N° 1433

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 10 octobre 2013.

AVIS

FAIT

AU NOM DE LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES
SUR LE PROJET DE LOI **de finances** *pour* **2014** (n° 1395)

TOME II

DÉFENSE

ENVIRONNEMENT ET PROSPECTIVE DE LA POLITIQUE DE DÉFENSE

PAR M. JEAN-YVES LE DÉAUT
Député

Voir le numéro : 1428 (annexe 10)

SOMMAIRE

___

Pages

INTRODUCTION

Le contexte budgétaire est contraint et les citoyens l'ont bien compris. Mais c'est précisément dans les périodes de crise comme celle que nous connaissons qu'il faut préparer l'avenir, et conforter l'excellence technologique des industries de défense.

Le programme 144 « Environnement et prospective de la politique de défense » a la particularité d'être tout entier tourné vers l'avenir. Simultanément indicateur de l'évolution du contexte international et incubateur de briques technologiques, il est un outil d'aide à la décision et concourt à l'autonomie de notre politique de défense.

Ce « petit » programme, qui représente environ 6 % du budget total de la Défense, est donc un programme important qui irrigue le tissu de la Défense et finance, outre le renseignement, une variété de projets et d'études mobilisant en synergie une multiplicité d'acteurs extérieurs, de l'école supérieure aux petites et grandes entreprises, et des instituts de recherche aux attachés de défense.

Jean-Yves Le Drian, ministre de la Défense, a rappelé devant la commission de la Défense, qu'il serait déterminé à défendre en toute priorité les études amont, ainsi que la préparation opérationnelle. On ne peut que s'en féliciter.

L'année à venir est une année importante qui sera observée attentivement puisqu'elle est le premier exercice budgétaire de la nouvelle loi de programmation militaire issue du nouveau Livre blanc sur la défense et la sécurité nationale dee 2013, voulu par le Président de la République au lendemain de son élection.

De ce nouveau Livre blanc émergent des priorités phares que le rapporteur a tenu à souligner en consacrant une partie de son avis aux drones et à la cyberdéfense, sujets qu'il estime déterminants tant pour la mise en œuvre de la politique de défense que pour l'avenir industriel de notre pays.

Le rapporteur avait demandé que les réponses à son questionnaire budgétaire lui soient adressées au plus tard ***le 23 septembre 2013****. À cette date, seules trois réponses étaient parvenues, soit un taux de 13 %.*

Au 10 octobre 2013, *date limite résultant de l'article 49 de la loi organique du 1er août 2001 relative aux lois de finances, 21 réponses étaient parvenues, soit* ***un taux de 91 %.***

Le rapporteur tient à mentionner que son travail a été rendu difficile en raison des nombreuses réponses à son questionnaire budgétaire portant la mention « Confidentiel Défense ». S'il comprend la nécessité d'une absolue discrétion concernant les informations stratégiques, il lui paraît en revanche peu utile de classifier, par exemple, une information telle que le nombre de thèses financées en 2012, voire des informations existant en source ouverte, parfois sur le site même du ministère de la Défense. Il serait donc souhaitable à l'avenir que ne soient classifiés que les éléments de réponse le nécessitant et non l'ensemble du document les contenant.

PREMIÈRE PARTIE : ÉVOLUTION GÉNÉRALE DES CRÉDITS

La vocation de ce programme est d'apporter au ministère de la Défense les éléments nécessaires à l'appréciation de son environnement stratégique, dans un contexte de rapide évolution des équilibres internationaux, afin de lui permettre de déterminer et de mettre en œuvre la politique de défense de notre pays.

En cohérence avec cette mission, le programme 144 regroupe donc des actions visant à :

– élaborer la prospective en matière d'évolution du contexte stratégique ;

– rechercher le renseignement de défense ;

– définir les systèmes de forces futurs et contribuer à la maîtrise de capacités industrielles et technologiques cohérentes ;

– orienter et de conduire la diplomatie de défense.

Les crédits demandés pour 2014 au titre du programme 144 **« Environnement et prospective de la politique de défense »** s'élèvent à 1 979,5 millions d'euros, en autorisations d'engagement et 1 979,41 millions d'euros en crédits de paiement, ce qui représente 6,3 % des crédits de la mission « Défense ». Les dotations proposées pour 2014 pour ce programme correspondent à une augmentation des crédits de 3,9 % en crédits de paiement, ce que salue le rapporteur en cette période de contrainte budgétaire.

Pour mémoire, le programme 144 était ventilé en six actions lors de l'exercice 2012. L'exercice 2013 a vu une simplification de son architecture qui ne comporte dorénavant que trois actions, de poids financier inégal, dont le périmètre n'a pas varié depuis l'exercice précédent :

– l'action 03 « Recherche et exploitation du renseignement intéressant la sécurité de la France », divisée en deux sous-actions « Renseignement extérieur » et « Renseignement de sécurité de défense », rassemble 37,6 % des crédits du programme ;

– l'action 07 « Prospective de défense », divisée en quatre sous-actions, « Analyse stratégique », « Prospective des systèmes de forces », « Études amont » et « Soutien et subventions », concentre 56,5 % des crédits ;

– l'action 08 « Relations internationales », divisée en deux sous-actions « Soutien aux exportations » et « Diplomatie de défense », comprend pour sa part 5,9 % des crédits du programme.

Les tableaux ci-après présentent l'évolution des crédits du programme.

BUDGET DU PROGRAMME 144 HORS TITRE 2

	LFI 2013		PLF 2014		Évolution	
	AE (En M€)	CP (En M€)	AE (En M€)	CP (En M€)	AE	CP
Action 3: Recherche et exploitation du renseignement intéressant la sécurité de la France	270,05	225,56	200,67	262,93	- 25,69 %	16,57 %
Sous-action 31 : Renseignement extérieur	*258,18*	*213,70*	*189,42*	*251,53*	*- 26,64 %*	*17,71 %*
Sous-action 32 : Renseignement de sécurité de défense	*11,86*	*11,86*	*11,40*	*11,40*	*- 3,95 %*	*- 3,93 %*
Action 7 : Prospective de défense	*1 035,37*	*1 002,93*	*1 099,23*	*1 037,00*	*6,17 %*	3,40 %
Sous-action 71 : Analyse stratégique	*8,11*	*5,11*	*6,08*	*6,89*	*- 25,04 %*	34,87 %
Sous-action 72 : Prospective des systèmes de forces	*24,67*	*24,67*	*25,44*	*25,35*	*3,15 %*	*2,79 %*
Sous-action 73 : Études amont	*732,31*	*702,87*	*809,27*	*746,31*	*10,51 %*	*6,18 %*
Sous-action 74 : Soutien et subventions	270,28	*270,28*	*258,44*	*258,44*	- 4,38 %	*- 4,38 %*
Action 8 : Relations internationales	*44,25*	43,70	35,13	35,13	- 20,60 %	*- 19,61 %*
Sous-action 81 : Soutien aux exportations	*7,19*	*6,92*	*6,52*	*6,52*	*- 9,26 %*	*- 5,70 %*
Sous-action 82 : Diplomatie de défense	*37,06*	*36,78*	*28,61*	*28,61*	*- 22,80 %*	*- 22,22 %*
TOTAL	**1 349,66**	**1 272,19**	**1 335,18**	**1 335,06**	**- 1,07 %**	**4,94 %**

Source : ministère de la Défense.

BUDGET DU TITRE 2 DU PROGRAMME 144

	LFI 2013 En M€	PLF 2014 En M€	Évolution
Action 3 : Recherche et exploitation du renseignement intéressant la sécurité de la France	469,46	480,98	2,5 %
Sous-action 31 : *Renseignement extérieur*	*386,34*	*399,19*	*3,3 %*
Sous-action 32 : *Renseignement de sécurité de défense*	*83,12*	*81,79*	*- 1,6 %*
Action 7 : Prospective de défense	77,34	82,21	6,3 %
Sous-action 71 : *Analyse stratégique*	-	-	-
Sous-action 72 : *Prospective des systèmes de forces*	*8,28*	*7,95*	*- 3,9 %*
Sous-action 73 : *Études amont*	-	-	-
Sous-action 74 : *Soutien et subventions*	*69,06*	*74,26*	*7,5 %*
Action 8 : Relations internationales	86,28	81,17	- 5,9 %
Sous-action 81 : *Soutien aux exportations*	*8,21*	*7,97*	*- 2,9 %*
Sous-action 82 : *Diplomatie de défense*	*78,06*	*73,20*	*- 6,2 %*
	633,08	644,45	+ 1,8 %

Source : ministère de la défense.

I. LA RECHERCHE ET L'EXPLOITATION DU RENSEIGNEMENT INTÉRESSANT LA SÉCURITÉ DE LA FRANCE

L'action **03** concentre la fonction **« Recherche et exploitation du renseignement intéressant la sécurité de la France »**. En conformité avec les orientations du Libre blanc sur la défense et la sécurité nationale 2013 et les priorités dégagées, l'action des services de renseignement sera renforcée en 2014.

Ainsi que l'a indiqué à la commission [(1)], M. Philippe Errera, directeur des Affaires stratégiques au ministère de la Défense, les moyens de la direction générale de la sécurité extérieure (DGSE) et de la direction de la protection et de la sécurité de défense (DPSD) seront mutualisés pour une plus grande interopérabilité et ces services verront leurs effectifs croître de 65 agents en 2014, afin de répondre aux besoins nouveaux issus de l'accroissement des flux d'informations et des besoins d'analyse engendrés.

Hors masse salariale, leur budget sera augmenté de 37,3 millions d'euros en 2014. Le budget de l'action 03 progresse donc de 16,57 % pour atteindre 263 millions d'euros de crédits de paiement, répartis entre la DGSE (251,5 millions d'euros) et la DPSD (11,4 millions d'euros). Masse salariale comprise, le budget proposé pour cette action est de 681,80 millions d'euros en autorisations d'engagement et de 743,91 millions d'euros en crédits de paiement soit respectivement une baisse de 7,8 % et une hausse de 7,03 %.

A. LE RENSEIGNEMENT EXTÉRIEUR

La sous-action **03-31** « **Renseignement extérieur** » comprend les crédits de la DGSE, le service de renseignement extérieur de la France, qui a pour mission d'apporter une aide à la décision gouvernementale et de contribuer à la lutte contre les menaces pesant sur la sécurité nationale ; la DGSE remplit une double mission de renseignement et d'action clandestine à l'étranger et assure dans ce cadre l'analyse, la synthèse et la diffusion des renseignements qu'elle recueille directement ou indirectement.

Les autorisations d'engagement pour cette sous-action étaient, dépenses de personnel comprises, de 644,52 millions d'euros en 2013 et il est proposé de les ramener à 588,61 millions d'euros au titre de l'année 2014. Les crédits de paiement s'élevaient à 600 millions d'euros en 2013 et atteindront 650,72 millions d'euros en 2014, soit une augmentation de 8,45 %.

Hors masse salariale, cette sous-action comprend trois opérations stratégiques.

(1) Le 2 octobre 2013.

La première, intitulée **« Activités opérationnelles »,** concerne les crédits de fonctionnement qui sont directement liés à l'activité de la DGSE. Elle comporte trois opérations budgétaires : alimentation, dépenses immobilières, déplacement et transport. Il s'agit notamment des capacités de projection du personnel de la DGSE, des frais de déplacement et des dépenses nécessaires au fonctionnement des bâtiments et des installations techniques. Avec 17,56 millions d'euros en autorisations d'engagement et en crédits de paiement, la dotation allouée à cette opération varie légèrement à la baisse.

La deuxième opération stratégique, intitulée **« Fonctionnement et activités spécifiques »**, comprend les dépenses liées au fonctionnement courant, à la mobilité des personnels, à la « compensatrice » SNCF, au soutien des personnels (frais de formation, d'habillement etc.) et au soutien des structures (frais d'entretien, de télécommunications…). Elle comporte cinq opérations budgétaires : compensatrice SNCF, mobilité des personnels, fonctionnement courant, soutien courant des structures, soutien des ressources humaines. La dotation de cette opération s'élève à 21,19 millions d'euros en autorisations d'engagement et en crédits de paiement, et connaît également une baisse modérée.

L'opération stratégique **« Renseignement »** se rapporte à la programmation des investissements et des dépenses opérationnelles de la DGSE qui concernent les besoins relatifs aux modes de recueil du renseignement, qu'il soit d'origine humaine, électromagnétique, informatique ou image. Elle comporte deux opérations budgétaires : appui au renseignement et renseignement. Les autorisations d'engagement s'élèvent à 15 millions d'euros et les crédits de paiement à 21,2 millions d'euros pour l'année 2014, soit respectivement une baisse de 25,6 % et une hausse de 41,2 %.

B. LE RENSEIGNEMENT DE SÉCURITÉ ET DE DÉFENSE

La sous-action **« Renseignement de sécurité et de défense »** comprend les crédits de la DPSD, dont la mission consiste à assurer la sécurité du personnel, des informations, des matériels et des installations sensibles. La DPSD est ainsi chargée d'une mission de protection associée au renseignement. À ce titre, elle est présente sur l'ensemble du territoire national ainsi qu'outre-mer et dans les pays étrangers où sont engagées les forces françaises. Son champ d'action comprend les forces armées, les établissements relevant du ministère de la Défense et les entreprises liées par contrat à la Défense.

Hors dépenses de personnel, sa dotation pour 2014 s'élève à 11,4 millions d'euros en autorisations d'engagement et en crédits de paiement, soit 4 % de moins qu'en 2013.

Hors masse salariale, cette sous-action comprend trois opérations stratégiques.

La première de ces opérations stratégique est intitulée **« Activités opérationnelles »** et se rapporte à l'activité hors métropole, aux déplacements aériens des personnels à l'étranger et au fonctionnement des bâtiments. Elle comporte deux opérations budgétaires : dépenses immobilières et déplacement et transport. Sa dotation pour 2014 de 706 394 euros.

La deuxième, intitulée **« Fonctionnement et activités spécifiques »,** concerne la communication, les relations publiques ainsi que des achats de matériels ou de véhicules ou encore le fonctionnement du site informatique de la direction. Elle comporte six opérations budgétaires : communication et relations publiques, compensatrice SNCF, fonctionnement courant, soutien courant des structures, soutien des matériels communs, soutien des ressources humaines ; les ressources allouées sont de 3 400 263 euros.

La dernière opération stratégique **« Renseignement »** se rapporte aux actions de contre-ingérence au profit des acteurs de la défense, institutionnels ou privés, dont le développement des moyens de contre-ingérence en matière de cyberdéfense. Elle comporte cinq opérations budgétaires : enquêtes-contrôles-sécurisation, matériels de transport, matériels divers, matériels techniques, systèmes d'information et de communication (SIC). Sa dotation est de 7,28 millions d'euros.

II. LA PROSPECTIVE DE DÉFENSE

L'action **07 « Prospective de défense »** est entièrement consacrée à la fonction stratégique connaissance et anticipation et mobilise 59,7 % des crédits du programme 144. Son périmètre couvre la totalité de l'analyse prospective, dont le financement d'une partie de la recherche par le ministère et celui d'écoles d'ingénieurs, opérateur de l'État sous tutelle de la direction générale de l'armement (DGA). Cette action comprend quatre sous-actions.

Pour l'année 2014, les autorisations d'engagement s'élèvent, hors dépenses de personnel, à 1,09 milliard d'euros et les crédits de paiement à 1,03 milliard d'euros, soit une hausse de 6,17 % des autorisations d'engagement et de 3,40 % des crédits de paiement.

A. L'ANALYSE STRATÉGIQUE

La sous-action **07-01 « Analyse stratégique »** a pour objet d'éclairer le ministre de la Défense sur l'évolution du contexte stratégique par l'analyse prospective de l'évolution de l'environnement international. Cette analyse associe, dans un cadre collégial, la délégation aux affaires stratégiques (DAS) du ministère de la Défense, la direction générale de l'armement (DGA), le secrétariat général pour l'administration (SGA) et l'état-major des armées (EMA). Il s'agit notamment de répertorier les risques et les menaces qui peuvent affecter la sécurité de la France et, au-delà, de l'Union européenne.

Les crédits alloués à cette sous-action financent notamment des études prospectives et stratégiques (EPS), qui bénéficient de 92 % des crédits au sein de cette sous-action, des programmes de post-doctorats ainsi que le programme « personnalités d'avenir défense », permettant au ministère d'inviter et d'accueillir en France des personnalités étrangères avec lesquelles il juge utile de nouer des liens.

L'Institut de recherche stratégique de l'École militaire (IRSEM) est transféré du programme 178 « Préparation et emploi des forces » au programme 144, les moyens consacrés à la recherche stratégique étant ainsi regroupés.

Pour 2014, les autorisations d'engagement s'élèvent à 6,08 millions d'euros, en baisse de 25 %, et les crédits de paiement à 6,89 millions d'euros, en hausse de 34,8 %.

Cette sous-action compte une opération stratégique intitulée **« Prospective et préparation de l'avenir »** qui comporte trois opérations budgétaires : études prospectives et stratégiques, programmes personnalités d'avenir et post-doctorat, recherche stratégique, dotées respectivement de 6 310 449 euros, 237 104 euros et 344 050 euros de crédits de paiement.

B. LA PROSPECTIVE DES SYSTÈMES DE FORCES

La sous-action **07-02 « Prospective des systèmes de forces »** vise à éclairer les choix concernant le futur de notre outil de défense. Les activités de cette sous- action, placées sous l'égide du comité d'architecture des systèmes de forces (CASF), sont conduites de manière collégiale par les officiers de cohérence opérationnelle (OCO) de l'EMA et les architectes de systèmes de forces (ASF) de la DGA.

Cette sous-action finance notamment l'élaboration par l'EMA, la DGA et les états-majors d'armée, en liaison avec la DAS, du « plan prospectif à 30 ans », ou « PP30 », qui dresse un état des réflexions prospectives destiné à orienter la réflexion sur les systèmes de force et leur cohérence capacitaire.

Ressortent également de cette sous-action les études à caractère opérationnel ou technico-opérationnel (EOTO), qui ont pour objet d'identifier les besoins opérationnels, de préciser les concepts à retenir en matière d'évolution des équipements et de leur doctrine d'emploi, puis d'orienter et d'exploiter des études de défense.

Outre les dépenses de fonctionnement du service d'architecture des systèmes de forces de la DGA, cette sous-action contribue également à la construction européenne en matière de sécurité et de défense car elle comprend la dotation annuelle de la France à l'Agence européenne de défense, soit 4,6 millions d'euros.

Il est proposé de fixer la dotation de cette sous-action pour 2014, hors frais de personnels, à 25,44 millions d'euros d'autorisations d'engagement et à 25,35 millions d'euros de crédits de paiement, ce qui correspond à une hausse respective de 3,15 % et 2,79 %.

Cette sous-action comprend quatre opérations stratégiques.

La première intitulée **« Activités opérationnelles »** comprend les dépenses de déplacement du service d'architecture des systèmes de forces (SASF) et du centre d'analyse technico-opérationnelle de défense de la DGA (CATOD) pour un montant de **145 994 euros** en autorisations d'engagement et en crédits de paiement.

La deuxième **« Fonctionnement et activités spécifiques »** couvre les dépenses de fonctionnement du service d'architecture des systèmes de force, celles du centre d'analyse technico-opérationnelle de la DGA ainsi que la part française du budget administratif de l'Agence européenne de défense (AED). Cette opération stratégique comporte cinq opérations budgétaires : communication et relations publiques, fonctionnement courant, soutien courant des structures, soutien des ressources humaines, subventions et transferts. Les autorisations d'engagement et les crédits de paiement proposés sont de **4,72 millions d'euros**

dont la subvention à l'AED représente 4,6 millions d'euros, soit une hausse de 2 %.

La troisième **« Opération stratégique : dissuasion »** concerne les études à caractère opérationnel ou technico-opérationnel (EOTO) nucléaires ; la prévision de crédits pour 2014 est de 3,09 millions d'euros en autorisations d'engagement et de trois millions d'euros en crédits de paiement.

La dernière **« Prospective et préparation de l'avenir »** concerne les études à caractère opérationnel ou technico-opérationnel (EOTO) hors dissuasion et comporte cinq opérations budgétaires : commandement et maîtrise de l'information, engagement-combat, études transverses, projection mobilité soutien, protection et sauvegarde. Il est proposé pour 2014, 17,4 millions d'euros en autorisations d'engagement et en crédits de paiement.

C. LES ÉTUDES AMONT

La sous-action **07-03 « Études amont »** a pour objet de financer des recherches et des études appliquées de nature technique en lien avec un besoin opérationnel prévisible et à amener des technologies nouvelles à un degré de maturité suffisant pour qu'elles puissent être maîtrisées par la base industrielle et technologique de défense (BITD) pour faire l'objet de programmes d'armement.

La dotation au titre de l'année 2014, s'élève à 809,27 millions d'euros en autorisations d'engagement et à 746,31 millions d'euros en crédits de paiement, correspondant respectivement à une croissance de 11 % et 6 % par rapport à l'exercice 2013.

Le rapporteur se félicitait déjà lors de l'examen des crédits du programme 144 pour 2013 que les crédits de ces études, restés stables, n'aient alors pas été utilisés par le Gouvernement comme variable d'ajustement dans un contexte budgétaire contraint. Il salue à nouveau l'effort consenti qui consacre l'importance déterminante de ces études pour la préparation des besoins militaires de demain.

Cette sous-action comprend deux opérations stratégiques.

La première est intitulée **« Prospective et préparation de l'avenir »**. Sa dotation est de 582,84 millions d'euros en autorisations d'engagement et de 520,31 millions d'euros en crédits de paiement.

Elle couvre les études amont qui seront, à partir de 2014, non plus gérées par systèmes de force, mais par agrégats sectoriels cohérents, hors dissuasion, rattachés aux six opérations budgétaires suivantes :

– Aéronautique et missiles - Les études concernent l'ensemble des aéronefs militaires ou à usage gouvernemental, avions et **drones de combat**, hélicoptères, avions de transport et de mission ; les technologies objet d'études

sont susceptibles de porter sur tous les éléments de l'aéronef, dont les capteurs et l'intégration des armements et des communications. Une partie des crédits 2014 sera notamment consacrée à la poursuite des essais du démonstrateur de drone de combat **Neuron** et des travaux de préparation du système de combat aérien futur, ainsi qu'aux évolutions du Rafale et du Tigre.

En matière de missiles, les études visent à conserver l'excellence de la filière européenne. En 2014, les travaux porteront notamment sur la préparation de la rénovation des missiles MICA ainsi que sur les senseurs, les liaisons de données et les futurs missiles de croisière et antinavires lourds.

La prévision de crédits pour 2014 est de 221 millions d'euros en autorisations d'engagement et de 149 millions d'euros en crédit de paiement.

– Information et renseignement classique - Participant de la souveraineté en tant qu'outil d'appréciation et de décision pour l'anticipation et la conduite des opérations, le renseignement et la maîtrise de l'information occupent une place centrale. Cette opération budgétaire inclut notamment les études portant sur le développement de la **cybersécurité** et *« les travaux visant à améliorer la protection des systèmes d'information, des systèmes d'armes mais aussi des systèmes industriels critiques »* [(1)]. Un accent particulier sera mis en 2014 sur la protection des systèmes d'armes. La proposition de dotation pour cette opération budgétaire est de 107 millions d'euros en autorisations d'engagement et de 129 millions d'euros en crédits de paiement.

– Information et renseignement espace - En 2014, les études porteront principalement sur les futurs systèmes de liaisons et de renseignement spatiaux et plus particulièrement sur la préparation du programme COMSAT NG en vue de la relève de l'actuel système Syracuse III à l'horizon 2019. Ces systèmes seront notamment utilisés pour les liaisons des **drones MALE** dont l'armée de l'air envisage de s'équiper. La proposition de dotation pour cette opération budgétaire est de 19,8 millions d'euros en autorisations d'engagement et de 20 millions d'euros en crédits de paiement.

– Naval - À la suite du programme d'études amont Espadon en voie d'achèvement sur le système de lutte anti-mine futur (SLAMF) faisant appel à des **drones de surface** et des **drones sous-marins**, les prochaines études porteront notamment sur la guerre électronique, les systèmes de combat modulaires, les capteurs et les émetteurs des bâtiments de surface. La proposition de dotation pour cette opération budgétaire est de 41 millions d'euros en autorisations d'engagement et de 26 millions d'euros en crédits de paiement.

– Terrestre, NRBC et santé - Les travaux sur la sécurité et la protection des combattants se poursuivront en 2014 ; des études sont notamment prévues sur la maîtrise des effets des munitions et leur guidage ainsi que sur l'autonomie décisionnelle en robotique. Les études sur la santé du militaire en opérations se

(1) PAP 2014.

poursuivent ainsi que sur l'alerte et la détection des agents biologiques et chimiques dans le cadre NRBC. La proposition de dotation pour cette opération budgétaire est de 52 millions d'euros en autorisations d'engagement et de 55 millions d'euros en crédits de paiement.

– Innovation et technologies transverses - Cette opération budgétaire concerne les technologies duales et a vocation à financer les projets innovants des PME/entreprises intermédiaires et de la recherche académique *via* le régime d'appui pour l'innovation duale (dispositif RAPID) en lien avec la direction générale de la compétitivité, de l'industrie et des services (DGCIS) et *via* l'accompagnement spécifique des travaux de recherche et d'innovation de défense (programme ASTRID) dont l'agence nationale de la recherche (ANR), qui dépend du ministère de l'Enseignement supérieur et de la recherche, assure la gestion. Entrent également dans le spectre de cette opération la participation financière du ministère de la Défense à la politique des pôles de compétitivité et le financement de thèses et de stages de recherche. La proposition de dotation pour cette opération budgétaire est de 140,2 millions d'euros en autorisations d'engagement et de 140,1 millions d'euros en crédits de paiement.

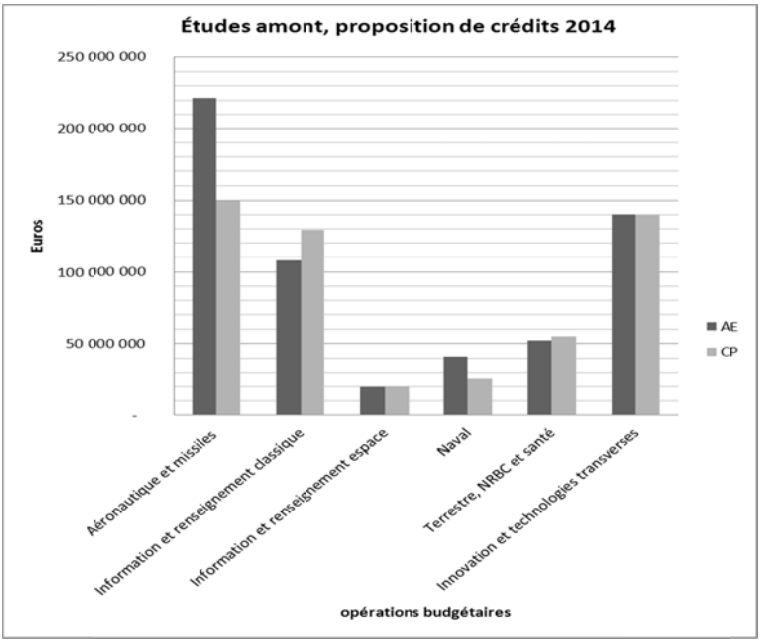
CRÉDITS DE PAIEMENT CONSACRÉS AUX ÉTUDES DE DÉFENSE ET À LA R&D ENTRE 2009 ET 2014 :

M€ courants	LFI 2009	LFI 2010	LFI 2011	LFI 2012	LFI 2013	PLF 2014
Budget défense [1]	42 541	41 990	41 844	41 227	41 274	42 057
EA	660,1	653,2	645,2	633,2	702,9 [2]	745,9
R&T	821,0	814,7	800,5	780,5	851,7 [2]	867,2
Études de défense	**1 571,3**	**1 620,1**	**1 647,9**	**1 644,0**	**1 728,4**	**1 728,0**
dont recherche CEA	527,4	585,5	626,6	647,7	615,0	640,8
dont EPS	3,9	3,5	4,2	4,5	**4,7**	5,8
dont EOTO	19,0	18,5	19,6	18,5	**19,8**	20,5
dont recherche duale	200,0	200,0	196,9	192,9	192,2	192,9
Études de défense (% Budget)	3,7 %	3,9 %	3,9 %	4,0 %	4,1%	4,1 %
Développements (NUC et hors NUC)	2 253,1	1 948,5	1 629,6	1 800	1 550,0	1 835,1
Total R&D	**3 824,3**	**3 568,6**	**3 277,5**	**3 444,0**	**3 278,4**	**3 563,1**

[1] Crédits regroupant ceux de la mission « Défense », ceux des programmes 167 et 169 de la mission « Anciens combattants, mémoire et liens avec la Nation » et ceux du programme 191 de la mission « recherche et enseignement supérieur ». Les crédits du programme 152 « gendarmerie nationale » ne sont plus dans le périmètre du ministère de la défense. En 2009 et 2010, les crédits présentés n'incluent pas le plan de relance de l'économie.

[2] Hors compte d'affectation spéciale « Gestion et valorisation des ressources tirées de l'utilisation du spectre hertzien » (CAS Fréquence) : 45 M€.

Source : ministère de la Défense.



La seconde opération stratégique de la sous-action 07-03 est intitulée « **Dissuasion** » et couvre les études amont nucléaires. La proposition de dotation est pour 2014 de 22,64 millions d'euros en autorisations d'engagement et de 22,6 millions d'euros en crédits de paiement.

D. LA GESTION DES MOYENS ET LES SUBVENTIONS

La sous-action 07-04 **« Gestion des moyens et subventions »** concerne les subventions pour charges de service public destinées à l'Office national d'études et de recherches aérospatiales (ONERA) ainsi qu'aux écoles sous tutelle de la DGA [(1)], à l'Institut Saint-Louis (ISL) et à des organismes d'études. Elle couvre également une partie des dépenses de fonctionnement courant de la direction de la stratégie de la DGA et le soutien des postes permanents à l'étranger [(2)]. Ces crédits financent également quelques mesures prises en faveur des PME-PMI stratégiques du secteur de la défense.

Il est proposé d'en fixer le montant à 258,44 millions d'euros en autorisations d'engagement et en crédits de paiement pour 2013, ce qui correspond à une baisse de 4,4 % par rapport aux montants fixés pour l'exercice 2013.

Cette sous-action comprend trois opérations stratégiques.

La première, intitulée **« Activités opérationnelles »**, couvre les dépenses immobilières et les déplacements de la direction de la stratégie de la DGA. Elle comporte deux opérations budgétaires, « dépenses immobilières » et « déplacement et transport ». La dotation proposée est de 449 248 euros en autorisations d'engagement et en crédits de paiement.

La deuxième opération stratégique **« Fonctionnement et activités spécifiques »** comprend les dépenses de fonctionnement de la DGA et les subventions à l'ONERA, l'ISL et aux écoles sous tutelle de la DGA. Elle comporte neuf opérations budgétaires : communication et relations publiques, compensatrice SNCF, fonctionnement courant, mobilité des personnels, prestations intellectuelles, relations internationales, soutien courant des structures, soutien des ressources humaines, subventions et transferts.

Le positionnement stratégique de l'ONERA est en cours de redéfinition par le ministère de la Défense, son autorité de tutelle. Un groupe de haut niveau intitulé ONERA 2020, devant rendre ses conclusions courant 2014, a été mis en place afin d'arrêter un nouveau modèle économique et d'orienter l'ONERA vers un partenariat accru avec la recherche académique et l'industrie.

---

(1) École polytechnique, Institut supérieur de l'aéronautique et de l'espace (ISAE), École nationale supérieure de techniques avancées ParisTech (ENSTA ParisTech), École nationale supérieure de techniques avancées Bretagne (ENSTA Bretagne, ancienne ENSIETA).

(2) Berlin, Londres, Madrid, Rome, Washington, Stockholm, OTAN et UE.

En ce qui concerne l'Institut Saint-Louis, le délégué général pour l'armement et le secrétaire d'État allemand à la Défense ont mandaté un groupe de haut niveau pour établir une stratégie à long terme pour l'ISL, en vue d'améliorer son attractivité et sa réussite scientifique et économique. Les grands axes en sont notamment la réduction des domaines d'activité, une meilleure valorisation industrielle des travaux réalisés et, à terme, l'évolution de l'institut vers un laboratoire européen de défense et de sécurité.

L'Institut Saint-Louis travaille depuis 2010 sur un mini-drone d'observation en milieu urbain (GLMAV) [1]. Il s'agit d'un projectile lancé par arme à tube. Arrivé à son apogée, il déploie des rotors d'hélicoptère, observe la scène quelques minutes et revient à son point de départ. Ce drone, essentiellement destiné aux forces de sécurité, pourrait également servir en opération extérieure, lors de conflits en zone urbaine et, à ce titre, intéresser les forces terrestres. Ce projet de recherche fait l'objet d'un cofinancement par l'ANR.

La dotation proposée pour cette opération stratégique est de 255,99 millions d'euros en autorisations d'engagement et en crédits de paiement. La subvention allouée à l'École Polytechnique comprend une dotation en fonds propres ponctuelle de 5,5 millions d'euros correspondant à la participation du ministère de la Défense à l'extension du laboratoire de l'école.

Le rapporteur observe que l'ensemble des subventions à l'ONERA et aux différentes écoles est en recul en moyenne de 3 % à 4 % [2]**; si, compte tenu des contraintes budgétaires, il lui semble normal de demander aux opérateurs de l'État de mettre en œuvre des efforts d'économie, il estime cependant qu'il convient de soutenir la formation des techniciens et des scientifiques dont notre pays risque de manquer demain** (*cf.infra*) **et que les crédits budgétaires consacrés à l'enseignement devraient suivre une courbe identique à celle des crédits du ministère de l'Enseignement supérieur et de la recherche qui ont été sanctuarisés.**

La dernière opération stratégique **« Prospective et préparation de l'avenir »** finance des subventions versées à des organismes d'études, des fondations, des confédérations d'officiers de l'armement, un soutien aux PME/PMI. La dotation proposée est de deux millions d'euros en autorisations d'engagement et en crédits de paiement.

(1) Gun launched micro air vehicle.

(2) ONERA –13 % (notamment en raison d'un abattement non pérenne de 10 millions d'euros correspondant à des crédits gelés pour une opération immobilière non réalisée), École polytechnique – 4,4 % (hors dotation laboratoire), ISAE – 3,2 %, ENSTA ParisTech – 3,1 %, ENSTA Bretagne – 2,6 %. La subvention de l'ISL reste stable.

III. LES RELATIONS INTERNATIONALES

L'action **08 « Relations internationales »** concentre 5,9 % des crédits du programme 144 et contribue à la politique extérieure de la France. Masse salariale comprise, elle est dotée, au titre de l'année 2014, de 116 millions d'euros en autorisations d'engagement et en crédits de paiement, soit une décrue de 10 %.

A. LE SOUTIEN AUX EXPORTATIONS

La sous-action **08-01 « Soutien aux exportations** » vise à contribuer à la vitalité de l'industrie de défense par le développement des exportations d'armement. Il est proposé de la doter, titre 2 compris, de 14,49 millions d'euros en autorisations d'engagement et en crédits de paiement pour l'année 2014, soit 5,91 % de moins qu'en 2013 en autorisation d'engagement et 4,23 % de moins en crédits de paiement. Cette baisse s'explique par l'absence du Salon du Bourget qui ne se tient que les années impaires ; en 2014 seront organisés les salons Eurosatory et Euronaval dont le coût est évalué à 2,2 millions d'euros, soit 0,57 million d'euros de moins que le Salon du Bourget.

Cette sous-action comprend deux opérations stratégiques.

L'opération stratégique **« Activités opérationnelles »** est destinée au financement des mutations du personnel ainsi qu'aux déplacements nationaux et internationaux du personnel en charge du soutien à l'exportation et de l'entretien des relations bilatérales. La dotation proposée est de 1,3 million d'euros en autorisations d'engagement et en crédits de paiement.

La seconde, intitulée **« Fonctionnement et activités spécifiques »**, concerne les dépenses liées à la promotion des exportations, dont le financement du pavillon Défense aux salons d'armement français, le soutien des PME/PMI à l'étranger, les dépenses de fonctionnement et de mobilité des postes permanents hors pays membres de l'OTAN. La proposition de dotation est de 5,2 millions d'euros en autorisations d'engagement et en crédits de paiement. Elle comporte cinq opérations budgétaires : compensatrice SNCF, fonctionnement courant, mobilité des personnels, promotion des exportations, relations internationales. La ligne « promotion des exportations » représente plus de 80 % de la dotation totale de cette opération stratégique.

Le tableau ci-dessous indique le montant des prises de commandes enregistrées de 2008 à 2012, étant entendu que les ventes d'armement sont des processus longs, à évaluer sur l'ensemble de la période et non en fonction des variations annuelles moins signifiantes.

MONTANT DES PRISES DE COMMANDES D'ARMEMENT À L'EXPORTATION

(en millions d'euros courants)

2008	2009	2010	2011	2012
6 583,5	8 164,1	5 117,6	6 516,9	4 817,2

Source : ministère de la Défense.

B. LA DIPLOMATIE DE DÉFENSE

La sous-action **08-02 « Diplomatie de défense** » a pour objet de contribuer à la diplomatie de défense dans le cadre de la politique extérieure de la France et de financer les activités de contrôle des transferts de biens et de technologies. Les crédits de cette sous-action couvrent notamment les dépenses nécessaires au fonctionnement et aux activités des postes permanents d'attachés de défense et de leurs adjoints, installés au sein des ambassades de France à l'étranger. Cette sous–action couvre également la contribution annuelle, de 21,23 millions d'euros en 2014, qui sera versée par la France au Gouvernement de la République de Djibouti en compensation de la présence des forces françaises sur son sol.

Le réseau diplomatique de défense a vu ses effectifs diminuer de 30 % depuis la réforme de 2008, alors même que, dans le cadre d'un redéploiement tenant compte la stratégie internationale du ministère, l'implantation française à l'étranger est passée de 86 à 88 pays. Un nouveau redéploiement tenant compte des conclusions du Livre blanc est à l'étude.

Pour 2013, cette sous-action est dotée, dépenses de personnels comprises, de 101,8 millions d'euros en autorisations d'engagement et en crédits de paiement, soit 11,56 % de moins qu'en 2013 en autorisations d'engagement et 11,35 % de moins en crédits de paiement.

Elle comporte trois opérations stratégiques.

L'opération intitulée « **Activités opérationnelles** » couvre les déplacements du personnel en poste dans les ambassades de France à l'étranger. Sa dotation est de 2,04 millions d'euros en autorisations d'engagement et crédits de paiement.

La deuxième opération, « **Fonctionnement et activités spécifiques** » couvre les dépenses, autres que les transports et les actions de coopérations, effectuées par les personnels en poste à l'étranger, la subvention versée à la République de Djibouti et l'indemnité compensatrice SNCF. Elle comporte deux opérations budgétaires, compensatrice SNCF et relations internationales. La dotation proposée pour cette sous-action est de 25,5 millions d'euros en autorisations d'engagement et crédits de paiement.

La dernière des trois opérations **« Prospective et préparation de l'avenir** » concerne la gestion, déléguée par l'État au commissariat à l'énergie

atomique et aux énergies alternatives (CEA), des actions entreprises dans le cadre du partenariat mondial contre la prolifération des armes de destruction massive et des matières connexes (PMG8), ainsi que des fonds versés. La dotation de cette ligne est de 1,01 million d'euros en autorisation d'engagement et crédits de paiement, soit une baisse de 4,7 millions d'euros par rapport à 2013, imputable à un recentrage des activités.

ÉVOLUTION DES CRÉDITS DESTINÉS À LA DIPLOMATIE DE DÉFENSE

En M€	LFI 2011	LFI 2012	LFI 2013	PLF 2014	Évolution 2013/2014 en %
Personnel	65,48	69,31	78,06	73,2	- 6,22 %
Fonctionnement	4,99 (1)	5,32	6,49	6,36	- 2 %
Intervention	31,14	26,04	30,29	22,25	- 26,54 %
Dont contribution Djibouti	*25,40*	*20,08*	*24,55*	*21,23*	*- 13,52 %*
TOTAL	70,47	100,67	114,84	101,81	- 11,35 %

(1) : auxquels se sont ajoutés 1 M€ en gestion par redéploiement.

Source : ministère de la Défense.

*

* *

M. Philippe Errera, directeur chargé des affaires stratégiques, a indiqué à la commission (1) qu'une réforme de la délégation aux affaires stratégiques du ministère de la Défense, qui s'achèvera en 2014, a été entreprise pour en faire une direction d'administration centrale unique rattachée directement au ministre.

Tout en conservant le pilotage du programme budgétaire 144, en veillant à la cohérence des ressources humaines et financières nécessaires à la fonction stratégique « connaissance et anticipation », dont celles des services de renseignement de défense et les études amont de la DGA, cette direction prendra en charge des fonctions à caractère international qui sont aujourd'hui exercées par l'état-major des armées et la direction générale de l'armement.

(1) Lors de la réunion du 2 octobre 2013.

DEUXIÈME PARTIE : LES DRONES AÉRIENS ET LA CYBERDÉFENSE

Dans le prolongement l'avis budgétaire de 2013 qui présentait une analyse approfondie des études amont, le rapporteur a choisi de donner un « coup de projecteur » sur deux sujets majeurs issus des priorités découlant du Livre blanc 2013 et du projet de loi de programmation militaire : les drones aériens et la cyberdéfense.

Mais le choix de ces deux sujets, qui ne sont pas sans liens, a également été dicté par l'actualité : par l'intervention de la France au Mali et l'opération Serval d'abord, et par l'affaire Snowden et les révélations d'espionnage étatique à grande échelle ensuite.

Dans le premier cas, la France, qui a conduit une opération militaire remarquable, a dû compter sur une ressource alliée pour compléter sa maigre flotte de drones MALE à bout de souffle, dans le second les divulgations successives révèlent une vulnérabilité dont l'ampleur était insoupçonnée à ce jour.

Le rapporteur pose donc clairement la question de la rupture capacitaire en matière de drones MALE et de drones tactiques et s'interroge en matière de cybersécurité sur l'adéquation des mesures mises en œuvre pour faire face à un enjeu dont la prise de conscience, bien réelle, semble toutefois rester cantonnée à un milieu de spécialistes et de décideurs informés.

Dans le cadre de la préparation du sommet de défense européen du mois de décembre, l'Agence européenne de défense (AED) et Mme Catherine Ashton, haut représentant de l'Union pour les affaires étrangères la politique de sécurité, ont présenté, le 15 octobre 2013, un rapport identifiant quatre priorités devant résulter en des coopérations entre les états membres, au rang desquelles sont la cyberdéfense et la mise au point d'un drone MALE à l'horizon 2020.

Il n'est donc pas interdit d'espérer.

I. LES DRONES AÉRIENS

A. QU'EST-CE QU'UN DRONE AÉRIEN ?

Craints, mais, jusqu'à une période récente, peu connus du grand public, relativement peu nombreux au sein des forces, les drones aériens militaires sont devenus en quelques années des éléments essentiels au renseignement et à l'appui des troupes en opération. Ils permettent en effet de voir au-delà de la colline ou beaucoup plus loin selon leur autonomie. Pour les plus puissants d'entre eux, ils présentent sur l'avion l'avantage de pouvoir demeurer au-dessus d'un site beaucoup plus longtemps. Les informations qu'ils recueillent en temps réel permettent d'adapter la stratégie et l'action. Ils contribuent ainsi à préserver la vie des soldats, celle des pilotes et celle des troupes au sol qui s'engagent sur un terrain plus sûr.

Amorcée dans les années 1960, alors qu'il s'agissait d'engins rapides apparentés à des missiles qui recueillaient de l'information en différé, la présence des drones dans les armées n'a cessé de prendre de l'importance et, qu'ils relèvent de l'armée de terre ou de l'armée de l'air, les drones ont été de tous les conflits des dernières années.

Les drones sont des objets pilotés à distance qui réalisent différentes opérations sans présence humaine à leur bord. Ils peuvent être de taille et d'aspect différents et se définissent d'abord par le milieu dans lequel ils opèrent : il existe des drones terrestres, maritimes et aériens. Ils s'apparentent donc selon les cas à un robot, un modèle réduit, un bateau, une torpille, un missile, un avion ou un hélicoptère.

S'il n'existe pas de classification universelle pour les drones aériens, il est communément admis de les définir principalement par leur autonomie et l'altitude à laquelle ils volent.

D'autres critères tels que leur taille, leur capacité d'emport, leurs liaisons (LOS [(1)] ou satellite) et leur puissance électrique disponible permettent d'affiner cette première définition. Les catégories de drones présentant une certaine porosité, des missions identiques peuvent être effectuées par des drones de différente nature bien que leur usage soit complémentaire en règle générale.

L'offre de drones se segmente ainsi :

– les micro ou minidrones, ou jumelles déportées du combattant, petits drones lancés à la main et extrêmement mobiles ;

(1) Liaison à portée optique, line of sight.

– les drones tactiques de la taille d'un petit avion et lancés par catapulte, ils ont une autonomie variable de l'ordre de cinq heures, volent à une hauteur maximum de 3 500 m et pèsent en général moins de 600 kg ;

– les drones MALE [(1)], moyenne altitude longue endurance, ou drones de théâtre, d'une envergure de 10 à 20 m, ils volent entre 5 000 et 15 000 m à une vitesse variant entre 200 et 400 km/h avec une portée de 1 000 km et des liaisons LOS et/ou satellite SatCom ;

– le drone HALE [(2)], haute altitude longue endurance, ou drones stratégiques, il vole à 20 000 m et peut effectuer des vols de très longue distance.

Un drone se distingue également par sa **charge utile** fixe ou interchangeable, c'est-à-dire par les équipements dont il dispose pour remplir sa mission. Il s'agit le plus souvent, et de manière non exhaustive, d'une caméra optronique ou infrarouge pour les vols de nuits, d'un radar GMTI [(3)] qui capte les mouvements, de capteurs électromagnétiques ou charge de guerre électronique de communication, mais il peut s'agir aussi d'un pointeur et désignateur de cibles laser, d'un système d'armes, d'un missile ou d'une charge à transporter.

La puissance électrique disponible, fournie par le drone, conditionne l'emport de capteurs en fonction de leur besoin d'énergie.

Mais un drone est un système complexe composé d'éléments interdépendants :

Si l'on parle communément de drone en se référant uniquement à la partie aérienne visible, le drone fait dans tous les cas partie d'un système sans lequel il ne pourrait être mis en œuvre et sans lequel l'information recueillie ne pourrait être exploitée.

Un système de drones se compose des éléments suivants [(4)] :

– le ou les vecteurs aériens, dont l'aspect tend à se rapprocher des appareils pilotés, avions ou hélicoptères ;

– les charges utiles (*cf. supra*) ;

– les liaisons de données partagées entre le vecteur et la station de contrôle ;

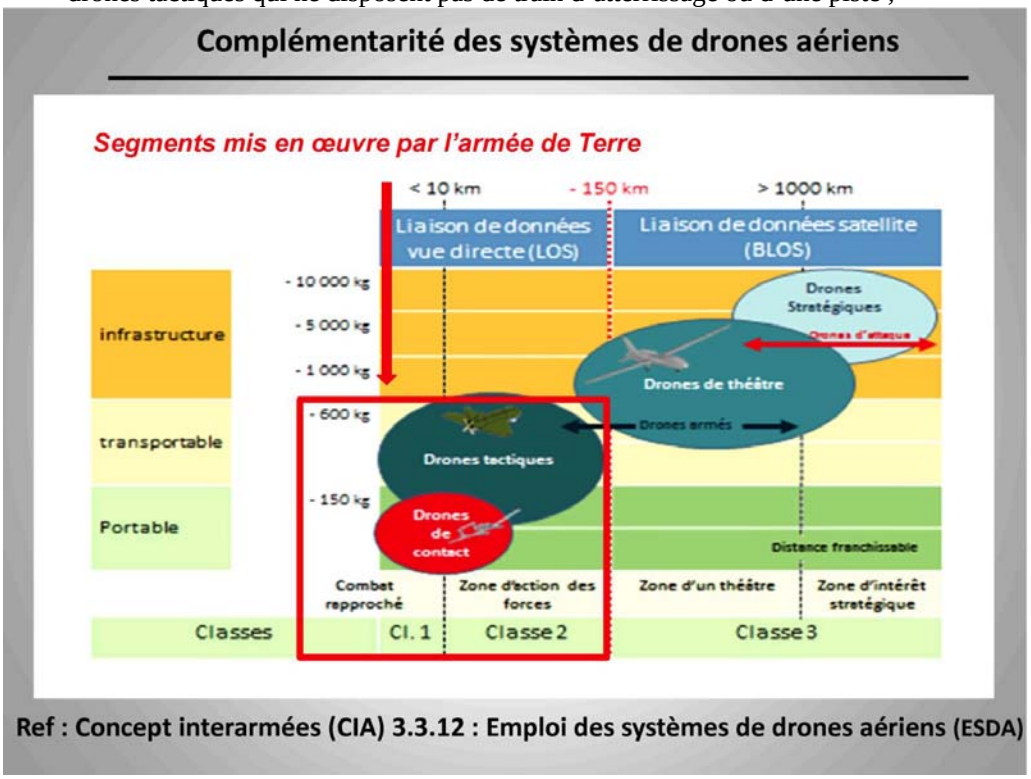
– la station de contrôle ;

---

(1) Medium altitude long endurance.
(2) High altitude long endurance.
(3) Ground moving target indicator.
(4) « Les drones aériens : passé, présent et avenir », Centre d'études stratégiques aérospatiales, La documentation française.

– le système de mise en œuvre : un système de lancement, de type catapulte, ou une piste ;

– le système de récupération sous forme de parachute et d'airbags pour les drones tactiques qui ne disposent pas de train d'atterrissage ou d'une piste ;



Source : État-major de l'armée de terre.

B. LA SITUATION CHEZ NOS PARTENAIRES EUROPÉENS

Nos principaux voisins européens mettant en œuvre des systèmes de drones sont essentiellement le Royaume-Uni, l'Allemagne et l'Italie. Il se trouve également des constructeurs, notamment dans le secteur des drones à voilure tournante, en Autriche avec Schiebel, en Suède avec SAAB et CybAero et en Espagne avec Indra et EADS/Cassidian.

Les Pays-Bas, la Suède, le Danemark et la Grèce utilisent ou ont utilisé des drones tactiques français *SDTI-Sperwer* de Sagem.

1. Le Royaume-Uni

En matière de drones aériens, les Britanniques sont notamment équipés de systèmes MALE américains *MQ-9 Reaper* (General Atomics), de systèmes

tactiques israéliens *Hermes 450* (Elbit), plateforme du *Watchkeeper* développé sous la co-traitance d'Elbit et de Thales-UK, ainsi que de systèmes portables américains *Desert Hawk III* (Lockheed Martins), *Tarantula Hawk* (Honeywell) et de micro-drones norvégiens *Black Hornet* (Prox Dynamics).

Le Royaume-Uni utilise depuis 2008 des drones *Reaper* armés en Afghanistan.

Le projet franco-britannique d'un programme de drone MALE, basé sur la solution Telemos proposée conjointement par Dassault-Aviation et BAE Systems elle-même dérivée du projet Mantis de BAE Systems n'a pas abouti.

Le Royaume-Uni travaille par ailleurs avec la France, dans le cadre des accords de Lancaster House, au programme d'études FCAS-DP (*Future Combat Air System-Demonstration Program*) portant sur les systèmes de drones de combat (UCAS)[(1)] sous la conduite de Dassault-Aviation et BAE Systems.

La marine britannique a mené des expérimentations dans le domaine des systèmes tactiques navals avec le *Scan Eagle* américain (Insitu Boeing).

2. L'Allemagne

La Bundeswehr est équipée notamment de drones portables légers *Luna* et de mini-drones allemands *Aladin* (EMT), ainsi que de systèmes tactiques allemands *KZO* (Rheinmetall puis Rheinmetall-Cassidian/EADS).

En matière de systèmes MALE, l'Allemagne utilise, dans le cadre d'un contrat de location dont les interlocuteurs du rapporteur ont indiqué qu'il se terminait en 2015, des drones israéliens *Heron 1* (IAI), actuellement mis en œuvre en Afghanistan. La Bundeswehr se trouve donc devant une vraie rupture capacitaire et devra donc, en l'absence de solution pérenne et en l'attente d'un hypothétique drone MALE allemand ou européen, recourir à une nouvelle solution intérimaire forcément israélienne ou américaine.

Le choix est suspendu au calendrier politique allemand, l'élection du Bundestag s'étant déroulée en septembre 2013. La décision dépendra donc des options prises par le nouveau gouvernement. Si la Luftwaffe semble préférer le *Predator Reaper* américain de General Atomics, il existe en Allemagne des tenants du *Heron TP* car il sera très difficile de certifier un drone américain pour le faire voler dans le ciel allemand. Or, les Allemands semblent souhaiter un drone qui puisse décoller d'Allemagne avec des stations au sol en Allemagne.

Le projet de système MALE Talarion proposé par Cassidian/EADS à l'Allemagne et à la France, n'a pas dépassé le stade d'une étape de levée de risques.

---

(1) Unmanned combat air system.

Le projet de drone HALE [1] germanisé, trop ambitieux, a été abandonné.

L'abandon de l'*EuroHawk*

Le 15 mai 2013, le ministère allemand de la défense a annoncé l'arrêt du programme de système HALE *EuroHawk*, dérivé du *Global Hawk* américain block 20 (Northrop Grumman) poursuivi dans le cadre du programme AGS [2] de l'OTAN, auquel elle n'a toutefois pas renoncé. Après avoir dépensé 560 millions d'euros, sur le contrat d'1,3 milliard d'euros, et réceptionné un seul des cinq démonstrateurs prévus, l'Allemagne aurait encore dû payer un nouveau surcoût de 500 millions d'euros [3] pour espérer certifier cet appareil et l'insérer dans la circulation aérienne, alors même que le premier vol d'essai avait été effectué avec succès en janvier 2013. Mais il semble que l'absence de système anti-collision ait été rédhibitoire pour l'Agence européenne de sécurité aérienne (AESA) dans le cadre d'une autorisation de survol de zones habitées.

Au-delà des décisions politiques, des problèmes de gouvernance dont a pu pâtir le projet, les difficultés rencontrées pour obtenir certaines informations techniques des États-Unis auraient pesé dans cette décision. De plus, l'abandon graduel par les forces américaines des plates-formes *Global Hawk* block 20 et 30 aurait conduit l'Allemagne à maintenir un micro-parc au soutien très coûteux avec un surcoût logistique évalué à un milliard d'euros pour la durée de vie du programme.

La décision allemande illustre :

– les difficultés posées par la sûreté de l'utilisation des drones et par leur certification pour garantir la maîtrise du risque encouru par les tiers survolés et pour s'assurer de leur aptitude à fréquenter des espaces aériens non spécifiques ;

– les difficultés techniques liées à l'intégration d'une charge utile complexe sur une plate-forme achetée sur étagère, dont le dossier de définition n'est pas maitrisé ;

– les risques logistiques inhérents à la mise en service d'un micro-parc acheté à l'étranger, sans maîtrise du dossier de définition, engendrant des coûts logistiques potentiellement prohibitifs.

L'Allemagne a tiré de cet échec les enseignements suivants dont le rapporteur estime que, en dehors du dernier point[4], ils peuvent s'appliquer de manière universelle et particulièrement aux achats et aux projets de conception de drones dans lesquels notre pays s'engage ou pourrait s'engager. Ainsi :

– il convient de clarifier le cadre de certification avant tout achat de drone, MALE notamment, dans l'hypothèse où il est souhaité de le faire voler sur le territoire européen ;

– il faut s'engager activement, au plus vite, au sein de l'UE et de l'OTAN pour que les questions de certification et d'insertion des drones dans l'espace aérien européen reçoivent une réponse conjointe et harmonisée s'appliquant à tous ;

– il est indispensable de s'assurer, le cas échéant, une maîtrise technique suffisante du projet, selon son cadre contractuel, pour ne pas être unilatéralement et

(1) Haute altitude longue endurance.
(2) Allied ground surveillance.
(3) Assertion contestée par EuroHawk GmbH dans un communiqué de presse, http://www.eurohawk.de.
(4) En France, la DGA est le certificateur des aéronefs militaires. La DGA a accordé à ce jour quatre certificats de type « drone » pour les modèles suivants : le Sperwer SDTI, le Tracker DRAC, le SIDM Harfang, et le Skylark I-LE UAV System (mini-drone en service dans les forces spéciales).

entièrement dépendant d'un partenaire étranger, surtout sur un projet aussi novateur et complexe que peut l'être un système de drones ;

– il est recommandé d'étudier la mise en place d'un mécanisme alertant le ministre très en amont en cas de problème d'ampleur sur les programmes ;

– il est nécessaire de créer une autorité allemande de sûreté aéronautique militaire indépendante.

Source : ministère de la Défense.

Les Allemands ont conduit par ailleurs plusieurs projets de R&T, dont le démonstrateur de drone de combat Barracuda de Cassidian/EADS associant l'Espagne et autofinancé par l'industrie, pour lequel deux prototypes ont été construits, le premier s'étant abîmé en mer lors d'essais.

La Marine allemande expérimente, pour sa part, des drones tactiques navals avec le *S-100* autrichien (Schiebel).

3. L'Italie

L'Italie utilise principalement des drones américains dont des drones tactiques *RQ-7 Shadow 200* (AAI) et des drones MALE *Predator A* non armés (General Atomics), fabriqués sous licence en Italie, tout en se dotant de *Predator B/MQ-9 Reaper*. Les Italiens emploient également des drones portables *RQ-11B Raven* (Aerovironment).

L'Italie participe au programme AGS de l'OTAN, systèmes HALE *Global Hawk* de Northrop Grumman, dont les drones sont stationnés sur l'aéroport de Sigonella en Sicile. Par ailleurs, l'Italie est présente au sein du programme de démonstrateur nEUROn au travers d'Alenia Aermacchi/Finmeccanica.

Une autre filiale de Finmeccanica, Selex ES, produit un drone tactique, le *Falco*, et développe un drone MALE, véhicule optionnellement piloté (OPV), le P.1HH Hammerhead, en association avec l'avionneur italien Piaggio Aero.

Il semblerait que l'Italie ait rencontré des difficultés pour obtenir des États-Unis l'autorisation d'armer les drones *Reaper* qu'elle engage en Afghanistan et pourrait de ce fait se tourner vers un projet européen de drone MALE.

C. LA PLACE DES DRONES DANS LES ARMÉES AUJOURD'HUI

1. L'armée de terre

a. Les mini drones

i. Leurs caractéristiques

L'armée de terre est équipée de drones de reconnaissance au contact *DRAC* (Survey Copter/Cassidian) qui fournissent un appui renseignement aux unités au contact du niveau de la brigade à celui du groupement tactique interarmes (GTIA).

D'un poids de 8 kg environ, ce drone léger de courte portée (10 km) lancé à la main dispose d'une autonomie de 60 à 90 mn. Il est équipé d'une liaison radio et d'une charge utile optique ou infrarouge. Mis en œuvre par deux opérateurs, il est également très mobile, deux vecteurs aériens et un terminal de liaison de données étant conditionnés pour être transportés dans deux sacs à dos.

L'armée dispose aujourd'hui de 62 systèmes et de 106 vecteurs aériens dont elle attend encore 35 exemplaires devant être livrés fin 2013.

ii. Leur emploi

Le système a d'abord été déployé dans le cadre d'expérimentations opérationnelles au Kosovo et en Afghanistan entre juillet 2008 et juillet 2010 avant de l'être sur deux sites en Afghanistan, entre octobre 2010 et juin 2012, où il a réalisé plus de 1 000 missions opérationnelles. Depuis février 2012, ce système est projeté au Mali et a déjà réalisé plus de 140 missions opérationnelles dans le cadre de l'opération Serval.

b. Le drone du génie

Le système ***Drogen*** (Infotron) est un nouveau système à voilure tournante destiné aux unités du génie dans le cadre de leur mission d'ouverture d'itinéraires piégés et de la lutte contre les engins explosifs improvisés. D'une portée de 3 km et d'une endurance de 30 minutes, ce système dispose de capteurs optiques bi-senseurs, visible et infrarouge, particulièrement performants et peut être mis en œuvre de manière totalement automatique par un seul opérateur. Acquis en urgence opération, trois systèmes ont été commandés : deux ont été réceptionnés en septembre 2012 et mai 2013, le dernier étant attendu fin 2013.

c. Les drones tactiques

i. Leurs caractéristiques

L'armée de terre dispose d'un seul type de drone tactique, le système de drone tactique intérimaire *SDTI Sperwer* de Sagem. Il s'agit de systèmes composés d'un segment sol [(1)]et de vecteurs aériens d'environ 300 kg équipés de liaisons radio, d'une charge utile optique et infrarouge qui décollent au moyen d'une catapulte et peuvent atteindre 180 km/h et voler durant 3 à 4 heures dans un rayon de 80 km de leur point de départ.

L'armée de terre possède deux systèmes *SDTI* comprenant chacun deux segments sol. Les vecteurs aériens qui étaient au nombre de 18 au départ ont dû être graduellement remplacés afin de maintenir en service une flotte de l'ordre de 15 vecteurs, dont six ont été achetés aux forces canadiennes en 2009. Une commande de six vecteurs de nouvelle génération a été passée en 2012 avant que Sagem ne ferme définitivement sa chaîne de production.

Les catapultes actuelles sont en cours de remplacement par de nouveaux lanceurs *Robonic* ménageant davantage les charges utiles et les vecteurs, très éprouvés lors du processus de lancement.

ii. Leur emploi

Le *SDTI* est employé au niveau d'une brigade ou d'une *task force* terrestre, sous les ordres de son chef tactique. Il permet de mener, avec une grande réactivité, des missions de surveillance ou de renseignement d'appui au plus près des unités engagées au contact qui disposent ainsi en temps réel, sans intermédiaire et au rythme des opérations des informations recueillies par le drone.

Un module constitué de deux segments sol et de six à huit vecteurs a été déployé de novembre 2008 à juin 2012 en Afghanistan où il a effectué plus de 770 missions.

Le rapporteur a pu constater, en se rendant au 61^{e} régiment d'artillerie de Chaumont, régiment de renseignement image de l'armée de terre et seul régiment de drones, la qualité des images produites et la plus-value apportée par ces informations que les soldats peuvent consulter en temps réel, à distance du segment sol, sur des terminaux individuels (RVT) [(2)]. Il a également pu apprécier la flexibilité et la facilité de la mise en œuvre du *DRAC*.

(1) Le vecteur du système SDTI peut être pris en main entre deux stations au sol, ce qui élargit son rayon d'action.

(2) Remote video terminal.

2. Les drones de l’armée de l’air

L’armée de l’air est équipée depuis 2008 du système intérimaire de drones MALE ***SIDM-Harfang***. Elle possède actuellement deux systèmes et quatre vecteurs aériens dont le dernier a été livré fin 2010.

Les drones MALE sont les seuls drones en service dans l’armée de l’air. Aucun besoin de drone HALE n’a été exprimé à ce jour par le ministère de la Défense.

i. Leurs caractéristiques

Le *SIDM* a été développé par EADS et IAI (Israel Aerospace Industries) à partir d’un *Heron TP* produit par IAI.

Les vecteurs aériens disposent d’une LOS et d’une liaison satellite ainsi que de plusieurs charges utiles : une charge multi-capteurs, optique, infrarouge et désignateur laser, et un radar à ouverture synthétique (*Synthetic Aperture Radar/Moving Target Indicator*) permettant la détection de véhicules en mouvement. Leur autonomie atteint 11 heures à une portée de 1 000 km. Équipés d’un train d’atterrissage, et dotés de la fonction décollage/atterrissage automatiques, ils décollent depuis une piste d’environ 1 200 m.

ii. Leur emploi

Le *SIDM* est employé à l’échelle du théâtre d’opérations. Il est le plus souvent intégré par le commandement de théâtre dans la coordination des moyens de renseignement et de ciblage mis en œuvre.

Le système a été déployé en Afghanistan de janvier 2009 jusqu’à mars 2012 où il aura effectué plus de 5 000 heures de vol. Lors du second semestre 2011, le deuxième système déployé à Cognac a été employé au profit de l’opération Harmattan à partir de la base italienne de Sigonella, en Sicile. Il a effectué 315 heures de vol pour cette opération.

Le système *SIDM-Harfang* est actuellement déployé à Niamey dans le cadre de l’opération Serval. Sa première mission opérationnelle au-dessus du Mali a été réalisée dès le 18 janvier 2013, son déploiement ayant été anticipé indépendamment du déclenchement de l’opération Serval. Il avait, mi-août 2013, déjà effectué près de 2 000 heures de vol dans le cadre de cette opération toujours en cours.

3. La marine nationale

La marine nationale expérimente sur *L’Adroit* un système embarqué de reconnaissance vecteur aérien léger (SERVAL) utilisant un *Camcopter* (Schiebel). Une acquisition d’un drone à voilure tournante de ce type est envisagée dans le

cadre du futur Système de drones tactiques aériens pour la marine (SDAM) à l'horizon post-2020.

D. LE REMPLACEMENT DES CAPACITÉS FRANÇAISES ACTUELLES : SDTI ET SIDM

1. Le drone tactique *SDTI Sperwer*

Le remplacement du *SDTI-Sperwer* est prévu dans le cadre du programme système de drones tactiques (SDT) initié en 2006 par l'état-major de l'armée de terre. En 2012, un document d'orientation (DOR) a prévu l'évaluation du drone tactique *Watchkeeper* par l'armée de terre et l'étude d'options d'acquisition de drones mono ou bi-charges utiles de 2015 à 2017.

Le projet de loi de programmation militaire (LPM) prévoit l'acquisition de deux systèmes de drones tactiques SDT et de 14 vecteurs aériens durant son application. Le matériel actuel, que la France est la dernière à mettre encore en œuvre, est frappé d'obsolescence à très court terme, aussi le rapporteur insiste-t-il sur l'importance de prendre une décision rapide quant à son remplacement, ce que confirme le général Ract-Madoux [(1)] qui estime qu'il ne faut pas reporter à 2018 ou 2019 la livraison du *Watchkeeper* dont il souhaite obtenir un ou deux exemplaires en *leasing* avant leur livraison, tant le besoin est grand.

a. Un drone certifié

Le système de drone *Watchkeeper* est développé par Thales UK à partir d'un vecteur israélien, *Hermes 450*, de Elbit Systems. Le drone a obtenu de l'autorité de l'aviation militaire du Royaume-Uni, le MAA, le certificat de type STDA (*Statement of type design assurance*) le déclarant conforme aux normes de conception approuvées par cet organisme. Ce certificat est une étape déterminante sur la voie de la mise en service.

b. Des essais à confirmer

Des essais se sont déroulés cet été dans le centre de la DGA d'Istres. Le délégué général à l'armement, M. Laurent Collet-Billon, a déclaré à la commission le 2 octobre dernier que cet appareil semblait manquer de maturité au terme de cet essai et qu'il entendait suivre les évolutions prévues de ce système en relation étroite avec son homologue britannique. Le général Ract-Madoux a, pour sa part, déclaré à la commission [(2)] qu'il estimait « *les résultats techniques prometteurs mais encore perfectibles* ».

Désireux de s'informer davantage, le rapporteur s'est rendu au 61e régiment d'artillerie, « Les diables noirs » de Chaumont, le seul régiment de drones en France, assurant la formation et l'entraînement des opérateurs. Il a ainsi

(1) Réunion du 16 octobre 2013, compte rendu n°13.
(2) Ibid.

pu avoir un retour direct des personnels qui avaient assisté à l'essai du *Watchkeeper* et se trouvaient être moins négatifs que le discours dominant. Si l'essai a unanimement déçu, il semble que cela soit principalement dû à une météorologie peu clémente associée à des conditions d'essai contractuelles extrêmement rigoureuses. De fait, seulement 40 heures d'essai ont pu être réalisées sur les 120 prévues, ce qui est tout-à-fait regrettable pour un essai qui a coûté huit millions d'euros, montant dont s'étonne le rapporteur qui souligne à ce propos que la coopération franco-britannique sur le projet *Watchkeeper* nécessite des précisions quant au partage des coûts et des retombées industrielles.

Quant aux problèmes constatés, il s'agit, selon les opérateurs, non de défauts de conception mais de problèmes mineurs, que le fabricant britannique, très réactif, a pour la plupart déjà corrigés sur une nouvelle version du système. Les Britanniques ont acheté à ce jour 22 stations au sol et 36 vecteurs.

L'achat français n'est pas finalisé à ce jour. Des alternatives existent sur le marché, le *Shadow 200*, drone américain de la société AAI, dont les performances sont reconnues et le *Patroller* de Sagem, conçu à partir du *S15*, avion allemand dronisé de marque Stemme, qui lui n'est pas testé, et présente le désavantage d'être, par son poids d'une tonne, à cheval entre le segment des drones tactiques et celui des drones MALE. Or le STANAG [(1)] 4670 de l'OTAN, signé par la France, considère les appareils de plus de 600 kg comme des drones MALE et impose pour le télépilotage des compétences correspondant à celles d'un officier pilote.

En l'espèce, le rapporteur estime difficilement envisageable, après l'annonce de l'achat de drones MALE américains, d'équiper également l'armée de terre d'appareils américains, et, pour ce qui concerne la deuxième option, il lui semblerait peu avisé, en cette période de contraintes budgétaires et de dépyramidage, de surqualifier un poste très bien tenu par un sous-officier aujourd'hui.

2. Le drone MALE

L'exemple de la filière de drones moyenne altitude et à longue endurance illustre le manque d'anticipation et l'incapacité nationale et européenne.

a. Un fiasco capacitaire, ou l'Arlésienne

Le rapporteur ne souhaite pas faire ici l'historique des décisions, des revirements, des atermoiements, des luttes et des renoncements qui ont conduit un pays, la France, et un continent, l'Europe, à se priver d'un équipement dont le besoin est aujourd'hui patent alors même que ne manquaient ni les ressources industrielles, ni les ressources intellectuelles, scientifiques et techniques. Personne n'a voulu croire à un avion sans pilote et à un pilote sans avion.

(1) Standardization Agreement.

Des décisions politiques contradictoires, un manque de vision des différents acteurs, une crainte de la nouveauté, des erreurs de stratégie industrielle — on rappellera à ce propos que la société américaine General Atomics, fabricant du *Reaper* , située à San Diego, aurait alors proposé, à ses débuts dans ce secteur, un partenariat à un industriel français, pour créer une filière de drones —, une coordination européenne défaillante ont mené à cet échec.

Un rapport d'information intitulé « Drones, la France à la croisée des chemins » de décembre 2009 (1) pointait déjà le risque de rupture capacitaire et l'absence de décision entre les différents projets, alors que la France aurait pu, si elle s'en était donné les moyens, être au cœur d'un programme de drone MALE européen. Rien ne semble avoir bougé entre 2009 et 2013 et la filière des drones MALE européens se résume à un catalogue de démonstrateurs qui n'a débouché sur aucun projet concret.

Les choses doivent enfin changer aujourd'hui. Il a malheureusement fallu en arriver, en 2008, au choc provoqué par le drame d'Uzbin en Afghanistan pour que s'imposent aux responsables politiques et militaires la dure réalité et la béance du trou capacitaire français en matière de drones.

b. Un besoin avéré

Les conflits récents ont tous été l'occasion de saluer l'utilité de drones MALE sur un théâtre d'opérations. Serval en est la dernière illustration. La capacité française, insuffisante, a été complétée, grâce à l'armée américaine, par les images fournies en accès direct par ses deux drones MALE stationnés à Niamey.

LE RETOUR D'EXPÉRIENCE DE L'OPÉRATION SERVAL

L'engagement au Mali est caractérisé par la nature asymétrique de l'affrontement, par la fugacité de l'adversaire, l'étendue de la zone d'intervention entraînant de fortes contraintes en matière de continuité de la communication et enfin par l'exigence forte de sûreté de l'action afin de limiter les dommages collatéraux ou fratricides.

Dans ce contexte, les drones MALE *Harfang* ont apporté une capacité précieuse, notamment grâce à leur endurance, leurs communications satellitaires et leur possibilité de diffuser de la vidéo en temps réel aux acteurs sur le théâtre. Cette diffusion est extrêmement utile pour donner à tous les échelons de commandement la perception identique d'une situation tactique en un point donné et autoriser une prise de décision dans les délais exigés par ce type de combat. Face à un adversaire qui a montré sa capacité d'adaptation aux modes d'action de l'armée française en cessant toute activité perceptible à la moindre suspicion, le drone MALE fait également preuve d'une discrétion appréciable.

Les drones *SIDM-Harfang* ont ainsi été employés sur l'ensemble du spectre, depuis la préparation des opérations jusqu'au guidage terminal d'armement. Ils travaillent simultanément au profit des niveaux tactique, opératif et stratégique, pour toutes les composantes : reconnaissance d'itinéraires au profit des troupes au sol, travail spécifique lors de l'action des forces spéciales et intégration dans la campagne aérienne.

(1) Rapport d'information de l'Assemblée nationale n° 2127, de MM. Yves Vandewalle et Jean-Claude Viollet.

Leur activité se répartit en 30 % de surveillance de zone, 15 % de reconnaissance, 15 % d'escorte de convois, et 40 % de participation aux actions offensives par la discrimination des cibles avant les frappes, par le guidage d'armement laser et l'évaluation du résultat des frappes.

Cependant la flotte *SIDM-Harfang* a confirmé ses limites déjà connues et identifiées lors de l'opération Pamir en Afghanistan ou Harmattan en Libye : vitesse de vol et autonomie sur zones insuffisantes, communications radio non sécurisées et absence de liaison de données tactiques L16, maintien en condition opérationnelle délicat et, surtout, impossibilité de conduire de front une opération et la régénération organique en métropole en raison du déploiement intégral de la flotte disponible au Mali, flotte dont un vecteur ne vole pas, cannibalisé pour les réparations de l'ensemble.

Par ailleurs, les systèmes de drones tactiques SDTI *(cf. supra)*, dont l'action est complémentaire de celle du drone MALE, ainsi que cela fut le cas en Afghanistan, n'ont pu être utilisés au Mali car ils étaient tous indisponibles.

c. L'option arrêtée par le Gouvernement

Les moyens dont dispose la France sont en nombre insuffisant et, semble-t-il, en fin de vie. Ce dernier point est toutefois nuancé par certains interlocuteurs du rapporteur qui estiment que le *SIDM-Harfang* aurait pu être maintenu à niveau, ce que le rapporteur pu vérifier lors d'une visite chez Cassidian qui a continué à faire évoluer les liaisons de la chaîne de communication et de la chaîne de mission et dispose aujourd'hui de briques technologiques utilisables pour un prochain système intérimaire. Mais l'échéance de la mise à niveau est dépassée pour le *SIDM-Harfang* et le constat est sévère.

En réponse à ce besoin, et en conformité avec les préconisations du Livre blanc de 2013 recommandant l'acquisition de douze vecteurs MALE, le Gouvernement a estimé, dans l'immédiat, n'avoir pas d'autre option que d'acheter du matériel sur étagère auprès de l'un des deux pays leaders sur le marché des drones : Israël, premier exportateur mondial, et les États-Unis. Aussi le ministre de la Défense a-t-il annoncé au printemps, tout en regrettant l'absence d'un drone MALE français [(1)], que la France achèterait aux États-Unis douze drones *Reaper*, dont deux en urgence avant la fin de l'année 2013, et dont les dix restants seraient acquis ultérieurement et francisés.

d. Les difficultés soulevées

Si le rapporteur comprend qu'il est important de combler cette lacune capacitaire, le recours à cet achat sur étagère pose selon lui plusieurs problèmes majeurs.

i. Une certification européenne impossible en l'état

Les *Reaper*, s'ils peuvent, voler aux États-Unis, en Afghanistan ou au Mali ne peuvent voler en Europe, faute d'une certification qu'ils ne sont pas en mesure d'obtenir sans modifications. Les appareils détenus par le Royaume-Uni

(1) Commission de la défense nationale et des forces armées, réunion du 22 mai 2013, compte rendu n°73.

ne survolent, par exemple, pas le territoire britannique où ils ne sont pas stationnés.

La France est l'un des rares pays européens à avoir réussi à insérer un drone MALE, le *SIDM-Harfang* en l'occurrence, dans l'espace aérien sous contrôle militaire, en collaboration avec les autorités civiles ; elle possède donc une expérience susceptible d'être valorisée.

Les deux premiers *Reaper* livrés à la France devront donc rester au Mali dans un premier temps. Il s'agit de *Reaper Block 1*, qui étaient en cours de livraison au Pentagone, dont les chaînes de liaisons de données, pilotage et capteurs, sont imbriquées et ne pourraient donc être européanisés ainsi que l'a indiqué à la commission, en réponse à une question du rapporteur, le général Denis Mercier, chef d'état-major de l'armée de l'air, le 8 octobre 2013.

Mais ces appareils, qui ne disposent, par exemple, pas de procédures de décollage et atterrissage automatiques, devraient, à terme, pouvoir être « rétrofités » aux standards des *Reaper Block 5*, version plus évoluée aux chaînes de pilotage et de capteurs distinctes, devant faire l'objet des dix livraisons suivantes.

ii. Des doutes sur la faisabilité d'une francisation ou d'une européanisation

Si le rapporteur estime la francisation ou l'européanisation des *Reaper* indispensable, elle lui paraît difficilement possible pour autant. La réponse des autorités américaines est encore inconnue et il est, par ailleurs, peu probable que le fabricant américain donne accès à toutes les informations nécessaires à l'opération, notamment les codes sources ou *« black boxes »*.

À une exception près, aucun des interlocuteurs du rapporteur n'a estimé que ce processus avait une quelconque chance d'aboutir, ce que semble confirmer l'expérience de nos voisins allemands, britanniques ou italiens.

Il conviendrait donc, avant de s'engager dans cette opération, d'en étudier la faisabilité avec la plus grande attention, notamment en ce qui concerne les exigences posées par l'autorité européenne de certification aérienne quant aux critères de navigabilité, quitte à revoir la décision d'achat initiale.

Les industriels rencontrés par le rapporteur se sont montrés très réservés quant à un tel projet qu'ils ne voudraient pas voir conduit par le fabricant américain, auquel ils ne souhaitent pas transmettre les « briques » technologiques qu'ils ont développées en matière de capteurs et de liaisons, notamment.

Néanmoins, un interlocuteur du rapporteur est d'avis qu'une autorisation américaine et une ouverture la plus large possible de la part de General Atomics permettant une francisation ou une européanisation réussie serait pour le fabricant

un argument commercial de premier plan qu'il pourrait faire valoir pour l'exportation des *Reaper*.

iii. Un coût final peu clair

Le budget consacré à l'achat de douze drones MALE dans la future loi de programmation militaire est de 670 millions d'euros pour l'ensemble des appareils, soit 56 millions d'euros par appareil. Il ne semble pas que la francisation de dix appareils soit comprise dans ce prix. Par ailleurs, le Congrès aurait donné son accord non pour douze mais pour seize drones d'un prix unitaire supérieur au prix anticipé.

Le rapporteur estime important que toutes les informations soient données sur le prix d'achat effectif des systèmes de drones et sur le coût prévisible de leur francisation/européanisation afin d'éviter une dérive budgétaire.

iv. Une perte de souveraineté

Il s'agit pour le rapporteur du point le plus préoccupant. Car la France doit pouvoir conserver son autonomie de décision, y compris vis-à-vis de ses alliés dont font partie les États-Unis. La France ne doit pas avoir à solliciter d'autorisations pour ses plans de vol et doit être le seul destinataire des informations recueillies. Le rapporteur insiste pour que tout soit mis en œuvre pour atteindre cet objectif.

Pour ce qui concerne les deux premiers *Reaper*, le général Denis Mercier a indiqué à la commission que, dans l'immédiat, la France pourrait, et c'est un point essentiel, choisir librement le satellite utilisé. Le personnel de maintenance de ces appareils est pour l'instant fourni par les États-Unis, mais il n'aura pas accès aux cabines d'opérateurs sans autorisation.

M. Laurent Collet-Billon a évoqué devant la commission l'annonce par le ministre de la Défense de la création d'un club des utilisateurs de *Reaper* en Europe, réunissant les Britanniques, les Italiens et peut-être bientôt les Allemands, qui aura ainsi plus de poids dans les négociations portant sur l'émancipation du *Reaper*.

e. La réponse des industriels

En réaction à cette annonce, EADS Cassidian, Dassault Aviation et Finmeccanica Alenia Aermacchi ont, le 16 juin 2013, appelé au lancement d'un programme de drone MALE européen et déclaré être prêts à se coordonner autour d'un tel projet. Le délégué général pour l'armement, M. Laurent Collet-Billon, a annoncé à la commission qu'il devait rencontrer les représentants de ces industriels dans le courant du mois d'octobre afin d'en discuter.

Plusieurs industriels européens ont donc montré leur volonté de coopérer. Il est grand temps qu'un signe politique fort des pays européens intéressés soit

donné et que **les objectifs de construction d'un drone MALE européen soient affirmés**, avec l'établissement d'un calendrier précis, lors du Conseil européen sur la Défense prévu en décembre 2013.

Le rapporteur a pu constater à la lumière des exemples tirés des conflits afghans ou maliens que les progrès apportés à la fonction image des drones SDTI ou SIDM démontrent la qualité de nos industriels.

f. Un futur drone MALE européen ?

Nonobstant l'achat de drones MALE sur étagère, le ministre de la Défense a exprimé à plusieurs reprises clairement son souhait de pouvoir disposer d'un drone MALE européen de troisième génération en 2020 ou 2025, des entretiens encourageants s'étant déroulés à ce sujet avec ses homologues britanniques et allemands.

Le rapporteur est également d'avis que l'Europe doit, à terme, construire un drone MALE européen et conserver ainsi sa capacité d'innovation dans ce domaine, alors que plus de dix ans ont été perdus et qu'il sera difficile de rattraper les constructeurs israéliens et américains.

La construction d'un drone permettrait également à l'Europe d'être active dans l'établissement des normes et des standards concernant ce type d'appareil, leur navigabilité et leur insertion dans le trafic aérien, champ qu'elle abandonnerait entièrement aux États-Unis dans le cas contraire.

Le principal écueil est l'insertion des drones dans le trafic aérien. Des études lancées par la Commission européenne, *RPAS Steering Group* (1), et par l'Agence européenne de défense, Air4All, SIGAT et MIDCAS (2), sont en cours. Leurs résultats devront être pris en compte dès le départ du projet.

Des décisions doivent donc être prises rapidement mais le rapporteur observe que rien n'est prévu en la matière ni dans le Livre blanc 2013, ni dans le projet de loi de programmation militaire.

Le rapporteur n'est donc pas persuadé que les décisions récentes, prises rapidement d'acheter sur étagères, pendant le conflit du Mali, deux *Reaper Block 1* aux États-Unis puis de commander dix *Reaper Block 5*, dotés d'un système de décollage et d'atterrissage automatique, sans avoir la certitude de pouvoir, à terme, les faire voler dans l'espace aérien européen et sans connaître les possibilités de les franciser ou de les européaniser, suffiront à combler notre déficit capacitaire.

Il faudrait, bien sûr, avoir l'assurance que l'ajout de systèmes embarqués dont on aura vérifié au préalable les failles informatiques soit autorisé par les

(1) Comité directeur sur les systèmes aériens téléopérés.
(2) système anti-collision en plein ciel, mid-air collision avoidance system.

États-Unis. Cela permettra d'éviter la mésaventure qu'ont connue les Américains en Iran, où ils ont perdu le contrôle d'un drone *(cf. infra)*.

Le démonstrateur de drone de combat furtif nEUROn

En 2003, le ministère de la Défense français a initié le programme de démonstrateur de drone de combat nEUROn, d'une part, afin de maintenir et de renforcer les compétences des avionneurs européens et, d'autre part, afin de développer le savoir-faire technologique européen dans le domaine des drones de combat furtifs. Ce démonstrateur technologique s'inscrit dans la préparation du Système de Combat Aérien Futur qui pourrait entrer en service à l'horizon 2030.

La France a fédéré autour d'elle l'Italie, la Suède, l'Espagne, la Grèce et la Suisse et a mis en place un schéma de coopération innovant : la DGA, qui a signé des accords étatiques bilatéraux, joue le rôle d'agence exécutive et Dassault Aviation est le maître d'œuvre. Les sociétés suédoise Saab, italienne Alenia Aermacchi/Finmeccanica (ex Alenia Aeronautica), espagnole Cassidian/EADS (ex EADS-CASA), grecque HAI et suisse RUAG sont les principaux sous-traitants.

L'Agence européenne de défense (AED) n'intervient pas dans ce programme.

Les principaux objectifs techniques pour nEUROn sont :

– un haut niveau de furtivité radar et infrarouge ;

– le largage d'un armement depuis une soute ;

– le contrôle de la plateforme par une station sol avec des capacités de décollage et atterrissage automatiques ;

– la détection et la reconnaissance automatique de cibles au sol grâce à un capteur optique embarqué et des algorithmes de détection et de reconnaissance automatiques ;

– l'utilisation de technologies permettant de réduire les coûts ;

– un haut niveau de sécurité permettant de survoler des zones peuplées.

Les principales caractéristiques sont :

– véhicule de classe sept tonnes, permettant l'emport d'armements et de charges utiles, capable de voler dans le haut subsonique (mach 0,8+) ;

– charges utiles : capteur infrarouge/laser pour la détection, la reconnaissance et la localisation de cibles déplaçables au sol ;

– armement : deux soutes à armement pouvant emporter chacune une bombe guidée laser de 250 kg ;

– deux liaisons de données à vue directe LOS.

Le contrat a été notifié le 8 février 2006. Le coût total du démonstrateur est de 440 M€ HT CE 07/04, dont une part de 203 M€ HT pour la France.

Le financement est assuré par la France à 46,1 %, l'Italie à 22,2 %, la Suède à 18,1 %, l'Espagne à 8,05 %, la Grèce à 4,55 % et la Suisse à 1 %.

Le premier vol qui s'est déroulé le 1er décembre 2012 à Istres représente un jalon majeur du programme. La campagne de mesure de furtivité, conduite par le centre Maîtrise de l'Information de la DGA dans la chambre de mesure radar *Solange*, a eu lieu entre février et avril 2013.

La reprise des vols est prévue au cours du 4e trimestre 2013 à Istres, pour une durée d'une année comprenant des vols d'ouverture de domaine suivi d'une campagne de

démonstration des performances de furtivité. Il est prévu ensuite une campagne de vols en Suède puis une seconde en Italie.

Le délégué général pour l'armement a indiqué à la commission(1) que les essais du nEUROn avaient parfaitement fonctionné et qu'il s'agissait là d'un exemple de coopération européenne réussie dont les résultats sont très encourageants dans le cadre du maintien des compétences des bureaux d'études aéronautiques en l'absence d'un programme d'avion de combat en Europe.

La fin du programme de démonstrateur de drone de combat nEUROn est prévue mi 2015.

Source. ministère de la Défense.

(1) Commission de la défense nationale et des forces armées de l'Assemblée nationale, réunion du 2 octobre 2013, compte rendu n° 3.

« *Le cyberespace est désormais un champ de confrontation à part entière* ».

Livre blanc de 2013

II. LA CYBERDÉFENSE

L'affaire Snowden a révélé que l'État a été depuis plus de dix ans aveugle et sourd… À quoi sert de classer des documents « *confidentiel-défense* » si nos réseaux, nos données, nos produits sont accessibles à tous les « *hackers* » de la planète, mais également à des gouvernements amis qui n'ont pas hésité à détourner des documents confidentiels et à espionner nos ambassades.

Le fait que l'Allemagne ou le Royaume-Uni aient subi les mêmes préjudices ne les atténue en rien. Le rapporteur salue les réactions du Président de la République et du ministre des Affaires étrangères, mais ces protestations doivent être suivies d'effets, notamment dans la modification de la gouvernance mondiale d'Internet.

Le sommet mondial d'Internet à Bali en octobre 2013, après ceux qui se sont tenus notamment à Tunis en 2005, doit rappeler les chartes éthiques des entreprises géantes de l'informatique, permettre à des commissions de contrôle d'avoir accès aux codes sources et à la recherche de failles, de logiciels espions, au stockage des données informatiques, à l'attribution des noms de domaine…

La gouvernance internationale d'Internet ne peut plus être du seul ressort de la souveraineté américaine. Une organisation internationale devrait s'y substituer.

Il faut prendre les menaces au sérieux et pour cela mieux les connaître. La cybersécurité doit devenir une grande cause nationale (*cf. infra*). Le cyberespace est un nouvel espace d'affrontement. C'est le cinquième espace de combat après la terre, l'air, la mer et le spatial. La Chine a, par exemple, investi ce nouvel espace pour tenter de rattraper son retard dans des domaines militaires conventionnels.

Depuis le Livre blanc de 2008 qui posait les premiers jalons en matière de cyberdéfense et contribuait à l'amorce d'une prise de conscience des risques auxquels sont soumis tous les pans de la défense, des progrès ont été enregistrés.

Le cyberespace est désormais reconnu comme un milieu à part entière et les cyberattaques se trouvent au troisième rang des risques et des menaces pris en compte par la stratégie de défense et de sécurité nationale énoncée dans le Livre blanc de 2013.

Plusieurs rapports importants ont marqué l'émergence puis la consolidation du concept de cyberdéfense : celui du député Pierre Lasbordes [1] en 2006, celui du sénateur Roger Romani [2] en 2008, année de parution du Livre blanc, et enfin celui du sénateur Jean-Marie Bockel [3] en 2012 auxquels il convient d'ajouter celui de la sénatrice Catherine Morin-Dessailly [4] qui, s'il n'est pas consacré spécifiquement à la cyberdéfense, traite bien de souveraineté numérique.

Une audition publique *« Le risque numérique : en prendre conscience pour mieux le maîtriser ? »* a été organisée en février 2013, conjointement avec les commissions de la défense des deux assemblées, par l'Office parlementaire des choix scientifiques et technologiques, dont le rapporteur est le premier vice-président. Les conclusions de ce débat, publiées sous le titre éponyme, présentent un tour d'horizon des aspects techniques et sociaux du risque numérique.

1. Le constat

Indépendamment de la cybercriminalité, en croissance constante, les principales menaces en provenance du cyberespace que doit affronter la France sont le cyberespionnage, les attaques contre les systèmes de contrôle des processus industriels et les attaques contre la disponibilité, étant entendu que les attaques les plus réussies sont celles qui demeurent inconnues.

a. Les opérations d'espionnage informatique

Un volume conséquent d'informations sensibles, voire classifiées, autrefois accessibles au prix de délicates opérations de renseignement humain, peut désormais être collecté de façon relativement aisée et peu coûteuse *via* des intrusions sur les réseaux informatiques. Le résultat est une multiplication des opérations d'espionnage informatique.

À côté d'opérations d'espionnage sophistiquées, furtives et difficilement attribuables - comme celle qui fut découverte cette année à la Commission européenne - la France, au même titre que ses alliés, est une cible permanente d'attaques de niveau technique et d'intensité variables.

Parmi ces attaques, il faut noter celles de type « *advanced persistant threats* [5] » (APT) qui reposent sur des techniques complémentaires de nature sociale *(phishing)* et de pénétration des réseaux qui tendent à se banaliser. Des attaques récentes témoignent d'un intérêt particulier pour les entreprises françaises des secteurs de l'aéronautique, du spatial, de la défense et de l'énergie. Des ministères régaliens sont également ciblés : Défense, Économie et Finances ou Affaires étrangères.

---

(1) Rapport remis au Premier Ministre : La sécurité des systèmes d'information : un enjeu pour la France, décembre 2006.
(2) Cyberdéfense : un nouvel enjeu de sûreté nationale, juillet 2008.
(3) La cyberdéfense : un enjeu mondial, une priorité nationale, juillet 2012.
(4) L'Union européenne, colonie du numérique ?mars 2013.
(5) Menaces persistantes avancées.

Les informations recherchées concernent des technologies civiles ou militaires ou encore des projets commerciaux, diplomatiques ou financiers en cours de négociation.

Il s'écoule en moyenne un an entre le début de l'intrusion et sa découverte par la structure touchée, généralement à la faveur d'un incident technique indépendant.

b. La déstabilisation d'entreprises ou d'États

Les attaques informatiques peuvent être utilisées pour tenter de déstabiliser des entreprises ou des états :

– par des opérations visant à nuire à la réputation des entreprises ou d'organisations, notamment par la révélation de documents sensibles volés sur les réseaux concernés ;

– par l'utilisation de données usurpées pour remporter des contrats ou faire échouer des négociations commerciales ;

– par le pillage du patrimoine technologique d'entreprise de haute technologie et notamment le détournement ou le vol de brevets.

De telles actions accompagnent désormais l'actualité qu'il s'agisse de conflits armés, d'une décision jugée inopportune ou d'un événement heurtant un groupe de personnes. Ainsi le site de recrutement de l'*US Marine Corps* a été victime, au cours du mois de septembre, de pirates informatiques syriens qui ont modifié, « défacé », l'apparence de son site pour diffuser des messages à caractère politique.

c. La saturation de réseaux et services essentiels

Il est désormais possible d'acquérir pour quelques milliers d'euros un réseau d'ordinateurs infectés et de les piloter à distance depuis Internet pour qu'ils saturent d'informations des réseaux de communications ou des services Internet. De telles attaques, dites en déni de service, touchent régulièrement des sites Internet gouvernementaux français, comme le site permettant de déclarer ses impôts en ligne, ou des sites de grandes entreprises. Les motivations affichées des attaquants sont généralement idéologiques mais peuvent avoir une finalité économique ou financière. Leurs actions n'ont toutefois pas d'impact notable pour le pays.

Mais, à une autre échelle, des attaques d'ampleur ont été conduites contre l'Estonie et la Géorgie lors de conflits diplomatiques ou militaires avec la Russie. Le résultat est une paralysie de services essentiels à la vie de la nation, administrations, commerce électronique, banques en ligne, téléphonie mobile, pendant une période plus ou moins longue. Dans le cas de la Géorgie, les

cyberattaques ont eu lieu en préparation de l'attaque militaire dont elles étaient une composante.

Durant le premier trimestre 2013, ce même type d'attaque a été conduit contre des banques américaines et coréennes et des médias coréens.

Le cas de l'Estonie

L'attaque subie par l'Estonie est emblématique car elle fut la première à avoir été dirigée contre un pays et non contre une cible particulière et a marqué les esprits à ce titre.

L'Estonie était, déjà en 2007, un pays très numérisé où la grande majorité des échanges s'effectuait par Internet. De nombreux services n'étant disponibles qu'en ligne, l'attaque visa à partir du mois d'avril 2007, et pendant plusieurs mois, administrations et acteurs économiques. L'attaque par botnet (réseau d'ordinateurs compromis) a consisté en un déni de service, les sites étant rendus inaccessibles par une saturation due à une multiplication des tentatives de connexion.

L'attaque ayant fait suite au déplacement, contesté par la minorité russophone, d'une statue dite *« Le soldat de bronze »*, érigée en mémoire des combattants de l'armée soviétique durant la deuxième guerre mondiale, d'une colline du centre de Talinn vers un cimetière militaire, et de nombreuses attaques ayant été identifiées en provenance de Russie, la responsabilité en a été attribuée aux autorités russes qui ont démenti.

Selon le représentant estonien rencontré par le rapporteur, les dégâts engendrés par cette attaque n'auraient pas été considérables bien que difficiles à chiffrer. Très en avance par rapport à de nombreux pays européens, l'Estonie disposait alors déjà d'une stratégie de cyberdéfense. En 2011, l'Estonie a mis en place la *Cyber League*, une réserve opérationnelle composée de volontaires.

L'Estonie a adopté une nouvelle législation, qui sera renforcée en 2014, imposant à ses opérateurs d'importance vitale l'obligation de garantir une continuité de service même s'ils dépendent de serveurs installés à l'étranger.

Les écoles sont toutes reliées à Internet et les enfants sont familiarisés avec le numérique dès cinq ans dans le cadre scolaire et parallèlement éveillés à la cybersécurité.

C'est à Tallinn que l'OTAN a installé en 2008 un Centre d'excellence en cyberdéfense, centre de recherche non opérationnel regroupant des experts autour de travaux portant notamment sur la doctrine et le cadre juridique international. Un expert français a rejoint le centre durant l'été 2013.

d. Le sabotage informatique

Les installations industrielles sont désormais très largement pilotées par des ordinateurs, lesquels peuvent être attaqués. En 2010, le ver informatique surnommé Stuxnet a ainsi mis en évidence qu'il était possible de perturber à distance le fonctionnement d'une installation nucléaire. Il ciblait les automates pilotant les centrifugeuses du site iranien de Natanz. L'introduction de ce type de logiciel malfaisant (*malware*) nécessite toutefois, comme ce fut le cas pour l'Iran, de pouvoir accéder physiquement à des réseaux protégés.

Au cours de l'été 2012, ce sont 35 000 ordinateurs de la compagnie saoudienne Aramco qui ont été détruits en quelques heures par une attaque

informatique, entraînant des difficultés de fonctionnement pendant plusieurs semaines.

e. Des équipements vulnérables

Les systèmes d'armes, qui comportent aujourd'hui tous des briques numériques de provenances diverses, doivent faire l'objet d'une attention à la hauteur de leur vulnérabilité potentielle.

Les drones et leurs liaisons de données doivent être particulièrement résistants aux cyberattaques. L'Iran (1) affirme avoir réussi, en décembre 2011, à détourner, en l'obligeant à se poser, un drone furtif américain *RQ-170 Sentinel* qui effectuait une mission d'espionnage des centrales nucléaires iraniennes. Après avoir dans un premier temps démenti la perte du drone, les États-Unis ont évoqué un problème technique. Des moyens russes permettant de détecter les avions furtifs ont été évoqués à cette occasion. Les Iraniens ont annoncé avoir réussi à percer les secrets du drone et en avoir fait une copie.

D'une manière plus générale, la vulnérabilité des équipements numériques est liée soit à l'usage qui en est fait, soit à des conditions d'emploi inadéquates ou encore à des défauts de conception du système. Il s'agit dans ce dernier cas de failles qui font l'objet d'une diffusion et d'un véritable marché. Certains États achèteraient des failles informatiques qu'ils conserveraient pour leur propre usage pendant une certaine période avant leur diffusion.

La vulnérabilité peut également tenir à la méconnaissance de l'utilisateur des conditions contractuelles d'emploi d'une fonctionnalité, telle que le recours à des annuaires sur les téléphones portables, par exemple.

L'intervention humaine *(cf. infra)* est également à compter au rang des vulnérabilités.

2. L'élaboration d'une doctrine française en matière de cyberdéfense

Une stratégie nationale en matière de sécurité des systèmes d'information, élaborée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et couverte par le secret de la défense nationale, a été approuvée au printemps 2010 par le « comité stratégique de la sécurité des systèmes d'information » institué par le décret portant création de l'agence. Deux réunions du comité, tenues en décembre 2010 et en décembre 2011, ont permis d'en suivre l'évolution.

La stratégie retenue fixe quatre objectifs :

(1) www.lemonde.fr, 22/4/12 et aerobuzz.fr 16/12/11.

– la protection de l'information de souveraineté de l'État, notamment par l'élaboration de produits de sécurité adaptés et la mise en œuvre des réseaux nécessaires ;

– la sécurisation des systèmes d'information des entreprises les plus sensibles, dont ceux des «opérateurs d'importance vitale» ;

– l'accompagnement du développement de la société de l'information en favorisant sa sécurité ;

– le positionnement de la France comme nation majeure en matière de cyberdéfense.

La version publique de cette stratégie nationale a été publiée en février 2011.

En matière de **lutte offensive**, le Livre blanc sur la défense et la sécurité nationale de 2008 indiquait que la France se doterait de capacités cybernétiques offensives. Déclarant que *« certains États développent des capacités informatiques offensives qui représentent déjà une menace directe contre des institutions, entreprises et secteurs clés pour la vie de la Nation. »*, le Livre blanc de 2013 a confirmé cet engagement sans qu'il soit, de façon compréhensible, possible d'en connaître ni les ambitions ni les moyens mis en œuvre.

3. Les réponses apportées

a. La création de l'ANSSI

L'avancée majeure a été la création de l'ANSSI en 2009, rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDN). Son rôle est d'assurer des missions de prévention et de réaction.

Sa mission de prévention consiste à conseiller les opérateurs d'infrastructures critiques pour la sécurité informatique de leurs installations. En réaction à une attaque, sa mission est de coordonner la réponse en s'appuyant sur son centre opérationnel.

L'ANSSI exerce également une activité de certification de produits de confiance.

b. L'organisation interne de la cyberdéfense au sein de l'armée

L'armée assure sa propre cyberdéfense. Une mission opérationnelle, dirigée par le contre-amiral Arnaud Coustillière, est chargée de traiter les attaques par l'intermédiaire du centre d'analyse en lutte informatique défensive (CALID) qui est désormais hébergé dans le même bâtiment que le centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI. Cette mission concerne

non seulement les réseaux informatiques mais aussi l'ensemble des systèmes d'armes déployés sur le territoire et hors de France.

c. La Direction générale de l'armement (DGA) et le centre Maîtrise de l'information de Bruz

La DGA assure la partie technique de la cyberdéfense et de la cybersécurité ; elle intervient en amont pour intégrer la sécurité numérique à toutes les étapes du développement des armements ou des systèmes. Elle dispose pour cela du centre Maîtrise de l'information de Bruz où sont mis au point, avec des industriels de confiance, les composants électroniques qui équipent les systèmes d'armes et les systèmes d'information des armées.

Une activité importante du centre est le test des « briques » technologiques achetées sur étagère composant les systèmes d'armes et celui des SCADA [(1)], présents partout aujourd'hui.

À ce titre, la DGA finance des études amont qui sont en très forte croissance dans le domaine de la cybersécurité, puisque leur montant est passé de 10 millions d'euros par an il y a quelques années, à 23 millions en 2013 pour atteindre bientôt 30 millions d'euros par an, ce que confirme le projet de loi de programmation militaire.

d. Les obligations imposées aux opérateurs d'importance vitale par le projet de loi de programmation militaire

Conformément aux préconisations du Livre blanc de 2013, l'État souhaite imposer aux opérateurs d'importance vitale une régulation de leurs systèmes d'information critiques par un dispositif législatif et réglementaire approprié, ce dont le rapporteur se félicite.

L'État fixera donc les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs d'importance vitale prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes **critiques**. Ce dispositif précisera les droits et devoirs des acteurs publics et privés, notamment en matière d'audit, de cartographie de leurs systèmes d'information, de notification des incidents... L'État pourra donc, si les dispositions de la LPM sont adoptées par le Parlement, fixer des règles, imposer des mesures et contrôler les systèmes dans le respect de la confidentialité des données recueillies.

Les opérateurs d'importance vitale devront signaler à l'ANSSI tout incident informatique affectant leur fonctionnement.

---

(1) Supervisory control and data acquisition.

Israël impose à ses opérateurs critiques des obligations légales de cet ordre depuis 2002, soit dix ans avant que les États-Unis n'aient tenté de faire adopter, en vain, une mesure identique.

Le rapporteur salue le fait que, pour la première fois, le projet de loi de programmation militaire prenne la mesure de ces nouvelles menaces, tant dans le domaine de la Défense nationale que dans le domaine industriel. La nécessité de promouvoir une **hygiène informatique** s'impose et il est bien sûr excellent que les opérateurs soient contraints de déclarer tous les **incidents** et les attaques et que l'État se réserve la possibilité de leur opposer une réponse offensive.

e. La réserve citoyenne et la réserve opérationnelle

L'idée de la réserve spécialisée en cyberdéfense est née à la suite de l'attaque du ministère des Finances, début 2011, lors de laquelle l'ANSSI est intervenue, mobilisant 300 personnes pour la reconquête du réseau. Constituée conjointement par l'ANSSI et le ministère de la Défense, elle aura deux composantes, la réserve citoyenne qui sera plutôt une enceinte de réflexion et de proposition, comptant aujourd'hui environ 75 personnes expertes dans leur domaine, et la réserve opérationnelle qui n'est pas encore constituée.

Dans cet esprit, un symposium académique national de recherche en cyberdéfense a été organisé par la réserve citoyenne, l'IRSEM et la direction des affaires stratégiques (DAS) du ministère de la Défense qui a rassemblé, le 17 septembre 2013, à l'École militaire des experts issus du monde militaire, de l'administration, de l'entreprise et du monde académique

f. La progression des effectifs

Conformément aux objectifs fixés par le Livre blanc, L'ANSSI verra ses effectifs augmenter graduellement, pour passer de 357 personnes fin 2013 à 500 en 2015.

L'amiral Édouard Guillaud, chef d'état-major des armées a indiqué à la commission le 3 octobre 2013 que plusieurs centaines de postes seront créés durant la période 2014-2019 dans le domaine de la lutte informatique et de la surveillance des systèmes d'information. Il souligne les difficultés rencontrées pour recruter dans ces domaines où les gens qualifiés sont rares.

La DGA Maîtrise de l'Information près de Rennes a annoncé un doublement de ses effectifs d'ici 2017, qui pourraient atteindre 400 personnes à cette date [(1)].

Le rapporteur tient à ce propos à tirer la sonnette d'alarme et à mettre en garde contre le « dépyramidage » annoncé dont il estime qu'il devrait être conduit au sein de la DGA avec la plus grande prudence, afin de ne pas « gratter l'os » et

(1) Audition de M. Guillaume Poupard par la commission, le 10 juillet 2013, compte rendu n°85.

priver l'institution de personnels très qualifiés difficiles à trouver sur le marché du travail.

Si chacun a compris la nécessité de restructurer l'armée pour l'adapter à ses missions, le ministre de la Défense, M. Jean-Yves Le Drian, a réaffirmé avec force la priorité de la recherche amont pour préparer l'avenir. Dans ces conditions, **il serait incohérent d'appliquer de manière homothétique le « repyramidage »**. Car on ne peut pas d'une part, affirmer qu'il faut recruter des ingénieurs et des docteurs de haut niveau à la direction générale de l'armement, et, d'autre part, leur refuser des postes qui correspondent à leurs qualifications. La priorité aux études amont doit se décliner en priorités de carrière pour les femmes et les hommes qui les mettront en œuvre. Ce serait un non-sens de demander à des spécialistes qualifiés de partir et se priver ainsi d'une main-d'œuvre rare, alors que dans le même temps, le Gouvernement a l'ambition de renforcer la DGA.

4. Les axes de progrès

a. Former des spécialistes

Il ressort de tous les entretiens du rapporteur que le nombre de spécialistes formés à la cybersécurité en France est tout à fait insuffisant, et ce quel que soit le niveau de formation requis.

Il est urgent de former dans ce domaine plus d'ingénieurs, plus d'universitaires et plus de techniciens. Un interlocuteur de la DGA indiquait au rapporteur qu'il était également très difficile de recruter des doctorants.

Le monde académique doit toutefois, selon le rapporteur, se remettre en question et considérer, enfin, dans les grandes écoles, les écoles d'ingénieurs et l'université, l'informatique comme une science et non comme une discipline accessoire accompagnant d'autres disciplines scientifiques.

Il faut développer les formations à la cyberdéfense dans les universités et les écoles françaises, car le présent rapport démontre que d'ici à cinq ans, le nombre d'ingénieurs et de docteurs formés ne suffira pas à satisfaire les besoins de l'État, de l'ANSSI, de la DGA, des autres ministères, des industriels, des universités, des organismes de recherche, les meilleurs éléments risquant par ailleurs d'être attirés par des offres alléchantes à l'étranger.

b. Encourager les échanges entre la Défense, le monde académique et l'industrie

Le rapporteur a été frappé au cours de ses travaux par l'absence de porosité, voire une coupure inquiétante, entre ces différents cercles et tout particulièrement entre la recherche académique, la Défense et l'industrie, ce qu'ont bien volontiers reconnu ses différents interlocuteurs.

Le défi de la cybersécurité passe par une reconnaissance de cette priorité dans les ambitions nationales en matière de recherche ou de formation universitaire. Le rapporteur préconise donc que le Gouvernement donne une priorité thématique à la sécurité des systèmes d'information, en renforçant d'une part l'Institut national de recherche en informatique et en automatique (INRIA), les universités et, notamment, les pôles de recherche de Grenoble, Nancy, Nice, Paris-Île-de-France et Rennes. Sans développement de la formation et de la recherche académique, il n'y aura pas d'amélioration des capacités françaises en matière de cybersécurité.

Si le sujet de la cyberdéfense est récent dans le monde académique, la recherche fondamentale débouche sur des résultats concrets dans le numérique comme le montre l'exemple ci-dessous.

La faille de Skype

En 2010, une équipe de l'INRIA en collaboration avec le *Polytechnic Institute* de New York a découvert une faille permettant de faire le lien entre une identité sociale et une identité sur Internet, ce que normalement seul le fournisseur d'accès à Internet est en mesure de faire. Il a été démontré qu'il était également possible de suivre les déplacements des utilisateurs de Skype ainsi que leurs téléchargements BitTorrent.

Cette faille est liée à la nature des communications pair-à-pair et à la nature ouverte d'Internet. En l'occurrence, Skype a été contacté avant la publication des travaux de l'équipe, un an plus tard, ainsi que Microsoft qui avait racheté Skype dans l'intervalle. Skype n'a réagi qu'après la publication des travaux en modifiant son architecture sans que l'on sache toutefois dans quelle mesure.

La découverte de cette faille démontre que la recherche fondamentale peut avoir un impact industriel et sociétal sur un équipement très répandu.

Source : www.inria.fr « Comment skyper sans être observé » + note INRIA.

Par ailleurs, le projet de loi de programmation militaire s'apprête à autoriser certains services de l'État à pénétrer dans des systèmes tiers pour comprendre et déjouer une attaque.

Mais le rapporteur estime qu'il faut aller plus loin dans la loi de programmation militaire, en autorisant les laboratoires spécialisés civils et militaires, car le monde cyber est dual [(1)], à mener des recherches offensives. Le droit ne permet pas aujourd'hui de trouver des solutions aux problèmes rencontrés, ce que l'on constate dans l'affaire de l'espionnage généralisé de la diplomatie et des industriels français.

Il faut renforcer les équipes qui travaillent sur la cryptologie et la virologie informatique et leur donner, y compris dans des laboratoires universitaires, sous le contrôle de l'ANSSI, la possibilité de débrider des systèmes d'exploitation, de déverrouiller, de désassembler des logiciels, de vérifier les flux informatiques, de

(1) 60 % dans le domaine civil, 40 % dans le domaine militaire.

faire de la rétroingéniérie [(1)] pour mieux comprendre la nature des menaces afin de se donner les moyens de tracer les flux véhiculant des logiciels malveillants. Il est incompréhensible que dans le droit actuel, un laboratoire universitaire de pointe n'ait pas la sécurité juridique lui permettant de désassembler un logiciel.

Le risque numérique est multi-factoriel, aussi la cyberdéfense et, particulièrement, l'analyse de la menace nécessitent-t-elles des compétences non seulement scientifiques et techniques mais également en sciences humaines et notamment en géopolitique, psychologie…

Mme Frédérick Douzet, titulaire de la Chaire Castex de cyberstratégie, a, par exemple, pu montrer au rapporteur un travail de cartographie des réseaux Internet mondiaux très éclairant sur les équilibres stratégiques régionaux.

Le programme d'études établi par la délégation aux affaires stratégiques en 2013 est un excellent indicateur de l'importance accordée à la cyberdéfense, aux drones et à l'industrie de la Défense et témoigne, si besoin était, de la nécessité de l'interdisciplinarité.

Études prospectives et stratégiques

À la suite d'une étude finalisée en 2013 sur « L'utilisation stratégique du cyber au Moyen-Orient », suivront :

Dans le domaine de la **cyberdéfense** :

« Quelles sont les évolutions possibles de la gestion du personnel de la défense pour lutter efficacement dans le cyberespace ? » ;

« Les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ? » ;

« Les réseaux sociaux sont devenus un espace de bataille. Quelles applications pour la défense ? » ;

« La balkanisation du web : chance ou risque pour l'Europe ? » ;

« Géopolitique du cyber en Asie » ;

« Comparaison de la manière d'aborder la cybercriminalité et la lutte informatique » ;

« Impact des réseaux sociaux sur la conduite des opérations » ;

« Conséquences des nouveaux usages technologiques pour la sécurité et le renseignement » ;

« Impact sur les systèmes d'armes de contrefaçons ou malfaçons ».

Dans le domaine des **drones** :

« Le marché civil des drones : perspectives et enjeux pour la Défense » ;

« Emploi des drones armés et rôle des opérateurs humains : une analyse sociologique et prospective au sein des systèmes de combat aérien futur » ;

« Aspects légaux et éthiques des frappes à distance sur les cibles humaines stratégiques » ;

(1) Le code de la propriété intellectuelle autorise la rétroconception des logiciels uniquement dans le cadre de l'interopérabilité et non de la sécurité.

Un « Observatoire du monde cybernétique » est en cours.

Dans le domaine de **l'industrie de Défense** :

« Les filières au service du développement des PME de la BITD » ;

« Fonds d'investissement armement pour les PME et les ETI de la BITD » ;

« Les stratégies nationales d'aide aux PME/PMI des technologies duales touchant à la robotique de sécurité et de défense des domaines aérien, naval et terrestre : le cas des États-Unis, de la Grande-Bretagne, de l'Allemagne, d'Israël et de la Norvège » ;

« Impact des marchés innovants de maintien en condition opérationnelle sur la stratégie des groupes de défense en matière de services ».

Source : ministère de la Défense.

c. Informer le grand public sur le risque numérique

Dans la plupart des attaques informatiques, et notamment celles qui ciblent un réseau fermé, intervient une faille humaine *via* des vecteurs aussi simples et courants qu'un spam, que l'ouverture de la pièce jointe d'un message Internet émanant d'un expéditeur connu ou inconnu, que des informations données sur les réseaux sociaux, que l'emploi d'une clef USB, qui ne sont pas identifiés comme des dangers, tant ils participent désormais de la vie quotidienne.

Ces pratiques de la vie courante sont, parfois au mépris des règles internes des entreprises, quand elles existent, transposées dans le comportement sur le lieu de travail. Une protection technique sophistiquée peut ainsi être déjouée par un geste en apparence anodin. Ainsi, Patrick Pailloux, le directeur de l'ANSSI, n'a de cesse de mettre en garde contre l'utilisation à titre professionnel (BYOD) [(1)] des équipements personnels, ordinateurs portables, clés USB, tablettes…

Il semble donc indispensable au rapporteur de sensibiliser les utilisateurs du numérique, c'est-à-dire l'ensemble de nos concitoyens, et par ricochet les entreprises, dans un souci de protection individuelle et collective.

Des campagnes de sensibilisation sur le modèle de celles qui ont été organisées de longue date pour la sécurité routière pourraient être lancées. L'analogie entre la sécurité routière et la cybersécurité est en effet frappante. La sûreté et la qualité des infrastructures routières et des véhicules n'ont cessé de progresser et jouent un rôle déterminant en matière de sécurité. Mais elles ne sont rien sans le comportement responsable des usagers, pourtant soumis au respect des obligations légales du code de la route. Il devrait en aller de même pour les usagers des systèmes d'information qui, parallèlement aux évolutions technologiques, seront incités à adopter graduellement des réflexes simples garantissant une sécurité de base.

Dans le même esprit, la stratégie proposée par l'UE *(cf. supra)* invite les états membres, avec la participation des autorités nationales concernées à *« organiser tous les ans à partir de 2013, avec l'aide de l'ENISA et la*

*(1) Apportez vos outils personnels,*bring your own device.

participation du secteur privé, un mois de la cybersécurité afin de sensibiliser les utilisateurs finaux. À partir de 2014, un mois de la cybersécurité sera organisé en même temps dans l'UE et aux États-Unis ». Le mois de la cybersécurité, dont c'est la deuxième édition, a débuté, en toute discrétion, le 11 octobre 2013. Le rapporteur déplore que cette action n'ait pas davantage de retentissement.

Des initiatives se développent partout en Europe : le ministère de l'intérieur britannique a lancé avant l'été un projet de campagne de sensibilisation à la cybersécurité en direction des entreprises et du grand public, doté de quatre millions de livres sterling ; le site du *Bundesamt für Sicherheit der Informationstechnik* (BSI), l'équivalent de l'ANSSI, propose des pages, illustrées de vidéos, destinées au grand public.

En France, le rapporteur salue l'initiative de la CNIL qui a lancé un collectif pour faire de l'éducation au numérique une « grande cause nationale » qui permettrait d'assurer à ce projet une visibilité et de le décliner sous forme d'actions concrètes. Il craint en effet que l'effort consenti par le ministère et la réelle priorité inscrite dans le programme 144 « Environnement et prospective de la politique de défense » n'apportent pas les résultats espérés si la cybersécurité ne devient pas une grande cause nationale.

d. Inclure le numérique dans les programmes éducatifs

Le rapporteur regrette que la sécurité des systèmes d'information ne soit enseignée que dans les cursus dont elle est l'objet.

Au-delà de la stratégie proposée par l'UE *(cf. supra)* qui invite les états membres à *« intensifier les efforts consacrés à l'éducation et à la formation à la sécurité des réseaux et de l'information (SRI) en milieu scolaire d'ici à 2014, une formation à la SRI, au développement de logiciels sûrs et à la protection des données personnelles dans le cursus des étudiants en informatique et une formation de base à la SRI pour le personnel des administrations publiques »*, il semble indispensable au rapporteur qu'un module de cet enseignement soit intégré dans toutes les formations supérieures (universités, grandes écoles, écoles de commerce, d'ingénieurs…).

À titre d'exemple, la formation à la cybersécurité et au chiffrement est enseignée en Israël à partir de la classe de seconde [(1)]. Le ministre britannique de l'Éducation, Michael Gove, a, pour sa part, pris la décision d'intégrer l'informatique dans les nouveaux programmes scolaires, à partir de septembre 2014, et d'enseigner aux écoliers dès l'âge de cinq ans comment produire de l'information et du contenu numérique, comment écrire et tester des programmes simples et comment organiser et stocker des données. La cybersécurité sera enseignée à un âge précoce ainsi que la protection des données personnelles. Au stade de l'école secondaire, les élèves apprendront différents

(1) www.csmonitor.com.

langages de programmation, les systèmes d'ordinateurs en réseau et l'interaction *hardware/software* [(1)].

La gendarmerie nationale envisage, pour sa part, de mener en fin d'année une action en direction des élèves de CM2 intitulée *« Permis Internet »*, sur le mode du *« Permis piéton »* existant.

5. Une stratégie nationale insérée dans une stratégie européenne

Il y a, enfin, **trop peu de coopération européenne dans la cyberdéfense** et les attaques conjointes que viennent de subir plusieurs pays devraient logiquement conduire les pays européens à mieux coordonner leurs efforts. La souveraineté nationale en dépend et l'on peut se féliciter de la décision du Premier Ministre de créer une filière thématique sur les questions de sécurité, qui devrait, de l'avis du rapporteur, faire l'objet d'un inventaire afin d'identifier des domaines à conforter parce qu'ils conditionnent le corps de la souveraineté.

Si la cyberdéfense est par nature un espace de souveraineté, au sein duquel les échanges sont contraints, la forme de la menace, qui ne connaît aucune frontière, et la nature des outils impliquent au-delà des mesures nationales également des mesures de cybersécurité à l'échelle internationale et, à tout le moins, européenne.

La prise de conscience semble donner des résultats et la Commission européenne a publié le 7 février 2013 deux documents importants :

a. Une stratégie en matière de cybersécurité pour l'Union européenne

Une stratégie intitulée **« Un cyberspace ouvert, sûr et sécurisé »**[(2)], élaboré conjointement par la Commission européenne avec la Haute représentante de l'Union pour les affaires étrangères et la sécurité.

Cette stratégie s'articule autour des grands principes que sont *« la prévalence des valeurs essentielles de l'UE dans le monde virtuel autant que dans le monde réel, la protection des droits fondamentaux, de la liberté d'expression, des données personnelles et de la vie privée, l'accès de tous à Internet, une gouvernance participative, démocratique et efficace ainsi qu'une responsabilité partagée pour assurer la sécurité »*.

Les priorités qui en découlent sont les suivantes *: « parvenir à la cyber-résilience, faire reculer considérablement la cybercriminalité, développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC), développer les ressources industrielles et technologiques en matière de cybersécurité, instaurer une politique internationale*

(1) Theguardian.com, 8 juillet 2013.
(2) JOIN(2013) 1 final. devenue Résolution du Sénat le 19 avril 2013.

de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE. ».

b. Une proposition de directive

Une proposition de directive concernant la sécurité des réseaux et de l'information [(1)] a été publiée par le Parlement européen et le Conseil de l'Europe. Elle imposerait notamment aux États membres de se doter d'une autorité de cybersécurité, de disposer d'une organisation opérationnelle d'assistance en cas d'incidents informatiques et de définir une stratégie nationale.

Parallèlement, un nouveau règlement visant à renforcer le rôle de l'ENISA [(2)], créée en 2004, et à moderniser son mandat est en cours de négociation entre le Conseil et le Parlement européen, ce dont se félicite le rapporteur qui a senti chez ses interlocuteurs une réserve quant à l'activité de cette agence, à ses retombées et à sa visibilité.

6. Le soutien à l'innovation

> *« La capacité de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs est devenue un des éléments de la souveraineté nationale. Pour y parvenir* ***l'État doit soutenir des compétences scientifiques et technologiques performantes*** *».*
>
> Livre blanc de2013

a. Mettre l'accent sur le caractère dual des projets

Qu'il s'agisse des drones ou de la cyberdéfense, les recherches doivent partager les applications duales civiles et militaires.

Les gouvernements de la France ont mis successivement l'accent, chacun à leur manière, sur le soutien à l'innovation au travers de la création des pôles de compétitivité en 2005 ou du lancement des investissements d'avenir en 2010. Plus récemment, les rapports Gallois, en novembre 2012, et Lauvergeon, en octobre 2013, ont été repris dans le soutien fort à l'innovation décidé par le Président François Hollande et par le Premier Ministre Jean-Marc Ayrault.

Mais invariablement, la dimension duale des technologies génériques est escamotée alors qu'elle est évidente, comme, par exemple, pour les soutiens accordés aux différents pans de l'économie numérique, pour la valorisation des données massives – le *big data* –, pour les technologies de sécurité et de résilience des réseaux ou bien pour les recherches concernant le recyclage des métaux rares. Ainsi les dernières avancées en matière d'aéronautique, et particulièrement de

(1) 3013/0027 (COD).

(2) Agence européenne de la sécurité des réseaux et de l'information, European network and information security agency.

drones, débouchent sur des équipements d'une grande diversité permettant la surveillance d'infrastructures, de feux de forêt…

De fait, la dualité est implicitement présente dans ces différents programmes de soutien à l'innovation à travers les grandes entreprises qui sont impliquées, comme Thales ou Dassault Systèmes pour la valorisation des données massives.

Dans le cadre de l'analyse précise de la dualité technologique, le rapporteur estime qu'il conviendrait de mettre l'accent sur le caractère dual des innovations **dans leur phase amont**, au niveau de la preuve de concept, c'est-à dire de la démonstration de faisabilité, comme, par exemple, dans le cas de la preuve des logiciels et regrette donc que les programmes d'investissement d'avenir n'aient pas intégré la nécessité de conforter les industries de défense en privilégiant la dualité des technologies. Le Gouvernement de Jean-Marc Ayrault a certes corrigé le tir, mais le rapporteur est d'avis qu'il eût été souhaitable de réserver une partie des crédits dégagés au lancement d'un programme sur les drones.

Présentation de projets de recherche conduits en coopération multilatérale ou bilatérale et part de R&T en coopération

En 2012, la France a consacré, en paiement, 15,5 % de son effort de recherche et technologie (R&T) à des coopérations internationales, essentiellement avec ses partenaires européens, en premier lieu, le Royaume-Uni dans un cadre bilatéral, et à travers l'Agence européenne de défense (AED) pour les coopérations multilatérales. Cette part est en diminution par rapport aux années précédentes, où elle s'approchait de 18 % : les restrictions des budgets de recherche et technologie de ses partenaires se sont traduites par un ralentissement du lancement de nouvelles coopérations et des engagements sur des montants financiers moindres en 2011.

En 2013, le taux de coopération devrait augmenter légèrement (autour de 17 %) en raison de la concrétisation de 10 nouveaux accords (de R&T à l'AED auxquels la France participe) engagés en 2012.

Le Royaume-Uni continue d'être le premier partenaire bilatéral de la France en matière de R&T de défense : outre les objectifs fixés par le traité de Lancaster House en 2010 (50 millions d'euros d'engagement par an et par nation dans des programmes communs de R&T), deux accords-cadres importants relatifs aux drones ont été signés à Londres en juillet 2012 en présence de Jean-Yves Le Drian et de son homologue britannique, Philip Hammond :

• Le premier porte sur un contrat d'études de 13 millions d'euros attribué à BAE Systems et Dassault Aviation pour lancer les premiers travaux sur l'éventuelle composante drone de combat du système de combat aérien du futur (SCAF) à horizon 2030. Ces deux industriels ont déjà travaillé sur ce sujet dans le passé : BAE avec son projet TARANIS et Dassault Aviation avec le NEURON, démonstrateur développé dans le cadre d'une coopération européenne, qui a effectué son premier vol cet automne ;

• le second accord est un prélude à la constitution d'une *task force* franco-britannique dans les drones tactiques aux alentours de 2014-2015.

Pour nos autres partenaires européens, une évolution de nos coopérations s'opère, depuis les cinq dernières années, d'un cadre majoritairement bilatéral vers l'Agence

européenne de défense. En 2012, 66 % des coopérations franco-allemandes sont placées sous le couvert de l'AED et la totalité des coopérations menées avec l'Italie sont effectuées dans un cadre multilatéral. La France est l'un des pays les plus actifs en matière de projets européens de R&T, avec une participation à 12 des 14 coopérations lancées par l'AED en 2012.

Le montant cumulé des différents marchés en cours et objets de coopération s'élève à 1 364 millions d'euros, dont 598 millions d'euros financés par la France (43,8 %).

Source : ministère de la Défense.

b. Soutenir l'innovation

Enfin, le rapporteur souhaite aborder le soutien à l'innovation scientifique, technologique et industrielle dont la vitalité est le gage d'équipements performants à la pointe du progrès qui génèrent emplois et croissance.

De nombreux dispositifs sont en place et fonctionnent de façon satisfaisante : RAPID pour les PME/ETI, ASTRID et ASTRID Maturation, le partenariat DGA-OSEO Innovation, les pôles de compétitivité (PEGASE en région Provence – Côte d'Azur et cluster AETOS en Aquitaine, par exemple), le club des partenaires académiques de la Défense, le partenariat DGA - Agence nationale de la recherche (ANR), le financement de thèses…

Le crédit impôt recherche apporte également un soutien appréciable aux recherches menées en France mais tous les interlocuteurs du rapporteur ont reconnu que ces crédits, qui irriguent de nombreux laboratoires de recherche privée, ne sont pas suffisants pour opérer de nouvelles inflexions dans les domaines où persistent des verrous technologiques.

Il semble toutefois que les PME rencontrent soit des difficultés à accéder à la commande publique soit des contraintes bloquantes imposées pour les grandes entreprises pour lesquelles elles interviennent.

Le rapporteur observe que les recommandations concernant le lien entre grands groupes et PME valent aussi bien pour le secteur civil que le secteur de la défense ; le rapport Gallois préconise de conditionner les aides aux grandes entreprises à leur capacité d'associer à leur action fournisseurs et sous-traitants.

Le ministère du Redressement productif labellise

la relation clients/fournisseurs

En 2010, a été élaborée conjointement par la Médiation inter-entreprises [(1)], la CDAF (Compagnie des acheteurs de France) et la Médiation des Marchés Publics [(2)] la *« Charte Relations fournisseurs responsables »* afin d'inciter les entreprises à adopter des pratiques responsables vis-à-vis de leurs fournisseurs.

Cette charte, basée sur la « *Liste des 36 pratiques commerciales abusives* » issue du rapport Volot [(3)] sur le « *dispositif juridique concernant les relations interentreprises et la sous-traitance* », définit *« Dix engagements pour des achats responsables »* [(4)] notamment en matière d'équité financière, d'appréciation du coût total et de ses aléas ainsi que d'implication des grands donneurs d'ordre dans leur filière. Au 30 septembre 2013, la charte compte 409 signataires dont de nombreuses entreprises de la filière Défense [(5)], dont le Ministère de la Défense.

Dans le sillage de cette charte, a vu le jour le « *Label Relations fournisseurs responsables* » qui vise à distinguer les entreprises françaises ayant fait preuve de relations durables et équilibrées avec leurs fournisseurs. Il s'agit d'un premier label d'État qui a été décerné à ce jour à onze grandes entreprises, dont Thales et Nexter Systems dans la filière Défense [(6)].

Le ministère du Redressement productif édite par ailleurs le « Guide pour la qualité des relations contractuelles clients-fournisseurs ».

Dans son précédent avis, le rapporteur avait appelé de ses voeux la conclusion d'un *Small Business Act* français. L'instruction ministérielle instituant le Pacte Défense PME a été signée en novembre 2012 et s'inscrit dans le cadre des orientations fixées par la communication de la Commission européenne n° 2008/394 du 25 juin 2008 relative au *Small Business Act* pour l'Europe.

Ce pacte rassemble quarante mesures destinées à faire évoluer les pratiques d'achat au sein du ministère et à soutenir la commande publique en direction des PME. L'action 19 institue un comité de pilotage à trois niveaux, dont le premier niveau se réunit mensuellement, puis trimestriellement, pour contrôler l'application de cette instruction ministérielle.

Mais ce pacte qui avait suscité beaucoup d'espoir semble lent à se matérialiser ainsi que le regrette le Comité Richelieu [(7)]. **Le rapporteur, ainsi qu'il l'a déclaré lors de la réunion de la commission du 9 octobre 2013, propose que, dans le cadre de sa mission de contrôle, la commission de la Défense procède à l'évaluation de la mise en oeuvre de cet ensemble de mesures.** Ce contrôle permettrait de vérifier, par exemple, *« le caractère proportionné des clauses appliquées aux PME »*, le respect du passage en trois ans

(1) Ministère du Redressement productif.
(2) Ibid.
(3) Jean-Claude Volot, Médiateur des relations inter-entreprises et de la sous-traitance.
(4) www.redressement-productif.gouv.fr/médiation inter-entreprises/chartes et labels/
(5) On peut citer, de manière non exhaustive, EADS, Safran, Thales, GIAT(Nexter), Eurocopter, DCNS, MBDA France, GIFIC, GICAN…
(6) www.redressement-productif.gouv.fr.
(7) Réunion de la commission le 9octobre 2013, compte rendu n° 9.

de 40 à 50 millions d'euros du montrant des crédits affectés au dispositif RAPID soutenant l'innovation duale des PME, de faire un premier bilan de l'aide effective apportée aux PME pour la conquête de nouveaux marchés en France et à l'exportation, de l'état d'avancement de l'expérimentation d'attribution de labels…

Le rapporteur est favorable à l'adoption du budget du programme 144 « Environnement et prospective de la politique de défense ».

TRAVAUX DE LA COMMISSION

EXAMEN DES CRÉDITS

Après l'audition de M. Jean-Yves Le Drian, ministre de la Défense, lors de la commission élargie (voir le compte rendu de la réunion du 23 octobre 2013 à 16 heures 15) [(1)]*, la commission de la Défense examine, pour avis, les crédits de la mission* ***« Défense*** *» pour 2014.*

La commission examine l'amendement DN22 de M. Fromion.

M. Yves Fromion. Je tiens à préciser que si cet amendement ne comprend que mon nom, j'y associe l'ensemble des commissaires du groupe UMP.

Nos forces armées sont confrontées à un réel déficit d'entraînement à cause de l'insuffisance des moyens qui leur sont accordés par le programme 178 « Préparation et emploi des forces ». La lecture des indicateurs de performance figurant dans le « bleu budgétaire » confirme cette appréciation. Elle permet de constater une réduction dangereuse, pour tout dire inacceptable, des ratios d'entraînement des forces. Les journées d'activité par homme, les heures de vol des pilotes et les jours de mer par bâtiment sont réduits de façon déraisonnable.

Je propose d'inverser cette tendance en prélevant un milliard d'euros sur le programme 402 « Excellence technologique des industries de défense » pour les verser au programme 178. Les crédits du programme 402 sont abondés cette année par les ressources exceptionnelles issues du plan d'investissements d'avenir (PIA) et je considère plus urgent de privilégier l'entraînement des forces aux dépenses de recherche, qui peuvent être légèrement décalées.

M. Jean-Jacques Bridey, rapporteur pour avis. Je suis totalement défavorable à cet amendement. Les ressources exceptionnelles attendues pour la mission « Défense » sont de 1,7 milliard d'euros pour l'année 2014, dont l'essentiel vient effectivement du PIA. Il est fondamental que notre recherche en bénéficie.

Mme la Présidente Patricia Adam. Je tiens à préciser que le programme 402 finance les recherches nécessaires en matière de dissuasion et d'observation spatiale, et notamment le programme MUSIS dont vous connaissez tous l'importance pour nos armées.

M. Yves Fromion. Je souligne que mon amendement ne concerne que l'action du programme 402 finançant la recherche en matière de dissuasion nucléaire.

---

(1) http://www.assemblee-nationale.fr/14/budget/plf2014/commissions_elargies/cr/C005.asp

Mme la Présidente Patricia Adam. Encore mieux, venant d'un gaulliste comme vous !

M. Yves Fromion. Je considère en effet que le nucléaire peut sans doute consentir un léger décalage dans le temps au profit de la priorité assumée de l'entraînement.

Suivant l'avis défavorable du rapporteur pour avis, la commission ***rejette*** *l'amendement DN22. Elle examine ensuite l'amendement DN18 de M. Fromion.*

M. Yves Fromion. Cet amendement propose d'abonder les crédits du programme 178 pour financer l'acquisition de nouveaux canons d'artillerie de gros calibre CAESAR. Alors que la précédente LPM prévoyait l'acquisition de nouveaux systèmes, le projet actuel de LPM ne prévoit aucune commande dans ce domaine. Nous risquons donc de perdre notre compétence artillerie de gros calibre. Cela irait à l'encontre de ce que nous avait affirmé le ministre tout à l'heure, à savoir que le projet de LPM ne comportait aucun risque de rupture capacitaire. Poursuivons donc le programme CAESAR, comme nous le faisons avec le Rafale, pour maintenir un seuil minimum de compétence.

M. Joaquim Pueyo, rapporteur pour avis. Le ministre vient de nous expliquer que ce risque de rupture capacitaire n'existait pas pour le moment. Il est trop tôt pour effectuer de nouvelles commandes. Je suis donc défavorable à cet amendement.

Suivant l'avis défavorable du rapporteur pour avis, la commission ***rejette*** *l'amendement DN18. Elle examine ensuite l'amendement DN19 de M. Fromion.*

M. Yves Fromion. Le ministre s'est déjà exprimé sur les équipements d'accompagnement et de cohérence (EAC) et a rappelé leur importance. La faible dotation qu'ils reçoivent au sein du programme 178 rend difficile l'accomplissement des missions de l'état-major de l'armée de terre. Année après année, les chefs d'état-major successifs de l'armée de terre attirent notre attention sur la faiblesse de ces dotations. Il faut donc remédier à cette situation et faire en sorte que ces équipements ne soient pas les laissés pour compte de la programmation.

M. Joaquim Pueyo, rapporteur pour avis. Je suis défavorable à cet amendement.

Suivant l'avis défavorable du rapporteur pour avis, la commission ***rejette*** *l'amendement DN19. Elle examine ensuite l'amendement DN20 de M. Fromion.*

M. Yves Fromion. Cet amendement est la déclinaison du précédent pour les forces navales.

M. Gilbert Le Bris, rapporteur pour avis. Cet amendement propose d'augmenter les crédits d'EAC des forces navales de 50 millions d'euros pour

2014. Mais le projet de loi de finances prévoit déjà de les augmenter de 45 millions en 2014, avec une augmentation de 86 % avec fonds de concours et attributions de produits par rapport à l'année passée. Je dirais donc que cet amendement est satisfait.

Suivant l'avis défavorable du rapporteur pour avis, la commission ***rejette*** *l'amendement DN20. Elle examine ensuite l'amendement DN21 de M. Fromion.*

M. Yves Fromion. Comme les deux précédents, cet amendement propose d'augmenter les crédits d'EAC mais, cette fois, de l'armée de l'air.

M. Serge Grouard, rapporteur pour avis. Je suis d'accord sur le fond de cet amendement et l'importance qui doit être accordée aux crédits d'EAC de l'armée de l'air. Mais le problème est que cet amendement prélève des crédits sur le programme 402, qui est tout aussi important.

On comprendra donc que je ne peux donner un avis favorable à cette proposition, car j'ai déjà annoncé que je donnerai un avis défavorable aux crédits « Préparation et emploi des forces » de l'armée de l'air. Je m'abstiendrai donc sur cet amendement.

La commission ***rejette*** *l'amendement DN21.*

Mme la présidente Patricia Adam. Nous allons maintenant passer aux votes sur les crédits de la mission « Défense ».

M. Alain Marty, rapporteur pour avis. Je tiens à préciser que je m'abstiendrai sur les crédits concernant le « Soutien logistique et interarmées ».

*

* *

Conformément aux conclusions du rapporteur pour avis, la commission émet un ***avis favorable*** *à l'adoption des crédits* ***« Environnement et prospective de la politique de défense »*** *de la mission* ***« Défense »***.

ANNEXE :
Liste des personnes auditionnées par le rapporteur

Auditions par ordre chronologique

- **Contre-amiral Arnaud Coustillière**, officier général cyberdéfense à l'état-major des armées.

- **Colonel Gilles Darricau**, officier de cohérence opérationnelle (OCO) renseignement commandement militaire Maîtrise de l'information 1 - état-major des armées.

- **Général Denis Mercier,** chef d'état-major de l'armée de l'air.

- **M. Kalev Stoicescu**, conseiller Défense de l'ambassade d'Estonie à Paris.

- **Général Hans-Dieter Poth**, conseiller Défense et **M. Reinhard Färber**, conseiller d'armement de l'Ambassade d'Allemagne à Paris.

- **M. Claude Kirchner**, délégué général à la recherche et au transfert pour l'innovation de l'Institut national de recherche en informatique et en automatique (INRIA).

- **M. Vincent Marfaing**, Thales vice-président, IT security/cybersecurity business line, **M. Marc Darmon**, directeur général adjoint, directeur général de l'activité systèmes d'information et de communication sécurisées, **général (2S) Pierre-Henri Mathe**, conseiller défense de la division systèmes de mission de défense, et **Mme Isabelle Caputo**, directeur des relations parlementaires et politiques.

- **Mme Frédérick Douzet**, professeure à l'Institut français de géopolitique de l'université Paris 8, titulaire de la Chaire Castex de cyberstratégie à l'Institut des hautes études de la Défense nationale.

Déplacements

- **Visite du centre Maîtrise de l'Information de Bruz** : ingénieur en chef de l'armement **Guillaume Poupard**, responsable du pôle de sécurité des systèmes d'information à la Direction générale de l'armement, **M. Christophe Pezron**, chef du service des recherches et technologies de défense et de sécurité (DGA/DS/STRS), Ingénieur général de l'armement **Olivier Lesbre**, directeur de DGA Maîtrise de l'Information (DGA/DT/MI), Ingénieur en chef des études et des techniques de l'armement **Hervé Le Goff**, adjoint au sous-directeur affaire de DGA MI, **M. Christophe Vaucouleur**, adjoint au sous-directeur technique de

DGA MI, Ingénieur en chef de l'armement **Frédéric Valette**, chef de la division sécurité des systèmes d'information de DGA MI, **M. Jean-Pierre Lebée**, adjoint au chef de division SSI, **M. Dominique Chauveau**, chef de département au sein de la division SSI, **M. Olivier Chenèble**, chef de département au sein de la division SSI, **M. Jean-Yves Guinamant**, chef de département au sein de la division SSI, **M. Christophe Baumann**, responsable projet à DGA MI, **M. Pascal Chantrenne**, architecte au sein de la division SSI, **M. Christophe Gautourneau**, ingénieur au sein de la division SSI.

➢ **Visite de Cassidian à Élancourt** : **MM. Jean-Marc Nasr**, président de Cassidian SAS, **Luc Boureau**, directeur général délégué, directeur commercial et marketing France de Cassidian, **Patrick Oswald**, directeur grands comptes Défense Cassidian, **Jean-Michel Orozco**, président de Cassidian Cybersecurity, **Gérard Moisselin**, conseiller sécurité et territoires du président d'EADS, **Mme Annick Perrimond-du-Breuil**, directeur des relations avec le Parlement d'EADS France

➢ **Visite du 61e régiment d'artillerie de Chaumont** : **colonel Aymeric Bonnemaison**, responsable de la coordination et de la maîtrise de l'information, état-major de l'armée de terre, bureau Plans, colonel **Philippe Jouve**, chef de corps du 61e régiment d'artillerie.

*

* *

Au cours des auditions organisées par la commission, le rapporteur a posé des questions figurant dans les comptes rendus à :

➢ **Contre-amiral Arnaud Coustillière**, officier général en charge de la cyberdéfense à l'état-major des armées ;

➢ **M. Guillaume Poupard**, ingénieur en chef de l'armement, responsable du pôle de sécurité des systèmes d'information à la Direction générale de l'armement ;

➢ **M. Patrick Pailloux**, directeur général de l'Agence nationale de la sécurité des systèmes d'information ;

➢ **M. Laurent Collet-Billon**, délégué général pour l'armement ;

➢ **Général Denis Mercier**, chef d'état-major de l'armée de l'air ;

➢ **MM. Philippe Berna**, président, et **Thierry Gaiffe**, président de la commission Défense du Comité Richelieu.

➢ **Général Bertrand Ract-Madoux**, chef d'état-major de l'armée de terre.

*

* *

➢ Audition publique conjointe de la commission avec l'Office parlementaire d'évaluation des choix scientifiques et technologiques et la commission des affaires étrangères, de la défense et des forces armées du Sénat, sur le risque numérique, le 21 février 2013.