EUROSATORY 2016 : QUEL AVENIR POUR L'ARMEMENT TERRESTRE?

QUEL AVENIR POUR L'INDUSTRIE EUROPÉENNE DE L'ARMEMENT TERRESTRE ?

CHRISTOPHE-ALEXANDRE PAILLARD
Directeur du domaine armement et économie de défense, IRSEM

Lancé pour sa première édition en 1967, le salon de l'armement terrestre baptisé Eurosatory se tient tous les deux ans à Villepinte, au nord de Paris. Il rassemble les principaux industriels français et étrangers de ce secteur industriel. L'édition 2016 est consacrée à « la solution terrestre et aéroterrestre ». Eurosatory est la première surface d'exposition de véhicules militaires, de systèmes anti-aériens toutes catégories ou de systèmes d'armes en Europe.

Ce salon est l'occasion de revenir sur l'industrie européenne de l'armement terrestre. Dans une note publiée le 13 juin 2006 à l'occasion d'une précédente édition d'Eurosatory et consacrée à l'industrie européenne des véhicules blindés, la Fondation pour la Recherche stratégique (FRS) estimait que « *les forces terrestres voyaient leur importance réaffirmée par rapport aux forces aériennes, notamment du fait des retours d'expérience essentiellement américains des opérations en Afghanistan et en Irak, et dans le cadre de la transformation. Du point de vue technico-opérationnel, il s'agit pour ces forces de maîtriser la mise en réseau des véhicules terrestres (par le biais de la numérisation de l'espace de bataille et de la communication entre l'ensemble des éléments hommes/machines), d'accroître la protection et la survivabilité des véhicules et des soldats, d'améliorer la mobilité terrestre et la fonction feu et de s'adapter au combat en zone urbaine* ».

Dix ans plus tard, ce constat reste parfaitement valable et se trouve largement conforté par l'ampleur des missions terrestres menées en Afrique subsaharienne par les forces françaises depuis 2013, pour ne prendre que ce seul exemple. Les besoins en armements terrestres restent considérables et l'instabilité qui demeure aux portes de l'Union européenne ne fait que souligner l'importance de maintenir une industrie de l'armement terrestre dynamique et répondant aux besoins opérationnels et capacitaires de nos forces armées. L'article proposé dans cette lettre de l'IRSEM par Nick Butler, professeur au King's College de Londres, sur la vision britannique de la défense européenne,- va dans le même sens et appuie l'intérêt d'un retour à une vraie réflexion sur les questions de défense européenne, et pas seulement dans l'armement terrestre.

L'absence de programmes européens structurants dans l'armement terrestre

Malgré l'ampleur des besoins capacitaires, force est de constater qu'en Europe, les cinq principaux axes d'une Europe de l'armement terrestre (programmes, institutions, règles juridiques, budgets, base industrielle et technologique de défense) sont bloqués pour l'essentiel. La dynamique de coopération des années 1970 et 1980 du dernier siècle, en lien avec les besoins des forces terrestres (avion de transport C160 Transall, hélicoptère Tigre, missiles, etc.), s'est éteinte. Aucun projet de coopération structurant, en particulier dans les domaines qui concentrent les principaux enjeux (les drones - sujet auquel fait référence l'article d'Océane Zubeldia et de Chantal Lavallée dans cette lettre de l'IRSEM -, les hélicoptères lourds ou le développement de projets de R&T), n'a effectivement été lancé ces quinze dernières années. Or, ce sont ces programmes qui entraîneront naturellement les regroupements industriels nécessaires entre des entreprises aussi diverses que KMW ou Nexter, comme le précise sur cette question l'article de Jean-Pierre Maulny, directeur adjoint de l'IRIS, consacré aux suites de l'accord signé le 29 juillet 2015 entre Philippe Burtin, PDG de Nexter, et Frank Haun, son homologue chez Krauss-Maffei Wegmann (KMW) et consacré au rapprochement entre ces deux entreprises de l'armement terrestre.

Comme l'a expliqué début 2015 à la commission de la défense de l'Assemblée nationale, le PDG de KMW, « *dans cinq ans, nous aurons avancé dans le processus de développement d'un nouveau char lourd – qu'il s'appelle Léopard 3 ou Leclerc, peu importe : il sera développé en commun, et pourra commencer à équiper nos forces à l'horizon 2025*

-2030 pour remplacer les chars Leclerc et Léopard 2 ».

Face à ces mutations industrielles, les structures institutionnelles de coopération créées ces trente dernières années, comme l'Agence européenne de défense (AED) ou l'OCCAR, ne jouent en réalité qu'un rôle limité. Les règles communautaires existantes ne favorisent pas les produits européens au titre d'une forme de « Buy European Act » en offrant un cadre dérogatoire aux dépenses de défense (article 296 du Traité relatif à l'Union européenne), alors que les mesures concrètes initiées par le « paquet Défense » auraient pu infléchir cette situation en faveur des produits et des industries de l'armement terrestre du continent européen (dans le cadre de ce « paquet Défense », les directives 2009/81/EC et 2009/43/EC instituent des règles de marchés publics adaptées aux spécificités de l'armement et destinées à faciliter les transferts intracommunautaires).

Au-delà des structures et des règles existantes, les avancées institutionnelles offertes par le traité de Lisbonne auraient pu offrir une fenêtre d'opportunité pour plus de coopération, mais la situation budgétaire de la plupart des États membres de l'Union européenne n'a pas entraîné de mutualisation des moyens, mais plutôt un repli national général, dans un contexte de crise de la dette, de crise des migrants et de crise identitaire d'échelle continentale.

Quels écueils éviter pour l'industrie européenne de l'armement terrestre ?

En l'absence de consolidation de l'industrie européenne de l'armement terrestre, trois écueils devraient impérativement être évités. C'est d'abord l'existence d'une « Europe des incompétences ». En effet, l'absence d'intérêt collectif européen sur ces questions, de la bonne tenue des délais de livraison des équipements au rapport qualité/coût des équipements pour les forces armées, et le maintien de stratégies nationales d'acquisition de compétences nationales au détriment de programmes en coopération, doit cesser. Le cas du logiciel de régulation du moteur de l'avion de transport A400M, confié à une société allemande insuffisamment qualifiée, fut révélé en 2009. Il a montré la nuisance d'une telle logique. De fait, les programmes européens ne sont pour l'instant pas moins chers que leurs équivalents nationaux, en raison notamment du principe de juste retour. Si un pays investit pour 20% du montant d'un programme, il exige le plus souvent au moins 20% du montant du programme en retombées économiques nationales. Ce principe a donc contribué à hausser le coût du programme A400M, en retenant également des entreprises qui n'étaient pas forcément les mieux qualifiées pour participer à ce programme très structurant d'Airbus.

Les États européens doivent aussi éviter l'écueil du mécano industriel. De fait, il n'existe pas de solution industrielle miracle. Les diverses formes de coopération entre industriels, comme la sous-traitance, la joint-venture, le groupe multinational ou multidomestique, sont toutes jugées fructueuses, si le contexte est économiquement et politiquement favorable. L'architecture industrielle de nos industries de l'armement terrestre doit être adaptée sur mesure aux programmes d'armement et non l'inverse.

Enfin, troisième écueil, la question est clairement posée du rôle assigné aux structures institutionnelles de l'Union européenne pour maintenir des compétences et des industries en Europe. Douze ans après sa création, la faiblesse des budgets des programmes de l'Agence européenne de Défense (AED) illustre surtout l'absence de volonté politique des États membres de l'Union d'avancer dans la direction d'une intégration de l'industrie européenne de l'armement terrestre. En lançant officiellement le programme Scorpion en décembre 2014, le ministère français de la Défense a montré sa détermination à faire travailler ensemble Nexter, Thales et Renault Truck Défense, pour le développement des futurs véhicules blindés de l'armée française destinés à remplacer les matériels existants du combat de contact. Cette initiative clef pour nos forces armées n'a toutefois pas de véritable équivalent ailleurs en Europe.

Cette situation ne remet pas en cause la nécessité d'un vrai marché européen de l'armement à l'échelle européenne, d'une nécessaire réflexion en amont sur nos besoins capacitaires communs et sur la conduite éventuelle de coopérations en matière de programmes de recherche à travers l'Europe.

Les besoins capacitaires et technologiques restent considérables

Comme l'expliquent très largement les articles de Nicolas Mazzucchi (IRSEM) consacré aux données, systèmes et capteurs et celui de Catherine Tessier (ONERA), consacré aux enjeux techniques de la robotisation sur le champ de bataille, les besoins restent effectivement considérables, justifiant l'intérêt que présente ce salon Eurosatory.

Quatre grands programmes d'équipement ont structuré l'industrie française de l'armement terrestre de ces dernières années : le programme FELIN (fantassin à équipements et liaisons intégrés) qualifié le 30 avril 2010, le programme CAESAR (camion équipé d'un système d'artillerie), le programme de VBCI (véhicule blindé de combat d'infanterie) et le programme d'hélicoptères de combat TIGRE.

Pour les prochaines années et pour la seule armée de terre française, les besoins couvrent le drone tactique, dont le contrat a été remporté par Sagem en février 2016, un nouveau véhicule blindé léger, le futur fusil de précision, etc. Or, comme avait tenu à le souligner le chef d'état-major de l'armée de terre (CEMAT) lors de son entretien avec les rapporteurs de la Commission de la Défense nationale et des Forces armées de l'Assemblée nationale, consacré à la revue capacitaire des forces armées, *« le milieu terrestre est celui dans lequel finissent par s'affronter physiquement toutes les volontés ».* C'est un « *milieu complexe* » où toute intervention est une combinaison de « *projection de puissance* » et de « *projection de force* ». « *La réactivité et la puissance opérationnelle de l'armée de terre reposent sur la cohérence de ses capacités et la complémentarité de ses équipements ».*

Pour conclure, si les prédictions en faveur d'un programme de char lourd commun franco-allemand telles que décrites par le PDG de KMW se confirmaient, il est évident qu'une telle action aurait une forte valeur symbolique pour l'harmonisation des besoins capacitaires entre l'Allemagne et la France. Cependant, cette question ne doit pas faire oublier d'autres projets qui doivent eux aussi avancer. La volonté exprimée en 2015 de fabriquer à trois pays (Allemagne, France et Italie) un drone MALE de troisième génération « made in Europe », si elle se confirmait, serait également un signal positif en faveur du maintien des capacités industrielles et technologiques européennes.

Cette lettre de l'IRSEM consacrée à ces enjeux européens et à l'armement terrestre permet donc de faire un tour d'horizon ciblé, en appelant l'attention de nos lecteurs sur ce qui est aujourd'hui à la pointe de l'actualité dans ces domaines industriels.

European defence: a British point of view

Professor Nick Butler

King's College

Defence policy, for any country, is driven by the combination of history, the current perception of threats and the financial capability of the national government. For Britain history weighs heavily in the mix – not always to the benefit of national security and defence.

Britain is no longer an imperial power or even a great power on most definitions. Its current interests are in maintaining trade links and protecting its own territory particularly from the risks of terrorism. It has obligations to its allies in NATO which involve deterrence as well as the maintenance of a capability to deploy forces and to intervene when necessary. Britain also has a commitment to assist in humanitarian crises where the deployment of forces can often make a crucial difference.

The requirement is therefore for flexibility, specialist skills and the ability to deploy the most advanced technology. The adjustment to this position from the large scale global military presence which the current generation inherited is proving a slow and painful task. The last two decades have demonstrated the limits both of the UK's power in the world and its financial capability to fulfil all the objectives and commitments it has taken on. In a time of austerity the UK struggles to meet its formal NATO commitment to spend 2 per cent of GDP on defence and has had to find creative ways of making the numbers add up. It is not clear to objective observers whether the payment of military pensions for instance should be counted as genuine defence spending.

The last two decades – including two wars in the Middle East and a botched intervention in Libya – have demonstrated both that initial military victories do not bring lasting security and that the UK (along with many others) lacks the will and financial resources to undertake the essential task of nation building. The net results – in Iraq, in Afghanistan and most of all in Libya – discourage Governments and the British public from acts of intervention which could make a difference. The worst impact of this has been felt in Syria where the failure to intervene contributed to the continuing refugee crisis. Along with its allies the UK struggles to understand how to cope with civil conflicts in countries which defy attempts to impose quick solutions but which if left to fester can produce lasting threats including the threat of radicalisation in communities within our own country.

The change in the nature of the main security risk is matched by the growing awareness that the US, for perfectly rational reasons, has its own agenda which will not always include acting as the world's policeman. The UK has lived (not always happily) in the shadow of that protective role for the last half century. That dependence is now fading but has yet to be replaced.

For some the logic is to build a closer defence alliance with our European neighbours but again history intervenes. Relations – especially with France - are very good and there is much which could be done together. But bilateral cooperation and the creation of a single European defence and security policy are two very different things. Different European countries, again because of their history, have very different approaches to defence and security questions. A few are happy to deploy troops and to take the risk of open conflict. Most are not except in the event of a direct challenge to their national territory. Different countries have different relationships – for instance with Russia or the countries of the Middle East. A fully integrated defence policy can only come when there is a single European government and a single European culture. That, to use a very British form of understatement, is some way off.

For the moment then the UK muddles through. Our commitments outweigh our capabilities and the imbalance sur-

vives only for so long as the commitments are untested. Old alliances are changing and new alliances are not quite within reach. Technology is more important now than brute force particularly when it comes to challenges such as cyber security but it is fiendishly expensive. Special Forces – in which the UK specialises and takes great pride – can be devastatingly effective at the moment of deployment but they cannot build a new nation out of the broken pieces of Libya or Syria or provide the subtle deterrence needed to contain the complex ambitions of someone like President Putin.

All these challenges are recognised even if they have not yet been addressed. Money is perhaps the biggest constraint of all. Aircraft carriers without aircraft are a telling symbol of the gap between rhetoric and reality. Britain, along with France, has some of the best forces in Europe – well trained, honest, and brave. Sadly, however, they are underpaid, often live in squalid conditions and too often lack the equipment they would need to win a real and serious conflict. It is not clear whether the UK military now have the ability to win a war for the Falklands as they did in the early 1980s.

The lesson of all this is that the UK – in common with many of its allies -will only take defence seriously when it faced with a direct challenge to fundamental national interests. In all the recent conflicts – Iraq, Afghanistan and Libya – it has proved too easy to walk away when the going got too tough. The consequences for the countries concerned have been awful but the consequences within the UK itself have been minimal. The lesson taken from these episodes has been that intervention doesn't work and should be avoided. But there may come a time when intervention is imperative and when the threats are not thousands of miles away but far more immediate. We might hope such threats will never emerge but vague hopes are not a very solid base on which to build a defence and security policy. If the last few years tell us anything it should be that the world is a dangerous place and that the UK, in common with its European friends, lives in a tough neighbourhood surrounded by failed states and conflicts which can all too easily spread.

ENJEUX TECHNIQUES DE LA ROBOTISATION SUR LE CHAMP DE BATAILLE

DR. CATHERINE TESSIER
ONERA

Les robots qui sont utilisés sur le terrain de manière opérationnelle, en particulier dans le domaine militaire, sont actuellement contrôlés par des opérateurs, même s'ils disposent d'automatismes embarqués (par exemple pour le pilotage et le guidage).

On parlera d'*autonomie* dès lors que le robot aura la capacité de fonctionner indépendamment d'un autre agent (humain, autre machine) [THR+09], en exhibant des comportements non triviaux, dans des environnements complexes, dynamiques, imprévisibles [CERNA14]. Si l'on envisage de conférer au robot une plus grande autonomie, il convient de définir précisément quelles fonctions sont déléguées aux algorithmes et quelles fonctions restent sous le contrôle de l'opérateur humain, ce *partage de l'autorité* étant dynamique, c'est-à-dire variable selon les phases de mission. Ainsi l'autonomie n'est pas une propriété intrinsèque du robot : sa conception et sa mise en œuvre doivent être considérées dans le cadre d'une collaboration homme-machine [DSB12] ; la machine n'est jamais isolée, et il y a toujours, sous une forme ou une autre, une implication de l'être humain.

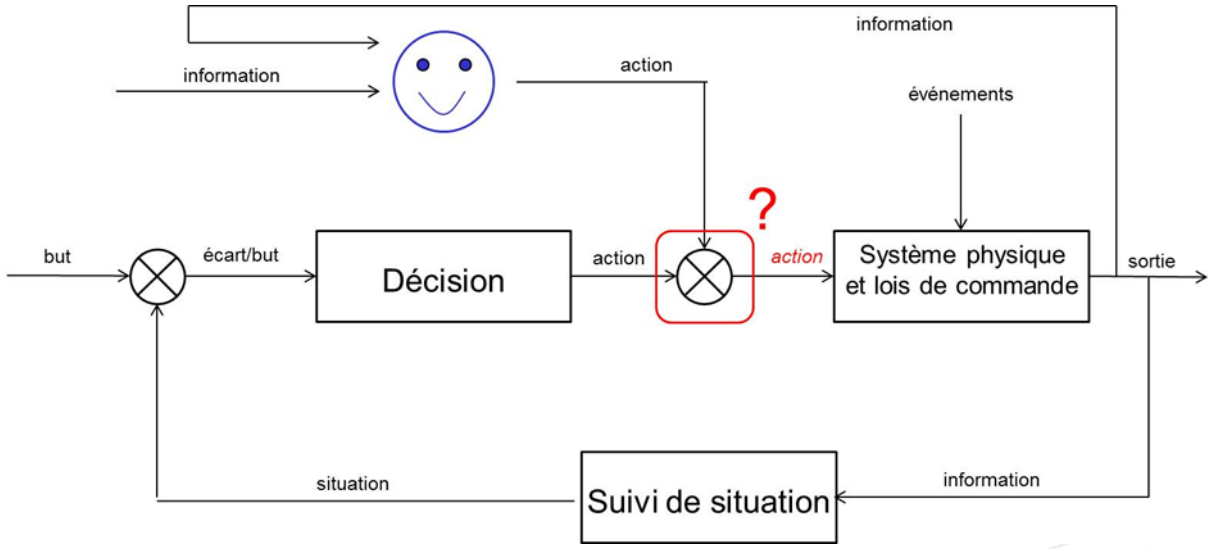


Figure 1 : la question du partage de l'autorité [Tes15]

Le partage de l'autorité entre un opérateur humain et un robot équipé de fonctions décisionnelles pose un certain nombre de questions techniques, relatives aux fonctions décisionnelles du robot, à l'opérateur humain, et à l'interaction entre l'opérateur et le robot [CERNA14, Tes15].

Les fonctions décisionnelles du robot sont assurées par des algorithmes capables d'interpréter et d'évaluer la situation, et de calculer des décisions. Le *suivi de situation* est réalisé à partir de données acquises par les capteurs du robot, des connaissances dont il dispose, et de modèles d'interprétation et d'évaluation. Ces connaissances et modèles permettent d'interpréter les données acquises, de les agréger sous forme de nouvelles connaissances, de déduire des relations entre ces connaissances. Il convient alors de se demander comment les modèles sont définis, quelles sont leurs limites (en particulier permettent-ils de caractériser correctement une situation, par exemple en regard de la propriété de discrimination ?), comment les incertitudes sont prises en compte, et comment valider, voire certifier, de tels modèles. La *décision* est calculée sur la base de la situation élaborée et évaluée et de ses potentielles évolutions dans le futur, ainsi que de modèles des actions décrivant pour chacune d'elles les précondi-

tions, les ressources requises, la durée, les effets. Les questions qui se posent relativement au calcul de la décision concernent la nature des critères permettant d'orienter ce calcul, comment ils sont agrégés s'il y en a plusieurs et s'ils sont antagonistes, comment se définit une action « adaptée » à la situation, en particulier si des critères d'ordre moral sont considérés.

L'opérateur est doté des capacités d'invention, de jugement, que ne possède pas une machine. Face à des situations qu'il juge « difficiles », il pourra différer ou déléguer sa décision, abandonner des buts, demander des informations supplémentaires ou des conseils, imaginer des solutions originales. Cependant l'opérateur ne doit pas être considéré comme le recours absolu « quand la machine ne sait pas faire », parce qu'il a lui aussi ses limites, et un certain nombre de facteurs peuvent altérer ses capacités d'analyse et de décision. En particulier il peut être soumis au phénomène de tunnélisation attentionnelle [RDR+14] ou focalisation excessive de l'attention sur une partie des informations au détriment de toutes les autres, au phénomène de *Moral Buffer* [Cum06] ou distanciation morale par rapport aux actions du robot, au phénomène de biais de confiance (*Automation bias* [Cum06]), c'est-à-dire la tendance à s'en remettre aux décisions du robot et à ignorer d'autres voies possibles.

Dans le cadre d'un partage de l'autorité, l'opérateur et le robot (*via* ses fonctions décisionnelles) ont des capacités de décision quant aux actions du robot. Dans certaines situations, les décisions de ces deux agents peuvent entrer en conflit, il s'agira alors de se demander si c'est la décision de l'opérateur qui doit toujours être retenue au détriment de celle de la machine ou si les défaillances possibles de l'opérateur peuvent être prises en compte par la machine et de quelle façon. Cela amène à se poser la question de la possibilité de reprise en main, par la machine, du contrôle de certaines fonctions du robot, au détriment de l'opérateur : une telle reprise en main doit se faire dans des circonstances bien définies, sur des critères précis, et ne pas occasionner chez l'opérateur le phénomène d'*Automation surprise* [SWB97] ou rupture dans sa compréhension de la situation due au fait que des décisions du robot ont été prises à son insu (par exemple parce que des actions ont été effectuées et n'ont pas été notifiées à l'opérateur, ou bien l'opérateur n'a pas perçu ces notifications).

Figure 2 : système de drone Ressac - ONERA

La répartition de l'autorité doit être clairement établie afin qu'à tout moment on puisse savoir quel agent a l'autorité sur telle fonction, quel agent prend une décision, à quel sujet et sur quelles bases. Cette connaissance est en particulier indispensable dans les situations où des responsabilités seront recherchées (dysfonctionnements, accidents). Enfin, compte tenu des différentes incertitudes portant sur l'interprétation de la situation, sur la décision et sur l'action, et compte tenu des défaillances possibles du robot et de celles de l'opérateur, la question – difficile – de la prévisibilité du système opérateur-robot est posée.

Références

[CERNA14] Commission de réflexion sur l'Ethique de la Recherche en sciences et technologies du Numérique d'Allistene – Éthique de la recherche en robotique. 2014 (http://cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf)

[Cum06] M.L. Cummings, M.L. – Automation and accountability in decision support system interface design, Journal of Technology Studies, vol 32:1, 2006.

[DSB12] Department of Defense, Defence Science Board – Task Force Report: The role of autonomy in DoD systems, 2012 (www.fas.org/irp/agency/dod/dsb/autonomy.pdf)

[RDR+14] N. Regis, Fr. Dehais, E. Rachelson, Ch. Thooris, S. Pizziol, M. Causse, C. Tessier – Formal Detection of Attentional Tunneling in Human Operator-Automation Interactions. IEEE Transactions on Human-Machine Systems, Vol 44 n°3, 326-336, June 2014

[SWB97] N. D. Sarter, D. D. Woods, C .E. Billings – Automation surprises. Handbook of Human Factors and Ergonomics, 2nd ed., Wiley, 1997

[Tes15] C. Tessier - Autonomie : enjeux techniques et perspectives. In Drones et killer robots : faut-il les interdire ? R. Doaré, D. Danet, G. de Boisboissel (direction). Presses Universitaires de Rennes, 2015

[THR+09] W. Truszkowski, L. Hallock, Ch. Rouff, J. Karlin, J. Rash, M. G. Hinchey and R. Sterritt. – Autonomous and autonomic systems with applications to NASA intelligent spacecraft operations and exploration systems, Springer, 2009

KRAUSS MAFEI WEGMANN / NEXTER : UNE INTÉGRATION RAPIDE COMME CLÉ DU SUCCÈS

JEAN-PIERRE MAULNY
DIRECTEUR-ADJOINT, IRIS

La fusion entre Krauss Maffei Wegmann (KMW) et Nexter, annoncée en 2014 et finalisée en 2015, revêt une importance dont les Français et les Allemands, et de manière générale tous les pays européens, doivent avoir conscience. Le mouvement de consolidation de l'industrie de défense européenne, engagée dans les années 1990, était motivé par deux objectifs. D'une part, la baisse des budgets de défense après la Guerre froide ne permettait plus de conserver un tissu industriel européen de défense en l'état car il était affecté de surcapacités. Il fallait que les entreprises se regroupent comme ce fut le cas aux États-Unis à partir de 1993. D'autre part, la construction européenne en matière de défense, initiée avec le traité de Maastricht en 1992 et consolidée en 1999 avec la mise en place des institutions de la Politique de sécurité et de défense commune (PSDC), allait donner aux entreprises le signal politique nécessaire à engager cette fusion. Les entreprises de défense n'ont en effet qu'un client, les États, et les entreprises européennes de défense n'ont intérêt à se regrouper que si elles ont le sentiment que ces États veulent définir leur besoin en équipements militaires en commun. Si des programmes en coopération voient le jour et si des structures comme l'Agence européenne de défense ou la commission européenne aident à définir ces besoins communs, la stratégie des entreprises sera alors de se consolider dans un cadre européen. A cause du manque de programmes en coopération, et faute d'une impulsion politique forte des pays de l'Union européenne pour mutualiser leurs capacités militaires, les entreprises européennes de défense privilégient alors des stratégies alternatives soit en privilégiant les exportations, soit en essayant de s'implanter sur le marché américain, tout ceci en se faisant concurrence entre elles.

La fusion KMW/Nexter succède à 10 ans de disette dans la consolidation de l'industrie européenne de défense, signe que les États n'ont pas réuni les conditions nécessaires pour inciter les entreprises à se regrouper. Pourtant, depuis 15 ans, les études, articles ou rapports se sont multipliés pour critiquer le nombre trop important de programmes terrestres ou navals européens, deux secteurs où le paysage industriel européen est trop émietté eu égard au volume du marché de ces équipements. Si KMW et Nexter ont décidé de se regrouper dans l'armement terrestre c'est que cette concurrence européenne destructrice couplée avec l'émergence de nouveaux entrants dans le domaine de l'armement terrestre en provenance des pays émergents faisait courir des risques à long terme à ces deux entreprises. L'initiative du rapprochement revient donc principalement aux deux sociétés même si les gouvernements français et allemands l'ont encouragée à des degrés divers. La fusion Nexter / KMW est-elle donc la fin de l'histoire ?

Certainement pas, on peut même dire que c'est aujourd'hui que l'histoire de ce rapprochement débute. Les défis sont devant nous, ils ne sont pas derrière.

Tout d'abord, le processus d'intégration des deux entreprises n'est pour le moment que partiel. Seul un certain nombre de fonctions ont été mises en commun : les achats, la R&D, la définition de la stratégie, le marketing et les ventes à l'international et la communication. Mais les deux marques subsistent. Comme l'a indiqué l'ancien président de Nexter, Philippe Burtin, quand il a présenté le projet en France à l'Assemblée nationale, « il faut parler de rapprochement et non de fusion ».

Le premier défi auquel va être confrontée la nouvelle entreprise est en effet celui de la réalité du rapprochement. Si les deux sociétés n'ont pas rapidement le sentiment de vivre un destin commun, il est à craindre que l'expérience fasse long feu. Le rapprochement KMW / Nexter ressemble aujourd'hui plus à un PACS ou à des fiançailles qu'à un véritable mariage.

Pour que ce mariage soit consommé, il faut relever un premier défi : celui des exportations. Les gammes de produits des deux entreprises sont largement complémentaires, mais il existe également des zones de concurrence comme c'est le cas avec le Boxer de KMW et le VBCI de Nexter. À ce niveau, il est primordial que ce que l'on appelle l'entreprise de tête décide au cas par cas du produit, provenant de l'une ou de l'autre entreprise, qui sera présenté sur les marchés à l'exportation et que les équipes commerciales de KMW et de Nexter travaillent de concert pour promouvoir ce produit. Etant donné l'importance que prendra cet accord de non-concurrence à l'exportation dans la réussite du rapprochement, les gouvernements franco-allemands devraient s'entendre également pour appuyer de concert ce produit, qu'il soit d'origine française ou d'origine allemande, afin de souligner que c'est bien un matériel de cette nouvelle entreprise franco-allemande qui est proposé à l'exportation et non un produit fabriqué par Nexter ou KMW.

L'autre moteur de la fusion sera la capacité des deux États à développer des programmes en coopération.
Aujourd'hui on évoque un futur char de combat franco-allemand, mais la nature de ce que pourrait être ce système n'est pas encore définie et la perspective d'entrer en service d'un tel équipement reste lointaine. Il est donc nécessaire que la France et l'Allemagne donnent dès maintenant des perspectives claires sur leur volonté de développer des programmes en coopération dans le domaine des équipements terrestres si l'on veut que les équipes des deux entreprises travaillent ensemble afin de donner cœur à l'intégration de l'entreprise. Si ce n'est pas le cas, le risque est qu'il y ait la juxtaposition d'une entreprise française et d'une entreprise allemande qui seront certes unies par leurs comptes financiers, mais sans qu'aucune synergie ne se dégage au niveau industriel au sein de l'entreprise. La pérennité d'une telle entreprise serait certainement sujette à caution.

Pour que la fusion soit un succès, il faut que les acteurs industriels et politiques aient une volonté forte de réussir cette intégration.

Pour ce qui est des équipes dirigeantes des deux entreprises, il ne faut pas hésiter à accélérer le mouvement qui doit conduire à leur intégration. La question de la présidence commune doit être posée rapidement et ne pas attendre huit ans comme ce fut le cas pour Airbus après la création d'EADS.

Il faut également que les États soutiennent ce projet. Cela ne veut pas dire donner des aides d'Etat ou octroyer des programmes à l'entité française ou à l'entité allemande de la nouvelle entreprise. Cela signifie qu'outre le soutien commun aux exportations et le lancement de programmes en coopération, la France et l'Allemagne doivent clairement inscrire la fusion KMW / Nexter dans le cadre d'une initiative franco-allemande pour relancer l'Europe de la défense. Il faut un moteur politique à cette fusion dans l'armement terrestre si l'on veut que celle-ci soit un succès, si on veut convaincre les hommes politiques de France et d'Allemagne ainsi que les personnels des deux entreprises que cette fusion est destinée à développer une entreprise compétitive pour le bien de tous et non pour brader son outil industriel à l'autre pays comme on l'entend encore trop souvent réciproquement des deux côtés du Rhin.

Les défis technologiques d'une Europe en quête de compétitivité : l'exemple des systèmes inhabités

Dr. Océane Zubeldia,
Chercheur Armement et économie de défense, IRSEM
Dr. Chantal Lavallée
Chercheur postdoctoral, IRSEM

L'évolution du contexte opérationnel, le retour d'expérience sur les conflits récents, et les nouvelles menaces qui se font jour, de la gestion des crises à la lutte contre le terrorisme, sont autant de facteurs invitants à une analyse des défis technologiques d'une Europe en quête de compétitivité et de moyens. À cet égard, le développement de systèmes inhabités, c'est-à-dire les drones et les robots, représente un axe d'innovation majeur. Initialement utilisés à des fins militaires, ces appareils offrent à présent des applications étendues à la sphère civile, voire d'usage dual.

Coopération versus souveraineté : quelle réalité ?

Le Conseil européen de décembre 2013, consacré aux questions de défense et surtout à la manière de relancer la Politique de sécurité et de défense commune (PSDC), insiste sur les synergies possibles entre les moyens des différents acteurs, institutionnels et industriels, ainsi que sur l'importance de renforcer les capacités avec des projets concrets. Les enjeux politiques, financiers et stratégiques liés à la défense, propres à chaque État membre, expliquent les blocages rencontrés jusque-là au sein de l'Union européenne (UE) en la matière. Les principaux arguments évoqués, par les dirigeants européens, demeurent liés à la souveraineté nationale, l'autonomie stratégique, et la préservation d'un tissu industriel de défense. Ils ont, par voie de conséquence, longtemps dispersé leurs programmes de recherche et de développement en privilégiant une politique industrielle nationale, comme dans le cas des drones. Les difficultés de lancer en commun une nouvelle génération de drones de moyenne altitude et longue endurance (MALE) européens en sont le parfait exemple[1]. À l'échelle européenne, les systèmes inhabités aéroterrestres et les robots n'ont par contre pas fait l'objet de projets de partenariats communs. Pour répondre aux défis de la compétitivité et de l'innovation, une phase d'ouverture et de coopération semble néanmoins voir le jour dans le cadre de discussions à Bruxelles.

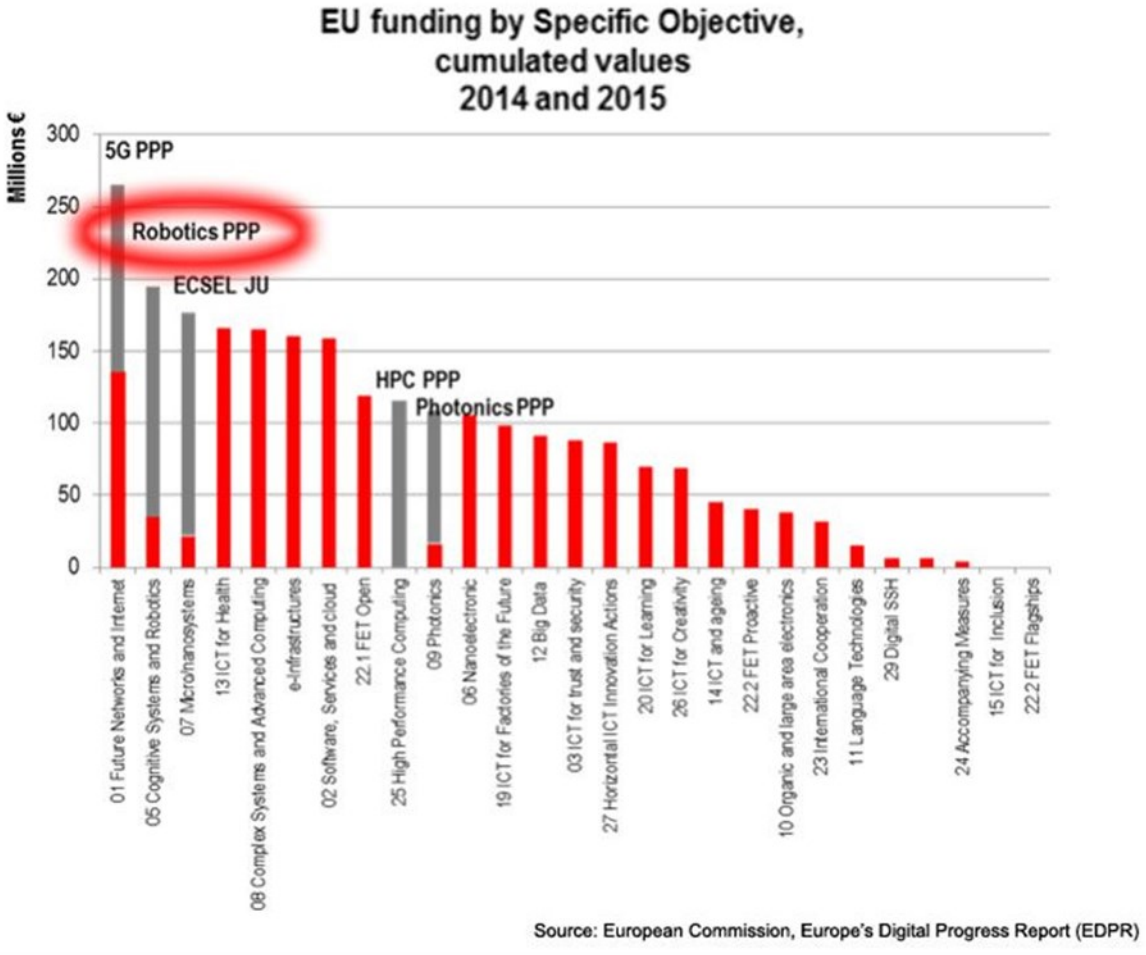
Le communautaire comme levier d'action

Depuis le milieu des années 1990, la Commission européenne a adopté une démarche inédite en proposant des initiatives dans le domaine de la défense même si elle ne dispose pas de compétence en la matière. Elle suggère des propositions pour consolider la PSDC sur la base de ses compétences, notamment en matière de recherche liée à la sécurité dans le cadre du 7e Programme-cadre pour la recherche et le développement (PCRD, 2007-2013), puis depuis 2014 avec le Programme Horizon 2020. L'action de la Commission peut s'expliquer du fait de la mondialisation et de ses effets sur l'industrie de défense. Par ailleurs, la stratégie de Lisbonne, qui vise notamment la recherche et le développement tout en assurant la croissance économique, confirme la prise de conscience de l'importance de mener un effort de programmation en vue de dynamiser l'innovation et les programmes scientifiques, y compris ceux relatifs aux drones[2]. L'innovation est un impératif pour permettre à l'Europe et à la France d'occuper un rang de premier ordre et d'être bien présent face aux géants émergents[3]. La force de l'Union européenne réside dans la richesse de ses niches technologiques qui peuvent produire des résultats spectaculaires si elles parviennent à se fédérer. D'ailleurs, les leçons tirées des limites de la stratégie de Lisbonne ont conduit à lier théorie et pratique dans un seul et même programme, Horizon 2020, qui se distingue ainsi des précédentes actions pour ac-

compagner l'ensemble de la chaîne d'innovation.

Les ambitions du programme Horizon 2020 dans le domaine de la robotique

L'indépendance technologique ne peut plus être assurée sur une seule base nationale française et fragmentée à l'échelle des pays européens. Dans le cadre du programme Horizon 2020, l'Union européenne semble porter une volonté marquée de stimuler la recherche en matière de robotique, comme en témoigne le cofinancement de 21 projets, totalisant une somme de 98.7 millions d'euros qui seront répartis sur 2 à 5 ans[4]. À ce titre, comme l'illustre le graphique ci-dessous[5], ce domaine occupe une place prépondérante par rapport aux autres secteurs visés. Parallèlement, des travaux de recherches sont en cours pour encadrer l'utilisation des robots et ont déjà donné lieu à une proposition de livre vert[6].



Les salons internationaux de défense et de sécurité, comme celui d'Eurosatory qui se déroule en juin, sont la vitrine des industriels français auprès des instances nationales, européennes et internationales. La concentration de l'ensemble des acteurs représente un réel catalyseur en termes de rayonnement et de nouvelles coopérations. Il est possible d'identifier deux axes d'efforts prioritaires afin que l'industrie européenne atteigne un degré de maturité suffisant : les programmes en robotique nécessitent une activité à travers le long terme et doivent être particulièrement pensés dans une perspective duale.

Une technologie en pleine expansion

L'apparition progressive sur les théâtres d'opérations de la capacité à opérer en réseau pour l'ensemble des équipements ouvre un champ d'application très étendu à la robotique. Le but est d'augmenter l'efficacité opérationnelle en réaffectant les êtres humains à des tâches pour lesquelles leur apport est plus approprié. Ainsi, les robots qui constituent un élément d'innovation doivent, indépendamment de l'aspect opérationnel, pouvoir contribuer à d'autres aspects tels que la réduction des coûts, la miniaturisation des senseurs et la recherche des synergies avec le domaine civil. À ce propos, la surveillance intérieure des entrepôts et des sites industriels (énergie, construction, agriculture, réseau), le contrôle des installations *offshore* ou les prises de vues aériennes vidéos et photos, média, l'assistance médicale, le transport et la livraison de colis, sont autant de domaines dans lesquels ces systèmes vont devenir de plus en plus incontournables.

L'historien des sciences, économiste et philosophe français, Jean-Jacques Salomon, s'interroge, dans son livre intitulé *Le destin technologique,* sur les possibles dans la dynamique de l'innovation. À cet égard, la généralisation de l'usage des drones et des robots révèle de nouveaux besoins et une manière de travailler à repenser. Ce processus de « destruction créatrice », fidèle à Schumpeter, pose les défis présents et futurs que l'Europe devra relever au-delà des questions de souveraineté nationale et des priorités économiques.

Notes

1. Il a fait l'objet de multiples propositions avortées (EuroMale, Talarion, Advanced UAV, Mantis/Telemos, Voltigeur) et est toujours sujet à de nombreux débats.

2. Philippe Ricard, « La Commission veut encourager un programme européen de drones », *Le Monde*, 24 juillet.

3. Jan Joel Andersson, Sven Biscop, Bastian Giegerich, Christian Mölling, Thierry Tardy, *Envisioning European defence : five futures*, Cahier de Chaillot, No137, 13 avril 2016.

4. Voir : http://robohub.org/horizon-2020-earmarks-e-98m-for-new-wave-of-european-robotics/

5. Voir : Horizon 2020 Research Projects in the ICT domain in the EU 2015 (ppt).

6. Voir : *Suggestion for a Green Paper on Legal Issues in Robotics*.

7. Voir : http://www.eurosatory.com/eurosatory-2016/le-concept-eurosatory.aspx.

8. Jean-Jacques Salomon, *Le destin technologique*, Gallimard, Paris, 1993, 331 p.

Données, systèmes et capteurs : le cyberespace dans l'environnement militaire

Dr. Nicolas MAZZUCCHI

Chercheur Armement et économie de défense, IRSEM

Longtemps l'ineffable cyberguerre a été au cœur du rapport entre le monde militaire et le cyberespace. Bientôt, nous prédisait-on dans les années 1990[1], les cyberconflits se généraliseraient et la guerre se livrerait à coup d'ordinateurs et de lignes de code. La peur du Cyber-Armageddon, dans lequel nos sociétés et nos armées s'effondreraient suite à des cyberattaques massives, qui tiraillait les décideurs politiques et militaires, a longtemps guidé les réflexions dans le domaine de l'intégration des outils cyber dans la défense. Aujourd'hui l'image de la cyberguerre s'éloigne peu à peu pour laisser la place à une réflexion plus apaisée sur le rôle du cyberespace dans les opérations militaires[2].

Du cyberconflit

L'absence de cyberguerre – à savoir d'un conflit mené de bout en bout dans le cyberespace et causant directement des morts à travers celui-ci – ne signifie pas que ce champ soit délaissé par les militaires. Des cyber-actions ont ainsi été conduites par plusieurs États, Israël et la Russie notamment, en appui à des opérations cinétiques[3]. Il n'y a maintenant plus lieu de se poser la question de la nécessité de disposer d'un potentiel de lutte informatique, mais bien de réfléchir à l'intégration de celui-ci au sein des forces armées. La question des luttes informatiques défensive mais aussi offensive occupe de plus en plus les dirigeants militaires avec la constitution de commandements dédiés (US Cybercommand américain, OG Cyber français, etc.). Si une telle floraison d'organisations consacrées au cyberespace se produit au sein des armées occidentales comme émergentes (institution d'un commandement cyber au Brésil, réforme de l'Armée populaire de libération chinoise intégrant le cyber dans les forces d'appui stratégique), c'est bien que celui-ci représente un lieu d'opportunités comme de menaces.

Le classement des cyber-vulnérabilités par le département de la Défense américain (DoD) nous renseigne sur la perception des menaces par celui-ci[4]. Tout en bas des 6 niveaux de menace, se trouve l'exploitation des vulnérabilités connues, par l'achat de logiciels prêts à l'emploi sur le *dark web*. Pour quelques dizaines de dollars américains (USD), il est ainsi possible de monter une mini-cyberattaque depuis chez soi, sans véritables connaissances en informatique. En revanche, au sommet de l'échelle se trouve l'intégration totale du cyberespace comme espace de combat au sein d'un conflit ouvert de type conventionnel. Accessible uniquement aux États, cette possibilité rappelle fortement les opérations menées par Israël en 2007 contre la Syrie, où le bombardement d'installations nucléaires syriennes avait été précédé d'une cyberattaque contre le réseau de Damas, et par la Russie en 2008 lors de la guerre contre la Géorgie.

Loin des seules opportunités offertes par des conflits interétatiques plus ou moins importants, il appartient d'intégrer aussi dans la réflexion l'ensemble des groupes terroristes ou combattants avec lesquels la France peut être en conflit. Ces derniers, souvent présentés comme rustiques ou faiblement dotés au niveau technologique, peuvent toutefois atteindre les systèmes des forces armées, si ceux-ci sont mal protégés. La progression du niveau moyen de connaissance en informatique et la volonté affichée par des groupes comme Al Qaeda et Daesh d'attirer dans leurs rangs ingénieurs et informaticiens, est une donnée à prendre en compte dans la lutte globale menée contre ces organisations. La vulnérabilité croissante, induite par l'augmentation de la connexion des forces et par la dépendance aux données, est un paramètre fondamental du combat du XXIe siècle. Les problématiques de numérisation du champ de bataille dans les armées françaises – prenant la suite des théories américaines de *network centric warfare*[5] – incarnées par des programmes comme Scorpion, induisent nécessités (systèmes de recueil, traitement

et partage) et vulnérabilités tout au long de la chaîne de valeur de l'information.

Cyber-vulnérabilités et technologies duales

Si la cyberguerre n'existe pas, il est demeure toutefois nécessaire de limiter, autant que faire se peut, les vulnérabilités des systèmes militaires. La hausse exponentielle de la production et de l'utilisation des données en opérations comme en état-major – pensons ici aux drones par exemple –, induit une plus grande interconnexion. Cette dernière ouvre nécessairement des vulnérabilités de deux ordres. La première est celle de la facilité d'usage. En s'habituant à disposer d'un grand nombre de données pour la prise de décision, il devient difficile ensuite de gérer leur absence en cas de disruption. La seconde est liée à la multiplication des capteurs et des connexions de différentes natures (filaires ou non). Cette inflation des réseaux et des liaisons augmente mécaniquement les points d'entrée potentiels pour les agresseurs éventuels.

La plus grande vulnérabilité réside toujours dans l'humain. Sans parler ici de la question de la guerre informationnelle[6] ou des pratiques d'espionnage sur les réseaux sociaux, la naïveté de certains praticiens peut conduire à des failles de sécurité majeures. En 2009, le *Wall Street Journal* révélait le piratage de drones Predator de l'US Air Force par des insurgés irakiens. Ces derniers, à l'aide d'un simple ordinateur portable équipé d'un logiciel russe coûtant 26 USD, avaient réussi à détourner les flux de communication du drone, récupérant en temps réel les images que celui-ci transmettait à sa base. La principale question soulevée ici n'est pas que les insurgés aient réussi à disposer des mêmes informations que les forces américaines, leur permettant de leur échapper, mais bien que les responsables militaires américains aient été au courant de la faille employée dès les années 1990. Jusqu'à cet incident, ils pensaient tout simplement que les adversaires n'auraient pas le niveau pour l'exploiter[7]… A la suite de cette affaire, l'ensemble de la flotte de Predator a dû être rappelé pour une mise à niveau sécuritaire du protocole de communication.

L'ingéniosité des adversaires, conventionnels ou non, ne cesse ainsi de progresser et d'ouvrir des failles dans les systèmes réputés – ou supposés – protégés. En 2011, toujours au sujet de drones américains de modèle RQ-170 Sentinel cette fois, l'un d'entre eux aurait été intercepté par les forces iraniennes, lesquelles l'auraient forcé à se poser en piratant son système de contrôle. Les images du drone capturé par les Iraniens ont ensuite fait le tour du monde[8]. La capture d'un engin représentant l'état de l'art de la technologie en la matière, puis la diffusion de celui-ci sur les chaînes de télé du monde entier, ont démontré la vulnérabilité des systèmes de contrôle à distance.

Au-delà des vulnérabilités intrinsèques aux systèmes proprement militaires, la multiplication des technologies duales pose également de nombreux problèmes. Les systèmes d'exploitation des différents matériels intégrés dans une approche numérisée du champ de bataille reposent le plus souvent sur la transformation de produits civils. Même en rajoutant par-dessus ces derniers des couches logicielles proprement militaires, ils possèdent toujours un certain nombre de vulnérabilités héritées de leur environnement d'origine. Les serveurs de données sont ainsi souvent issus de technologies provenant des grands industriels comme Microsoft et soumis aux mêmes risques que toute entreprise utilisant ces derniers. En 2009 le virus Conficker, utilisant une faille commune aux systèmes d'exploitation Microsoft (MS 08-67) de type Windows (2000, XP, Vista, Seven) et Windows Server (2003 et 2008) se répand dans le monde. Or les ministères de la Défense des pays occidentaux sont de grands consommateurs de ces systèmes, pour des questions tant de facilité d'utilisation que d'interopérabilité. Ainsi certains réseaux informatiques du DoD américain, du MoD britannique, du ministère de la Défense français et de la Bundeswehr, ont été infectés par le virus. Ce dernier, ne causant pas de dommages directs, mais se multipliant rapidement tout en bloquant les processus de mise à jour, a ainsi démontré les pièges de l'interopérabilité et de la dualité des systèmes civils et militaires. De la même manière, il a mis en lumière les problématiques inhérentes aux chaînes de comman-

dement très verticales, y compris pour l'application des correctifs en matière de cybersécurité qui exigent pourtant des temps de réaction courts.

Dans ce contexte, on comprend mieux, même si c'est loin d'être la seule raison, la volonté des autorités russes et chinoises de se doter de systèmes purement nationaux. Car au-delà de la question des technologies duales qui se pose dans le cyber comme dans de nombreux domaines, c'est bien celle de l'universalité des systèmes par rapport aux besoins et aux contraintes spécifiques au monde militaire qui est en jeu.

Cyber-BITD et indépendance technologique

Si l'on reprend la classification des menaces du DoD, la 5e en termes de dangerosité, juste avant la guerre ouverte, est celle de la collusion entre un Etat et des entreprises pour introduire dans les produits de cette dernière des éléments malins (chevaux de Troie, portes dérobées, etc.). Elle est révélatrice de la perception par les autorités militaires des dangers de la collusion entre autorités nationales et entreprises. En France, le rapport du sénateur J-M. Bockel sur la cyberdéfense insistait en 2012 sur les liens existant entre les entreprises chinoises et Pékin, recommandant de bannir purement et simplement les produits Huawei[9], pourtant leader sur les routeurs cœur de réseau.

L'interdiction d'achat et d'utilisation de tel ou tel produit, pose donc la question de l'indépendance technologique des armées et de la capacité industrielle à produire en nombre et qualité suffisants les appareils nécessaires. De la même manière que pour les industries de défense plus traditionnelles, fournissant avions, navires et blindés, une réflexion est menée sur la notion même de cyber base industrielle et technologique de défense.

Les grands industriels du monde de la défense ont également décidé de se lancer depuis des années sur le secteur des produits destinés aux télécommunications. Que ce soit dans le domaine purement militaire ou dans une optique plus large, intégrant la cybersécurité à destination des entreprises privées, de nombreuses grandes entreprises de défense disposent de divisions dédiées. Comme souvent, les entreprises américaines sont en pointe dans ce domaine, avec Lockheed-Martin et Boeing comme chefs de file[10]. Ainsi, ils développent souvent des solutions transverses comme des systèmes de contrôle industriels. En 2015, Lockheed-Martin vendait pour 7,5 milliards USD de systèmes dédiés au cyberespace, soit 16% de l'ensemble de son activité, Boeing environ autant pour 8% du total de l'activité de l'entreprise. Si le cyber est une activité secondaire, elle gagne de plus en plus de place au sein de l'ensemble du portefeuille de l'entreprise et concentre maintenant des efforts de R&D très importants[11].

Côté français, si on peut remarquer l'excellence de Dassault, Thalès et Safran, sans oublier toutes les entreprises de taille plus modeste qui concourent au développement de solutions de cyberdéfense, il convient de noter que le secteur demeure éclaté. Point ici de puissant groupement d'entreprises comme le GICAT, le GICAN ou le GIFAS. Les acteurs sont plus isolés et les PME plus vulnérables aux tentatives de rachat de la part des géants étrangers du secteur. Des travaux sont néanmoins en cours sous tutelle de l'Etat avec en 2012 le lancement du projet DAVFI d'antivirus national, destiné en partie aux administrations dont la Défense, ou la création du pôle d'excellence cyber de Rennes en 2015. Toutefois, comparativement à nos alliés, l'effort reste récent et modeste économiquement.

La question d'un système d'exploitation souverain, si elle est loin de la réalité pour le grand public et les entreprises, s'avère cruciale dans le monde militaire[12]. Permettant de contourner, du moins partiellement, les grands fournisseurs étatsuniens[13], un système d'exploitation souverain renforcerait l'indépendance matérielle des armées, tout en garantissant des débouchés aux entreprises nationales. La question qui se poserait alors serait celle de l'interopérabilité avec nos alliés, notamment dans le contexte d'un renforcement du rôle de l'OTAN dans le domaine du cyber, lequel entraînera certainement une politique de normalisation de la part de l'Alliance.

L'info-dépendance semble devenir l'un des nouveaux paradigmes des armées. La volonté d'intégrer toujours plus de numérique au sein des forces, oblige à penser très amont les problématiques associées de dépendance technologique et de vulnérabilités. Par le passé, Etats, groupes armés et hacktivistes ont prouvé qu'ils pouvaient agir sur les réseaux et les matériels de défense. La question de l'intégration du cyberespace au sein des armées doit donc se penser de manière transverse en offensif et en défensif bien sûr, mais aussi comme l'aboutissement d'un écosystème intégrant fournisseurs industriels, décideurs politiques et commandements militaires. La numérisation des armées occidentales, en cours depuis les premiers pas de la RMA américaine, fragilise, paradoxalement, les forces déployées en opérations. Par conséquent, la solution ne peut que passer, là aussi, par un paradoxe : intégrer des éléments technologiques les plus souverains possibles, tout en maintenant une interopérabilité avec les systèmes de nos alliés.

Notes

1. Arquila J., Ronfeldt D. (1993), *Cyberwar is coming*, Santa Monica, RAND.

2. Libicki M., 2012, « Cyberspace is not a warfighting domain », *I/S: A Journal of Law and Policy for The Information Society* vol. 8:2, pp. 321-336 ; RID, T. (2012), « Cyber War Will Not Take Place », *Journal of Strategic Studies*, vol. 35, n°1, pp. 5–32.

3. Ceci sans mentionner des opérations souveraines à but géopolitique comme Stuxnet.

4. DOD Defense Science Board, 2013, *Resilient Military Systems and the Advanced Cyber Threat,* Washington, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

5. Alberts D. et *allii* (2000), *Network Centric Warfare: Developing and Leveraging Information Superiority*, Washington, DoD C4ISR Cooperative Research Program.

6. Mazzucchi N. (2014), « L'économie, cible privilégiée de la guerre informationnelle », *Revue Défense Nationale* n° 770.

7. Gorman S., Dreazen Y. J., Cole A., 17 décembre 2009, "Insurgents Hack U.S. Drones", *Washington Post*.

8. Le Figaro, 9 décembre 2012, « L'Iran diffuse les images du drone américain »

9. Bockel J-M., (2012), *Rapport d'information sur la cyberdéfense,* Paris, Sénat, p. 119.

10. Sans minorer le rôle d'autres acteurs comme L3-Com.

11. Même BAE Systems, un des premiers acteurs européens dans le domaine est tributaire des Etats-Unis puisque le gouvernement américain représente 61% des ventes de ses produits cyber.

12. Un amendement (CL129) au projet de loi « République numérique » a été déposé en ce sens et adopté le 6 janvier 2016.

13. Même avec un système d'exploitation souverain, la problématique du big data (stockage, traitement et diffusion des données massives) demeurerait.