaine civil bénéficie au domaine militaire et vice-versa. En ce sens, on peut voir dans la R&D militaire un moteur de la croissance nationale[5], même si les travaux économétriques tendent à montrer un affaiblissement de ce lien[6]. En somme, la croissance repose sur le moteur de l'innovation civile et le moteur de l'innovation militaire.

---

[2] Gary Hamel, "Strategy as Revolution", *Harvard Business Review*, juillet-août 1996, p. 69-82.

[3] Ministère de l'Industrie, disponible sur : http://www.industrie.gouv.fr/enjeux/innovation/politique.html. On retrouve le même objectif dans le Programme-cadre européen sur la compétitivité et l'innovation (2007-2013), disponible sur : http://cordis.europa.eu/innovation/fr/policy/cip.htm, dernière consultation le 4 mars 2015, transformé ensuite en programme pour la compétitivité des entreprises et les PME (COSME) 2014-2020.

[4] Rosa Harmut, *Accélération. Une critique sociale du temps*, Paris, La Découverte, 2013.

[5] Daniel Reiner, Yves Pozzo di Borgo, Jacques Gautier, Alain Gournac, Gérard Larcher, Rachel Mazuir, Jean-Claude Peyronnet et Gilbert Roger , « Les Capacités industrielles militaires critiques », *Rapport d'information du Sénat*, n° 634, 4 juillet 2012.

[6] Renelle Guichard, « Éléments pour un repositionnement de la R&D de défense au sein du système d'innovation français », *Revue d'économie industrielle*, vol. 108, 2004, p. 7-20. Voir aussi J. Paul Dunne et Derek Braddon, "Economic Impact of Military R&D", *Flemish Peace Institution Research Report*, juin 2008, pour qui l'effet est inefficace. La thèse de doctorat en économie de Julien Malizard, *Dépenses militaires et croissance*

Une innovation réduite tendanciellement au domaine économique marchand

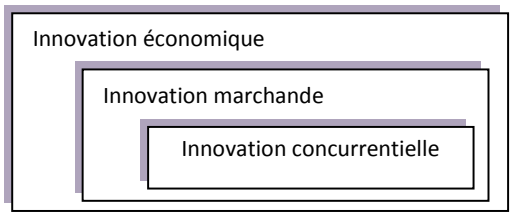
Une étude un peu attentive de l'innovation montre toutefois que celle-ci est généralement entendue au sens concurrentiel et marchand, minimisant d'autres domaines d'application de l'innovation. Cette réduction épistémique doit beaucoup à l'influence prise par l'économie sur le politique d'une part, et par les mathématiques sur l'économie d'autre part.

En effet, la tradition économique libérale s'est appliquée au cours du XIX[e] siècle à instaurer une économie de marché supposée correspondre aux tendances humaines naturelles, afin de parvenir à un système autorégulé. En concevant le gain comme le moteur principal et naturel de l'action humaine, la société libérale l'élevait au rang de justification du comportement dans la vie quotidienne. En acceptant de se soumettre aux exigences du marché, supposé autorégulateur, la politique et les autres domaines de la vie sociale se transformèrent en appendices du système économique. L'économie est ainsi devenue une fin en soi, alors que « normalement, l'ordre économique est simplement fonction de l'ordre social qui le contient », rappelle Karl Polanyi[7].

Poussée par divers facteurs, l'économie se mathématise dès la deuxième moitié du XIX[e] siècle. Le phénomène s'est poursuivi au point qu'après la Deuxième Guerre mondiale, le modèle coût-avantage devient prédominant dans les analyses des politiques publiques. Tout étant quantifié puis monétarisé, tous les scénarios de choix possibles se soldent par un chiffre : le politique n'est désormais plus appelé qu'à comparer des chiffres, raconte Jean-Paul Karsenty, un économètre qui a longtemps travaillé au ministère de la Recherche[8].

Ainsi, le marché est devenu l'instance de déchiffrement et de mesure de l'économie, tandis que la mathématisation de la société nous fait voir le monde par le prisme du calcul. Pour Jean-Paul Karsenty, ce contexte nous fait envisager aujourd'hui les innovations principalement à travers le calcul et les destiner généralement à une mise sur le marché dans une démarche concurrentielle.

Figure 2. Réduction de l'innovation à l'innovation économique, marchande et concurrentielle



Dans le même temps, les discours politiques, tant nationaux qu'européens, appellent l'innovation de leurs vœux. Cela sonne, écrit Karsenty, « comme une charge désespérée contre un ennemi invisible ; un ennemi qui empêcherait l'innovation d'émerger et qui la retiendrait comme prisonnière… ! [...]

économique, dirigée par Jacques Aben, Université de Montpellier 1, 2011, fait état d'une absence de consensus sur le sujet.

[7] Karl Polanyi, *La Grande Transformation*, Paris, Gallimard, p. 121.

[8] Jean-Paul Karsenty, « L'Innovation responsable par le dépassement de la logique économiciste », *Ars Industrialis*, 4 février 2012.

On l'invoque de manière d'autant plus incantatoire que sa définition devient tout à la fois plus restreinte et plus floue : comme une sorte de galimatias qui désigne tout mouvement visant une valeur ajoutée d'ordre économique, mesurée par des indicateurs ayant perdu tout lien avec des finalités ou même avec des intentions caractérisables »[9]. On pourrait ainsi sortir de l'économisme et jouer sur les effets à travers les innovations d'intérêt scientifique, social, écologique, politique, ou encore culturel, ou bien nous pourrions réfléchir en termes géographiques : l'innovation profite-t-elle au niveau local, régional, national, international, mondial ?

À cet égard, le milieu militaire se montre plus ouvert que le milieu civil puisqu'on y entend des réflexions sur l'innovation portant sur l'organisation, la doctrine ou les effets opérationnels. Un des principaux moteurs de l'innovation dans le milieu militaire est, précisément, l'atout opérationnel.

L'innovation comme atout opérationnel

L'exigence de supériorité technique

Alors que Jean-Paul Karsenty déplore une perte de finalité dans le domaine civil, le milieu militaire paraît au clair sur les raisons qui poussent à innover : les armées ont besoin sur le terrain d'un « petit plus qui fera la différence » sur le plan des matériels, afin d'emporter la victoire. Il s'agit alors d'une innovation incrémentale : avoir une allonge supérieure à celle de l'adversaire, détecter plus tôt les intrusions dans l'espace aérien, avoir l'information plus vite que l'adversaire, etc. La supériorité peut aussi relever d'une innovation de rupture, auquel cas elle change les règles du jeu, surprend l'autre et doit permettre de reprendre l'avantage. Tant les acteurs impliqués dans la conception des armements que les combattants sont convaincus de l'importance de jouir d'une supériorité technique pour vaincre, même si une partie de ces derniers estime que cet atout n'est pas indispensable.

Les acteurs appuient souvent leur position d'exemples historiques, parmi lesquels l'introduction de l'arme à feu et le char occupent une grande place, aux côtés de la figure biblique de David contre Goliath. Pourtant, l'arme à feu seule n'eut qu'un faible impact. Il fallut en réalité quelques siècles pour que la poudre modifie en profondeur la façon de se battre. Pour prendre l'exemple de l'arquebuse, elle ne permettait pas de tirer précisément, contrairement à l'arbalète, et prenait du temps pour être rechargée. Vu en termes d'ennemis tués par unité de temps, elle apparaissait moins « rentable ». Mais elle avait un avantage qui fit pencher la balance en sa faveur : le temps de formation était très réduit et son coût unitaire moindre. Autrement dit, le chef militaire pouvait très rapidement accroître ses troupes au lieu d'attendre quelques années que des archers ou arbalétriers soient formés, et compenser numériquement la faiblesse qualitative des tirs[10]. Ce n'est donc pas la supériorité technique de l'arme proprement dite qui conféra l'avantage, mais l'organisation (en ligne serrée) et le format de l'armée grâce au gain de temps de formation.

C'est à la Renaissance qu'eurent lieu, en Occident, les premières réflexions scientifiques appliquées à la puissance militaire, après l'éclipse des premières réflexions grecques. Les fortifications furent, avec la Marine, un domaine privilégié.

[9] Jean-Paul Karsenty, *op. cit.*
[10] Thomas F. Arnold, *Les Guerres de la Renaissance, XV^e^-XVI^e^ siècles*, Paris, Autrement, 2002.

Ce fut la guerre de Sept Ans (1756-1763) qui persuada le duc de Choiseul que la technique allait désormais occuper une place essentielle parmi les facteurs de victoire[11]. Au XIX[e] siècle, les inventions navales telles que l'adaptation de la machine à vapeur, la propulsion à hélice ou le cuirassier, couplées à la suprématie commerciale, industrielle et financière des Britanniques, contribuèrent fortement à la domination mondiale du Royaume-Uni à cette période.

Néanmoins, l'atout conféré par la technique se révèle souvent transitoire car le camp adverse finit par élaborer une parade. L'avantage fluctue entre le jeu offensif et le jeu défensif, et l'illustration la plus fameuse concerne la perforation et le blindage. Le major-général Charles Fuller (1878-1966) appela ce phénomène la loi du facteur tactique constant[12]. Par conséquent, les scientifiques sont constamment mobilisés et incités à produire de nouvelles connaissances. Un rapport étatique de 1923 constate ainsi que les armements voient leur « valeur tomb[er] à peu de choses s'ils n'étaient tenus à hauteur des progrès de la science »[13].

Par conséquent, la France se donna pour ambition dans l'entre-deux guerres de posséder un armement moderne « tenu à hauteur des derniers perfectionnements » et des engins nouveaux, « conçus d'après des indications tenues secrètes et surgissant au moment du besoin pour produire sur l'ennemi l'effet de surprise et la rupture d'équilibre qui donnerait la victoire avant que la résistance ennemie ait pu s'organiser pour amener la guerre d'usure »[14]. Derrière ces engins nouveaux pointe le fantasme de l'arme secrète permettant d'emporter la victoire sur un ennemi pris par surprise — non une surprise tactique ou stratégique, mais technique. De telles armes secrètes émaillent la Deuxième Guerre mondiale, mais avec également les fusées allemandes V1 et V2, la bombe atomique américaine ou le projet de sous-marin porte-avions japonais[15]. Par la suite, la recherche de la supériorité technique devint centrale, systématique, voire obsessionnelle : elle est perçue comme un élément déterminant, reléguant à un rôle secondaire les autres facteurs de victoire.

Puis, dans les années 1990 en France, le DGA Helmer introduit l'approche capacitaire, consistant à penser le besoin en termes d'effets recherchés : il faut « être capable de ». Encouragés par cette approche du combat comme affrontement de capacités, les États-majors imaginent emporter la victoire s'ils gagnent le rapport de force ou s'ils possèdent la capacité qui fait défaut à l'adversaire et/ou qui constitue un réel atout dans la bataille. Dans ce dernier cas, on parle de « rupture capacitaire ». Ainsi est établie l'adéquation dans les représentations mentales entre besoin et performance technique. Cette logique, partagée par les ingénieurs et les États-majors, ne s'entend pas nécessairement dans les discours des combattants.

---

[11] Patrice Bret, *L'État, l'armée, la science. L'invention de la recherche publique en France (1763-1830)*, Presses Universitaires de Rennes, 2002, p. 170.

[12] La loi énonce que l'apparition d'une arme nouvelle a toujours été suivie d'un contre-perfectionnement qui prive cette dernière de sa supériorité (Charles Fuller, *L'Influence de l'armement sur l'histoire. Depuis le début des guerres médiques jusqu'à la Seconde Guerre mondiale*, Payot, 1948).

[13] Sébastien Soubiran, *Les Processus d'innovation technologique dans l'armement français, 1919-1939 : rapport final définitif en édition provisoire,* Fondation pour la recherche stratégique, 2002, p. 36.

[14] *Idem*.

[15] Voir le documentaire « L'Arme secrète du Japon », diffusé sur National Geographic Channel et repris sur le site *Theatrum Belli*, disponible sur : http://www.theatrum-belli.com/archive/2010/08/20/seconde-guerre-mondiale-l-arme-secrete-du-japon.html, dernière consultation 4 mars 2015.

On peut dire qu'elle est propre aux réflexions stratégiques — on en trouve trace dans de nombreux documents institutionnels —, mais se diffuse plus péniblement au fur et à mesure qu'on se rapproche des praticiens.

La technique, un facteur de victoire parmi d'autres

De fait, quand on écoute les combattants, on s'aperçoit que la supériorité technique apporte une plus-value au plan tactique, mais que celle-ci est plus discutable au plan stratégique et politique. En effet, éliminer de nombreux ennemis (gain tactique) ne sert pas en soi les buts poursuivis par une entrée en guerre (gain stratégique), car la destruction de l'adversaire n'est qu'un « moyen » en vue d'une « fin politique ». Dès lors, se focaliser sur les apports de la technique au plan tactique ferait courir le risque de renforcer une tension vers la dépolitisation de la guerre et la « tactisation » des opérations, comme le souligne Joseph Henrotin[16]. Au contraire, les guerres totales, marquées par l'affirmation sans retenue de la force, la puissance extrême procurée par les armes nucléaires et le développement des conflits asymétriques, poussèrent l'Europe à maîtriser sa force au degré nécessaire à l'obtention de l'effet recherché[17]. Cela se traduisit par des exigences nouvelles en matière d'armements : gamme de puissance du feu, circonscription de l'espace ciblé, priorité accordée au renseignement..., ce qui alimenta le besoin de nouvelles innovations, au-delà de la simple ambition de supériorité technique.

Par conséquent, l'appréciation de la puissance apportée par les armements est relative parmi les combattants. Ces derniers ont plutôt tendance à voir dans la technique un facteur de victoire parmi d'autres, aux côtés des forces morales (force psychologique humaine, cohésion des groupes, endurance, maîtrise de soi), de l'entraînement, ou encore de la ruse, et certains n'hésitent pas à minorer le poids des ressources matérielles[18].

D'ailleurs, l'histoire ne confirme pas la nécessité de la supériorité technique. Les batailles passées, en particulier Crécy (1346), Poitiers (1356) et Azincourt (1415), témoignent du caractère non-essentiel de la technique dans l'obtention de la victoire. « Dans ces trois batailles », rappelle l'historien François Cochet, « comme dans d'autres (dont le scénario fut différent pour chacune d'elles), ce ne fut jamais la supériorité technique ou l'emploi d'une arme spécifique qui décida de la victoire. Celle-ci revint à celui des adversaires qui, faisant fi des préjugés et des traditions, avait compris l'importance d'une action coordonnée et la complémentarité des mouvements des cavaliers et des archers à l'intérieur d'un dispositif tactique commun »[19]. Plus près de nous, le géographe britannique Simon Reid-Henry montre que la crise des missiles de Cuba a été détournée pour bâtir au moins quatre mythes, dont celui d'affirmer que la sécurité nationale est mieux assurée par l'entremise d'une supériorité technico-militaire. Les photographies des avions-espions n'ont fait que confirmer les renseignements obtenus sur le terrain, dit-il, et les survols de l'île ont en réalité contribué à une

[16] Joseph Henrotin, *La Technologie militaire en question. Le cas américain*, Paris, Economica, 2e éd., 2013, p. 31.
[17] General Rupert Smith, *The Utility of Force, The Art of War in the Modern World*, Penguin Books, 2006.
[18] Pour en avoir des témoignages, cf. *ibid.*, mais aussi Richard Gabriel, *À la manière des guerriers : un traité d'éthique militaire*, Académie canadienne de la défense, 2009), selon qui l'analyse des batailles montre des constantes parmi les éléments contribuant à la victoire : les forces morales, la cohésion entre soldats et l'efficacité du commandement. Mes entretiens, notamment parmi les forces spéciales, confirment ces analyses.
[19] François Cochet, *Armes en guerre. XIXe - XXe siècle Mythes, symboles, réalités*, Paris, CNRS Éditions, 2012, p. 64.

escalade de la crise[20]. À vrai dire, il faudrait plutôt penser la victoire comme la combinaison d'un ensemble de facteurs selon des proportions appropriées. Cela veut dire que, selon les cas, la technique peut ne jouer qu'un rôle mineur.

D'ailleurs, plusieurs combattants décrivent la technique comme un outil sans influence sur les fondamentaux de la guerre, à l'instar de ce colonel pour qui la décision repose toujours sur l'humain, quels que soient les moyens mis à sa disposition : « La guerre, ce sera toujours une réflexion humaine qui répondra à des contingences du moment. Par conséquent, le stratège restera au cœur du combat, ou le tacticien, tout dépend à quel niveau on se place, et il ouvrira sa boîte dans laquelle il y aura des outils. Ces outils sont effectivement des matériels, des hommes, mais au final on restera toujours dans des schémas qui sont millénaires »[21]. Dans la même ligne de pensée, l'ingénieur de l'armement Marc Défourneaux estime que « le progrès technique élargit le champ de la guerre mais il n'en supprime pas les formes traditionnelles »[22], ce qui explique que le soldat n'abandonne pratiquement jamais un type d'arme : « de même que la mécanisation n'a jamais aboli la marche à pied, la baïonnette fait toujours partie des dotations, ainsi que le pistolet et la grenade à main, et on a même vu réapparaître l'arbalète dans certaines unités de commandos, redécouverte au XX^{e} siècle pour les vertus de son fonctionnement silencieux »[23].

L'innovation technique et le besoin opérationnel

En somme, sous l'effet de la technicisation et la « scientifisation » de la guerre, l'innovation est principalement appréhendée sous l'angle de la recherche de supériorité technique, même si l'innovation doctrinale et organisationnelle, par exemple, ne sont pas oubliées dans les instances de réflexion. Les deux Guerres mondiales et la Guerre froide ensuite ont constitué une sorte de point d'acmé dans la quête de perfectionnement technique, et la direction n'a depuis pas dévié dans un souci de positionnement concurrentiel des entreprises d'armement, d'indépendance stratégique du pays et de supériorité technique des armées dans le cas où surviendrait un conflit symétrique. Pourtant, l'histoire montre que la supériorité technique n'est qu'un facteur de victoire parmi d'autres, et qui plus est pas autant indispensable que les concepteurs et la plupart des militaires ne le supposent. L'innovation dans le domaine militaire souffrirait-elle également d'une tendance à la réduction épistémique ? Nous pourrions imaginer mettre moins l'accent sur la dimension technico-scientifique et ouvrir davantage la réflexion au domaine tactique, à la ruse, tout en préservant soigneusement les forces morales, lesquelles participent tout autant sinon plus à l'obtention de la victoire.

Mais changer d'orientation ne serait pas aussi aisé si l'on en croit l'étude de Stephen Peter Rosen. Ce politologue montre que, contrairement à une image répandue, l'innovation technologique aux États-Unis sur la période 1930-1955 était faiblement liée aux capacités et aux intentions ennemies. Les avancées techniques relevaient d'un processus plutôt autonome, où les actions et les acteurs au sein de l'*establishment* militaire étaient les principaux déterminants de l'innovation[24].

[20] Simon Reid-Henry, "The Cuban Missile Crisis through the Prism of Self-Serving Myths", *The Guardian*, 23 octobre 2012.
[21] Entretien personnel, 2010.
[22] Marc Défourneaux, *Guerre des armes - Guerre des hommes*, Paris, Addim, coll. Esprit de défense, 1994.
[23] *Ibid*., p. 183.
[24] Stephen Peter Rosen, *Innovation and the Modern Military. Winning the Next War*, 1991, p. 250.

Une actualisation de cette étude serait fort utile pour évaluer le degré actuel de dépendance de l'innovation militaire envers le comportement de l'adversaire. En France, on peut observer que la représentation qui préside au choix technique n'est pas toujours fondée sur une observation des combats qui se déroulent réellement, ni sur ceux qui sont les plus probables, mais parfois sur une recherche d'excellence technique[25]. Par conséquent, le risque de voir la recherche scientifique décrocher par rapport aux capacités et intentions adverses semble toujours réel.

La fascination exercée par la technique apparaît comme un élément explicatif de la recherche d'excellence technique. Elle joue sur les ingénieurs, certes, mais également sur les armées, pour qui avoir un appareil dernier cri peut être aussi une question de rang et de prestige. La technique est en effet le réceptacle d'attentes humaines, ce qui renvoie à une dimension socio-anthropologique.

L'innovation comme élan humain

La technique comme réponse aux attentes humaines

L'approche opérationnelle montre que l'humain attend de la technique qu'elle le rende plus fort que son adversaire ; le fait de citer le combat de David contre Goliath montre assez bien l'attente placée en elle. De manière générale, l'homme projette ses espoirs et des croyances sur la technique.

Prenons un exemple simple : le cas des États-Unis. Cet allié mise sur la technique pour lui conférer un rang de supériorité dans la compétition mondiale. Le champ économique en donne une illustration éclatante : il utilise une large gamme de moyens pour encourager la recherche technico-scientifique et dépasser ses concurrents afin de maintenir ou accroître leurs parts de marché mondial. Mais le champ militaire n'est pas en reste : ils sont à ce jour le seul pays à posséder un aéronef convertible, le V-22 *Osprey*, jouissent d'une avance sur les lasers de puissance embarqués, ont été parmi les pionniers dans la conception et l'emploi des drones militaires et tiennent à préserver leur supériorité technique face à n'importe quelle armée étrangère.

Les Français projettent eux aussi des espoirs sur la technique. La protection des soldats en est une : le ministère de la défense et les politiques investissent beaucoup sur la technique à travers le développement de systèmes de détection de départs de coup, l'achat de gilets pare-balles, ou encore l'insertion de tourelleaux téléopérés et d'autres systèmes d'écran pour éviter aux combattants d'avoir à sortir la tête du véhicule. D'ailleurs, les Français justifient leur besoin de poursuivre leur quête de supériorité technique dans les combats asymétriques – où *a priori* cela est inutile puisqu'ils sont déjà le « fort » – par le décalage dans le rapport à la mort entre les parties en présence.

[25] Mon étude de cas sur le système antichars Milan montre que cette arme est finalement assez peu utilisée contre des chars, mais que ces derniers demeurent l'élément dimensionnant (*Représentations et usages des armements. Pour une socio-anthropologie de la complexité technique*, thèse de sociologie des techniques, Université Paris 1-Panthéon Sorbonne, septembre 2014). Cf. aussi William Genieys, Laura Michel, « Le Leclerc ou l'invention du "meilleur char du monde"», *dans* William Genieys (dir.), *Le choix des armes. Théories, acteurs et politiques*, Paris, CNRS Éditions, 2004, p. 83-114.

Une étude attentive montre que, dans les conflits asymétriques, le décalage sur le plan des valeurs (rapport au temps, droit des conflits armés...) et des intérêts en jeu (souvent *de facto* plus faible chez celui qui a la supériorité technique) est contrebalancé par des performances techniques. Celles-ci serviraient donc de contrepoids à des différences d'ordre social[26].

Dans un autre registre, le discours des acteurs laisse transparaître un besoin d'ordre, qui peut s'expliquer par une raison conjoncturelle et une raison plus structurelle. Premièrement, la fin de la Guerre froide a fait disparaître un monde connu et ordonné, laissant derrière elle un vide déstabilisant qualifié de « crise des fondements »[27] par le général Lucien Poirier. Deuxièmement, sous l'impulsion de Johannes Kepler, Galilée, Descartes et Newton, pour n'en citer que les principaux, la science moderne s'est donné pour ambition de déchiffrer les règles de la nature. Une fois maîtrisées, on peut les utiliser à son profit pour concevoir des objets techniques, mais on s'attend également à ne plus être surpris par le comportement de la nature[28]. Pour le philosophe de la technique Langdon Wiener, notre société est passée de la notion de « danger » à celle de « risque » à partir du moment où elle a commencé à calculer les probabilités[29] d'occurrence. C'est cette mutation qui permet d'espérer une « guerre zéro aléa », pour reprendre l'expression de François-Bernard Huyghe : « Plutôt qu'une guerre zéro mort, c'est une guerre zéro aléa dont rêvent les stratèges post-modernes : éliminer l'incertitude liée aux hasards du champ de bataille comme celle qui résulte du facteur humain. La stratégie cesserait d'être un jeu à information imparfaite, où il faut parier sur les résultats du combat, sur les projets de l'autre, sur sa résistance, sur le comportement de ses propres troupes, etc., pour devenir une science de gestion des peines »[30].

Ainsi, nous attendrions de la technique qu'elle nous rassure devant l'incertitude de notre monde, ce qui expliquerait l'essor des techniques de modélisation et d'outils informatiques d'aide à la décision, et la multiplication de capteurs ISR. Jacques Perriault avait identifié dès 1999 le rôle d'assurance que nous faisons jouer aux machines à communiquer : assurance-enregistrement avec le magnétoscope, assurance-présence avec le répondeur. « Nantis de leur parc d'appareils, les usagers auscultent ainsi quotidiennement le monde et leurs proches, et constatent qu'ils réagissent. [...] Ces machines servent finalement à rassurer sur le fait que tout continue à fonctionner. Dans cette optique, l'usage a une fonction de contrôle, par celui qui le pratique, de sa famille, de la société et de ses mythes. Ce contrôle est instantané : appuyer sur un bouton, composer un numéro ou un code suffisent en effet pour obtenir un retour d'information quasi immédiat »[31]. De même, le sociologue Gérard Dubey montre que dans l'aéronautique, le virtuel et les procédures jouent un rôle d'assurance : « conçue pour permettre une reprise en main rapide de l'avion, les pilotes savent aussi que la procédure – la

[26] Sophie Lefeez, *Représentations et usages des armements. Pour une socio-anthropologie de la complexité technique*, thèse de sociologie des techniques, Université Paris 1-Panthéon Sorbonne, septembre 2014.
[27] Lucien Poirier, *La Crise des fondements*, Paris, Economica, 1994.
[28] La prévision des catastrophes naturelles en est une application. Ainsi, les fortes chutes de neige qui ont affectées l'Ile de France pendant l'hiver 2010-2011 ont suscité l'incompréhension du chef de l'État, qui jugeait inacceptable la désorganisation qui s'en est suivie, tandis que le Premier ministre reprochait à Météo France de ne pas avoir prévu l'intensité de l'épisode neigeux. Voir par exemple *Challenges*, « Neige : Sarkozy tente de faire retomber la polémique », 10 décembre 2010, disponible sur : http://www.challenges.fr/economie/20101210.CHA2310/neige-sarkozy-tente-de-faire-retomber-la-polemique.html, dernière consultation 15 décembre 2014.
[29] Langdon Wiener, *La Baleine et le réacteur. A la recherche de limites au temps de la haute technologie*, Descartes & Cie, 2002.
[30] François-Bernard Huyghe, « Croire *contre* », *Les cahiers de médiologie*, vol. 2, n° 8, 1999, p. 13.
[31] Jacques Perriault, *La Logique de l'usage*, Paris, Flammarion, 1999, p. 199-200.

réalité formelle du simulateur – aide surtout à retrouver sa sérénité, son assise, à dominer l'angoisse, qu'elle est un support mental (nous dirions symbolique) autant que technique pour l'action »[32].

Le rapport humain à la création

Les choix techniques que nous faisons dérivent donc en partie de ce que nous y projetons. Si la technique sert quelquefois à corriger des déséquilibres sociaux, Aristote voyait dans la *technè* une disposition à créer de la nouveauté pour combler les lacunes de la puissance naturelle[33]. Par la technique, l'homme poursuit donc une créativité naturelle. Plusieurs siècles plus tard, Henri Bergson rejoint Aristote sur ce point, se demandant s'il ne serait pas plus juste de définir l'homme comme *homo faber*, celui qui fabrique et invente des objets techniques, bien plus que comme *homo sapiens*, parce que « l'invention technique a d'abord été sa démarche essentielle, qu'aujourd'hui encore notre vie sociale gravite autour de la fabrication et de l'utilisation d'instruments artificiels, que les inventions qui jalonnent la route du progrès en ont aussi tracé la direction »[34].

Le moteur humain de l'innovation semble donc être un processus inhérent à la nature humaine, ce qui fait de l'innovation un phénomène des plus classiques en soi. C'est l'accélération de son rythme qui attire l'attention, ainsi que le sentiment de ne pas assez réfléchir en amont sur les formes et les directions que pourrait prendre la recherche[35]. Par exemple, sait-on ce que l'on cherche précisément quand on vise la collecte massive d'informations, quand on demande rapport sur rapport ? Pour savoir si la réponse technique est la plus appropriée, il faut soigneusement avoir formulé le problème, car la réponse ne préexiste pas à la question, elle y est contenue. Une illustration littéraire nous est donnée par Douglas Adams, auteur du *Guide du voyageur galactique*[36]. La réponse à la Grande Question sur la Vie, l'Univers et le Reste, trouvée après 7,5 millions d'années de calculs, est 42 :

— « Quarante-deux ! cria Loonquawl. Et c'est tout ce que t'as à nous montrer au bout de sept millions et demi d'années de boulot ?

— J'ai vérifié très soigneusement, dit l'ordinateur, et c'est incontestablement la réponse exacte. Je crois que le problème, pour être tout à fait franc avec vous, est que vous n'avez jamais vraiment bien saisi la question »[37].

Nous insistons sur la façon dont est posée la question initiale car le milieu – social, économique, écologique, ... – dans lequel évolue l'humain propose sans jamais imposer de solutions : c'est l'Homme, être vivant et historique, qui, par son imagination, se représente le « désirable » qui va mobiliser sa volonté, diriger son action et lui donner, en définitive, le sens du possible.

Il faut bien distinguer ici la science de la technique : tandis que la connaissance requiert la nécessité, la permanence et l'ordre, la *technè* présuppose un monde de contingence qui suscite l'action. D'un côté, un monde déterministe où l'humain réagit et tire profit des lois de la nature.

---

[32] Gérard Dubey, *Le Lien social à l'ère du virtuel*, Paris, PUF, 2001, p. 224.
[33] Pierre Aubenque, *La prudence chez Aristote*, Paris, PUF, 2014, p. 69.
[34] Henri Bergson, *L'Évolution créatrice*, Paris, PUF, 1996 (1907), p. 138.
[35] De nombreuses études sociales sur la technique parviennent à cette conclusion, comme par exemple Jean-Jacques Salomon, *Prométhée empêtré. La résistance au changement technique*, Paris, éditions anthropos, 1984.
[36] Douglas Adams, *Le Guide du voyageur galactique*, Paris, Gallimard, 2005 (1979), p. 232.
[37] Idée et citation que je dois à Boris Solinski, « Le fruit du hasard : de l'incertitude dans le jeu au jeu de l'incertain », XIX[e] Congrès de l'Association internationale des sociologues de langue française, Rabat, 4 juillet 2012.

De l'autre, un monde inachevé où l'humain donne libre cours à son élan créateur. Contrairement à une image répandue, il n'y a pas de déterminisme technique ni d'unilinéarité de l'évolution technique : si les lois scientifiques sont fixes, l'homme est libre de donner l'orientation qu'il souhaite à ses créations dans le respect desdites lois. Les différentes formes du vélo donnent une illustration claire de la contingence qui accompagne la création technique et des influences sociales dans la sélection de la (ou des) forme(s) définitive(s)[38].

En conclusion, l'innovation condense l'avantage de porter les espoirs de victoire militaire et de croissance du pays, tant au plan civil que militaire. Dans les deux cas, on observe une réduction épistémique car on charge la technique d'aspirations : pour favoriser la croissance, on encourage surtout l'innovation marchande et concurrentielle, et pour remporter la victoire, on recherche en premier lieu une domination au plan technico-scientifique. Innover est un élan humain et s'inscrit dans un monde de contingences. Être conscient du rapport que nous entretenons avec la technique peut nous permettre de réfléchir sur la place que nous lui accordons dans l'innovation, et sur ce que nous en attendons. Peut-être pourrions-nous ainsi envisager une innovation qui requière des dépenses de R&D moins importantes, ce qui serait davantage compatible avec l'état actuel des finances publiques.

[38] Trevor Pinch et Wiebe Bijker, "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other", *In*: Wiebe Bijker, Thomas Hughes, Trevor Pinch (dir.), *The social construction of technological systems: New Directions in the Sociology and History of Technology*, Cambridge, The MIT Press, 1987.

AU CŒUR DES PRATIQUES DE GESTION DE L'INNOVATION TECHNOLOGIQUE DES ENTREPRISES DE LA DEFENSE

Jérôme ROSELLO
Doctorant en science de gestion à l'Ecole Doctorale de Management Panthéon Sorbonne - ESCP Europe

Introduction

Dans un contexte de mutations de l'économie de défense, l'innovation est un enjeu clé pour la compétitivité des entreprises. Elles sont par conséquent contraintes d'adapter leurs pratiques existantes pour être encore plus innovantes. Selon les propos d'un directeur d'innovation d'une entreprise de la défense : « l'innovation, tout le monde en parle, mais on ne la voit jamais ». Cette phrase reflète tout le caractère intangible, complexe, itératif, autrement dit le caractère systémique de la capacité d'innovation d'une entreprise, nécessitant de mobiliser des ressources, des connaissances et des compétences. Cette phrase reflète également le caractère cycle long des produits de la défense. La durée du chemin entre la nouvelle idée et le résultat visible par un client étatique est variable ; il peut parfois être court, parfois extrêmement long, voire ne jamais aboutir. La notion d'innovation se réfère ainsi à des innovations concrètes, qui sont des offres commerciales, des produits, des services, des procédés qui apportent à un marché, au sens large du terme, une offre différenciant. L'innovation peut résulter soit d'une nouvelle technologie, soit d'une nouvelle demande.

L'innovation technologique est souvent considérée comme un enjeu stratégique dans les politiques de défense[39]. Elle permet à la fois de garantir l'autonomie stratégique et l'avantage concurrentiel dans les missions opérationnelles. L'innovation technologique est le résultat de la capacité d'une entreprise à choisir, acquérir, intégrer et utiliser de nouvelles technologies pour améliorer l'opérabilité et la souveraineté des systèmes. Le développement de cette capacité nécessite des pratiques clairement établies, voire de nouvelles pratiques pour gérer efficacement l'innovation technologique.

Peu de recherches ont été menées jusqu'à présent pour identifier les pratiques existantes et les nouvelles pratiques de gestion de l'innovation technologique au sein du secteur de la défense. À partir d'entretiens semi-directifs réalisés auprès d'acteurs de l'innovation au sein d'un panel représentatif d'entreprises du secteur de la défense[40] et de documents internes à ces entreprises, nous avons cherché à identifier ces pratiques. Parmi toutes celles identifiées, nous nous intéresserons particulièrement aux pratiques collaboratives actuellement existantes pour le développement des produits de demain, puis nous ouvrirons le sujet dans la discussion sur de nouvelles pratiques collaboratives.

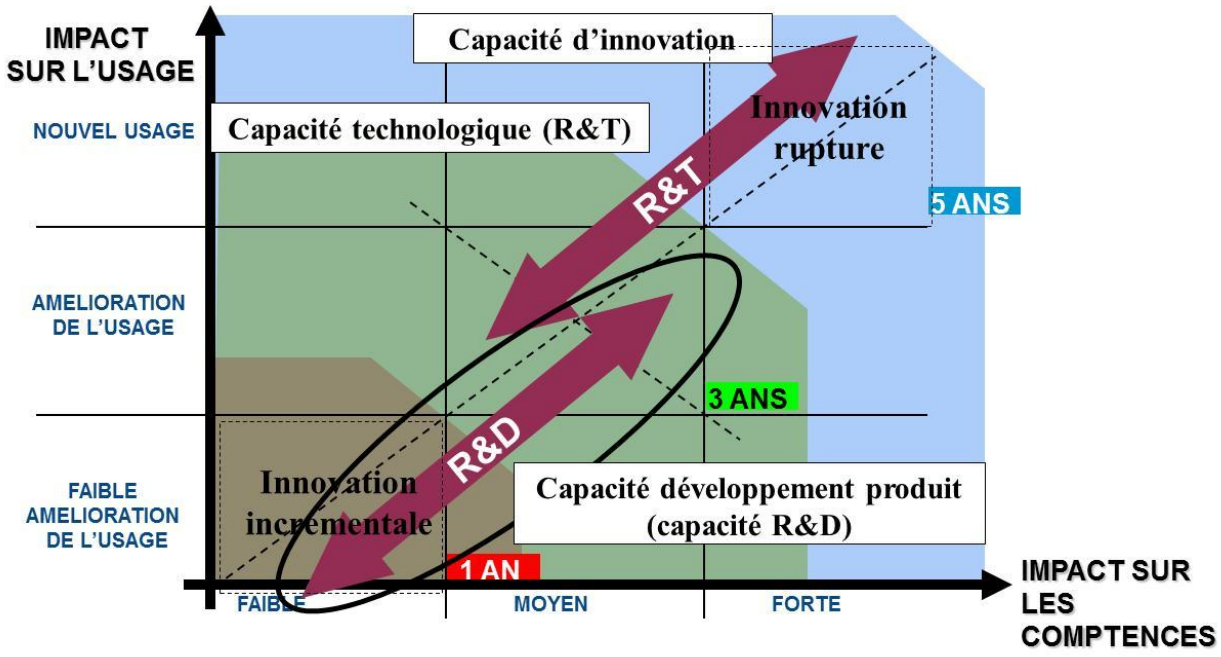
[39] David Versailles, Valérie Mérindol et Patrice Cardot, *La Recherche et la technologie, enjeux de puissance*, Economica, 2003.
[40] Safran, Thales, EADS.

La réflexion stratégique au cœur des pratiques de gestion de l'innovation technologique

La réflexion stratégique est au cœur des pratiques de gestion de l'innovation technologique des entreprises de la défense. Cette réflexion nécessite d'avoir un cadre pour penser le futur et définir des éléments qui vont être nécessaires à sa construction. L'entreprise doit posséder une capacité à se projeter dans l'avenir, à travers ses rituels et ses règles de gestion interne, tout en considérant ses ressources et ses compétences actuelles et futures ainsi que son cœur de métier. La réflexion stratégique a pour objectif de construire un PMT[41] en général sur 5 ans, à travers une démarche RTDI[42].

Selon le graphique ci-dessous, la démarche R&T[43] identifie de nouvelles technologies permettant d'obtenir une différenciation en termes d'usage des produits dans une logique d'innovation de rupture, alors que la démarche R&D développe et industrialise les nouveaux produits dans une logique d'innovation incrémentale[44] :

Graphique 1. Démarche R&D et démarche R&T



La réflexion stratégique aide à obtenir un consensus sur un ensemble de besoins et de technologies exigé pour satisfaire une application militaire. Certaines entreprises de la défense mettent en place de manière annuelle, voire bisannuelle, des séminaires de réflexions stratégiques auxquels de nombreux acteurs internes à l'entreprise allant de la R&D jusqu'au commerce participent.

Quatre axes de réflexions sont souvent privilégiés : (1) les aspects commerciaux (marché), (2) les aspects économiques (bilan économique de l'année précédente), (3) l'aspect positionnement

[41] Plan Moyen Terme.
[42] Recherche, Technologie, Développement et Industrialisation.
[43] Recherche et Technologie.
[44] Une logique d'innovation incrémentale consiste à améliorer l'existant.

(positionnement stratégique visé) et (4) l'aspect planification technologique (feuilles de route produit – technologie).

Les aspects commerciaux sont au cœur de la réflexion stratégique des entreprises de la défense. Cet aspect de la réflexion a pour objectif de déterminer quelle part de marché est accessible par l'entreprise en prenant en compte des études de marché, des tendances de produits ainsi que des contraintes d'export et de concurrence. La concurrence est perçue comme assez agressive sur certains segments de marché militaire, et le marché est relativement concentré pour certains domaines d'application, ce qui pénalise les entreprises de la défense. Le contexte géopolitique, l'accessibilité de certains marchés, les évolutions réglementaires d'exportation et la situation budgétaire des pays cibles sont alors pris en compte pour établir des priorités au sein de la réflexion stratégique.

Les aspects économiques en sont d'ailleurs la pierre angulaire. Cet aspect de la réflexion est une étape nécessaire qui consiste à faire le bilan des succès et des échecs technico-commerciaux de l'année précédente. Elle permet également de capitaliser sur certains retours d'expérience. Le ratio des dépenses réalisées par rapport au budget prévu est un critère déterminant pour mesurer l'atteinte des objectifs de l'entreprise.

Les aspects de positionnement permettent de quantifier des orientations stratégiques à court, moyen et long terme. Les aspects de positionnement sont fondamentalement empreints de la pensée porterienne : « une stratégie concurrentielle met en place une action offensive ou défensive pour créer une position défendable dans une industrie ou un marché afin de faire face avec succès aux forces de la concurrence et générer un niveau supérieur de retour sur investissement »[45]. Il existe des positions stratégiques plus intéressantes économiquement que d'autres, et l'entreprise définit la sienne à partir d'une analyse de ses ressources et de ses compétences. Les critères prépondérants pour définir une bonne stratégie sont le positionnement prix/produit et la cible marché. L'avantage concurrentiel peut s'obtenir soit par un *leadership* sur les coûts, soit par une réelle différenciation, comme la différenciation technologique. La source de l'avantage concurrentiel est considérée avant toute chose comme la satisfaction client. La différenciation et la réduction des coûts sont des domaines auxquels les entreprises de la défense consacrent beaucoup d'efforts. Toutefois, les aspects commerciaux, de positionnement et économiques priment souvent sur les aspects technologiques car l'introduction d'une nouvelle technologie coûte cher à l'entreprise. Pour opérationnaliser la réflexion stratégique, les entreprises de la défense utilisent des pratiques collaboratives pour le développement des produits de demain, en essayant d'intégrer de nouvelles technologies.

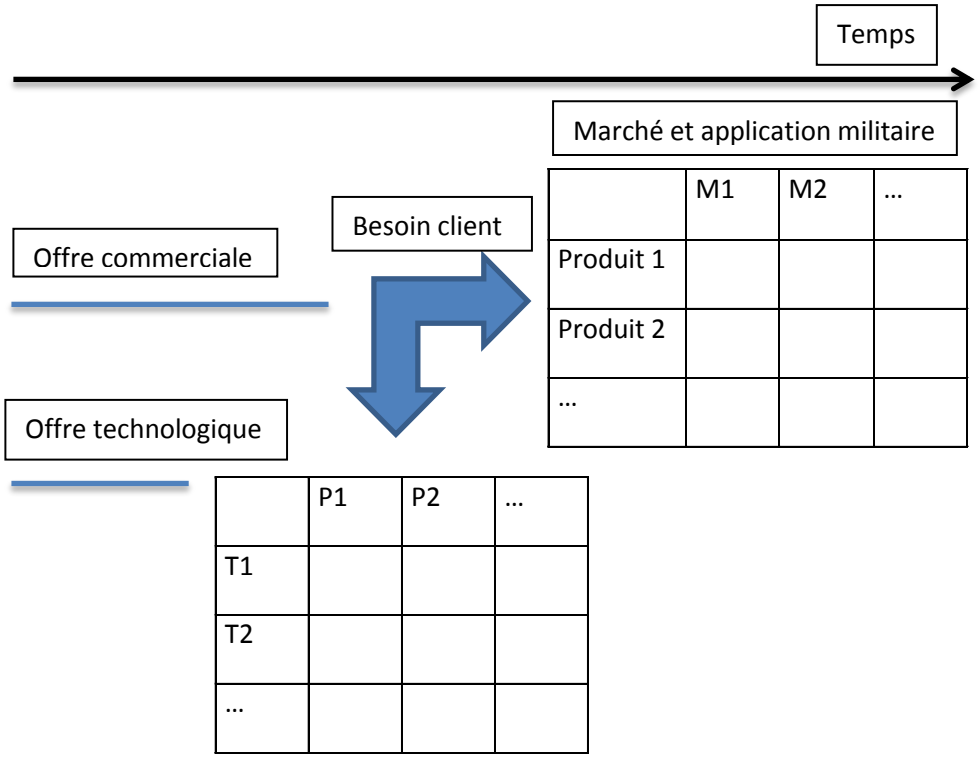
[45] Michael E. Porter, *Competitive Strategy*, Free Press, New York, 1980. Ce livre a été élu 9e livre de *management* le plus influent du XXe siècle par les Membres de l'*Academy of Management*.

Les pratiques collaboratives pour le développement des produits de demain

La feuille de route (roadmap technologie-produit)

Intéressons-nous plus particulièrement aux pratiques de planification produit-technologie. Une pratique communément répandue dans les entreprises de la défense pour planifier le développement des nouveaux produits est la feuille de route, appelée également *roadmap* technologie-produit[46]. Motorola, une société à forte intensité de R&D, pionnière dans le domaine des méthodes de gestion de l'innovation, semble être la première à avoir formalisé l'approche *roadmap*. Selon Motorola, le *roadmapping* permet de produire « un plan stratégique produit qui est argumenté, suivi et mis à jour au fur et à mesure du changement des relations entre la technologie et le marché ». La feuille de route est une cartographie à court terme et long terme de solutions technologiques pour répondre à de futurs besoins. Elle permet de lier les chemins des technologies aux produits qui eux-mêmes répondent à des besoins opérationnels[47]. Le schéma suivant en donne une illustration de principe.

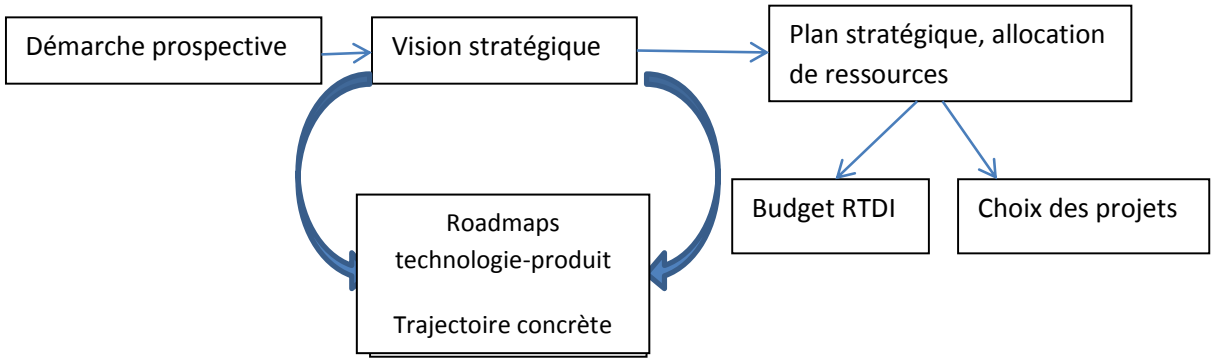
Graphique 2. *Roadmap* technologie-produit



[46] Robert Phaal, Clare Farrukh et David Probert, *Technology Roadmapping: Linking Technology Resources to Business Objectives*, Centre for Technology Management, University of Cambridge, 2001.
[47] Robert Treitel, « Orienter et planifier la technologie par le *roadmapping* », 2003, disponible sur : http://www.ig-a.com/articles/index.htm.

Cette pratique permet de planifier le développement des nouvelles technologies, en le traduisant en actions concrètes et en formulant un plan explicite pour disposer des bonnes ressources technologiques au bon moment. Elle constitue le nerf central de la capacité d'innovation, au sens large du terme, d'une entreprise. La feuille de route sert à informer, aligner et synchroniser tous les acteurs de l'entreprise qui devront contribuer au lancement des nouveaux produits[48]. Autrement dit, la feuille de route est une pratique qui permet d'allonger l'horizon de vision d'une entreprise. Réalisée de manière efficace, elle permet de mettre en lumière des opportunités technologiques et marketing, des vulnérabilités, des potentiels ainsi que des risques. La feuille de route s'inscrit dans le cœur de métier de l'entreprise et permet également de la faire converger vers des objectifs de rentabilité. La trajectoire à définir est transversale et prospective car elle concerne plusieurs fonctions de l'entreprise, suivant le schéma suivant :

Graphique 3. Plan stratégique des allocations de ressources

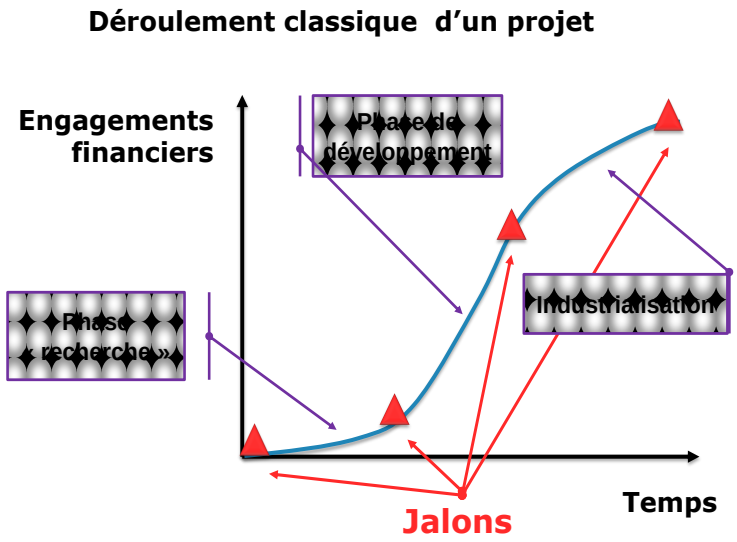


Pour assurer le succès de sa réalisation, la feuille de route doit être guidée par un dirigeant qui a une vision et s'appuyer sur un réseau de compétences à la fois internes et externes ainsi que des ressources[49]. Il faut en général attendre la 2e ou la 3e génération de feuille de route soutenant un même produit pour obtenir des résultats réellement satisfaisants, engendrés par des échanges multiples avec la direction et les services technico-fonctionnels. Deux grandes catégories de feuilles de route existent : les **feuilles de route ciblées** avec un client ou un marché identifié, et les **feuilles de route exploratoires** pour lesquelles il n'y a pas d'application *a priori*. La feuille de route nécessite une mise à jour périodique pour détecter les évolutions de l'environnement concurrentiel, en général, tous les 6 mois à 1 an.

Une fois les feuilles de route établies, les entreprises de la défense se donnent des règles de gestion pour les opérationnaliser à travers un référentiel qualité de gestion de projet. Un tel référentiel est propre à chaque firme, mais tout projet géré en entreprise se déroule généralement conformément au schéma ci-dessous, par phase et par jalon[50] :

[48] Robert Galvin, "Science Roadmaps", *Science,* vol. 280, n° 5365, 1998, p. 803.
[49] Dirk Bartelink, "Processes of the Future: The Roadmap Can Help Collaboration, but Shouldn't Stamp out Competition", *Solid State Technology*, vol. 38, n° 2, février 1995.
[50] Robert Cooper, "Perspective: The Stage-Gate Idea-To-Launch Process-Update, What's New, And Nexgen Systems", *Journal of Product Innovation Management*, n° 25, 2008, p. 213-232.

Graphique 4. Déroulement classique d'un projet



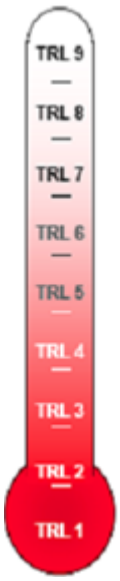
Lors du passage de chaque « jalon », des décisions importantes sont prises, engageant des dépenses parfois significatives. L'entreprise a besoin de mesurer et d'objectiver ces risques financiers pour les rendre acceptables pour la poursuite des projets. Le risque d'échec est d'ailleurs inhérent à la nature même de l'innovation[51]. Il est élevé en phase recherche et diminue progressivement lorsque les jalons sont passés avec succès, une démarche appelée « dérisking ». Pour gérer ce risque, l'entreprise doit donc se doter d'indicateurs de mesure.

Gestion du risque technologique : l'indicateur TRL

Toutes les entreprises de la défense utilisent les niveaux de maturité technologique[52] développés par la NASA en 1995. Le niveau de maturité d'une technologie est un indicateur largement utilisé par beaucoup de grands donneurs d'ordre occidentaux, militaires et civils comme le ministère de la défense britannique, la DGA en France, les grands avionneurs Boeing et Airbus, ou encore l'agence spatiale européenne. La mesure de la maturité réelle d'une nouvelle technologie permet de juger, à un instant donné, le risque encouru par le projet. Savoir mesurer la maturité d'une technologie, c'est donc savoir gérer les risques. Les TRL, décrits dans le schéma suivant, sont sur une échelle de 1 à 9 :

[51] Clayton Christensen, "The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail", Boston MA, Harvard University Press, 1997.
[52] En anglais, TRL pour *Technological Readiness Level.*

Graphique 5. Définition des niveaux de maturité TRL



Système réel « prouvé en vol » par des missions opérationnelles réussies
Système réel achevé et « qualifié en vol » par des tests et des démonstrations
Démonstration d'un prototype du système dans un environnement opérationnel
Démonstration d'un prototype ou modèle de système/sous-système dans un environnement représentatif (terre ou espace)
Validation de composants et/ou de maquettes en environnement représentatif

La Cour des comptes fédérale américaine a effectué de nombreuses études sur le sujet et a notamment édité deux rapports importants, l'un en 1998 et l'autre en 1999[53]. Dans les années 1990, le département de la défense américain a noté que les problèmes de développement de nouvelles technologies stratégiques étaient une cause importante d'augmentation des coûts et de retards des systèmes d'armements. Les durées de cycle d'acquisition d'armement américain étaient, en moyenne, de 10 à 15 ans, dépassant la durée de cycle de produits commerciaux classiques.
Cette longue durée se justifiait par la complexité des hautes technologies. Par exemple, le F-22 a eu presque 600 composants obsolètes alors que l'appareil était toujours en phase d'étude. Le laboratoire de recherches de l'armée de l'air américain a alors adopté les TRL pour mesurer la maturité de certaines technologies, depuis le démonstrateur jusqu'au système d'armement fini. Ce laboratoire a montré que la maîtrise de la maturité d'une nouvelle technologie était l'une des causes déterminantes du succès d'un système d'armement. En réponse à différents services étatiques américains, la Cour des comptes fédérale américaine a fait réaliser différentes évaluations, notamment l'impact de la maturité des technologies sur le taux de défaillance des nouveaux produits en opération. À partir de ce retour d'expérience, elle a recommandé au secrétaire à la défense américain qu'il adopte une approche fondée sur l'évaluation de la maturité d'une nouvelle technologie, à partir des indicateurs de TRL, point à partir duquel une harmonisation est réalisée entre la ou les nouvelles technologies stratégiques et les conditions de systèmes d'armement.

La maturité d'une technologie doit d'abord être évaluée avant d'être incorporée dans un système ou un sous-système d'armement. D'une façon générale, quand une nouvelle technologie est inventée, elle trouve rarement à s'appliquer immédiatement.

[53] GAO/NSIAD-56, "Best Practices: Successful Application to Weapon Acquisitions Requires Changes in Dod's Environment", 24 février 1998.
GAO/NSIAD-162, "Best Practices: Better Management of Technology Development Can Improve Weapon System Outcomes", 30 juillet 1999.

Par exemple, l'exosquelette, inventé par la société RB3D[54], issu d'une technologie de rupture en domotique, illustre bien ce phénomène car cette invention cherche actuellement des applications aussi bien dans le domaine civil que militaire. À partir d'une démarche de recherche, une nouvelle technologie est habituellement soumise à l'expérimentation, à l'amélioration puis à l'essai avant d'être vendue à un client.

Les indicateurs de TRL présentent toutefois des avantages et des inconvénients. Ainsi, ils donnent de la lisibilité aux feuilles de route et une compréhension commune du statut d'une technologie. Ils facilitent la gestion et la prévention du risque, et aident une organisation à prendre des décisions sur l'adoption d'une nouvelle technologie. Intégrés dans les référentiels qualité des entreprises de la défense, ces chiffres leur permettent de disposer d'un référentiel objectif d'avancement des projets technologiques. De plus, l'estimation d'un niveau de TRL peut être réalisée en un temps relativement bref (une réunion de deux heures avec quelques participants). Les règles et les critères de franchissement des niveaux de TRL sont propres à chaque entreprise et à chaque type de technologie. Si une cible de TRL est identifiée, l'analyse peut être réalisée en écart par rapport à cette cible. En outre, la demande de lisibilité par les clients « défense » est croissante et cet indicateur permet d'objectiver la maturité d'une technologie.

Dans le même temps, le niveau de TRL dépend du contexte du projet. Si le périmètre du projet change au cours du temps, le niveau de maturité peut également évoluer, augmenter ou diminuer. Une mesure de TRL doit donc être prise dans la globalité du projet. Si les critères de passage de TRL sont mal définis, le résultat de la mesure peut être relativement subjectif et parfois « orienté ». L'utilisation des TRL nécessite la détermination d'éléments techniques clés[55] et l'identification claire du contour technique du projet. L'une des difficultés est de déterminer à quoi la technologie développée va s'appliquer car le niveau de maturité peut différer. Il est donc nécessaire de préciser la ou les applications militaires envisagées. Par exemple, les environnements thermomécaniques sont différents pour un produit aéroporté sous avion et un produit pour une application terrestre. Le tableau suivant précise, dans le cas d'une entreprise de la défense interviewée, la nature de l'environnement et l'élément influençant le niveau de maturité d'une technologie :

[54] RB3D, une jeune société auxerroise, a développé un robot collaboratif capable d'accompagner les mouvements de son utilisateur tout en décuplant ses forces. Cet exosquelette a été présenté au salon Milipol (salon dédié à la sécurité) qui se tenait du 18 au 21 octobre 2011 à Paris. Ce projet a été financé par la DGA.

[55] Un élément technique est dit « clé » si le produit ou le système considéré pour l'évaluation dépend de lui pour atteindre ses fonctionnalités principales avec un coût et une durée de développement, ainsi que des coûts de production acceptables.

Tableau 1. Éléments influençant le niveau de maturité d'une technologie

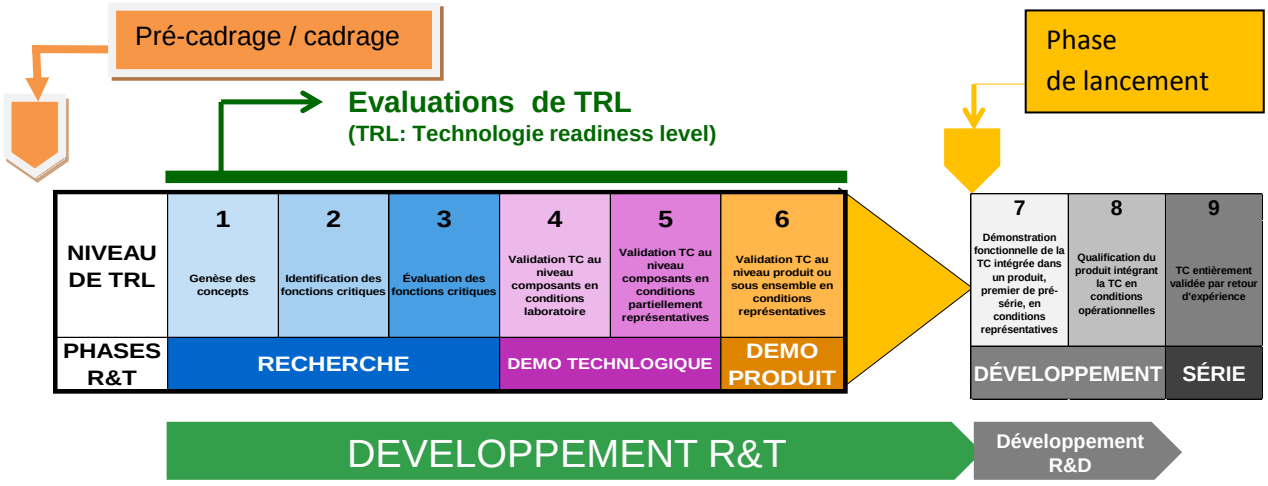
Nature de l'environnement	Éléments impactant le niveau de maturité d'une technologie
Environnement physique	nouveaux composants mécaniques, nouveaux processeurs, nouvelle électronique ; nouvel environnement thermique, vibratoire, climatique, chimique
Performance technique	exigence de performance à un niveau jamais encore réalisé pour telle ou telle fonctionnalité
Environnement logique	nouvel algorithme, redéveloppement logiciel significatif
Environnement des données	nouveaux formats de données ou de bases de données, exigence de vitesse de transfert, nouvelle mise en forme des données
Environnement humain	compétences des développeurs différentes, nouvel environnement de production (*off-shore*), …

L'utilisation de l'indicateur TRL est donc au cœur des pratiques collaboratives pour le développement des produits et technologies de demain. De manière plus globale, les indicateurs TRL s'incluent dans le cadre de la gestion de projet dont nous allons aborder les pratiques.

La gestion de projet : définition d'un référentiel entreprise

La gestion de projet nécessite un cadre bien établi. Le schéma ci-dessous décrit le processus de gestion de projet classiquement utilisé par les entreprises de la défense :

Graphique 6. Processus de gestion de projet



Une fois le développement R&T arrivé à maturité, au niveau TRL 6, la R&D prend alors le relais pour assurer le développement jusqu'à la mise en série du système d'armement. Toutes les entreprises de la défense se sont dotées ces dernières années d'un référentiel qualité de gestion de projet, permettant de gérer leurs projets de manière générale. Ce référentiel propre à chaque entreprise permet de définir la nature des jalons, afin de valider formellement le passage ou non d'une phase à l'autre. Il formalise, simplifie, rationalise la répartition des rôles et des responsabilités de l'équipe projet sur tout le cycle de vie du produit. Le chef de projet est alors responsable de la planification des jalons qui sont tous obligatoires. Les jalons du projet précèdent les jalons externes imposés par les donneurs d'ordre, comme la DGA. Ce référentiel permet d'assurer la cohérence du projet.

2.3.1 Les phases de pré-cadrage et de cadrage : préparation du lancement du projet

Le passage de tous les jalons s'effectue de façon formelle suite à une « revue » de passage de jalons, permettant un examen critique des résultats obtenus pour toutes les composantes du projet, sur la base de preuves, à un moment donné. Ces « revues » permettent d'identifier collectivement les risques et d'anticiper ceux à venir. Le référentiel définit une "*check-list*" de revue qui répertorie les livrables attendus. Les acteurs au sein de l'équipe projet ont alors pour rôle de collecter les informations nécessaires au franchissement des jalons.

Avant tout lancement de projet, une revue de pré-cadrage, de cadrage et de convergence de cadrage interne est nécessaire pour préparer son lancement. Le tableau ci-dessous en présente les différents objectifs :

Tableau 2. Les objectifs de chaque phase pour la préparation du projet

Phase	**Objectifs**
Pré-cadrage	- Identifier le besoin pour le nouveau produit - Définir les objectifs et les options (économiques, techniques, industriels, etc.) - Évaluer le marché potentiel - Vérifier la mise en place de l'équipe projet
Cadrage	- Valider le besoin et le marché - Vérifier la conformité à la stratégie de la société - Analyser et statuer sur la disponibilité des ressources et des compétences - Vérifier l'identification et le traitement des risques
Convergence de cadrage	- Vérifier que la proposition répond au besoin du donneur d'ordre - Vérifier que la proposition est compétitive commercialement - Vérifier que le choix des nouvelles technologies est validé - Vérifier que le plan de réduction des risques a été défini et engagé - Vérifier la mise en place de la stratégie industrielle - Vérifier que la proposition est en adéquation avec les ressources et les compétences attribuées au projet - Statuer sur la faisabilité et la rentabilité du projet

Une fois la convergence du cadrage faite, la revue de lancement du projet peut être réalisée au sein de l'entreprise. La phase de lancement d'un nouveau projet est toujours critique.
Elle doit vérifier la prise en compte des évolutions du besoin du client, avec la mise à jour du planning et des livrables, s'assurer que les ressources et les compétences sont bien allouées et définir la stratégie de mise en place du schéma industriel, avec notamment la sélection des fournisseurs.
Le plan de développement en est la pierre angulaire car il permet de définir la logique interne du projet dans son exécution. Il doit être validé par les donneurs d'ordres. Une fois cette phase passée, le développement R&D peut démarrer.

La phase de développement R&D

La phase de développement R&D possède également 5 phases internes : (1) conception préliminaire, (2) la conception détaillée, (3) la préparation à la production série, (4) le lancement de la production série et (5) l'aptitude à l'entrée en service du produit.

Tableau 3. Les objectifs de chaque phase pour le développement R&D

Phase	**Objectifs**
Conception préliminaire	- Valider les choix technologiques et vérifier que la conception technique préliminaire et l'industrialisation préliminaire sont conformes aux exigences du client ainsi qu'aux objectifs de coût et de maintenabilité
Conception détaillée	- Vérifier que la conception est industrialisable en interne et chez les fournisseurs - Valider les aspects juridiques avec les fournisseurs « série » - Valider les plans de qualification (essais, tests, etc.) et la certification - Vérifier que la conception du produit répond aux exigences de coûts, de qualité, de délai et de performance
Préparation à la production série	- Valider les éléments du dossier industriel - Valider la définition de la mise en place des moyens industriels nécessaires à la production - Maîtriser la chaîne d'approvisionnement (pouvoir produire de façon itérative, conformément à la cadence voulue)
Lancement de la production série	- Vérifier que le produit est utilisable par le client en environnement réel - Vérifier les résultats des essais de qualification/certification et les limitations éventuelles - S'assurer que la qualification et/ou la certification sont cohérentes avec les exigences client/autorités compétentes - Mettre en place les supports nécessaires au client (documentation, service de MCO) - Vérifier les moyens industriels et la chaîne logistique
L'aptitude à l'entrée en service du produit	- Vérifier l'obtention de la certification et la maîtrise des actions - Vérifier l'efficacité de l'organisation série et du support client

Nous pouvons noter que certains référentiels prévoient également l'exploitation et la capitalisation du retour d'expérience sur le produit, en vue de planifier des travaux d'amélioration (réduction des coûts, gestion des obsolescences).

Discussion

Un référentiel qualité projet définit les exigences et les recommandations qui s'appliquent au projet depuis l'appel d'offres jusqu'au retrait du produit. Il est construit selon des logiques de processus et de description de fonctions afin de pouvoir être mis en œuvre, quels que soient l'organisation et le produit considéré.
Au-delà, le référentiel apporte un cadre et un langage communs profitables à tous, en externe, aux clients et aux fournisseurs et partenaires ; en interne, aux équipes ainsi qu'aux sociétés internes à un groupe associant plusieurs d'entre elles. Un tel référentiel s'inscrit dans la politique qualité de l'entreprise et dans la démarche de progrès continu. Il vise précisément à hisser des pratiques en matière de gestion des projets au meilleur niveau de l'état de l'art et à combler les disparités qui existent entre les acteurs d'origines différentes. L'appropriation d'un tel référentiel par les acteurs du projet se fait à travers un dispositif de formation de l'entreprise, établissant des « règles d'or » de la gestion. Notre analyse du terrain nous a permis de retenir 5 règles d'or : (1) maintenir à jour le plan de gestion de projet, (2) être conforme aux exigences, (3) planifier et respecter les jalons, (4) piloter la performance économique et, (5) maîtriser les risques. La construction et la validation d'un tel référentiel concernent toutes les entités opérationnelles de l'entreprise et se diffusent à travers les réseaux de l'entreprise. La tenue des jalons et la maîtrise des livrables en coût et en performance technico-économique sont des leviers majeurs de compétitivité. Le jalonnement structure et discipline, dans la durée, toutes les activités du projet et induit naturellement l'amélioration continue. La référence constante aux fondements de la conduite de projets est un vecteur majeur pour gagner en efficacité et satisfaire les clients. De plus, un tel référentiel possède une capacité d'agilité puisqu'il s'adapte au contexte de chaque projet.

Discussion générale et perspectives

Les mutations de l'économie de défense conduisent les entreprises à adapter leurs pratiques existantes pour améliorer la gestion de l'innovation technologique. Nous observons que les pratiques existantes, telles que le *roadmapping*, l'utilisation des TRL et les référentiels qualité de gestion de projets, sont bien ancrées au sein des entreprises de la défense et que peu de nouvelles pratiques ont été identifiées. Les pratiques existantes consistent à augmenter la visibilité de l'entreprise qui engage des dépenses importantes dans l'innovation technologique pour satisfaire ses clients.

L'entreprise doit être capable de gérer les risques au sens large du terme. L'innovation technologique de rupture se caractérise toujours par un risque technique et commercial important, des perspectives incertaines, une taille de marché initiale faible. Le retour sur investissement est bien souvent loin des attentes à court terme. La réflexion stratégique est au cœur des pratiques de gestion de l'innovation technologique. Toutefois, les aspects commerciaux, de positionnement et économiques priment souvent sur les aspects technologiques. Mécaniquement, l'entreprise favorise les projets correspondant à une innovation technologique incrémentale consistant à améliorer les offres existantes. Ce constat est également soutenu par le besoin des entreprises de satisfaire en

priorité leurs clients existants. Le potentiel des innovations technologiques de rupture est souvent difficile à chiffrer, bien que la DGA incite les entreprises de la défense à innover vers la rupture. Il existe souvent une inadéquation entre les technologies de rupture et les marchés actuels[56].

Les attributs qui rendent une technologie de rupture inintéressante pour un marché établi sont souvent ceux qui constituent ses meilleurs atouts pour les marchés de demain. En effet, le client ne peut pas savoir ce qu'il attend d'une nouvelle technologie qui n'existe pas encore. Certaines recherches mettent en évidence qu'il est extrêmement complexe et coûteux d'extraire de l'information sur les besoins des utilisateurs et de la transférer dans l'entreprise, d'autant plus que les utilisateurs sont souvent bien incapables de formaliser leurs besoins de manière explicite[57]. Inversement, l'impact des innovations technologiques incrémentales est facile à chiffrer car elles sont réclamées par les clients actuels : un client veut en général toujours le même produit plus performant et moins cher.

Autrement dit, dans le mécanisme rationnel d'allocation de ressources et des compétences de l'entreprise, l'innovation technologique incrémentale est privilégiée au détriment de l'innovation technologique de rupture. De plus, le chiffre d'affaires issu des technologies de rupture est en général très faible dans les premières années. Celles-ci ne constituent donc pas de vrais relais de croissance à court terme et, par conséquent, l'entreprise ne s'y intéresse pas ou peu. Cependant, les innovations technologiques de rupture qui changent les industries n'arrivent en fait pas si souvent. Faut-il rechercher l'innovation technologique de rupture à tout prix ? Ne vaut-il pas mieux bien gérer l'innovation technologique incrémentale et explorer des pistes de croissance autour de son cœur de métier pour limiter le risque ?

Depuis ces dernières années, les entreprises de la défense ont mis en place des démarches d'amélioration pour s'adapter aux mutations de l'économie de défense, constituant de nouvelles pratiques. Celles-ci restent malheureusement limitées du fait de freins culturels importants. Le terme amélioration s'entend au sens large, comprenant l'amélioration technologique et non technologique. Les entreprises de la défense s'orientent notamment vers la création d'espaces dédiés à la créativité comme des espaces « osez innover », d'incubateurs d'idées, l'utilisation de réseaux sociaux d'entreprise, de démarches d'innovation participative qui récompensent les meilleures idées ou de démarches d'amélioration LEAN SIGMA qui visent à améliorer la performance économique de l'entreprise. L'investissement dans l'amélioration continue est devenu une nouvelle pratique au sein de la gestion de l'innovation technologique et une forme de rempart contre les mutations de l'économie de défense.

[56] Jean-Yves Prax, Bernard Buisson, Philippe Silberzahn, *Objectif : innovation*, édition Broché, 2005.

[57] Eric Von Hippel, "Learning from Lead Users", *In* : Robert D. Buzzell, *Marketing in an Electronic Age*, Boston, Harvard Business School Press, 1985, p. 308-17 ; Eric Von Hippel, ""Sticky Information" and the Locus of Problem Solving: Implications for Innovation", *Management Science,* n° 4 (40), avril 1994, p. 429-439.

Références

BARTELINK Dirk, "Processes of the Future: The Roadmap Can Help Collaboration, but Shouldn't Stamp out Competition", *Solid State Technology*, vol. 38, n° 2, février 1995.

CHRISTENSEN Clayton, "The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail", Boston MA, Harvard University Press, 1997.

COOPER Robert, "Perspective : The Stage-Gate Idea-to-Launch Process-Update, What's New, and Nexgen Systems", *Journal of Product Innovation Management*, n° 25, 2008, p. 213-232.

ESCORSA CASTELLS Pere, CRUZ JIMÉNEZ Elicet et GUIXÉ SIMÓN Jordi, « Les Relations entre la prospective, la veille technologique et les schémas technologiques (*Roadmaps*) », *Conference Paper : VSST 2004*, Toulouse, 2004.

GALVIN Robert, "Science Roadmaps", *Science*, vol. 280, n° 5365, 1998, p. 803.

GAO/NSIAD-56, "Best Practices: Successful Application to Weapon Acquisitions Requires Changes in Dod's Environment", 24 février 1998.

GAO/NSIAD-162, "Best Practices: Better Management of Technology Development Can Improve Weapon System Outcomes", 30 juillet 1999.

PHAAL Robert, FARRUKH Clare et PROBERT David, *Technology Roadmapping: Linking Technology Resources to Business Objectives*, Centre for Technology Management, University of Cambridge, 2001.

PORTER Michael E., *Competitive Strategy*, New York, Free Press, 1980.

PRAX Jean-Yves, BUISSON Bernard, SILBERZAHN Philippe, *Objectif : innovation*, édition Broché, 2005.

TREITEL Robert, « Orienter et planifier la technologie par le *roadmapping* », 2003, disponible sur : http://www.ig-a.com/articles/index.htm.

VERSAILLES David W., MÉRINDOL Valérie et CARDOT Patrice, *La Recherche et la technologie, enjeux de puissance*, Economica, 2003.

VON HIPPEL Eric, "Learning from Lead Users," *In*: BUZZELL Robert D., *Marketing in an Electronic Age*, Boston, Harvard Business School Press, 1985, p. 308-17.

VON HIPPEL Eric, ""Sticky Information" and the Locus of Problem Solving: Implications for Innovation", Management *Science*, n° 4 (40), avril 1994, p. 429-439.

PRESENTATION DES AUTEURS

Lucie BERAUD-SUDREAU

Lucie Béraud-Sudreau est doctorante en sciences politiques, à l'Université Paris 2 Panthéon-Assas. Elle a été chercheuse invitée au Stockholm International Peace Research Institute (SIPRI). Ses recherches portent sur les politiques de défense et d'armement en France et en Suède, et sont financées par une bourse de la Direction générale de l'armement (DGA). Elle a publié récemment dans la revue Gouvernement et action publique et la rubrique "Paris Paper" de l'IRSEM.

Dr. Vincent BOULANIN

Vincent BOULANIN est chercheur au Stockholm International Peace Research Institute (SIPRI) depuis 2008. Il s'intéresse aux questions relatives à la production, à la prolifération et au contrôle des nouvelles technologies militaires et de sécurité. Sa thèse de doctorat défendue en octobre 2014 à l'EHESS a porté sur la diversification de l'offre des firmes d'armement en matière de sécurité.

Danilo D'ELIA

Danilo D'Elia est doctorant à l'Institut français de géopolitique de l'université Paris VIII Vincennes-Saint-Denis et chercheur associé à la chaire Castex de cyberstratégie. Il est titulaire d'une convention CIFRE avec Airbus Defence & Space- Cybersecurity. Ses travaux de recherche portent sur les représentations et les rivalités de pouvoir entre acteurs de la sphère publique et du monde privé dans la mise en place de la stratégie française de cybersécurité des infrastructures critiques.

Alix DESFORGES

Alix Desforges est doctorante à l'Institut français de géopolitique où elle a obtenu son Master de géopolitique en 2009 et chercheuse au sein de la chaire Castex de cyberstratégie. Sa thèse analyse la géopolitique du cyberespace et les enjeux pour la sécurité du territoire français. Allocataire de l'Institut de recherche stratégique de l'École militaire (IRSEM) pendant deux années, ses recherches en thèse ont également bénéficié du soutien financier de l'IHEDN sur la même période.

Paul HERAULT

Paul Hérault réalise une thèse en Sciences économiques à l'université Paris-Dauphine sur l'internationalisation des chaînes de valeur dans l'industrie de défense. Il s'agit plus précisément d'étudier l'impact de l'internationalisation des chaînes d'approvisionnement civiles ou « duales » sur les filières militaires ainsi que l'adaptation des entreprises de défense à l'évolution des stratégies

d'acquisition des États-clients (exigences de contenu local et de transferts de technologie). Cette thèse a été initiée dans le cadre d'une Convention CIFRE entre DCNS et l'Université Paris-Dauphine. Monsieur Hérault est diplômé de Sciences Po Paris et de l'Université Paris-Dauphine.

Dr. Sophie LEFEEZ

Sophie Lefeez est docteur en sociologie des techniques de l'université Paris I Panthéon-Sorbonne et rattachée au Centre d'études des techniques, des connaissances et des pratiques (CETCOPRA). Elle est diplômée en science politique et en économie. Après avoir entamé une carrière militaire, elle reprend des études et exerce divers métiers avant de revenir aux questions de défense. Elle s'est récemment tournée vers les matériels militaires, comme un faux détour par les objets pour mieux parler des humains. Sa thèse porte sur les choix techniques dans la conception des matériels militaires et fut financée par EADS Innovation Works.

Dr. Hugo MEIJER

Hugo Meijer est *Lecturer* en études de défense, au King's College London. Docteur en Science politique, associé au Centre d'Études et de Recherches Internationales (CERI) de Sciences Po, il a été chercheur postdoctoral à l'Institut de recherche rtratégique de l'École militaire (IRSEM), *Visiting Scholar* au Sigur Center for Asian Studies de George Washington University et Attaché Temporaire d'Enseignement et de Recherche (ATER) en Science politique à l'Université de Montpellier 1.

Alice PANNIER

Alice Pannier est doctorante en Relations internationales à Sciences Po Paris (Centre d'études et de relations internationales, CERI) et au King's College London (*War Studies*). Ses travaux portent sur la coopération entre la France et le Royaume-Uni dans le domaine de la défense dans le cadre des Traités de Lancaster House, et bénéficient du soutien du programme franco-britannique de thèses de la DGA et du DSTL. Diplômée de King's College London et de l'Université Panthéon-Sorbonne, elle a également travaillé à l'Institut français des relations internationales (IFRI) ainsi qu'au ministère de la défense.

Jérôme ROSELLO

Jérôme Rosello est doctorant en science de gestion à l'École doctorale de management Panthéon Sorbonne (EDMPS - ESCP Europe) et travaille dans les démarches d'améliorations continues au sein de l'entreprise Sagem Défense Sécurité, groupe Safran. Diplômé en physique de l'université Polytechnique d'Orléans et d'un master en management de l'ESCP-Europe, Jérôme Rosello a travaillé sur de nombreux programmes militaires R&D puis R&T au cours de ces 15 dernières années. Depuis 2010, il conduit des travaux de recherches en management de l'innovation. Il est associé aux travaux

de l'IRSEM et de l'IHEDN et a participé également à des groupes de réflexions sur la stimulation de l'innovation en entreprise, notamment avec le CGARM, la MRIS et la 3AF.

Emma SOUBRIER

Emma Soubrier est doctorante en Science politique à l'université d'Auvergne et rattachée à l'Institut de recherche stratégique de l'École militaire (IRSEM). Depuis 2008, elle a développé une expertise régionale sur le Moyen-Orient grâce à des travaux de recherche, des expériences de terrain et la maîtrise de la langue arabe. Elle s'est par ailleurs spécialisée dans les questions de défense et de sécurité. Alliant ses domaines de compétence et aires géographiques de prédilection, sa thèse porte aujourd'hui sur l'évolution de la politique de défense et des stratégies d'acquisitions militaires du Qatar et des Emirats arabes unis. Cette recherche est rendue possible par le soutien de la Délégation générale pour l'armement (DGA) et l'entreprise Airbus Defence & Space.

ETUDE DE L'IRSEM N°38

QUELLES STRATÉGIES FACE AUX MUTATIONS DE L'ÉCONOMIE DE DÉFENSE MONDIALE ?

Cette étude est le fruit d'une réflexion initiée en 2012 au sein du groupe des jeunes chercheurs en « Armement et économie de défense » associés à l'Institut de recherche stratégique de l'École militaire (IRSEM). Il détaille les stratégies mises en place par les États et les entreprises dans le contexte des transformations qui affectent le marché de l'armement mondial et les budgets publics de défense depuis les années 1990.

La première partie de l'étude, centrée sur les États, montre pourquoi et comment ceux disposant d'une industrie d'armement de premier rang ont mis en œuvre des politiques visant à faciliter et soutenir les exportations de leurs entreprises, tandis que les États importateurs utilisent de plus en plus leur capacités d'acquisitions comme levier d'influence. D'autres pensent trouver dans la coopération un moyen de conserver des capacités industrielles, quitte à les partager. Enfin, l'évolution des menaces a provoqué un regain d'intérêt envers les politiques industrielles. Mais chacune de ces options comporte des difficultés que l'étude expose.

La seconde partie, consacrée à l'offre, montre comment et pourquoi les grands acteurs de l'industrie de défense ont élargi leur champ d'action en se tournant vers le secteur de la sécurité et en s'internationalisant davantage. Enfin, les postulats sous-tendant la quête de supériorité technique sont questionnés, d'autant que la logique de l'activité de production militaire tend à favoriser en réalité l'innovation incrémentale dans les entreprises de défense au détriment de l'innovation de rupture, recherchée pour l'avantage opérationnel qu'elle est censée conférer.

Sous la direction d'Aude-Emmanuelle FLEURANT

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE

IRSEM
Institut de Recherche Stratégique de l'École Militaire

École Militaire
1, place Joffre – Case 38 - 75700 Paris SP 07
http://www.defense.gouv.fr/irsem

ISSN : 2268-3194 - ISBN : 978-2-11-138931-1