CHOCS FUTURS

SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

CHOCS FUTURS

Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité

SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

A vocation pédagogique, cet exercice de prospective n'exprime pas de position officielle et ne correspond pas à une quelconque doctrine, livre blanc ou politique publique. Il reflète le point de vue de chercheurs et l'état des réflexions sur un ensemble de sujets. Le choix des thématiques résulte du travail de veille technologique réalisé par le SGDSN, en relation étroite avec le monde de la recherche. Il pourra être actualisé et augmenté par l'étude ultérieure d'autres sujets.

Sommaire

Avant-propos

Quand Robert Fulton, inventeur du premier sous-marin poseur de mines, soumit son projet au Directoire puis à Napoléon, celui-ci fut rejeté comme inepte et militairement déloyal. L'Amirauté britannique, plus perspicace, en vit tout l'intérêt, mais préféra soudoyer Fulton pour qu'il ne développe pas une invention potentiellement dangereuse pour la suprématie de sa flotte. L'Amérique n'en voulut pas davantage.

Malgré l'engouement technologique de notre siècle, la résistance à l'innovation existe toujours, par paresse intellectuelle, par force des habitudes, par choix de doctrine, ou du fait de contraintes économiques. A côté des ruptures stratégiques qui, subrepticement ou brutalement, affectent l'agencement du monde, il existe des sauts ou des ruptures technologiques qui, même ressentis comme imminents, n'ont pas été anticipés avec clairvoyance. Le choc est alors plus violent et les effets moins bien maîtrisés. Dans tous les cas, l'accélération du temps technologique au XXIe siècle rend le rattrapage des occasions manquées plus difficile et le prix du déni plus élevé.

Dans un monde travaillé par des dynamiques contradictoires, où l'équilibre des puissances est fortement évolutif et où les mécanismes d'une gouvernance mondiale sont enrayés, il est devenu plus essentiel encore de ne pas se tromper sur les révolutions scientifiques et techniques qui vont bouleverser notre futur et toutes les équations de sécurité et de défense.

Le présent rapport, élaboré en lien avec la Fondation pour la recherche stratégique (FRS), est justement consacré à l'impact sur notre environnement stratégique de quelques transformations technologiques en gestation ou déjà en cours. Il ne s'enhardit pas trop loin, mais braque le projecteur sur l'horizon 2030, horizon raisonnable pour les politiques publiques. Il se propose d'attirer l'attention du lecteur sur une série de thématiques d'intérêt, notamment technologiques, et s'interroge sur leur impact dans les quinze ans à venir.

L'introduction de ce document rappelle les profondes transformations qu'a connues notre environnement international depuis cinq ans, et dresse le tableau géostratégique d'un monde menacé par le désordre et le regain des tensions. Elle met en évidence, également, l'influence majeure que pourraient exercer le progrès et la diffusion des technologies sur les équilibres stratégiques.

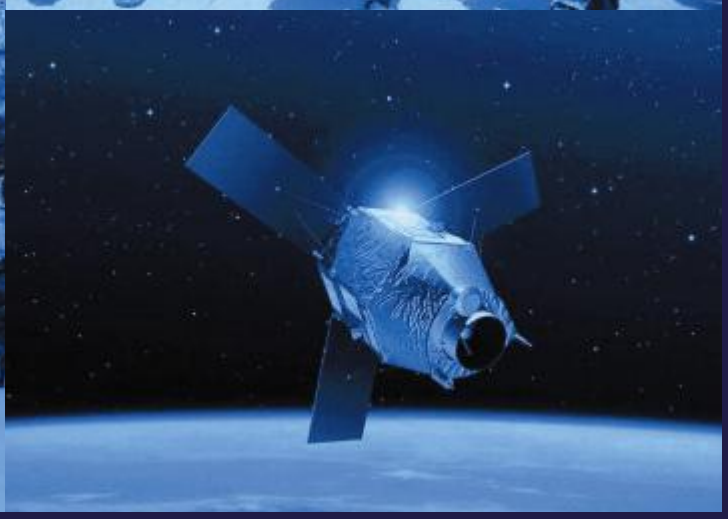
Certaines évolutions déjà observables, comme l'émergence de la conflictualité dans le cybermonde, ou la montée des risques associés à la présence de nouveaux acteurs dans l'espace extra-atmosphérique, pourraient se prolonger dans les quinze prochaines années. Ces tendances qui se consolident font l'objet de la première partie du rapport.

La seconde partie, quant à elle, envisage les ruptures technologiques susceptibles d'engendrer des ruptures stratégiques. Ainsi, par exemple, la diffusion de la biologie de synthèse et l'impression 3D pourraient entraîner une individualisation de la menace en mettant des capacités non négligeables à la disposition d'acteurs non étatiques. En revanche, le développement des vecteurs hypervéloces pourrait conférer une avance militaire considérable à un club restreint d'Etats détenteurs.

Cette étude ne prétend ni être exhaustive, ni apporter un éclairage définitif sur les thèmes qu'elle a choisis. Elaborée dans un dessein pédagogique, elle ne définit pas davantage une doctrine, ni ne fixe une feuille de route pour les politiques publiques dans les domaines qu'elle aborde. Elle espère, en offrant des « regards » sur des défis à venir pour l'Europe et pour notre pays, proposer des pistes de réflexion à l'ensemble des acteurs de la communauté stratégique française (administrations, *think tanks*), voire alimenter utilement le débat public, dans une période où les questions de sécurité et de défense s'imposent au cœur des préoccupations.

Louis Gautier
Secrétaire général
de la défense
et de la sécurité nationale

Introduction



Parler de chocs futurs, c'est introduire la violence et la rupture dans la réflexion sur l'avenir. Rencontre brutale de personnes ou de choses ; conflit, affrontement entre entités mais aussi entre idées ou intérêts ; émotion fortuite et soudaine qui frappe l'intégrité physique, la sensibilité ou le psychisme ; syndrome clinique aigu nécessitant une thérapie médicale d'urgence… L'**espace sémantique du mot choc est inquiétant mais ambigu.** Il renvoie à l'action, militaire notamment, à la secousse, à la blessure, au traumatisme. Comme il implique en creux la résilience, le renouveau et l'espoir.

L'environnement dans lequel s'inscrivent les études prospectives réunies dans cet ouvrage est celui d'un monde apolaire qui émerge, qui voit s'affirmer de nouvelles stratégies de puissance et qui met à l'épreuve les fondements communs de la paix, notamment dans leur incarnation européenne. Les évolutions profondes de l'environnement géopolitique et les ruptures technologiques prévisibles à l'horizon 2030 sont-elles de nature à remettre en cause les équilibres stratégiques ? Et les Etats, par les nouvelles capacités et les systèmes de régulation dont ils se dotent, peuvent-ils résister à l'individualisation de la menace qui se profile à travers les progrès techniques ? Dans ce contexte international troublé, entreprendre une réflexion prospective peut sembler délicat. L'exercice est pourtant indispensable, dans un genre qui ne permet jamais de prévoir le cours exact que les événements prendront dans le futur, mais qui prétend au moins éclairer les grandes tendances qui vont influer sur les équilibres stratégiques de demain.

Le monde est confronté à une menace terroriste omniprésente, qui a franchi un nouveau seuil avec la progression depuis l'été 2014 de *Daech*, avatar particulièrement dangereux du terrorisme d'inspiration jihadiste.

La menace véhiculée par *Daech* se superpose à celle portée de façon continue par *Al Qaïda* et ses groupes affiliés. Cette structuration de la scène jihadiste en deux pôles rivaux contribue à un phénomène de surenchère terroriste au niveau mondial. Elle s'exprime à travers une stratégie d'expansion géographique des groupes terroristes qui cherchent à étendre leur zone d'influence. Profitant de l'effondrement ou de la faiblesse des Etats, de la porosité de leurs frontières et de l'absence de contrôle, ils cherchent à s'implanter dans des zones de non-droit, du Nord du Nigeria au Sahel et à l'Afrique du Nord (Sud algérien, Libye, Sud tunisien), du Levant (Sinaï, Syrie, Irak) à la péninsule arabique (Yémen) et jusqu'à la Corne de l'Afrique. L'acquisition par ces groupes terroristes de capacités militaires très significatives leur permet désormais d'engager des combats de forte intensité pour le contrôle ou la conquête de territoires. En outre, la désinhibition dont font preuve les jihadistes, au regard de la violence des outils de propagande, favorise l'imitation et le passage à l'acte chez des individus ou des organisations incontrôlés, mus par d'autres motivations idéologiques.

La France est pour sa part confrontée à une nette aggravation de la menace terroriste. Les incitations répétées à commettre des attaques planifiées ou inspirées contre nos ressortissants et nos intérêts se sont tragiquement concrétisées par les attentats qui ont frappé la France et l'Europe depuis 2015. Et le retour des combattants étran-

gers, chassés désormais des sanctuaires des organisations jihadistes, constitue une menace renforcée pour les pays frontaliers et les pays d'origine de ces revenants. Elle implique une continuité absolue de la lutte antiterroriste, de l'intérieur à l'extérieur de nos frontières.

Car l'équilibre géostratégique est affecté par de multiples facteurs politiques, démographiques ou économiques, qui entraînent des risques importants de déstabilisation et de crises.

La faillite des Etats a entraîné **l'instabilité et même la déstructuration de régions entières, hier en Afghanistan, aujourd'hui au Levant et en Afrique.** Après la vague des révolutions arabes, **elle s'incarne avant tout dans la guerre civile qui sévit en Syrie,** à l'origine d'un chaos sécuritaire et politique sur le flanc sud de l'Europe qui a favorisé le développement de *Daech*. Même si cette organisation terroriste perd de son emprise territoriale, elle continuera de représenter une menace pour la région dans les années à venir.

L'**effondrement de l'Etat libyen** et l'incapacité des autorités issues des printemps arabes à répondre aux causes profondes des révolutions de 2011 font peser **une menace sur la stabilité de l'Afrique du Nord et de la bande sahélo-saharienne.** En Libye, la dégradation sécuritaire continue de favoriser l'émergence d'un *hub* terroriste qui constitue une zone de brassage, de connexion et de collusion entre les différents groupes jihadistes libyens ou de la bande sahélo-saharienne (BSS), se revendiquant d'*Al Qaïda* ou de *Daech*. Le territoire libyen constitue ainsi une zone refuge et une plateforme logistique où les groupes jihadistes de la BSS peuvent se régénérer.

Par ailleurs, l'incapacité des pouvoirs en place **en Afrique du Nord** à améliorer la situation socio-économique interne contribue à alimenter une contestation sociale, source potentielle de déstabilisation pour ces Etats et pour la région tout entière.

Au Sud de la bande sahélo-saharienne, l'expansion de la secte islamiste *Boko Haram*, forte de plusieurs milliers de combattants dans le Nord-est du Nigéria fait peser un risque sur la stabilité de la région du lac Tchad par les implications humanitaires liées aux flux de réfugiés qu'elle entraîne et par l'essaimage de ses thèses dans l'ensemble des pays riverains.

La multiplication des menaces et des crises politiques au Maghreb, au Proche et au Moyen-Orient comme dans l'Afrique subsaharienne a profondément déstabilisé l'ensemble de la zone. En facteur commun, les divisions confessionnelles entre Sunnites et Chiites, exacerbées par les **rivalités entre l'Iran et l'Arabie Saoudite,** augmentent le risque de tensions. Or, celles-ci, outre qu'elles alimentent des mouvements massifs de migrants et de réfugiés, ne semblent pas devoir trouver de solutions à court ou moyen terme et devraient peser sur le contexte régional des 15 prochaines années.

L'accroissement des flux de réfugiés est l'une des conséquences majeures de ces conflits et représente, par son caractère massif, une autre source de déstabilisation. Fuyant la pauvreté ou la guerre, plusieurs millions d'individus ont ainsi été déplacés en raison des crises récentes (Syrie, Irak, Libye, Nigéria, RCA, RDC). Cet afflux concerne en premier lieu les Etats voisins des foyers de crise, marqués par une grande fragilité économique, et fait peser sur eux une pression importante

alors même que leur stabilité politique est déjà menacée. Mais ce vaste mouvement migratoire touche aussi tout particulièrement l'Europe – le nombre de migrants traversant chaque année la Méditerranée a ainsi triplé depuis 2011 – où certains pays y voient à la fois des risques sécuritaire et économique inacceptables dans la conjoncture actuelle.

Car l'économie mondiale connaît de grandes incertitudes et une nouvelle crise catalyserait les tensions nationales comme internationales.

La reprise de l'activité économique mondiale, soutenue par un ensemble de politiques publiques interventionnistes (Etats-Unis, zone euro), reste aléatoire tant les facteurs d'incertitude – politique de la nouvelle administration américaine, ampleur des effets du *Brexit*, orientations de la politique budgétaire et résultats des élections à venir en Europe – sont nombreux.

Une nouvelle crise économique mondiale aurait des conséquences graves qui pourraient affecter la stabilité internationale. Elle pourrait avoir plusieurs origines : résurgence de la crise de la dette européenne (Italie, Grèce…), éclatement de la zone euro pour des raisons politiques, éclatement d'une bulle spéculative (exemple de l'immobilier), ralentissement brutal du commerce mondial en raison de la mise en place de mesures protectionnistes, chute des cours des matières premières (qui pourrait provoquer l'arrêt de la croissance des pays les plus dépendants de cette rente, dont l'Afrique).

Dans les économies émergentes, habituées depuis plus d'une décennie à une croissance très dynamique mais irrégulière, le ralentissement prolongé de l'économie mondiale pourrait entraîner la contestation croissante des pouvoirs en place et une escalade non maîtrisée des tensions. Un nouveau ralentissement en **Chine** serait préjudiciable à l'ensemble de l'économie mondiale. **Les réformes structurelles profondes des autorités chinoises** visent en particulier à soutenir la demande intérieure et à réduire la vulnérabilité de l'économie chinoise aux variations des prix des matières premières.

Une détérioration de la conjoncture internationale aurait par ailleurs des conséquences préjudiciables en Europe, où une majeure partie des Etats membres voit sa capacité d'action contrainte par des impératifs d'assainissement budgétaire. Elle conduirait mécaniquement à un effet de ciseau (baisse de l'activité et donc baisse des ressources, déclenchement des stabilisateurs automatiques et accroissement de la dépense sociale). Une réactivation de la crise des dettes souveraines, sous l'effet d'une hausse marquée des taux d'intérêt auxquels les Etats empruntent pour racheter celles-ci, pourrait à son tour entraîner une dislocation de la monnaie unique.

Dans ce contexte économique incertain, les risques de déstabilisation politique n'épargnent plus les Etats les plus développés.

Les Etats du continent européen et de son environnement proche sont en effet eux aussi exposés à des enjeux d'ordre politique qui peuvent modifier en profondeur les équilibres actuels. Les fragilités intrinsèques de la Russie – faiblesse de la démographie, ralentissement économique, contestations potentielles du pouvoir – sont de nature à entraîner une remise en cause du système politique actuel préservé

par l'autoritarisme. La montée des populismes en Europe ne permet plus d'écarter l'hypothèse de l'élection du leader d'un parti nationaliste et xénophobe à la tête d'une démocratie européenne. Cette victoire pourrait entraîner de fortes protestations à l'intérieur des Etats-membres et ferait peser une grave menace sur le périmètre, le cadre institutionnel et les principes fondateurs de l'Union européenne.

Surprise stratégique par excellence, **le vote en faveur du *Brexit*,** lors du referendum du 23 juin 2016, a provoqué la crise la plus grave que la construction européenne a connue depuis ses débuts. Les négociations de sortie, qui doivent durer *a minima* deux ans à partir du déclenchement de l'article 50 du traité sur l'Union européenne, placeront l'Union dans une situation inédite et mettront son unité à l'épreuve. A l'issue, l'Europe peut en sortir renforcée si la solidarité de ses membres se confirme sous l'effet de politiques ambitieuses de relance du projet européen ; *a contrario*, le *Brexit* risque de constituer un précédent dangereux pour certains Etats.

Sur le plan stratégique, la sortie du Royaume-Uni prive l'Union européenne d'une puissance nucléaire, membre permanent du conseil de sécurité des Nations unies, investie à titre national dans la prévention des conflits et capable de se projeter au-delà de sa périphérie immédiate. Elle peut également venir renforcer la frilosité d'Etats membres désireux de voir l'Europe limiter ses interventions extérieures à celles de « basse intensité », voire ne remplir que des missions purement civiles. La stature politique, stratégique et militaire de l'Union s'en trouve d'autant affectée.

Or le spectre d'un affrontement Est-Ouest a fait son retour sur le continent européen avec la crise de Crimée en 2014. Par la remise en cause des principes internationaux de souveraineté des Etats et d'inviolabilité des frontières qu'elle suppose et par l'implication directe ou indirecte de la Russie dans le conflit (soutien à peine masqué aux séparatistes du Donbass, politique d'intimidation, déploiement de moyens potentiellement nucléaires en Crimée et à Kaliningrad), cette annexion a provoqué un très fort regain de tension entre l'Est et l'Ouest fait revenir à nos portes de vieux relents de Guerre froide que l'on croyait révolus.

Ces risques politiques européens sont d'autant plus préoccupants que l'élection de Donald TRUMP à la présidence des Etats-Unis suscite de fortes interrogations sur la politique qu'il va mettre en œuvre. Le candidat avait alterné une rhétorique militariste visant à restaurer la place des Etats-Unis dans le monde et un discours isolationniste, répondant aux attentes d'un électorat méfiant du reste de la planète. Ses prises de position marquent en tout état de cause un tournant dans les objectifs que se fixent les Etats-Unis, traditionnellement porteurs de valeurs universalistes, sur le plan international. Elles posent également la question des garanties de sécurité que la puissance américaine est prête à offrir à ses Alliés historiques, que ce soit en Asie ou en Europe.

De ces évolutions émerge un ordre mondial apolaire caractérisé par la fin de l'hyperpuissance américaine, un recul relatif de la supériorité économique et militaire des nations occidentales, la réaffirmation de la nation russe et une ascension inexorable de la Chine. Cette

nouvelle donne **voit s'affirmer de nouvelles stratégies de puissance et met le multilatéralisme et l'Europe à l'épreuve.**

Les Etats-Unis conservent tous les moyens de tenir une place majeure sur la scène internationale par le niveau renforcé de leurs dépenses militaires, la puissance intacte de leur l'armée, leur potentiel d'innovation technologique et le statut international privilégié de leur monnaie. Toutefois, ils ne semblent plus désireux de jouer le rôle hégémonique qu'ils ont traditionnellement incarné dans la diffusion des idéaux démocratiques. Amorcée sous l'administration OBAMA, soucieuse de tourner la page d'une décennie d'opérations extérieures coûteuses et aux effets contestables, cette tendance prend désormais une nouvelle ampleur. Le président TRUMP entend en effet recentrer fortement la stratégie de son pays autour des intérêts américains (« *America First* »).

Ce désengagement est surtout préoccupant pour la sécurité des alliés européens bénéficiant de la protection américaine. Il favorisera probablement une montée en puissance des dépenses militaires des Etats européens et la mise en place progressive d'une défense commune, mais ces évolutions prendront nécessairement du temps.

Or **la Russie remet aujourd'hui ouvertement en cause l'ordre mondial** hérité de la fin de la Guerre froide. Face à la volonté de réguler les relations internationales par le droit, elle tente de réhabiliter une approche réaliste des relations internationales, fondée sur des rapports de force. De manière opportuniste, elle affirme son influence dans ses zones d'intérêt traditionnel (« étranger proche ») ou celles qui servent sa stature de puissance planétaire (Syrie, Libye).

La modernisation de ses armées, le renforcement de son autonomie dans la conception et la fabrication de ses programmes capacitaires et l'investissement dans des nouveaux domaines de guerre (hybrides, cybernétique, désinformation) constituent les vecteurs privilégiés de la réaffirmation de sa puissance. Sa contestation du modèle libéral (politique, économique) empêche cependant la mise en place de réformes qui lui permettraient de développer et de diversifier son économie, encore très dépendante des exportations de matières premières et de produits de l'industrie lourde.

La Chine, quant à elle, s'affirme non seulement comme une puissance soucieuse de son « pré carré » et de ses approvisionnements – les tensions en mer de Chine en témoignent – **mais aussi, et de plus en plus, comme un acteur global,** susceptible d'exercer un *leadership* parmi les pays émergents et de promouvoir un multilatéralisme alternatif, comme l'illustrent l'Organisation de coopération de Shanghai (mise en place avec la Russie) ou le projet de « nouvelle route de la soie ».

Sur le plan militaire, Pékin poursuit sa montée en puissance et se dote de capacités qui lui permettent d'être présent sur tout le spectre : à terre, en mer, mais aussi dans les airs, *via* le développement d'avions furtifs et de systèmes de défense antimissile balistique. C'est enfin dans l'espace, où la Chine dispose de programmes couvrant l'ensemble de l'activité spatiale (communication, navigation, reconnaissance militaire) que les ambitions chinoises se renforcent.

Sur le plan économique, une opposition à fronts renversés se dessine, entre des Etats-Unis tentés par un virage protectionniste

et une Chine prête à se poser en défenseur de la mondialisation et du libre-échange.

A l'appui de ces stratégies de puissance, de nouveaux modes opératoires sont mis en œuvre et de nouveaux espaces stratégiques de confrontation apparaissent.

L'évolution et la diffusion rapide des techniques, le recours à des outils nouveaux d'endoctrinement, de déstabilisation et de provocation ainsi que la multiplication des terrains possibles d'affrontement transforment l'art de la guerre. A la stratégie et la tactique classiques succèdent des modes d'action asymétrique incarnés aujourd'hui par le terrorisme et qui risquent de perdurer même après la défaite de l'Etat islamique en Syrie et en Irak. La frontière entre la guerre et la paix devient ainsi de plus en plus poreuse.

Cette compétitivité accrue entre des acteurs stratégiques toujours plus nombreux se traduit par **une remise en cause des normes de régulation d'accès aux espaces d'intérêts communs ou *Global Commons* (mer, cyberespace, espace),** considérés comme symboles de l'hégémonie occidentale d'après-guerre, dont la maîtrise devient un enjeu majeur et l'appropriation la source de rivalités nouvelles.

Les espaces maritimes font en effet l'objet d'une compétition accrue et sont à l'origine de nombreuses tensions. Pour garantir leur accès à certaines ressources et accroître leur contrôle sur des lieux et des voies stratégiques, des Etats multiplient les revendications sur leurs frontières maritimes, par une interprétation exorbitante du droit international de la mer. De nombreuses menaces criminelles (trafics en tous genres, piraterie, brigandage) se développent par ailleurs dans les espaces maritimes, profitant de l'insécurité générale et alimentant celle-ci. Les câbles sous-marins assurant les communications numériques deviennent par exemple de potentielles cibles dans le jeu des puissances.

Le cyberespace, qu'une vision idéale avait initialement érigé en havre de liberté et d'échanges sans entraves, **est d'ores et déjà traversé par de multiples formes de tensions et de risques,** qu'il s'agisse de la cybercriminalité, des pratiques de désinformation et de manipulation de l'opinion, ou des attaques informatiques perpétrées par des Etats comme par d'autres types d'acteurs. Les actions malveillantes, parfois à forte visibilité, ont par exemple systématiquement accompagné les crises que notre pays a traversées, comme celle des attentats de janvier 2015, et elles ponctuent désormais la vie démocratique. Pour éviter que le cyberespace ne soit un nouveau *Far West*, l'avenir proche verra les pouvoirs publics et les sociétés civiles affronter un triple défi : acquérir une culture de la cybersécurité et remédier le plus efficacement possible aux vulnérabilités ; se doter, dans le cas des Etats, de capacités offensives et défensives ; poser, enfin, les fondements d'une régulation du cyberespace au niveau international.

Alors que la **pérennité d'un accès sûr et pacifique à l'espace extra-atmosphérique s'impose** comme condition indispensable à l'indépendance stratégique nationale, l'augmentation de l'insécurité accompagne au contraire la démocratisation de son usage. La multiplication des acteurs qui y évoluent et la transformation des technologies utilisées vont de pair avec une sorte de militarisation de l'espace où de nouvelles menaces apparaissent (armes

antisatellites, en particulier pour les satellites en orbite basse).

A la recrudescence de ces tensions et l'affirmation de politiques agressives de puissance, l**a communauté internationale peine à opposer la régulation des enceintes multilatérales traditionnelles.**

La prolifération met ainsi à l'épreuve les régimes de contrôle. Le pouvoir syrien a prouvé, par l'emploi d'armes chimiques contre ses opposants, qu'il était prêt à violer le droit international et aller contre tous les tabous concernant les armes de destruction massive. L'impunité dont il a bénéficié jusqu'à présent pourrait encourager d'autres Etats à entrer dans une logique de contournement des régimes de contrôle des armements et de désarmement, et altérer le traitement des crises à venir. Dans le même temps, **la poursuite des provocations nucléaires du régime nord-coréen** impose une réévaluation de cette menace et une réflexion sur la gestion d'un Etat proliférateur nucléarisé.

De manière générale, il convient de souligner la complexité des méthodes déployées par les acteurs proliférants pour contourner les mesures mises en place par la communauté internationale contre eux (sanctions, entraves des flux physiques ou financiers, contrôle à l'export). Les réseaux proliférants se réorganisent en permanence, masquent les caractéristiques techniques des biens interdits et dissimulent l'identité des destinataires finaux.

Enfin, même si les arsenaux nucléaires de la plupart des Etats dotés ont été fortement réduits après la prorogation indéfinie du Traité de non-prolifération (TNP), la dissuasion nucléaire fait actuellement l'objet de programmes de modernisation, portant essentiellement sur la diversification des vecteurs et leur amélioration, que ce soit en termes de portée, de capacité de pénétration des défenses ou de précision (Chine, Inde, Pakistan, Russie). Certains programmes sont, le cas échéant, menés en parallèle de la conduite d'un programme spatial. De leur côté, une partie des Etats non dotés, galvanisés par certaines ONG, prônent la mise en place d'une interdiction immédiate des armes nucléaires pour des raisons humanitaires. Les initiateurs de ce projet devraient être mieux avisés que ce faisant, ils risquent ainsi une rupture du régime global de prolifération, beaucoup plus grave et immédiate dans ses effets et sans doute contraire à leurs intentions initiales.

L'impunité avec laquelle la Syrie a pu utiliser des armes chimiques contre sa population ou la Russie violer le droit international des frontières en Crimée, illustre l'affaiblissement du système international de sécurité. Il envoie un signal d'irrésolution propice à l'émergence de nouvelles agressions.

L'ONU est à la fois une enceinte de négociation et un cadre normatif qui vise à maintenir un consensus minimum sur les conditions du recours à la force et les réponses à apporter aux atteintes à la paix. Dans un monde de plus en plus menaçant, une telle architecture ne peut servir de force de rappel que si les principales puissances restent engagées en sa faveur. A défaut, et si le régime international de sécurité résultait de la simple addition de politiques nationales de sécurité, le risque d'instabilité générale serait dominant, par la difficulté à désigner des menaces communes et à mettre en place à l'échelle mondiale des réponses coopératives adaptées.

Mais il est peu probable que l'évolution du système de sécurité collective d'ici 2030 permette de répondre efficacement aux tensions mondiales. La puissance des Etats dans leurs sphères d'influence semble plus probable, les Etats-Unis et la Chine étant seuls en mesure de l'exercer à l'échelle mondiale.

Dans cet environnement stratégique en profonde mutation, l'Europe est à l'épreuve. Le projet européen est en effet menacé à l'intérieur comme à l'extérieur des frontières de l'Union. Ebranlée par le retrait britannique, la volonté partagée d'édifier un espace de paix, de prospérité et de libertés, qui fondait la double dynamique d'intégration et d'élargissement de l'Union et assurait son attractivité, est affaiblie. L'Union est écartelée entre un *statu quo* qui ne satisfait personne, une intégration plus poussée que refusent de nombreux Etats et le risque de dislocation, dans l'éventualité où le *Brexit* créerait un précédent contagieux.

A l'extérieur de ses frontières, l'Union européenne est en outre menacée par la survenance de crises nombreuses et simultanées. La solidarité européenne, valeur fondatrice du projet européen, doit ainsi faire face à de multiples défis majeurs.

Le défi est donc d'abord politique et il revient aux pays fondateurs, dont la France et l'Allemagne, de trouver les moyens de relancer le projet européen.

Il est ensuite économique et financier, alors même que l'espace européen et la zone euro ne sont toujours pas parvenus à retrouver le niveau de production intérieure brute qui était le leur avant la crise de 2008. L'Europe n'est par ailleurs pas à l'abri d'une nouvelle attaque des marchés financiers sur la dette de certains des Etats membres. Et les perspectives économiques sont obérées par le défi démographique qu'entraîne le vieillissement de la population européenne, sous le double effet d'une réduction de la natalité et d'un allongement de l'espérance de vie.

Cet « hiver démographique » est à opposer à la « contre-transition démographique » observée en Afrique du Nord et au Moyen-Orient ainsi qu'à la croissance démographique spectaculaire et inédite de l'Afrique subsaharienne. Alimentés par les effets déjà dévastateurs du réchauffement climatique dans cette partie du monde, les effets de déstabilisation régionale de ces croissances risquent de se traduire par des flux migratoires potentiellement massifs à destination de l'Europe. S'il se pose dès lors avec une acuité toujours plus forte la question du développement de l'Afrique subsaharienne, et tout particulièrement sahélienne, l'afflux de migrants et de réfugiés attise d'ores et déjà les dissensions entre Etats européens.

La question de l'accès aux ressources constitue également un des grands défis que devra relever l'Union au cours des prochaines années. Il s'agit de réduire la dépendance de l'Europe, à l'égard notamment de la Russie et de la Chine, en ce qui concerne les matières premières énergétiques et les matériaux critiques (terres rares), dans une logique de sécurisation des productions, des approvisionnements et des voies d'acheminement.

Enfin, le défi est sécuritaire. L'Union est confrontée aux répercussions des crises qui affectent son voisinage proche. Sur son flanc Est, l'Europe fait face, impuissante, à une intensification et à un durcissement des manifestations de réaffirmation de la

puissance russe depuis le déclenchement de la crise ukrainienne, tandis que les signes d'une dégradation de la situation dans les Balkans occidentaux se multiplient. Au Sud, la concomitance des crises ouvertes ou larvées représente également un enjeu par son effet de projection de la menace, notamment terroriste, jusque sur le territoire européen. La fin prévisible du « Califat » n'entraînera pas la disparition du péril jihadiste mais sa dispersion, à travers la constitution de nouveaux sanctuaires et la possible persistance d'une menace endogène, alimentée par le retour des « revenants » en provenance des zones de combat.

Sur le plan social, la persistance d'un climat politique et économique dégradé en Europe (maintien du chômage de masse, baisse du niveau de vie, difficulté d'intégration des populations immigrées) **pourrait conduire à des crises** d'importance remettant en cause la cohésion nationale, y compris en France. Elles auraient *de facto* des conséquences sécuritaires fortes.

Ces défis se profilent au moment même où les cadres institutionnels qui assuraient depuis des décennies la stabilité du continent européen se trouvent fragilisés.

L'Union européenne, en dépit de la volonté de certains de ses membres, peine toujours à présenter un projet robuste de politique commune de défense. Le ralentissement économique a provoqué une réduction des budgets de défense qui ne dépassent guère 1 % du produit intérieur brut de la plupart des Etats. Par ailleurs, en dépit des appels répétés, au sein de l'Union ou à l'extérieur, à une prise en charge croissante par les Européens de leur sécurité, certains Etats membres manquent encore d'appétence pour un engagement militaire en dehors de leurs frontières nationales et pour accroître leurs dépenses militaires. L'accroissement de la mutualisation capacitaire, qui figure parmi les objectifs des Etats membres dans un contexte où leur marge de manœuvre reste limitée par les contraintes budgétaires, tarde à se développer.

De son côté, **l'Alliance atlantique, confrontée aux critiques de Washington quant aux différences de contributions financières des Etats membres, pourrait aussi être victime d'une forme de désintérêt stratégique** de la part des Etats-Unis, polarisés par les enjeux de la zone Asie-Pacifique. L'OTAN pourrait connaître également **de profondes divisions internes,** notamment s'agissant des finalités de l'Alliance, mais aussi du respect de ses valeurs fondamentales (tensions avec la Turquie). L'OTAN ne peut assurer sa pérennité qu'en se transformant ou en s'adaptant. Les pays européens sont ainsi placés au pied du mur et incités à augmenter leurs dépenses militaires par l'allié américain sous la protection duquel ils s'étaient, pour la plupart, placés.

Le relatif désengagement de ses Alliés historiques (Etats-Unis, Royaume-Uni) pourrait renforcer **l'isolement stratégique de la France,** qui serait davantage isolée à l'horizon 2030 qu'elle ne l'est aujourd'hui. Un rapprochement de l'Allemagne, principal partenaire politique et économique, pourrait avoir un sens à condition de voir les deux pays rapprocher leurs visions des politiques de sécurité et défense.

Dans cet environnement géopolitique instable, de grandes tendances se profilent et **la technologie apparaît à la fois enjeu,**

arbitre et perturbateur des équilibres stratégiques.

A l'horizon 2030, des évolutions ou des ruptures technologiques seront apparues, dont certaines pourraient alimenter l'instabilité de l'environnement géostratégique. Les grandes puissances vont poursuivre le développement de capacités dans le cadre éternel de la lutte entre l'épée et la cuirasse. Les technologies anti-missiles, anti-aériennes, voire anti-satellites vont aller de pair avec le développement de moyens plus intrusifs, qu'ils aient une forme physique comme les missiles hypervéloces ou virtuels, notamment dans le domaine cybernétique ou informationnel.

Les progrès techniques remettent par ailleurs en cause le fait que seuls les Etats peuvent disposer de certains instruments de puissance. La diffusion rapide de nombreuses technologies, souvent issues de marchés civils comme l'impression additive ou la biologie de synthèse, permet désormais à des individus isolés ou des groupes de développer des capacités potentiellement nuisibles dans de nombreux domaines jusqu'ici réservés au pouvoir régalien. En facilitant l'accès de tous à des moyens jusque-là étroitement contrôlés par l'Etat ou la communauté internationale (dans les domaines nucléaire, bactériologique, chimique ou des armements), **la technologie multiplie ainsi les risques d'usage et a pour corollaire** une individualisation de la menace. Elle offre aussi de nouveaux instruments et de nouvelles possibilités de trafics aux **réseaux de criminalité organisée,** dont l'activité se joue des réglementations nationales et dont l'influence dans certaines régions risque de mettre à mal l'autorité des Etats les plus fragiles. Parfois difficiles à cerner, ces filières ne pourront être combattues efficacement que par une mobilisation internationale étroite.

* *
*

A partir de ce tableau de notre environnement rapidement brossé, le SGDSN a choisi de traiter sous l'angle des défis technologiques, de possibles évolutions ou ruptures stratégiques à l'horizon 2030.

Les études menées distinguent les grandes tendances qui se font jour avec une dynamique de modernisation des arsenaux nucléaires, le développement des défenses anti-missiles, l'émergence de nouveaux acteurs dans l'espace et le cyberespace avec une possible dérégulation et enfin le renforcement des besoins actuels pour le contrôle de la frontière ou la prise en compte d'acteurs non-étatiques utilisant des moyens NRBC.

Ces études anticipent également les éventuelles ruptures stratégiques induites par des innovations ou des progrès technologiques majeurs. Elles portent sur les instruments de puissance classique intégrant le développement de nouvelles capacités comme les armes hypervéloces ou la militarisation de l'espace ; sur les bouleversements de la conflictualité avec la robotisation du champ de bataille, le développement des neurosciences ou de l'informatique quantique. Elles abordent les sujets liés à l'individualisation de la menace avec, par exemple, la diffusion de la biologie de synthèse et le développement de l'impression 3D.

Les choix technologiques ne sont pas nécessairement les causes premières ni principales des bouleversements stratégiques du monde. Mais leur prise en

compte, en temps et en lieu, déterminera largement la capacité des Etats, et de la France en particulier, à assurer la pérennité de leur souveraineté et de leur défense dans un environnement transformé. La France, au cours des 15 dernières années, a su anticiper les évolutions et adapter son outil de défense en conséquence. C'est pour qu'elle fasse de même dans les 15 années à venir qu'il convient de prendre en compte ces « chocs futurs ».

Partie 1

Des tendances qui se consolident

1

La défense antimissile balistique en 2030 : un système militaire mature au cœur des équilibres stratégiques

L'essentiel

A l'horizon 2030, les avancées technologiques sur les missiles amèneront les Etats à poursuivre le développement des systèmes de DAMB déjà lancés afin d'accroître leurs performances. La combinaison de la maturité des technologies et de la multiplicité des programmes permettent d'imaginer une défense antimissile intégrée aux équilibres stratégiques. Pour autant, elle restera un complément et non un substitut à la dissuasion.
Pour la France, si la dissuasion constituera toujours son ultime garantie de sécurité à l'horizon considéré, cela n'exclut pas sa participation à la DAMB de l'OTAN, ni un investissement national dans certaines briques technologiques. Sur la base des compétences industrielles qu'elle possède déjà, la France renforcera ses capacités pour une défense de théâtre. Son intérêt industriel est en effet de favoriser le développement de coopérations européennes qui pourraient amener à la constitution d'un acteur unique, sur le modèle mis en place pour les missiles.

La défense antimissile balistique (DAMB) est entendue comme l'ensemble des mesures et moyens nécessaires pour protéger des forces, des populations ou des territoires contre les menaces liées aux missiles balistiques.

Un système de défense antimissile repose sur quatre piliers :

- un dispositif d'alerte avancée ayant pour missions principales la caractérisation de la menace adverse (dont l'acquisition d'informations précises sur les vecteurs), la détection des départs de missiles, l'identification de l'agresseur et l'alerte aux populations. Ce système repose notamment sur l'utilisation de satellites et de radars très longue portée employés de manière complémentaire ;
- un système de commandement et de contrôle (système dit C2) permettant de gérer l'ensemble des informations liées à la bataille balistique (détection et trajectoire des missiles balistiques assaillants, gestion des intercepteurs et politique de tir associée, résultats des interceptions) ;
- des senseurs, essentiellement de type radar, capables de déterminer précisément la trajectoire des missiles assaillants et de discriminer les ogives parmi les leurres aux fins d'engagement ;
- des missiles intercepteurs des missiles assaillants (généralement par impact direct ou par détonation de proximité).

Les moyens à mettre en œuvre pour assurer la mission de DAMB dépendent tout particulièrement des paramètres techniques de la menace considérée (portée et vitesse à la rentrée dans l'atmosphère des missiles assaillants).

On peut ainsi distinguer deux types de missions :

- **la défense de théâtre (TBMD)**[1], qui concerne des missiles balistiques de quelques centaines de kilomètres à 1 500 km de portée environ. Elle repose le plus souvent sur des systèmes de DAMB, dits de basse couche (interception dans l'atmosphère). L'apport actuel de la défense antimissile de théâtre réside avant tout dans la garantie d'accès aux théâtres d'opérations dans un contexte de menace balistique ;
- **la défense de territoire (BMD)**[2], qui concerne plutôt les missiles de portée intermédiaire et intercontinentaux (plus difficiles à intercepter compte tenu de leur vitesse plus importante à la rentrée dans l'atmosphère). Elle repose sur des systèmes intercepteurs de haute couche (interception dans les hautes couches de l'atmosphère) ou exoatmosphériques (interception au-delà de l'atmosphère) avec des zones à défendre de taille beaucoup plus importante.

Ainsi, à la lumière des éléments qui composent un système de DAMB, il apparaît que celui-ci, pour être opérationnel, repose à la fois sur la maîtrise d'éléments d'ordres :

- politique (pouvoir proposer au politique les paramètres de décision dans des délais extrêmement réduits) ;
- technique (disposer d'un ensemble de technologies suffisamment avancées pour être en mesure de détecter, suivre et intercepter un missile assaillant) ;
- opérationnels et humain (être capable d'analyser les informations recueillies et de mettre en œuvre une chaîne opérationnelle efficace).

1 - *Theater ballistic missile defense.*

2 - *Ballistic missile defense.*

1 - Etat des lieux en 2017

1.1 - Menace balistique en 2017

Si des programmes balistiques préoccupants il y a encore quelques années ont aujourd'hui été démantelés (Irak, Libye) ou largement réduits (Syrie), la prolifération balistique conserve une grande acuité. Certains pays, parmi lesquels l'Inde, la Corée du Nord, l'Iran et le Pakistan, parviennent désormais à développer des engins d'une portée de plusieurs milliers de kilomètres qui, pour partie, peuvent ou pourront atteindre à brève échéance l'Europe et même la France. Plusieurs de ces pays travaillent également sur des lanceurs spatiaux qui, par leur dualité, peuvent contribuer au développement de missiles balistiques à longue portée et entretiennent, parfois volontairement, la confusion entre les deux domaines.

L'Iran conduit ainsi, depuis la fin des années quatre-vingt, un programme de missiles balistiques. Débuté avec une assistance étrangère (Russie, Chine, Corée du Nord), puis mené sur un mode de plus en plus autonome, ce programme est particulièrement dynamique et ambitieux. Il se distingue par sa diversité, avec des missiles balistiques opérationnels à propulsion liquide et solide, de portées comprises entre 250 et 2 000 kilomètres, et des projets de missiles intercontinentaux. L'Iran a aussi procédé à des tests sur des technologies de têtes à capacité manœuvrante.

Les programmes balistiques nord-coréen et iranien, dont la montée en puissance s'accompagne chaque année de campagnes de tirs de missiles balistiques de plusieurs catégories, sont les plus préoccupants. Leurs développements peuvent de surcroît donner lieu, en particulier dans le cas nord-coréen, à une prolifération secondaire par l'exportation de systèmes balistiques ou de leurs composants à des pays tiers.

Des puissances majeures, comme la Chine et la Russie, poursuivent par ailleurs des programmes dynamiques de modernisation de leurs arsenaux de missiles tactiques, de portée intermédiaire ou intercontinentaux. Ces deux pays sont également exportateurs de technologies et de missiles, même si cela est plus limité dans le cas de la Russie qui est membre du Régime de contrôle de la technologie des missiles (MTCR).

Dans un tel contexte, un peu partout dans le monde, de nombreux pays ou organisations se sont dotés de systèmes de DAMB plus ou moins performants en se fournissant auprès des Etats-Unis, de la Russie ou de la Chine, ou en développant eux-mêmes leurs propres programmes, à l'instar de l'Inde ou d'Israël.

1.2 – Etat des lieux des programmes de défense antimissile balistique en 2017

a) Capacités américaines

La défense antimissile américaine actuelle est issue du *National Missile Defense Act* de 1999 qui a entraîné la sortie en 2002 des Etats-Unis du traité ABM[3], conclu trente ans plus tôt avec la Russie avec pour objectif d'encadrer strictement le développement des DAMB. Les Etats-Unis justifient le déploiement d'une DAMB de territoire par la menace balistique croissante représentée par les Etats proliférants (Corée du Nord, Iran). Washington a néanmoins progressivement revu à la baisse son niveau d'ambition, notamment en raison de l'importance de l'effort financier qu'il faut lui consacrer. L'envergure future du programme est d'ailleurs soumise à des arbitrages budgétaires qui restent à prendre par la nouvelle administration américaine.

La DAMB américaine comprend plusieurs systèmes, qui remplissent à la fois une mission de défense des forces en opération et une mission de défense de territoire :

- un système de commandement et de contrôle (C2), associé à un réseau complexe de moyens d'alerte et de surveillance disséminés dans le monde entier. Les moyens d'alerte et de détection reposent à la fois sur des satellites et des radars longue portée ;
- des systèmes d'interception exo-atmosphériques, fondés sur des intercepteurs longue portée basés sur le sol américain (GBI)[4] et sur le système *AEGIS* embarqué à bord de frégates ;
- des intercepteurs haut endo-atmosphériques mobiles (*THAAD*[5]) et d'autres intercepteurs de courte et moyenne portée (*PATRIOT*) déployables sur des théâtres d'opération ou dans des zones exposées (Guam, Hawaï, Corée du Sud).

Les Etats-Unis considèrent la DAMB comme un élément à part entière de leur « triade » stratégique (aux côtés du nucléaire et du conventionnel). Elle est censée à la fois maximiser l'effet de la dissuasion nucléaire, en élevant le seuil d'efficacité d'une attaque balistique, et assurer une flexibilité de réponse plus importante si la dissuasion venait à échouer.

b) DAMB de l'OTAN

En Europe, l'Alliance atlantique (OTAN) développe depuis les années 2000 un programme de défense antimissile. A l'origine limité à la défense de théâtre, c'est-à-dire destiné à protéger les forces de l'OTAN déployées en opérations, le projet vise depuis 2010 (sommet de Lisbonne) le développement d'une DAMB « des territoires et des populations ».

A l'heure actuelle, les capacités de DAMB de l'OTAN reposent essentiellement sur des moyens américains déployés dans le cadre de « *l'European Phased Adaptative Approach* » (*EPAA*). L'*EPAA* prévoit trois étapes de montée en puissance, qui s'échelonnent de 2011 à 2018, et qui reposent sur la mise à disposition de moyens déjà

3 - *ABM : Anti Ballistic Missile*.

4 - *Ground Based Interceptor*. Les sites de GBI se situent à Fairbanks en Alaska et à Vandenberg en Californie ; un troisième site est envisagé sur la côte Est. A terme, une centaine d'intercepteurs devrait être déployée.

5 - *Terminal High Altitude Area Defense*.

opérationnels (dispositifs d'alerte avancée, de veille et de poursuite, ainsi que frégates AEGIS) et la mise en place de nouveaux moyens sur le territoire de l'Alliance (radars, sites terrestres d'intercepteurs, notamment en Turquie, en Roumanie et, à terme, en Pologne).

La France s'est impliquée avec prudence dans le développement de la DAMB de l'OTAN. Elle a posé plusieurs principes directeurs, depuis le sommet de Chicago en 2012, qui visent à préciser le cadre politique dans lequel s'inscrit la DAMB :

- la DAMB ne peut se substituer à la dissuasion, elle est complémentaire de cette dernière ;
- les Alliés doivent pouvoir exercer un contrôle politique total sur le système. Ce point essentiel résulte du constat que les Alliés n'exercent aujourd'hui qu'un contrôle formel sur la DAMB de l'OTAN qui repose à ce stade sur des moyens essentiellement américains ;
- la DAMB de l'OTAN est conçue et dimensionnée pour répondre à une menace de pays proliférants. Elle n'est pas dirigée contre la Russie. Les systèmes déployés ne sont pas aptes à intercepter des systèmes balistiques russes sophistiqués et elle n'a pas vocation à porter atteinte aux capacités de dissuasion stratégique russes ;
- l'évolution de la menace, la faisabilité technique et la soutenabilité financière de la DAMB constituent les trois critères clés pour le développement de la capacité ;
- le financement commun est strictement limité au système de commandement et de contrôle (C2) et chaque allié peut apporter sur une base volontaire des contributions en nature complétant le C2 (capteurs, intercepteurs) ;
- un dialogue doit être entretenu avec les Etats tiers, en particulier ceux qui pourraient être affectés par le système de l'OTAN (en cas d'interception au-dessus de leur territoire, par exemple).

Dans la ligne de ces principes, la France a constamment insisté pour que l'OTAN se dote d'un véritable système de commandement et de contrôle (C2) multinational. Toutefois, les progrès sont lents en raison des difficultés inhérentes à la mise en œuvre de programmes d'armement complexes dans un cadre multinational, et du moindre allant des autres Alliés. Pour parvenir à un contrôle politique collectif de la DAMB de l'OTAN, le développement de la capacité ne devra pas être précipité (*a minima* à l'horizon 2025) et devra continuer d'emporter le soutien d'une majorité d'Alliés afin de surmonter certaines difficultés (divergences de perception de la menace, complexité technique du programme, importants coûts de développement de la capacité, etc.).

c) Russie

La Russie a déployé, autour de sa capitale, le dispositif de défense antimissile que le traité ABM l'autorisait à acquérir, et celui-ci est toujours en place. Cette capacité s'est développée autour de moyens de surveillance de l'espace, d'alerte avancée et d'interception, organisée dans un premier temps autour d'intercepteurs à charges nucléaires *GALOSH* (système A-35), et dans les années 1990 (système A-135) des intercepteurs endo-atmosphériques *GAZELLE* et

exo-atmosphériques *GORGON*. Ces derniers sont maintenant retirés du service.

Pour des raisons probablement financières, le dispositif de DAMB russe est inachevé et vieillissant (alerte avancée limitée, moyens d'interception seulement endo-atmosphériques).

La perception par la Russie du maintien d'une menace balistique orientée contre elle l'amène à travailler à la modernisation progressive de ses défenses, autour d'une version non nucléaire (système A-235). La modernisation complète de la DAMB de Moscou, compte tenu des investissements qu'implique toute avancée dans ce domaine, devrait se prolonger au-delà de 2020.

De manière connexe, la Russie renforce son outil de défense anti-aérien de façon incrémentale, fondé sur les systèmes *S300*, *S400* et dans le futur *S500*, intercepteurs sol-air à capacité anti-balistique et contre les missiles de croisière. Ces systèmes viennent compléter la défense de Moscou et protègent également d'autres sites stratégiques russes. Vu des autorités militaires russes, le positionnement des sites de déploiement progressif de ces systèmes à l'Ouest de la Russie est au demeurant en train d'assurer à la Russie une robuste capacité de déni d'accès aux moyens stationnés en Europe.

d) Chine

La Chine possède une capacité antibalistique de théâtre, lui permettant d'intercepter des missiles balistiques de courte portée. Elle ne dispose en revanche pas encore d'un système complet de DAMB opérationnel pouvant intercepter des missiles intercontinentaux. Pékin conduit des programmes technologiques dans ce sens, y compris dans le domaine de l'interception exo-atmosphérique.

e) Israël

Depuis la guerre du Golfe, en 1991, Israël a pris conscience de l'existence d'une menace balistique régionale dirigée contre son territoire et a entrepris de contrer cette menace avec une importante aide américaine. Cette démarche a abouti à l'acquisition d'un ensemble de moyens multicouches contre :

- les roquettes d'artillerie de courte portée, Israël s'est doté en 2010 du système *IRON DOME* (système mobile de très courte portée) ;
- les roquettes d'artillerie à longue portée et les missiles balistiques à courte portée, Israël a développé le système d'interception basse couche *DAVID'S SLING* ;
- les missiles balistiques de portée intermédiaire, Israël dispose du missile *ARROW-2* (interception haut-endoatmosphérique) ;
- les missiles balistiques de portée plus importante (menace iranienne), Israël dispose du missile intercepteur exoatmosphérique *ARROW-3*.

1.3 – Etat des lieux industriel

Seuls les **Etats-Unis** maîtrisent actuellement l'ensemble des technologies de défense antimissile (intercepteurs, capteurs, systèmes de commandement et de contrôle et architectures permettant de fonctionner sur le théâtre des opérations autrement que sur des points de défense ponctuels). Les Etats-Unis restent aussi très en avance sur la question des communications et des transmissions de données.

La **Russie** dispose d'un réel savoir-faire en termes de capteurs et d'intercepteurs, autant au niveau des systèmes de théâtre que des systèmes stratégiques. Elle semble en revanche plus en retard sur les systèmes de C2, notamment sur les architectures distribuées qui, en répartissant les fonctions de détection et d'engagement puis d'interception sur de multiples plates-formes, permettent d'élargir l'empreinte de la défense antimissile et sa résilience.

Les **pays européens** restent très en retard sur l'ensemble de ces questions, même s'ils maîtrisent plusieurs briques capacitaires (capteurs, C2, intercepteurs basse couche). Si l'ambition de disposer à terme d'un C2 OTAN structure une partie de l'effort de défense européen, la difficulté d'aboutir à une approche commune sur le rôle des défenses antimissiles dans les conflits à venir conduit les Etats européens à adopter une approche dispersée. Leurs capacités nationales isolées sont certes interopérables avec les systèmes OTAN, mais sans cohérence d'ensemble.

La **France** dispose de capacités significatives dans le domaine des systèmes basse couche, à partir de la famille de missiles antiaériens *ASTER*, déclinée en versions terrestre (*SAMP/T*) et navale (*PAAMS*), qui ont fait l'objet de coopération avec l'Italie et le Royaume Uni. Le missile *ASTER* dispose d'un véritable potentiel de croissance lui permettant d'évoluer vers l'interception des menaces balistiques jusqu'à 1 500 km de portée (ce qui a été lancé avec la version *ASTER BLOCK 1 NT*). Afin de passer à une véritable capacité antibalistique basse couche cohérente et complète, il lui faudrait compléter ces systèmes par des systèmes d'alerte avancée et des radars de veille/poursuite. Des travaux technologiques et de démonstration ont été conduits dans ces domaines, mais peu valorisés ensuite au sein des forces armées *via* des programmes d'équipement, les priorités budgétaires étant ailleurs. Ces savoir-faire permettent de répondre aux besoins nationaux dans le cadre de la mission de défense de théâtre et de faire de la France un acteur influent et critique sur les questions de DAMB au sein de l'OTAN.

Par comparaison, **l'industrie israélienne** est déjà en mesure de se positionner sur les principaux segments de la DAMB (capteurs, C2 et intercepteurs) en proposant des solutions clef en main sur tout ou partie de la mission. La **Chine**, comme l'**Inde**, restent dépendantes de transferts de technologies et d'importations (Russie et Israël pour l'Inde, Russie pour la Chine) pour développer leur capacité opérationnelle mais devraient progressivement apparaître comme des acteurs importants (y compris dans la composante spatiale), la défense antimissile étant un élément de plus en plus présent dans leur défense.

2 - Situation en 2030

2.1 – La menace balistique en 2030

a) Progrès technologiques sur les vecteurs

A l'horizon 2030, les progrès technologiques sur les missiles balistiques se seront poursuivis et continueront de faire de cette menace un enjeu de premier ordre. Les vecteurs auront progressé en termes de :

- portée, avec un accroissement de celle-ci grâce à des architectures multi-étages ;
- précision ;
- capacités de pénétration, grâce à des corps de rentrée manœuvrants associés à des leurres et l'emport de plusieurs têtes susceptibles de saturer les défenses ;
- facilité d'emploi, grâce à un usage généralisé de propergols solides comme mode de propulsion (facilité de stockage, rapidité de déploiement et de mise en œuvre).

b) L'espace euro-atlantique sous la menace d'une frappe balistique par un Etat proliférant

S'agissant des Etats actuellement qualifiés de proliférants, et plus particulièrement de l'Iran, une partie de leurs arsenaux leur permettra, à l'horizon 2030, d'atteindre l'essentiel de l'Europe, même si leurs stocks de missiles aptes à cette mission resteront probablement limités.

La Corée du Nord qui a procédé et procèdera à de nouveaux tests de missiles à longue portée dans le Nord de l'océan Pacifique, par-dessus le Japon pourrait être parvenue à achever son programme de développement d'un missile intercontinental (ICBM). Ce pays, s'il n'est pas entravé avant, serait dès lors en mesure d'atteindre l'Ouest américain et une partie de l'Europe. L'Iran aura de son côté procédé à un tir démontrant sa capacité à atteindre l'océan Atlantique. Sur le pourtour méditerranéen, plusieurs Etats pourraient en outre disposer de missiles balistiques courte portée susceptibles d'atteindre l'Europe occidentale.

L'impact militaire de ces développements devrait rester contenu, les systèmes anti-missiles dont disposeront les Alliés devant pouvoir prendre en compte efficacement cette nouvelle menace balistique. Ils induiront en revanche une plus grande incertitude politique et une potentielle remise en cause des menaces prises en considération par l'Alliance atlantique.

c) Des stratégies de déni d'accès et d'interdiction de zone (A2/AD) profitent pleinement des progrès technologiques

En Asie, la Chine disposera en 2030 d'un nombre suffisant de missiles balistiques dérivés de l'actuel *DF 21* **pour faire peser une menace significative sur les espaces maritimes** jusqu'à 1 500 / 2 000 km de

ses côtes. Certains de ces vecteurs devraient emporter des planeurs hypersoniques probablement impossibles à intercepter à cet horizon. Dans ces conditions, la stratégie A2/AD déployée par Pékin dans la zone se trouverait substantiellement renforcée[6]. Ceci suppose la poursuite par la Chine d'une activité soutenue. Les avancées récemment observées sur les développements industriels des missiles chinois et l'attention portée par les Américains que les Japonais, aux progrès de Pékin dans ce domaine, sont des indicateurs forts de la réalité de cette prospective.

Le déploiement de tels systèmes imposerait aux Etats-Unis un effort de modernisation des défenses antimissile de ses infrastructures fixes (Guam) et de ses moyens navals situés à portée des missiles chinois. Les autres nations affichant des velléités de déploiement naval dans cette zone devront impérativement disposer de DAMB de théâtre performantes.

2.2 – Les défenses antimissiles en 2030

a) Les Etats-Unis dominent et maîtrisent l'ensemble du spectre de la DAMB

A l'horizon 2030, les Etats-Unis conserveront leur maîtrise sur l'ensemble du spectre des différentes composantes de la défense antimissile. Sauf arbitrage budgétaire contraire peu vraisemblable, ils continueront d'investir dans cette capacité qui leur permet de renforcer leur propre sécurité et de garantir partiellement celle de leurs alliés les plus proches. Cet état de fait constituera aussi un réel atout pour leurs industries de défense (sur leur marché national comme à l'export). Ils devraient continuer à exporter des systèmes vers de nouveaux Etats amis souhaitant acquérir des capacités de DAMB.

b) La DAMB de l'OTAN est opérationnelle

En Europe, face à la croissance des arsenaux balistiques à l'horizon 2030, **la DAMB de l'OTAN devrait poursuivre son développement** (mais avec une cadence de réalisation très incertaine en raison de son coût et sans rationalisation collective de l'effort budgétaire en matière de défense). En plus des capacités déjà déployées sur le flanc Sud, le système pourra s'appuyer sur le nouveau site d'interception terrestre basé en Pologne afin d'assurer la protection du flanc Nord-Est. Ainsi, en s'appuyant sur des moyens déployés en Méditerranée et sur le sol des Alliés, une large partie du territoire de l'Alliance sera couverte par la DAMB.

La « capacité finale opérationnelle », synonyme que le système a atteint son stade de développement optimal, aura été déclarée. Il y aura un système de commandement et

6 - *Cf.* note relative aux armements hypersoniques.

7 - Le processus de validation politique ne passera pas par une autorisation préalable des 29 (impossible à obtenir sur les délais de réaction à une attaque balistique). Il confirmera que la DAMB peut être déclenchée quelle que soit l'angle d'entrée d'un tir balistique. Il pourra discriminer les rares cas où les retombées de débris d'une interception d'un tir vraisemblablement conventionnel sont supérieures à l'impact.

de contrôle (C2) opérationnel et les Alliés auront trouvé un accord sur les règles d'engagement et le processus politique associé. On ne sait cependant dire aujourd'hui si ce C2 reposera sur des capacités développées en commun ou sur des moyens strictement américains[7].

c) *Russie et Chine ont développé et modernisé leurs capacités de DAMB*

La Russie aura poursuivi la modernisation de son système de défense antimissile. Les lacunes qui compromettent en 2017 la capacité de la Russie à faire face à une partie de la menace auront vraisemblablement été comblées à l'horizon 2030. Celles-ci portent essentiellement sur l'échelon spatial du système d'alerte avancée (insuffisant pour assurer une veille permanente), son échelon terrestre (performances de détection dégradées), de même que sur le système d'interception (qui repose uniquement sur des missiles de gamme endo-atmosphérique et qui réduit *de facto* le domaine d'interception).

De surcroît, la Russie, à l'horizon 2030, aura maintenu voire renforcé des capacités balistiques pouvant constituer une menace sur le flanc Est de l'Europe. Ainsi, le déploiement de missiles *ISKANDER* (capables d'emporter des charges conventionnelles ou nucléaires) à Kaliningrad, qui était annoncé comme provisoire (au titre de l'exercice Grom-2016) aura été rendu permanent à l'horizon 2030.

La Chine pourrait de son côté avoir pris la décision de développer et déployer un système de DAMB complet. Jusqu'ici, la Chine a manifesté son intérêt d'acquérir des connaissances en effectuant des recherches et essais dans le domaine antimissile, ainsi que l'acquisition de différentes briques technologiques concernant l'alerte avancée et les intercepteurs. Au regard des progrès accomplis en 2017, et si l'on se fie aux précédents américain et russe à qui il a fallu une quinzaine d'années pour maîtriser la capacité, le système chinois pourrait être opérationnel à l'horizon 2030.

La modernisation des systèmes de défense anti-missile des grandes puissances militaires augmentera leur efficacité d'interception face aux missiles balistiques assaillants. Cette meilleure performance du système d'interception entraînera mécaniquement une érosion plus ou moins forte de la capacité opérationnelle des missiles balistiques assaillants à atteindre leur but même si, dans l'immédiat, cette érosion devrait être compensée par le travail accompli par les grandes puissances sur l'amélioration d'efficacité de pénétration des têtes balistiques. A cet égard, dans le jeu de « l'épée contre la cuirasse », à niveau technologique égal, il faut noter qu'il reste plus simple de concevoir et développer des missiles balistiques plus performants que de se doter de capacités anti-missiles exhaustives couvrant l'ensemble du spectre de la menace.

Les performances accrues des défenses antimissiles auront par ailleurs conduit les potentiels Etats proliférateurs et les Etats nucléaires hors TNP, qui ne disposeront que de petits arsenaux, à s'interroger sur la pertinence d'utiliser l'arme nucléaire dans une situation où son interception serait probable (anéantissant ainsi l'effet recherché). La planification nucléaire pour les petits arsenaux en sera ainsi rendue plus complexe.

d) Un risque de course à l'armement entre l'Inde et le Pakistan

Des effets de rupture sont à attendre, plus particulièrement pour les puissances nucléaires ayant une relation de dissuasion de niveau régional, telles que l'Inde et le Pakistan.

Les vecteurs nucléaires de courte et moyenne portée seront potentiellement plus faciles à intercepter. Dans un tel contexte, une course aux armements pourrait se voir relancée entre les deux Etats, soucieux de conserver la crédibilité de leur outil de dissuasion, avec des répercussions progressives sur le format des arsenaux et sur la posture des autres Etats nucléarisés qui percevront progressivement l'émergence d'une menace (Chine d'abord, mais ensuite Israël – ce pays regardant l'accroissement de l'arsenal pakistanais avec une méfiance croissante – et enfin Russie et P3).

2.3 – Aspects industriels et technologiques

A l'horizon 2030, les technologies actuellement développées devraient avoir permis des avancées importantes en matière de DAMB, sans pour autant qu'elles soient incarnées dans un grand programme emblématique du type « guerre des étoiles » de l'ère REAGAN. Les progrès pourront aussi bien porter sur les matériaux, les composants électroniques, les algorithmes, les interfaces, les capacités de traitement et de transmission de données. Seront ainsi améliorées :

- la détection des missiles et des corps de rentrée ;
- la capacité à discriminer les têtes des leurres ;
- l'optimisation de l'interception dans les différentes phases de vol du missile et des têtes ;
- l'exploitation des technologies non cinétiques (armes laser ou micro-onde).

Au-delà de la simple amélioration des performances, **les efforts porteront par ailleurs sur l'obtention de systèmes DAMB plus fiables et résilients** au travers d'architectures systématiquement distribuées. La mise en réseau d'effecteurs et de capteurs permettra un partage d'informations entre l'ensemble des éléments du réseau et la répartition des fonctions de détection et d'engagement puis d'interception sur de multiples plateformes. L'ensemble du système pourra ainsi tirer parti de potentielles redondances sur les capteurs.

Ces architectures pourraient avoir des effets rapides en termes tactiques, en permettant à la défense aérienne élargie, incluant la DAMB de théâtre, de devenir une composante plus fiable et plus opératoire dans des environnements complexes ou en situation dégradée, ce qui n'est pas encore le cas aujourd'hui.

Enfin, la multiplicité des moyens de frappe balistique et leur utilisation éventuellement coordonnée avec des capacités de frappe dans la profondeur (missile de croisière, frappe aérienne) conduit à une complexification de l'analyse de la menace et des mécanismes de prise de décision. Or, la rapidité des tirs balistiques exclut de procéder à ces opérations autrement que de manière automatisée (un missile balistique tiré du Moyen-Orient atteindrait l'Europe occidentale en moins de vingt minutes). D'ici 2030, cette automatisation sera devenue systématique.

3 - Enjeux pour la France et pour l'Europe

3.1 – Stratégie nationale

A l'horizon 2030, la garantie ultime de sécurité de la France demeurera la dissuasion nucléaire. Cette position de principe n'exclut pas pour autant une participation à la défense antimissile des territoires et des populations de l'Alliance atlantique, conformément à la déclaration du sommet de Chicago de 2012, ni un investissement national dans certaines briques d'un système DAMB, l'investissement concomitant dans la modernisation de la dissuasion nous obligeant toutefois à faire des choix. Ainsi, dans un contexte d'accroissement de la menace balistique, la France pourrait procéder aux arbitrages nécessaires pour investir dans une capacité d'alerte avancée, en capitalisant sur ses acquis technologiques antérieurs, notamment *via* le démonstrateur *Spirale* (*cf. infra*). Un tel système renforcerait la dissuasion nucléaire en permettant l'identification immédiate de l'auteur d'une attaque balistique, constituerait un contre-point aux systèmes américains alimentant la DAMB de l'OTAN et pourrait contribuer à l'alerte aux populations européennes, dans l'esprit de la clause de solidarité du traité de Lisbonne de l'Union européenne.

A l'OTAN, le déploiement opérationnel d'une capacité de DAMB sera, en 2030, devenu une réalité. A côté du sujet traditionnel, porté par la France, du développement en commun du système de commandement et de contrôle (C2) et à présent de ses améliorations à venir, la question délicate sera le renforcement des capacités en Europe du Nord-est et le langage déclaratoire sur la possibilité ou non que cette capacité puisse concerner une menace autre qu'émanant d'un Etat proliférant, en particulier si la Russie persiste dans sa logique d'intimidation vis-à-vis du flanc Est de l'Alliance.

Au-delà de ces considérations sur la protection des territoires et des populations, la priorité nationale, en matière de défense antimissile, devrait demeurer la protection des forces déployées sur les théâtres d'opérations.

3.2 – Déclinaison industrielle

La France dispose d'ores et déjà de briques de compétences industrielles concentrées sur les capacités d'interception de basse couche, ainsi qu'en matière de capacités de détection et d'alerte avancée. Sur cette base, un système national complet de DAMB basse couche et des briques d'un système plus ambitieux pourraient avoir été développés à l'horizon 2030.

En matière d'alerte avancée, le démonstrateur *Spirale* (*AIRBUS DEFENCE AND SPACE*), composé de deux satellites géostation-

naires infrarouge, a démontré la maîtrise de la technologie de détection et d'alerte des tirs de missiles balistiques. Dès lors, aucun obstacle technique ne s'oppose à la mise en orbite à l'horizon considéré d'un ou plusieurs satellites d'alerte avancée produits dans un cadre national ou européen. En matière de radar, les travaux amont réalisés avec l'ONERA sur le programme de radar *TLP* (*Très Longue Portée*) permettent à *THALES* d'être en capacité de développer d'ici 2030 un radar d'alerte avancée et de trajectographie.

La France a également démontré un excellent savoir-faire en matière de radar à antenne active (avec le démonstrateur *M3R – Multimission Modular Radar* – développé par *THALES*). La poursuite des travaux réalisés dans ce domaine permettrait à la France de disposer assez rapidement d'un radar de ce type qui donnerait toute sa cohérence à un système de défense antimissile basse-couche national intégrant le système *ASTER Block 1 NT.* Il pourrait aussi constituer une contribution en nature française à la DAMB de l'OTAN et ouvrir des perspectives à l'exportation.

S'agissant des intercepteurs, le savoir-faire est maîtrisé et démontré pour la basse-couche par *MBDA* avec le programme *ASTER Block 1 NT*, qui permet d'ores et déjà de traiter la menace des missiles balistiques de portée inférieure à 1 500 km. A l'horizon 2030, les performances de ces intercepteurs auront été améliorées. Les compétences acquises dans le domaine de la propulsion balistique et des acquis technologiques dans le domaine de l'interception positionnent, en outre, *AIRBUS DEFENSE AND SPACE* comme fabriquant potentiel de missiles intercepteurs exoatmosphériques.

A l'horizon 2030, il est fort probable que les Etats-Unis, seul Allié à disposer de moyens d'interceptions exoatmosphériques, auront conforté et même accru leur savoir-faire en la matière. Dans ce contexte, la France pourrait faire le choix d'une spécialisation dans les capacités de basse couche, en s'appuyant le cas échéant sur des coopérations européennes (à l'instar de la coopération avec l'Italie et le Royaume-Uni pour le développement de la famille *ASTER*). Cette option, qui pourrait amener à la constitution d'un champion européen autour des capacités françaises, permettrait non seulement de contribuer utilement au développement de la DAMB au sein de l'OTAN, mais aussi de constituer une capacité d'excellence pour l'exportation.

4 - Scenarii alternatifs

4.1 - Une rupture technologique majeure dans le domaine de l'interception balistique

L'aboutissement des travaux américains dans le domaine de l'interception laser (*airborne laser*) constitue une rupture technologique remettant en cause la supériorité des capacités de pénétration des forces balistiques les plus modernes face aux systèmes de défense antimissiles. Si elle ne conduit pas à l'obsolescence de la technologie des missiles balistiques, cette évolution doit être prise en compte par l'acquisition de capacités nucléaires reposant sur d'autres vecteurs (missiles de croisière, missiles hyper véloces).

4.2 - Un accord d'*arms control* portant sur la DAMB

Des discussions entre les Etats-Unis, la Russie et la Chine conduisent à des restrictions sur le déploiement ou les capacités de la défense antimissile afin de maintenir une stabilité stratégique. Si ces discussions ne concernent pas les systèmes couches basses et moyennes, déjà développés et déployés par les Etats-Unis, elles permettent la conclusion d'un accord sur les dispositifs à vocation stratégique.

2

La démocratisation de l'accès à l'espace

L'essentiel

Dans le domaine des satellites, la concurrence est forte et s'accroîtra tout en se diversifiant. Une restructuration ne peut être exclue, compte tenu de l'apparition de nouveaux acteurs et de cette « vulgarisation » de l'accès à l'espace. Une politique industrielle adaptée et des arbitrages internes en France seront nécessaires afin de maintenir un niveau concurrentiel crédible, seul gage de la pérennité de nos compétences.

Depuis peu, plusieurs sociétés privées américaines, parmi lesquelles *SPACE X* et *AMAZON*, ont manifesté l'ambition de développer et d'exploiter de nouveaux systèmes spatiaux sur des bases industrielles et technologiques entièrement nouvelles. L'objectif consiste à rendre accessibles au plus grand nombre, et pour des coûts de développement et d'exploitation modiques, de multiples services tels que les lancements de satellites ou de vaisseaux spatiaux, les télécommunications ou encore l'observation de la Terre à très haute résolution et à très grande capacité de revisite.

Certains industriels, notamment français, ont bien compris les extraordinaires enjeux économiques de cette évolution technologique majeure et tentent de participer à ce nouveau paradigme très prometteur, connu sous l'appellation de *New Space*.

Cette dynamique n'est pas sans engendrer d'importants risques de prolifération et de dissémination liés à l'utilisation de composants et d'équipements largement accessibles sur le marché. Elle a aussi pour conséquence un accroissement très significatif de l'espace circumterrestre qu'il sera nécessaire de contrôler et de limiter, notamment au moyen d'instruments juridiques plus contraignants.

1 - Etat des lieux en 2017

Plusieurs annonces de projets de constellations de micro-satellites de télécommunication ont récemment retenu l'attention. Celle du réseau *OneWeb* comporterait près de 700 satellites ; le nombre de 4 000 satellites est évoqué pour l'initiative de *SPACE X* ou plus encore pour celle de *SAMSUNG*, ces deux dernières démarches restant à l'état de projets aujourd'hui.

Le secteur des télécommunications n'est pas le seul à connaître ces bouleversements. L'observation de la Terre fait l'objet d'importantes transformations, avec le développement des satellites d'observation commerciaux. Ainsi, des sociétés comme *PLANET LABS* ont émergé en mettant en avant des micro-satellites à haute performance (permettant même la prise de vidéos

HD pour le projet *TERRA BELLA* de cartographie de la Terre) ou l'emploi de dizaines de nano-satellites « *Cubesats* » délivrant des images de résolution moyenne ou faible mais avec un taux important de revisite (détails *infra*.)

Si cette dynamique se poursuit (les satellites *OneWeb* ou *Blacksky Global* sont déjà en construction), elle induira un changement d'échelle majeur dans une activité dont la production mondiale annuelle est aujourd'hui tout au plus d'une trentaine de satellites commerciaux de télécommunication et de moins de 100 micro-satellites[1] destinés aux orbites basses.

Enfin, ces évolutions pourraient voir la multiplication des projets de petits, voire de micro-lanceurs terrestres ou aéroportés offrant la possibilité de mise en orbite à bas coûts de petits satellites.

L'ensemble de ces projets de satellites et de lanceurs pourrait transformer durablement le secteur et ses usages, aussi bien dans les domaines civils que dans les domaines militaires. Ces nouvelles capacités pourraient induire d'importantes évolutions, par la banalisation de technologies autrefois étroitement contrôlées et par la vulgarisation des usages liés à l'extension de la clientèle.

1.1 – L'observation de la Terre à bas coût au moyen de micro-satellites

La multiplication récente des projets de micro-satellites à haute résolution et les perspectives d'une industrialisation de leur production à coûts réduits témoignent des progrès constants de la technologie commerciale concernant aussi bien les plateformes que les charges utiles ou les segments-sol.

Il existe aujourd'hui près de vingt entreprises privées qui opèrent ou envisagent d'exploiter des satellites d'observation de la Terre. A côté des acteurs traditionnels comme l'Européen *AIRBUS* ou l'Américain *DIGITALGLOBE*, de nouvelles sociétés sont apparues au cours des quatre dernières années, essentiellement sous la forme de *start-ups* fondées aux Etats-Unis ou au Canada. Elles misent sur l'emploi de très petits satellites disposés en grand nombre en orbite basse et visent la diffusion en masse de véritables flux d'images au plus grand nombre de clients possibles.

Certains projets commerciaux faisant usage de *Cubesats* existent depuis quelques années. Ces projets tirent parti d'un accès facilité à la technologie (COTS[2]), de coûts réduits ainsi que de cycles de production et de mise en œuvre raccourcis. Ils sont en revanche affectés par des performances relativement limitées qui les cantonnent à des applications misant sur le nombre (revisite), plutôt que sur la précision et la résolution.

Des sites proposant des produits liés à la plateforme ou à la charge utile pour produire des *Cubesats* à moindre coût sont aujourd'hui disponibles. Ainsi, *Cubesatshop.com* ou *cubesatkit.com* proposent à la vente l'ensemble des systèmes nécessaires au fonctionnement du satellite, en incluant des

1 - Les micro-satellites, comparables en taille à une machine à laver, ont une masse comprise entre 50 et 150 kg au lancement. Comme les mini-satellites, d'une masse au lancement comprise entre 150 kg et 2 tonnes, ils sont exploités en orbite basse, principalement pour des applications de reconnaissance ou d'observation de la Terre.

2 - *Commercial off the Shelf*.

capteurs stellaires (pour 80 000 dollars quand les viseurs stellaires des grands satellites commerciaux actuels en coûtent plusieurs millions) ou des roues à réaction supposément éprouvées pour le vol spatial.

Plus récemment, les performances de ces *Cubesats* ont été améliorées par le biais de nouvelles sociétés d'observation de la Terre. Ainsi, les sociétés les plus avancées (de type *PLANETLABS*), ont été en mesure de concevoir un *Cubesat* de 5 kilogrammes offrant une résolution de 3 à 5 mètres avec une durée de vie de 3 ans. *PLANETLABS* bénéficie d'un réseau-sol implanté dans différents pays (Etats-Unis, Royaume-Uni, Nouvelle Zélande, Allemagne et Australie) avec des antennes de réception de 5 m en bandes X et L. Chaque satellite se présente sous forme d'un parallélépipède de 10 x 10 x 30 centimètres et ne pèse que 5 kilogrammes, permettant ainsi leur lancement en grand nombre à bord d'un seul lanceur.

Une autre société américaine, *HERA*, nettement plus ambitieuse que *PLANETLABS* en termes de performances, bénéficie pour bâtir ses systèmes de composants sur étagère disponibles à la *NASA*. Elle vise 31 centimètres de résolution avec des satellites de classes 300 kilogrammes et envisage aussi l'utilisation de *Cubesats* agrégés d'une vingtaine de kilogrammes.

Enfin, les sociétés canadiennes *URTHECAST* ou américaines *TERRA BELLA* ou *BLACKSKY GLOBAL* (qui ambitionne de déployer 60 micro-satellites de capacités métriques à l'horizon 2019) pourraient apparaître comme de nouveaux acteurs du domaine.

1.1 – Les constellations de micro-satellites de télécommunication

Une industrialisation plus massive encore pour les « megaconstellations » est prévue dans le domaine des télécommunications. On parle d'une production de 14 satellites par semaine pour *OneWeb*.

Dans le cas de la constellation *OneWeb*[3], qui apparaît aujourd'hui avec *Leosat*[4] comme le projet le plus avancé, des micro-satellites d'environ 150 kilogrammes seront lancés par grappe. On peut ainsi imaginer l'envoi de 70 satellites en un lancement. La plateforme est pointée vers le centre de la Terre avec une précision de plus ou moins 0,5 degré et génère une puissance totale supérieure à 500 watts.

Les exigences de fiabilité sur le système de contrôle d'attitude et d'orbite du satellite sont similaires à celles d'un satellite classique ; ceux qui arrivent en fin de vie seront désorbités vers la Terre pour être détruits en pénétrant dans l'atmosphère terrestre. L'utilisation d'une propulsion électrique de basse puissance (quelques centaines de watts, contre quelques kilowatts pour les satellites géostationnaires) est dès lors nécessaire.

Les satellites étant relativement simples, la faisabilité technique semble garantie. Des inconnues demeurent néanmoins, concernant certaines technologies liées à l'amplification de puissance, les cellules solaires, la propulsion électrique, dite à effet Hall, qui se présente comme l'enjeu industriel principal dans ce type de projet.

3 - 640 satellites en orbite basse fournis par *AIRBUS*.

4 - 100 satellites en orbite basse fournis par *THALES ALENIA SPACE*.

Les terminaux demeurent l'un des éléments essentiels de la conception d'ensemble. Par choix, leur prix est limité, ce qui conduit à une relative simplicité technique. Ainsi, par exemple, le champ de vue des terminaux a été limité à un cône étroit depuis le zénith. La faisabilité de ce type de terminaux repose sur vingt ans de développement et de production dans l'industrie spatiale[5]. La conception du système garantit donc *a priori* un coût terminal faible.

Le choix de l'orbite, à 1 200 kilomètres et en inclinaison quasi-polaire, pour une durée de vie de 5 ans, permet d'envisager des composants issus de l'industrie non spatiale. Les doses de radiations reçues sont en effet largement inférieures à celles existant dans l'environnement des satellites géostationnaires. Les effets dus aux particules de haute énergie (basculement définitif des portes logiques) devront être compensés par le système. En revanche, l'encombrement de ces orbites basses pourrait à terme poser un problème de pollution électromagnétique.

La plateforme est d'une conception assez robuste et le choix de micro-satellites devrait relâcher les contraintes sur les actionneurs mécaniques et donc sur le coût récurrent. Elle doit néanmoins délivrer une puissance importante et c'est l'enjeu principal pour l'objectif de coût annoncé. La recherche d'industriels aptes à livrer des cellules solaires capables de tenir l'environnement radiatif de cette orbite, tout en offrant des flux et des volumes de production, laisse penser qu'une solution à base de cellules silicium monocristallin (génération précédente) pourrait être adaptée.

La charge utile est parmi les plus simples qui puissent être envisagées pour un satellite de télécommunication. Il subsiste cependant certains points techniques à valider sur le plan industriel comme, par exemple, le rendement des amplificateurs de puissance. Sur ce sujet, les industriels américains semblent mieux placés que leurs homologues européens. Le contrôle des satellites ne pose *a priori* aucun problème.

1.3 – Les petits lanceurs

La mise en place du *New Space* semble être l'occasion d'un regain d'intérêt pour les petits lanceurs, dont une vingtaine de projets visant une capacité de mise en orbite basse (LEO[6]) de 500 kg ou moins est en développement dans le monde. Seuls quelques-uns d'entre eux font l'objet d'un financement affiché et crédible. La multiplication de ces projets correspond à un besoin de marché. Mais en multipliant les acteurs et les échanges industriels, elle a pour conséquence de créer les conditions d'une nouvelle prolifération de technologies servant aux missiles balistiques.

5 - Une société comme *THINKOM*, par exemple, serait en capacité de produire ces terminaux. *OneWeb* a déposé un brevet pour ses propres besoins.

6 - *Low earth orbit*.

2 - Situation en 2030

Sous réserve d'avoir maîtrisé certaines avancées techniques, **le *New Space* pourrait avoir en 2030 singulièrement modifié la situation dans l'espace,** ainsi que le paysage de l'industrie de ce secteur et le rapport du grand public avec le domaine spatial.

Dans le domaine des télécommunications, après plusieurs échecs industriels, **au moins deux grandes constellations de satellites devraient avoir été placées en orbite basse à l'horizon 2030.** L'une, composée d'une centaine ou plus de satellites, serait destinée à servir les acteurs étatiques et institutionnels. L'autre, qui pourrait compter plusieurs milliers de satellites, permettrait de distribuer partout à la surface du globe un service internet à haut débit. **Les grands industriels** qui fabriquent des plateformes et des charges utiles (*BOEING*, *AIRBUS* et *TAS*) **seront probablement amenés à changer leurs procédés de fabrication** et à miser sur une standardisation de plus en plus massive des composants. La faible durée de vie des satellites lancés justifiera la mise en place et le maintien de chaînes de fabrication capables de produire plusieurs unités par semaine.

Dans le domaine de l'observation de la Terre, ces mêmes industriels devront affronter la concurrence de plusieurs fabricants de micro-satellites rustiques destinés à intégrer des constellations évoluant en orbite basse. La commercialisation des images issues de ces satellites à bas coût pourrait en effet être devenue rentable du fait du rôle croissant joué en aval par les techniques algorithmiques d'exploitation des données. En d'autres termes, les techniques de développement de la plateforme prendront de moins en moins d'importance dans la chaîne de valeur, tandis que **la maîtrise des techniques algorithmiques de fusion et d'exploitation des données deviendra probablement le véritable « centre de gravité » stratégique de l'activité.** Cette évolution pourrait donner un avantage décisif aux pays qui auront investi le plus massivement dans ce secteur « aval », et notamment aux Etats-Unis, qui auront bénéficié des investissements massifs réalisés par les grandes « *majors* » de l'Internet depuis le début de la décennie 2010.

Cette moindre importance des plateformes pour l'accès à l'information générale ouvrira un accès aux **petites entreprises qui construiront des systèmes polyvalents « *low cost* »,** d'environ 150 kilogrammes, susceptibles de répondre aux exigences du marché (télécommunications en orbite basse ; observation submétrique à très forte revisite). Cette nouvelle activité stimulera le marché des composants à faibles coûts pour l'espace avec l'apparition d'un secteur tiers du spatial « *low cost* ».

Le **développement de quelques petits lanceurs bon marché** (après une « sélection naturelle » des projets les plus sérieux), permettant de placer 400 kilogrammes en orbite basse sous faible préavis, répondra par ailleurs aux besoins des constellations en complément d'autres capacités de lancement plus lourdes.

3 - Enjeux pour la France et pour l'Europe

3.1 - Quelles conséquences possibles ?

Pour la France, les évolutions évoquées dans le scénario de référence sont susceptibles de poser certains problèmes.

Elles pourraient entraîner une concurrence accrue au sein de la base industrielle et technologique de défense (BITD) européenne et hors Europe pour capter le marché du spatial « *low cost* ». Par exemple, l'abaissement des exigences techniques liées aux plateformes ou aux instruments dans le domaine de l'observation de la Terre réduit le coût du ticket d'entrée pour de nouveaux concurrents qui cherchent à investir le marché de l'observation. Cette nouvelle concurrence va chercher à amplifier ce basculement en pratiquant une politique de prix agressive. On risque alors d'assister à une restructuration du tissu spatial européen privilégiant de nouveaux acteurs et des produits relativement simples au détriment des acteurs traditionnels (*TAS* et dans une moindre mesure *AIRBUS*) capables de concevoir des plateformes de très haute performance. Or, au-delà de l'aspect commercial, le maintien de ce type de compétences est nécessaire à la pérennité de nos moyens satellitaires de défense.

Les évolutions envisagées donneraient une importance croissante aux sociétés qui mettent au point des logiciels complexes de fusion, d'analyse et de traitement des données. La France, qui possède des compétences dans ce secteur, reste néanmoins en retrait s'agissant de leur viabilisation et de leur développement commercial. Un risque accru de fuite de ces compétences vers l'étranger, notamment vers les Etats-Unis, devrait apparaître.

Le développement de filières de composants spatialisés « *low-cost* » autorisant une qualité minimale (rapport coût/probabilité de pannes) compatible avec les coûts de maintien en condition opérationnelle (MCO) des constellations, devrait aussi prendre corps. Les fabricants de ce type de composants se trouvent pour l'essentiel en dehors de l'Europe (Asie notamment) et comptent intensifier encore leur production pour réaliser des économies d'échelle en multipliant les synergies avec l'électronique grand public.

Le développement de lanceurs capables de mettre en orbite basse des charges de quelques centaines de kilos posera, par ailleurs, la question du positionnement de l'industrie spatiale européenne sur ce créneau. L'Allemagne, le Royaume-Uni et des acteurs industriels s'y intéressent actuellement.

De surcroît, la situation décrite *supra* pourrait soulever des risques en matière de prolifération. En particulier, le déploiement de l'activité spatiale sera très propice aux développements d'activités balistiques. Le lancement de satellites exigeait jusqu'à présent le développement de systèmes de propulsion très spécifiques compte tenu des masses importantes à propulser. Les efforts spécifiques dans le domaine des missiles balistiques restaient dans ces conditions relativement identifiables

compte tenu des différences de dimensions et de masses. Avec l'avènement de petites charges et la création possible d'un nouveau marché du lancement spatial léger, il sera sans doute plus difficile d'identifier une politique de développement de vecteur balistique derrière les efforts consentis au profit des lanceurs légers, activité qui va devenir de plus en plus légitime.

3.2 – Types d'accompagnement possibles

La mise en place du *New Space* devrait conduire à accroître la place de nouveaux entrants dans le tissu industriel existant. Aussi, face à une concurrence féroce et sans cesse plus variée, il s'agira d'accompagner les développements technologiques et industriels créateurs d'emplois et de services, tout en préservant une capacité industrielle de haut de gamme technologique.

Il faudra également protéger notre patrimoine technologique et industriel et éviter la prolifération de technologies sensibles, notamment au niveau de la maîtrise d'œuvre des systèmes.

a) Investir le secteur des micro et mini-satellites par le soutien aux PME et l'alignement des grands acteurs

Cette priorité de premier rang nécessite de mettre en capacité de nouveaux acteurs, souvent petits aujourd'hui, et de pousser les constructeurs de lanceurs à s'y adapter.

Les PME ont une forte capacité d'innovation et une réactivité adaptée aux nouveaux enjeux. Toutefois, la création d'une nouvelle base technologique dans le domaine des mini et micro-satellites nécessite des investissements et un soutien financier important pour affronter une concurrence sévère.

Dès lors, il apparaît nécessaire de coordonner les initiatives industrielles privées et de mettre en place les moyens d'un fort soutien gouvernemental français et européen. Ceci devra se traduire à la fois par l'établissement des conditions nécessaires à la disponibilité des financements de ce type de capital risque, par l'inclusion du créneau des micro-satellites dans les instruments qui auront succédé au Plan d'Innovation d'Avenir (PIA 3) et au programme de R&D européen « Horizon 2020 » et par la mise en place d'un accès privilégié à un marché institutionnel européen conséquent.

L'effort à mener sur les micro-satellites devrait aussi aller de pair avec un effort proportionnel sur le secteur des petits lanceurs, sachant que le coût de lancement est un facteur majeur du développement du nouveau paradigme spatial et de son essor. Réussir cet effort nécessitera de parvenir à ce qu'une coopération efficace se mette en place entre les acteurs publics et les industriels, sachant que tous n'auront pas spontanément envie de faire évoluer le paradigme actuel consistant à lancer un gros objet avec un gros lanceur.

S'agissant des capacités de calcul algorithmique et, derrière lui, de la question du *Big*

Data, il y a là aussi une vraie question de décloisonnement des compétences : il existe en France des capacités exceptionnelles dans le domaine du calcul à haute performance et sur le traitement de flux massifs de données. L'un des enjeux de politique publique sera de les rendre accessibles.

b) Soutien de l'industrie traditionnelle pour le développement de systèmes spatiaux de hautes performances

Les systèmes traditionnels de hautes performances devraient conserver une importance majeure pour nombre d'applications exigeantes tant civiles que militaires. En particulier, elles sont indispensables à la pérennité de la dissuasion et à notre capacité de projection de force, points clés en terme de souveraineté. Ces aptitudes sont aujourd'hui chez *TAS*, *ASL* et *AIRBUS DS*. Il va donc falloir maintenir les compétences associées.

La préservation des capacités de hautes performances pour les systèmes spatiaux nécessite également un soutien des filières de composants de hautes performances, en laissant le créneau du low-cost aux chaînes de production asiatiques. La France, avec des sociétés comme *ST MICROELECTRONICS* et *NANOXPLORE* en particulier, a une carte à jouer dans la généralisation de l'utilisation de composants programmables sur les satellites, amenant à améliorer très sensiblement les performances de calcul embarqué tout en diminuant fortement l'encombrement et le poids de l'électronique embarquée.

c) Protection des « nouveaux savoir-faire » et renforcement de la sécurité spatiale

Un certain nombre de mesures – de protection, d'encadrement normatif international et législatif – sont par ailleurs nécessaires pour accompagner le mouvement de modernisation industrielle décrit plus haut.

Compte tenu des enjeux industriels et économiques liés au domaine spatial, les savoir-faire techniques doivent être protégés. Ceci concerne bien entendu les technologies de base (système, équipements, composants…) mais également les logiciels de traitement qui se trouveront au cœur de la valeur ajoutée des données spatiales.

Le souci de prolifération doit également être au centre des préoccupations compte tenu notamment de l'arrivée massive de nouveaux entrants. Comme cela a été dit plus haut, la non-prolifération ne s'exercera plus par le contrôle de composants et matériaux (qui se seront banalisés) mais par le contrôle des compétences en matière de conception des systèmes. Cela nous éloignera significativement du référentiel actuel du contrôle national (CIEEMG et CIBDU) et international (MTCR, Wassenaar).

Mais ces mesures nationales de protection doivent être accompagnées d'une prise de conscience plus large.

Il s'agit de renforcer le respect des normes de sécurité spatiale (IADC[7], futurs codes de conduite/traités, etc.) pour hausser les exigences techniques et limiter la prolifération de l'industrie spatiale « *low cost* ».

7 - *Inter-agency Space Debris Coordination Committee.*

Il s'agit également de promouvoir l'adoption de nouvelles réglementations en matière de contrôle des satellites (par exemple au titre de la hausse du trafic spatial), de contrôle des explosions en orbite et des réentrées pour les lancements (du fait de la prolifération des petits lanceurs). Cela suppose :

- une implication redoublée de la France dans les négociations internationales en cours sur le « développement durable des activités spatiales » engagées au *Comité des utilisations pacifiques de l'espace extra-atmosphérique* (CUPEEA) des Nations unies ou dans les discussions visant à revitaliser l'idée d'un code de conduite ;
- une mise à jour des textes nationaux (loi sur les opérations spatiales de 2008 par exemple) pour « montrer l'exemple » si nécessaire.

Enfin, il faut renforcer l'adhésion des pays aux mesures de transparence en place pour encadrer l'activité balistique et de lancement (de type *Code de conduite de la Haye*) à travers des pré-notifications de lancement, des bilans annuels d'activité balistique et spatiale, des visites de sites, etc.

4 - Scenarii alternatifs

4.1 – Les technologies spatiales font l'objet d'une complète reprise en main par l'industrie de l'information : les applications spatiales se privatisent complètement et l'Etat ne pèse plus dans les orientations industrielles

Ce scénario fait le pari d'une accélération des tendances actuelles. Il correspond à la description de ce qui se passerait si la France et l'Europe ne mettaient pas en œuvre les préconisations de politiques publiques précédemment énumérées. On observerait alors avec le temps une disproportion croissante entre les investissements privés et publics, ces derniers diminuant sous l'effet :

- de tensions croissantes sur les budgets publics (notamment militaires) avec le souci d'optimiser les dépenses ;
- de l'existence de services applicatifs privés de plus en plus performants et qui « rendent le service » de manière satisfaisante.

L'acteur public en France garde dans ce scénario une capacité minimale de satellites « patrimoniaux » (observation de la Terre, télécommunications), mais la réalité des pratiques montre une dépendance accrue vis-à-vis du monde industriel pour l'exploitation des données et pour l'exploitation de services extérieurs :

- l'Etat ne peut plus assurer son rôle de prescripteur pour décider des orientations technologiques et dépend largement des

technologies mises au point par l'industrie ;

- la France, faute d'avoir su développer une solide industrie dans le domaine du traitement de l'information spatiale et de la fusion de données en comparaison des investissements qui ont été réalisés outre-Atlantique, ne peut plus contrôler la conception des techniques qui ont été développées à l'étranger (aussi bien pour les capteurs que pour les logiciels de traitement de données).

La France court le risque de perdre sa souveraineté de façon sans doute irréversible sur un pan d'activité essentiel à son information stratégique.

4.2 – Les projets de « megaconstellations » sont bloqués pour des raisons de règlementations internationales et des questions se posent sur la pérennité du secteur du New Space

Ce second scénario alternatif se fonde lui aussi sur des précédents industriels (échec des premières grandes constellations comme par exemple *Iridium* ; récurrence des effets de bulle dans les nouvelles technologies) ou sur la réalité connue des effets accidentels dû à la présence de débris dans l'espace.

A la suite des annonces faites par *SPACE X*, *SAMSUNG* ou *BOEING*, pour des constellations de plusieurs milliers de satellites (entre 1 500 et 4 500) en orbite basse, l'ensemble des industriels se dirige vers la mise en place de constellations gigantesques, essentiellement pour les télécommunications.

Dans les années suivantes, les débris générés par le tir antisatellite chinois dix ans plus tôt provoquent un accident avec un satellite d'observation, produisant de nombreux débris nouveaux. Cette fois, l'événement a des répercussions importantes sur la gestion de l'orbite de la station spatiale qui doit être surveillée pour empêcher tout accident catastrophique. Aucune activité extravéhiculaire des astronautes n'est désormais envisageable. Compte-tenu de la gravité des éventuelles conséquences, la communauté internationale prend conscience de la nécessité d'une réglementation très stricte sur le « contrôle du trafic spatial » (*Space Traffic Management*). Ce concept, déjà à l'étude depuis plusieurs années, serait alors au centre des négociations internationales.

Le débat se situe désormais au niveau des Nations unies où se dégage un large consensus en faveur de l'idée « d'un développement durable des activités spatiales ». Dans ce contexte, le débat met alors particulièrement en évidence le danger que représentent les constellations de plusieurs milliers de satellites placés sur des orbites basses et qui impliquent de surcroît des activités de navigation des satellites à travers différentes altitudes[8] (d'ailleurs déjà largement affectées par la multiplication des débris pour certaines d'entre elles).

8 - Avec notamment la nécessité de redescendre les satellites en fin de vie et de « gérer » des constellations comprenant plusieurs milliers d'objets.

Des projets de textes internationaux circulent donc sur l'interdiction pure et simple de méga-constellations en orbite basse. En dépit de l'opposition des Etats-Unis, une large majorité de pays emmenés par la Russie et la Chine obtient que soit considéré un projet de traité dans ce sens.

Compte-tenu des incertitudes liées aux retombées économiques de ces constellations, mais aussi en raison de ces perspectives nouvelles de restrictions internationales, l'industrie renonce à ses projets de « méga-constellations » et se replie massivement sur les technologies terrestres et aériennes (drones, ballons) de réseaux de l'information.

Dans son ensemble, le secteur du *New Space*, fondé sur la multiplication de petits satellites à bas coût (micro, voire nano-satellites de quelques kilogrammes), connaît alors un ralentissement généralisé des investissements et l'industrie spatiale, qui avait misé sur son essor, doit trouver des solutions alternatives pour son développement.

Dans une telle situation, l'activité industrielle pourrait connaître deux évolutions majeures :

- le renforcement des programmes spatiaux traditionnels dans le domaine des télécommunications avec la mise en place de gros satellites géostationnaires toujours plus performants (qui pourrait aller jusqu'à favoriser l'essor de l'observation à très haute résolution depuis l'orbite géostationnaire). Cela ne pourrait intervenir que grâce à une politique soutenue de maintien des compétences industrielles ;
- le développement d'activités soutenues dans le domaine des plates-formes haute altitude (ballons, drones) sur l'exemple des programmes initiaux engagés par les sociétés *THALES ALENIA SPACE* ou *AIRBUS DS*. Ces solutions feraient néanmoins l'objet de très fortes concurrences internationales et devraient sans doute être portées par un investissement gouvernemental.

Incidemment, une telle évolution ne serait pas sans conséquence sur la future politique européenne des lanceurs, avec un investissement à reconsidérer compte tenu de la nature des charges à lancer. Si *ARIANE 6* demeurerait probablement un choix encore valide, la question pourrait cependant se poser d'un nouveau lanceur lourd pour l'Europe, pour répondre à d'éventuels besoins pour de futures grosses charges géostationnaires.

3

Paix et guerre dans le cyberespace

L'essentiel

Dimension en perpétuelle évolution, le numérique influe de façon de plus en plus déterminante sur la vie quotidienne des individus et des institutions. Les évolutions de moyen terme sont particulièrement difficiles à anticiper. Elles légitiment la mise en place de mécanismes de veille sur les évolutions des pratiques et des normes internationales. En outre, une gouvernance interministérielle plus étroite s'impose, face aux enjeux de sécurité physiques (attaques) ou sociétaux (situation de normes en la matière).

Certains acteurs et plusieurs applications du numérique qui ont transformé la vie de nos sociétés n'existaient pas il y a 15 ans. Dès lors, penser à 15 ans l'évolution du domaine et ses conséquences en matière de défense et de sécurité nationale se révèle un exercice délicat.

L'avenir de cet espace toujours en construction pose d'ores et déjà la question du rôle des Etats et de la responsabilité des futurs acteurs pour mieux assurer la sécurité du cyberespace et les modalités de régulation.

1 - Etat des lieux en 2017

1.1 - Le numérique : un domaine en construction

Le « cyberespace » est entendu ici comme l'espace d'accès au numérique. En expansion permanente, le cyberespace est essentiellement constitué d'internet et des systèmes d'information embarqués par les éléments qui lui sont connectés ou qui se connectent entre eux. Rapportée à la surface terrestre, sa densité peut atteindre 667 millions de milliards de systèmes d'information par millimètre carré. Le numérique est entendu comme un domaine d'activités dématérialisées aux enjeux de sécurité propres.

a) L'espace des convergences

Le numérique naît de convergences technologiques.

La première convergence est issue de la conversion en données numériques du texte, du son et de l'image. Associée à l'invention de protocoles de transferts de ces données spécifiques (TCP/IP), cette conver-

gence conduit à la création et à l'essor d'internet.

La deuxième convergence est en cours. Elle résulte de l'apparition de technologies nouvelles, de la poursuite de la numérisation systématique des activités humaines traditionnelles et du développement de nouveaux usages. Ces évolutions débouchent sur :

- le recueil de la donnée (objets connectés de toutes natures, terminaux mobiles plus performants et moins consommateurs en énergie) ;
- la transmission et la disponibilité de la donnée (réseau de communications électroniques « 5G », « informatique en nuage ») ;
- le traitement des données (« *big data* », « *deep learning* », intelligence artificielle).

Ces technologies sont le plus souvent développées hors du contrôle des Etats, qui n'ont plus la capacité de les anticiper.

b) Les enjeux liés au numérique dépassent, en les englobant, les questions de sécurité et de défense

Le numérique met à l'épreuve le cadre de souveraineté des Etats et redéfinit partiellement leurs frontières et leurs modes d'action. Dans l'espace numérique, des monnaies sont créées, des mouvements d'opinion d'envergure mondiale se développent, un nouveau type de confrontation voit le jour et la criminalité s'y répand. Les plus puissants acteurs privés du numérique disposent de moyens bien supérieurs à ceux des Etats les moins riches. Les entreprises comme les individus jouissent de formes de libertés nouvelles mais aussi de moins de protection, affaiblissant les relations de citoyenneté et le sentiment d'appartenance à une nation. Au nom d'une liberté sans entrave, certains acteurs dits « technolibertaires » n'hésitent d'ailleurs pas à contester les décisions politiques des gouvernements pour peu qu'elles visent à la régulation de leurs activités ou à la taxation de leurs profits.

C'est pourquoi, au nom de cette révolution des activités et des comportements, certains considèrent que le numérique pourrait conduire à une redéfinition des repères de l'humanité. Laurent ALEXANDRE, figure française du transhumanisme, estime ainsi que « *l'humanité est déjà lancée sur un toboggan transgressif* » par le silence de dirigeants, présentés comme dépassés par le progrès des technologies et peu conscients des questions éthiques soulevées. Cette méconnaissance serait susceptible d'impacter nos principes ancrés dans le droit des libertés individuelles, tels que la protection des données à caractère personnel. A moyen terme, avec l'introduction de « l'Homme augmenté » et l'interconnexion des objets, c'est tout l'écosystème humain qui serait bouleversé. Cette tendance est cependant jugée anecdotique par certains.

1.2 – Le cyberespace : un espace aux caractéristiques propres

Le numérique a besoin d'électricité et de réseaux de communications électroniques pour être accessible *via* le cyberespace. Contrairement à une idée souvent reprise, le cyberespace comprend donc un nombre de frontières plus élevé que les domaines naturels. Ces frontières naturelles et immatérielles sont éventuellement superposées mais elles ne coïncident pas entre elles. Le « territoire national numérique » d'un Etat, dont les contours restent à définir, ne se limite pas aux infrastructures numériques situées sur son territoire. Dans le cyberespace, et alors que tout système d'information connecté est accessible depuis tout autre point, lorsqu'une attaque informatique est détectée, elle s'est déjà produite ailleurs et a éventuellement réussi.

Enfin, les infrastructures physiques du cyberespace sont essentiellement développées par des acteurs privés, même si les utilisateurs du numérique considèrent le cyberespace comme un bien commun, non appropriable et les Etats comme un bien collectif – voire comme un bien tutélaire – auquel doivent s'appliquer à la fois la réglementation qu'ils établissent et le droit international.

1.3 – Le numérique : un domaine qui favorise l'offensive et qui offre un large spectre d'objectifs

a) Un domaine favorable à l'attaquant

Quel qu'il soit - hacker, individu curieux, activiste, délinquant isolé ou membre du crime organisé, terroriste, agent d'un service de renseignement, soldat en opération – le « cyberattaquant » utilise des techniques comparables et bénéficie d'un environnement permissif. L'avantage est à l'attaquant.

Le numérique est en effet un domaine exposé aux actions offensives pour des raisons :

- techniques (faiblesse du niveau de sécurité informatique, disponibilité de logiciels et d'équipements peu sécurisés, complexité croissante de « systèmes de systèmes », disponibilité d'armes informatiques proliférantes à coût d'acquisition marginal, modes d'attaques industrialisables) ;
- humaines (sensibilisation insuffisante, carence de compétences, organisations obsolètes) ;
- économiques (analyses de risques incomplètes, coût, existence d'un marché des failles informatiques) ;
- politiques et juridiques (choix d'organisation, absence d'effectivité du droit, absence de sanction, législations laxistes, libre circulation des données).

Le cyberespace est parallèlement favorable à l'action clandestine. Les techniques d'attaques habituellement utilisées préservent l'anonymat de l'attaquant ou rendent son

identification longue et coûteuse, sans garantie de succès. Ainsi, l'attribution d'une attaque informatique relève d'une décision judiciaire ou politique, prise en fonction d'un faisceau d'indices, sans certitude technique absolue et rarement des preuves opposables.

b) Un spectre large d'objectifs

L'objectif de l'attaquant peut être le gain financier (vol de propriété intellectuelle, chantage au chiffrement de fichiers, à la révélation de données, à la disponibilité de ressources). La déstabilisation de l'entité visée (personne, OIG, Etat, entreprise, ONG) constitue un deuxième type d'effet recherché : défiguration de site internet, dénis de services, révélation de données. La diffusion de fausses données, qui ne constitue pas forcément en soi une attaque informatique, fait en revanche partie de la panoplie d'instruments utilisés dans des tactiques hybrides. L'espionnage (politique, économique, scientifique et technique), est aussi un objectif fréquemment à l'origine d'attaques informatiques.

Une attaque informatique peut être utilisée pour remplir un objectif militaire de basse intensité : renseignement, modification de données ou piégeage de ressources ou de réseaux en amont d'actions de haute intensité.

Mais elle peut aussi être un acte de sabotage par la modification ou la destruction de ressources informatiques, avec d'éventuelles conséquences très critiques : dérèglement de systèmes de production, destruction d'équipements de sécurité.

Enfin, les attaques informatiques peuvent être menées dans le cadre d'un conflit armé, par exemple en visant des infrastructures stratégiques et critiques (réseaux énergétiques, de transport et de communication notamment) au risque de dommages collatéraux importants, le cyberespace étant dual par nature.

1.4 – Les modèles nationaux, les acteurs

a) Les modèles nationaux

L'organisation des Etats en matière de défense et de sécurité des systèmes d'information est généralement de deux types, identifiables selon la localisation du centre de gravité de l'instruction des sujets, de la prise de décision et de la mise en œuvre des actions.

Dans le premier modèle, le centre de gravité est proche ou intégré aux services de renseignement du pays concerné qui coordonnent voire assurent à la fois la sécurité, les opérations de défense et d'attaques informatiques. La stratégie de ces pays favorise plutôt le développement de capacités offensives. Parmi les pays les plus actifs, les Etats-Unis, le Royaume-Uni et la Russie ont adopté ce modèle.

Dans le second modèle, les capacités défensives et offensives sont séparées. L'organisation en matière de sécurité et de défense développe une stratégie de protection qui passe par l'augmentation du niveau de sécurité des systèmes d'information étatiques et de ceux des

infrastructures critiques de la nation, sans exclure le recours à des actions offensives de prévention ou de rétorsion. Parmi les pays les plus actifs, l'Allemagne, la France, la Chine et Israël ont adopté ce modèle. Les orientations portées par la directive européenne « *Network information security* » adoptée en 2016 et qui visent à organiser la protection de la disponibilité des services produits par les infrastructures devraient favoriser ce second modèle.

b) Les acteurs

« La stratégie nationale pour la sécurité du numérique », adoptée par la France en 2015, désigne les acteurs qui doivent être mobilisés et impliqués dans la sécurité du numérique du pays et ceux qui nuisent à la sécurité du numérique dont l'action doit être entravée.

Dans la 1ère catégorie, on retrouve la plupart des administrations et services de l'Etat, les opérateurs d'importance vitale, les opérateurs et fournisseurs de produits et de services de sécurité informatique, mais aussi les entreprises et citoyens qui doivent également être sensibilisés aux enjeux de la cybersécurité et adopter un comportement responsable.

Parmi ceux qui nuisent à la sécurité du numérique, citons les délinquants isolés, les officines et les mercenaires au service d'entreprises ou d'Etats, souvent appelés « proxys ».

Il est à noter le rôle dual de certains Etats qui piègent les équipements de sécurité ou les systèmes d'information d'infrastructures critiques de pays adverses, ainsi que celui d'entreprises qui développent des armes informatiques ou font le marché de failles de sécurité.

1.5 – La défense et la sécurité du numérique dans les organisations internationales

Aucune organisation spécifique n'est véritablement chargée de la sécurité du numérique. De nombreuses organisations internationales traitent en revanche, parmi d'autres, des questions liées à la défense et à la sécurité du numérique, qu'elles soient d'envergure mondiale, régionale ou à compétence thématique (ONU, UE, OCDE, OTAN).

a) Les organisations mondiales : l'exemple de l'ONU

La question de la sécurité de l'information est inscrite à l'ordre du jour de l'Organisation des Nations unies (ONU) depuis que la Fédération de Russie a, en 1998, présenté pour la première fois un projet de résolution à la Première Commission de l'Assemblée générale de l'ONU. Sous l'égide du bureau des affaires de désarmement des Nations unies, un groupe d'experts gouvernementaux « chargés d'examiner les progrès de

l'informatique et de la télématique et la question de la sécurité internationale » a publié plusieurs rapports dont les deux dernières livraisons affirment l'applicabilité du droit international dans le cyberespace, y compris celle de l'article 51 de la Charte des Nations unies sur la légitime défense, sans toutefois préciser les notions juridiques qui permettraient une telle applicabilité.

Organisme rattaché à l'ONU, l'Union internationale des télécommunications (UIT) organise des sommets mondiaux de la société de l'information et a lancé dès 2007 un agenda global de cybersécurité tendant à mettre en place un cadre de coopération international.

b) Les organisations régionales : l'exemple de l'Union européenne

Dans le respect de la souveraineté des Etats-membres, l'Union européenne a pris en compte les questions liées à la sécurité des systèmes d'information, notamment par la création d'une agence européenne de sécurité des réseaux (ENISA) et par l'élaboration d'une directive destinée à favoriser la lisibilité de l'organisation des Etats-membres et à renforcer la continuité de services des opérateurs de services essentiels à l'économie et à la société. La directive « *Network information security* » a été publiée en juillet 2016.

L'Union européenne a par ailleurs créé un organisme opérationnel destiné à protéger les réseaux de l'organisation, le CERT-UE. Compte tenu de l'étroite imbrication des politiques nationales et européennes sur toute une gamme de sujets stratégiques au plan économique, les systèmes informatiques de l'Union sont tout aussi importants que ceux des Etats membres en termes de sécurité numérique.

c) Les organisations spécialisées : les exemples de l'OTAN et de l'OCDE

En juin 2016, à l'issue d'une réunion des ministres de la défense des pays membres de l'organisation du traité de l'Atlantique nord (OTAN), le cyberespace a été déclaré espace de combat, au même titre que la terre, l'air et la mer.

Le centre d'excellence de l'OTAN (Tallin, Estonie) a publié en 2013 un manuel relatif à l'applicabilité du droit des conflits armés aux cyber-attaques employées dans le cadre d'un conflit armé international ou non international. Les pays baltes et la Pologne, très sensibles aux capacités offensives russes en matière cyber, ont fortement poussé la prise en compte de cette dimension dans l'action de l'organisation.

Pour l'OTAN, le problème de l'attribution des attaques informatiques, fondement de toute réflexion juridique, est considéré comme résolu.

L'organisation de coopération et de développement économiques (OCDE) a, pour sa part, publié en 2008 une recommandation à propos des « systèmes et réseaux d'information interconnectés, dont la perturbation ou la destruction aurait un sérieux impact sur la santé, la sécurité, la sûreté ou le bien-être économique des citoyens ou sur le fonctionnement efficace du gouvernement ou de l'économie » puis en 2015 une recommandation « sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale ».

D'autres enceintes comme l'Organisation pour la sécurité et la coopération en Europe (OSCE) ou les organisations internationales sectorielles ont proposé des normes techniques ou de comportements destinées à renforcer la sécurité du cyberespace. Il n'existe pas, semble-t-il, de lieu où les diverses recommandations de ces organisations, souvent redondantes, sont consolidées.

2 - Situation en 2030

Fin 2016, le « *Center for long-term cybersecurity* » de l'université de Berkeley (Californie, Etats-Unis) a rendu public un travail collectif d'experts de tous horizons présentant cinq *scenarii* pour internet à l'horizon 2020. Ils sont peu optimistes mais reflètent bien la panoplie d'évolutions vraisemblables sur les années à venir et, au-delà, à l'horizon 2030 qui pour le cyber apparaît déjà de très long terme. Le point commun de ces *scénarii* est l'atteinte systématique aux libertés individuelles.

Trois scénarios retiennent l'attention et sont susceptibles de se produire en tant que tels ou bien de combiner entre eux leurs modes opératoires. Le scénario « *The New Normal* », banalisant le vol de données par attaques informatiques plus ou moins généralisées, ne présente que peu d'intérêt puisqu'il est consubstantiel au développement des activités numériques, comme de toute activité humaine. Quant au scénario caricatural « *Sensorium, internet of emotion* », qui aboutit au schéma ultime de prédiction de la vie et de manipulations d'individus, il relève d'un scénario de science-fiction. En effet, les questions éthiques et humanistes qui ne manqueront pas de se poser tout au long du processus de transformation numérique interfèreront inéluctablement et empêcheront une telle issue extrême.

Dans le premier scénario « *Omega* », les technologies prédictives permettent un ciblage précis des goûts, habitudes et désirs des personnes, les rendant prévisibles et influençables. Ceux qui refusent de transmettre leurs données sont considérés comme des marginaux voire de potentiels criminels. Les données prédictives sont utilisées par les Etats pour comprendre les envies et les craintes des citoyens, sécuriser une ville en canalisant la surveillance uniquement sur les individus enregistrés à risque, décider des peines encourues par les justiciables ou prévoir les fluctuations de l'économie de marché selon l'évolution du pouvoir d'achat. **Les pays autoritaires connaissent peu d'insécurité alors que les Etats qui cherchent à encadrer ces technologies, les démocraties européennes en particulier, ont des taux d'insécurité élevés.** Néanmoins, l'instabilité plus ou moins exacerbée et la résistance de mouvements humanistes refusant le tout numérique conduisent les démocraties à mettre en place une forme de régulation et de contrôle.

Dans le second scénario « *Bubble 2.0* », en raison d'une faible création de valeur

réelle et de l'augmentation du coût du travail dûe à l'intermédiation numérique de la société, **une crise économique touche les grands acteurs du numérique.** Ceux-ci choisissent de rendre leurs services payants et de vendre leurs données. Finalement, les géants du numérique américains (GAFA) sont vendus et **le centre du monde numérique se déplace de la Silicon Valley vers Singapour, Pékin et Séoul.** L'Union européenne, de par une législation exigeante en matière de données à caractère personnel, voit ses choix politiques récompensés sur le plan international et son poids diplomatique accru. A l'inverse, les Etats-Unis sont pointés du doigt, le *soft power* américain décline et ouvre des brèches diplomatiques dans lesquelles les monarchies pétrolières s'engouffrent, renégociant à la hausse le prix du pétrole. On assiste ainsi à un nouvel éclatement de la bulle numérique et à une forme de rééquilibrage entre la nouvelle et l'ancienne économie, le marché mondial s'autorégulant plus ou moins rapidement avec un retour de balancier proportionnel au niveau de maturité atteint dans la transformation numérique.

Dans le dernier scénario « *Intentional Internet of Things* », l'internet des objets s'implante dans les grandes villes du monde grâce aux propositions technologiques qui répondent aux problématiques liées à la surpopulation urbaine (trafic routier, santé, dépenses publiques, écologie). Les objets connectés sont adaptés pour les services de sécurité et de police puis au domaine militaire, créant une baisse des violences urbaines. L**es écarts se creusent entre villes dont les moyens d'investissements diffèrent, puis entre urbains et non urbains.** Cet écart se reflète aussi en matière d'éducation, de valeur du travail et de santé des populations ainsi que dans le coût des assurances, plus élevé pour les personnes ne pouvant fournir des données en flux constant à leurs assurances. **Les régimes autoritaires voient leurs pouvoirs renforcés.** Ceci accroît encore plus les inégalités sociétales entre les centres urbains et les déserts numériques ainsi qu'entre les classes sociales.

La dimension pédagogique de ces *scenarii*, caricaturaux mais pas irréalistes d'un point de vue technologique (les équipementiers travaillent déjà à un « internet des émotions »), devrait favoriser le débat démocratique, voire éthique ou philosophique, qui fait aujourd'hui défaut sur les grandes orientations sociétales portées par le numérique.

3 - Enjeux pour la France et pour l'Europe

Les propositions présentées ci-après fournissent les éléments d'une prise de décisions favorables à la défense de nos intérêts, à la paix et à la sécurité internationales dans le cyberespace. Ces propositions appartiennent aux champs politique, économique ou relèvent de l'élaboration de doctrines ; elles complètent les orientations choisies dans la stratégie nationale pour la sécurité du numérique de 2015 et la stratégie dédiée à la défense et à la sécurité des systèmes d'information portée par l'agence nationale de la sécurité des systèmes d'information (ANSSI) qui demeurent pertinentes. Elles couvrent, à défaut de pouvoir préserver une autonomie stratégique, la maîtrise de la dépendance. Elles incluent la constitution de cursus de formation pour disposer de la ressource humaine nécessaire, les politiques industrielles, qu'il reste à évaluer, la protection des infrastructures critiques et l'assistance aux victimes. Ces propositions ont été complétées, sur le plan des capacités offensives, par la création d'un commandement cyber au sein des armées le 1er janvier 2017.

3.1 – Création d'un observatoire des stratégies internationales

L'objectif de l'observatoire serait d'éclairer la décision publique en matière de sécurité du numérique et du cyberespace.

Ses missions seraient notamment :

- de suivre les stratégies des Etats en matière de numérique, de défense et sécurité du numérique et du cyberespace ;
- de consolider les normes, propositions ou recommandations formulées par les organisations internationales (OIG et ONG de tous secteurs) en matière de sécurité du numérique ;
- d'effectuer des analyses et travaux d'anticipation et de prospective dans les sujets susceptibles d'avoir un impact en matière de défense et de sécurité du numérique et du cyberespace.

Cet observatoire pourrait être confié à l'ANSSI ou à un think tank orienté par l'agence qui se spécialiserait sur les questions numériques.

3.2 – Elaboration d'une doctrine interministérielle de réponse aux attaques informatiques

Les attaques informatiques traitées ces dernières années par l'ANSSI ont montré que les autorités gouvernementales comme les intérêts diplomatiques, économiques, scientifiques et technologiques de la France pouvaient être gravement atteints. Un risque majeur existe également quant à la sécurité de la population.

Dans le respect du droit international, une doctrine de réponse aux attaques informatiques touchant aux intérêts fondamentaux de la Nation doit être élaborée et évoquer les mesures de rétorsion, les contre-mesures (à l'instar de celle prévue par l'article 21 de la loi n°2013-1168 du 8 décembre 2013) ou les actions de légitime défense pouvant être menées.

Ces mesures peuvent être de différentes natures : diplomatiques, économiques et financières, commerciales, militaires, etc. La coordination de l'élaboration de ces mesures pourrait être confiée au secrétariat de la défense et de la sécurité nationale (SGDSN), en raison de leur dimension interministérielle.

3.3 – Elaboration et défense des positions françaises sur les questions clés

Il s'agit d'élaborer de manière interministérielle les positions françaises sur les sujets les plus structurants à court terme et de porter ces positions dans les organisations internationales.

Les premières concertations pourraient avoir lieu autour des sujets suivants :

- soutenir le maintien de l'illicéité des attaques informatiques versus laisser se généraliser l'autorisation donnée aux acteurs privés de riposter (« *hack back* ») ;
- faire adopter comme règle de bonne conduite l'interdiction du piégeage préemptif des réseaux civils (« grilles » énergie, communications, transports) ;
- promouvoir un marché encadré des failles de sécurité, voire l'interdire, et favoriser le « *responsive disclosure* » ou les pratiques de « *bug bounty* » *versus* laisser se développer un libre marché des « *0 day* » ;
- dans les traités commerciaux, permettre par exception la localisation territoriale et la maîtrise juridique et technique de certains types de données versus soutenir le « *free flow of data* ».

Nous nous trouvons aujourd'hui dans ce domaine, comme dans plusieurs technologies de rupture, dans une situation non coopérative. Mais, la conflictualité déjà à l'œuvre dans le cyberespace amènera très vite à devoir établir des éléments de régulation internationale. Pour peser, la France doit conforter sa position de crédibilité sur le plan domestique, utiliser le cadre euro-

péen pour commencer à promouvoir certaines règles comportementales et construire une coalition d'Etats pragmatiques. C'est le sens des actions de coopération et de la réflexion sur les mécanismes d'alerte et de désescalade qu'elle a engagées.

4 - Scenarii alternatifs : généralisation du « *hack back* » ou régulation

Les choix faits par les Etats dans les mois et années qui viennent sur les sujets de la réponse aux attaques informatiques, du marché des vulnérabilités et de la libre circulation des données seront structurants.

4.1 - Généralisation du « *hack back* »

Si, comme certains Etats le proposent, il est permis aux acteurs privés de répondre à une attaque informatique par une attaque informatique (principe du « *hack back* ») alors même que l'attribution reste incertaine, la sécurité du numérique ne pourra plus être assurée et les tensions internationales s'accroîtront (nombreuses attaques créant des effets « domino »). Ce choix dévastateur favoriserait le développement d'un mercenariat cybernétique au service d'acteurs étatiques ou non. La pratique du « *hack back* » fait à l'heure actuelle l'objet d'un lobbying appuyé en faveur de sa légalisation auprès des gouvernements et au sein des organisations internationales.

L'essentiel des armes informatiques utilisent les failles techniques des systèmes d'information comme vecteurs d'attaques, la partie du code informatique utilisé qui représente la charge active dépend ensuite de l'objectif recherché (modification ou vol de données, piégeage, destruction). Les mises à jour publiées par les éditeurs de logiciels ou les producteurs d'équipements embarquant un système d'information permettent à la fois d'améliorer les fonctionnalités disponibles mais également de corriger les failles de sécurité identifiées. Il est d'usage courant que ces failles, appelées « *0 day* », soient signalées aux éditeurs et équipementiers par des utilisateurs ou des chercheurs en sécurité les ayant identifiées. Ces signalements donnent parfois lieu à une récompense financière (le « *bug bounty* »). Toutefois, un marché des failles informatiques s'est développé. Illégal, librement accessible via internet, il permet à des criminels d'acheter avec une monnaie virtuelle les failles qu'ils peuvent intégrer à leur code malveillant pour exercer leur activité. Légal, il est développé par des entreprises qui revendent les failles

découvertes, par exemple à des services de renseignement. Le contrôle de ces entreprises est désormais l'objet de réflexions dans le cadre de l'arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage. L'apport de ce marché à la sécurité du numérique reste à démontrer.

4.2 – Régulation et utilisation plus sûre du numérique

Un scenario alternatif serait celui d'un aboutissement des efforts en cours, notamment dans le cadre de l'ONU, de plusieurs Etats, grands opérateurs et de nombreux acteurs industriels en faveur d'un usage pacifique du cyberespace. En appui de cette dynamique, l'ANSSI a organisé en 2017 la première conférence internationale sur les rôles et responsabilités des acteurs publics et privés de la société numérique. Dans ce scenario, un consensus international aura été dégagé pour réguler les échanges dans le cyberespace. Au-delà des principes et des bonnes pratiques, un organe international de régulation aura été mis en place. L'instauration de pratiques et de comportements favorables à un usage pacifique du cyberespace permettra de concentrer les actions des Etats vers la lutte contre une cybercriminalité en croissance constante.

4

La dissuasion, atout de puissance et facteur de paix

L'essentiel

En 2017, la dissuasion nucléaire est une pièce maitresse des politiques de défense. Neuf[1] pays conduisent aujourd'hui des programmes nucléaires à finalité militaire de manière officielle ou non. Une dynamique générale de modernisation des arsenaux est observée, tandis que se forme aux Nations unies un front de pays opposés aux armes nucléaires.

Le scénario prospectif privilégié pour 2030 est celui d'une certaine continuité dans le panorama général des forces nucléaires. A cet horizon, les forces stratégiques occidentales seront toutes en train de renouveler la génération actuelle de leurs moyens. Cependant, les forces nucléaires seront probablement confrontées à des défis plus robustes qu'aujourd'hui à la faveur de développements capacitaires comme celui des défenses antimissiles et anti-aériennes. La notion de dissuasion non nucléaire ou de dissuasion inter-domaines (*cross-domain deterrence*) devrait avoir pris une importance accrue dans le débat stratégique avec les développements cybernétiques.

1 - Etat des lieux en 2017

1.1 - La dissuasion nucléaire reste une pièce maitresse des politiques de défense

La place de la dissuasion dans les politiques de défense des puissances nucléaires est centrale, l'arme atomique présentant un rapport « pouvoir dissuasif – efficacité technique » inégalé.

C'est au premier chef le cas en Russie où, depuis son arrivée au pouvoir, Vladimir POUTINE n'a cessé de réaffirmer sa volonté de redonner aux forces nucléaires russes leur lustre de l'époque soviétique, affichant même l'intention d'en moderniser 70 % des moyens à l'horizon 2020. De fait, depuis 2010, les moyens de la dissuasion russe bénéficient d'une priorité dans un contexte de hausse continue du budget de la défense. Un nouveau sous-marin lanceur d'engins équipé d'un nouveau missile balistique a ainsi pu être mis en service opérationnel ces dernières années, la chaine de production du bombardier stratégique *Blackjack* a été relancée et des grands moyens de simulation mis en chantier. La crise ukrainienne en 2014 a pris, par ailleurs, une dimension nucléaire – certes contenue –, lorsque Vladimir POUTINE a publiquement indiqué qu'il aurait été prêt à mettre en alerte ses forces nucléaires si les Etats-Unis ou l'OTAN avaient cherché à contrer son action en

1 - France, Etats-Unis, Russie, Chine, Royaume-Uni, Israël, Pakistan, Inde, Corée du Nord.

Crimée. Des responsables militaires russes ont également présenté le Danemark et certains pays accueillant des infrastructures de la défense anti-missiles de l'OTAN comme des « cibles stratégiques ».

En Occident, ces initiatives russes et la politique de puissance déployée par la Chine contribuent à maintenir la dissuasion nucléaire au cœur des stratégies de défense. Aucune évolution stratégique n'est venue invalider la pertinence de la dissuasion nucléaire qui joue même régulièrement un rôle dans le champ déclaratoire et visible. Ainsi, face à une Russie qui multiplie les missions provocantes de son aviation stratégique le long des côtes américaines et européennes, une Corée du Nord qui menace et défie et une Chine qui décrète unilatéralement sa souveraineté sur des zones maritimes étendues, les Etats-Unis n'hésitent pas à répondre en déployant des bombardiers stratégiques de manière permanente en Asie ou de manière ostensible en Europe, accompagnant ces initiatives de déclarations politiques non ambigües.

L'Asie s'affirme par ailleurs comme le continent le plus nucléarisé. Dans le domaine civil, d'importants projets y sont en cours ou y sont prévus. Surtout, on trouve en Asie le plus grand nombre d'Etats détenteurs de l'arme atomique (Chine, Inde, Pakistan, Corée du Nord[2], mais aussi Russie) et les garanties de sécurité nucléaire américaines en Asie du Nord-est amplifient encore l'importance du fait nucléaire dans les équilibres stratégiques régionaux. Parmi les membres permanents du Conseil de sécurité des Nations unies, la Chine est le seul Etat qui accroit en volume son arsenal nucléaire et qui n'a pas formellement déclaré de moratoire sur la production de matière fissile pour les armes, ni démantelé ses installations de production, comme l'a fait la France. Elle développe une force nucléaire océanique et modernise sa composante terrestre. De son côté, sur fond de rhétorique belliqueuse, la Corée du Nord poursuit méthodiquement un programme nucléaire militaire. Ce faisant, dans cette partie de l'Asie, on assiste à la mise en place d'un schéma stratégique nouveau dans lequel un Etat nucléaire, totalitaire et agressif menace ses voisins (Japon, Corée du Sud) sous garantie nucléaire américaine. Plus à l'Ouest, le Pakistan déploie, dans des conditions de sécurité qui inquiètent, des armes nucléaires dans une logique de rivalité exacerbée avec l'Inde. C'est bien en Asie que le risque d'emploi de l'arme reste le plus fort. On ne peut, en effet, écarter tout à fait l'éventualité d'un geste fou de Pyongyang, ni l'hypothèse d'un emploi plus rationnel afin de compenser une situation d'infériorité conventionnelle sur le champ de bataille (cas du Pakistan face à l'Inde).

2 - Le caractère d'Etat détenteur de la Corée du Nord est discuté, dans la mesure où sa capacité à intégrer une tête nucléaire sur un vecteur n'est pas encore établie ; elle dispose ceci dit de capacités de fabrication de matières militaires, a réalisé plusieurs essais, possède un programme balistique très avancé et s'intéresse à la sortie d'eau de missiles tirés depuis des sous-marins.

1.2 – Une dynamique de modernisation des arsenaux nucléaires partout engagée

Les trois puissances nucléaires occidentales sont désormais toutes les trois engagées dans un mouvement de modernisation et de renouvellement de leurs moyens de dissuasion. Donald TRUMP vient de confirmer une modernisation ambitieuse de la triade nucléaire américaine, les Britanniques viennent de s'engager dans le programme d'un nouveau sous-marin lanceur d'engins, tandis que les accords anglo-américains de coopération dans le domaine nucléaire, conclus au début de l'ère atomique, ont été prorogés jusqu'en 2024. La France modernise quant à elle ses deux composantes et vient de lancer le programme de renouvellement de sa composante océanique (sous-marin de troisième génération et nouveau missile balistique). Elle poursuit en parallèle son programme de simulation, en partie en coopération avec le Royaume-Uni, et devrait prochainement s'engager dans un programme de renouvellement complet de sa composante aéroportée (porteur, vecteur et tête nucléaire). Ces efforts de modernisation et de renouvellement mobiliseront sur plusieurs années d'importantes ressources budgétaires.

Moscou modernise aussi ses moyens nucléaires de dissuasion et envisage pour eux des successeurs. Progressivement les forces sous-marines russes se redressent avec l'entrée en service opérationnel des sous-marins lanceurs d'engins *Boreï* équipés du missile *Boulava* ; elles devraient prochainement assurer à nouveau une permanence à la mer. Un nouveau bombardier stratégique devrait intégrer les forces nucléaires dans la seconde moitié de la décennie prochaine, tandis que sont développés les missiles sol-sol *Sarmat* et *Rubzeh* qui s'annoncent très performants. La trajectoire de redressement des forces nucléaires russes, entamée il y a une dizaine d'années, ne semble donc pas devoir s'achever.

Alors qu'elle s'apprête à mettre en service opérationnelle une composante océanique, la Chine modernise sa composante terrestre en renforçant sa capacité de survie (durcissement des installations, dispersion) et en améliorant sa performance en matière de pénétration. Alors qu'elle « mirve » certains de ses missiles (*DF 41* à 3 têtes aux essais) et qu'elle va se doter de sous-marins opérationnels, la Chine va devoir augmenter de manière quasi inéluctable le nombre de ses têtes nucléaires. Pékin voit déjà plus loin en communiquant sur la mise en service d'un planeur hypersonique, possiblement vecteur nucléaire, vers 2020 et sur l'arrivée d'un sous-marin, plus discret que l'actuel *Jin*, capable de lancer un missile d'une portée supérieure au *JL 2* d'aujourd'hui. Confrontée au vieillissement de ses têtes nucléaires et alors qu'un faible nombre d'essais a été réalisé, la dissuasion chinoise doit par ailleurs développer un important programme de simulation proche des standards occidentaux. Une ambitieuse démarche est lancée dans ce sens.

En 2016, l'Inde a mis en service opérationnel le SNLE *Arihant*, se dotant ainsi d'une triade nucléaire complète. Elle poursuit plusieurs programmes de missiles balistiques destinés à sa composante

océanique en devenir (missile *K 4* de 3 500 km de portée) et à sa composante terrestre (missiles de la famille Agni de portée allant jusqu'à 6 000 km environ). Le Pakistan a officialisé en retour, mi 2016, une commande de huit sous-marins chinois de la classe *Yuan* équipés d'un système de propulsion anaérobie. Ces submersibles, les plus silencieux de la marine chinoise, devraient être livrés à partir de 2028 et pourraient emporter un dérivé du missile de croisière *Babur*. La perspective de voir se concrétiser ce projet de composante océanique pakistanaise demeure cependant incertaine pour des raisons techniques, financières et politiques (contrôle gouvernemental). En parallèle, comme en témoigne l'essai réussi d'un premier missile « mirvé », l'*Ababeel*, début 2017, Islamabad cherche à améliorer les capacités de pénétration de sa composante terrestre, alors même que l'Inde développe des défenses anti-missiles.

La Corée du Nord ne dispose pas encore d'une capacité nucléaire opérationnelle mais elle affiche une ferme ambition en la matière et poursuit ses efforts pour y parvenir. S'agissant des vecteurs, Pyongyang s'active pour améliorer ses capacités sol-sol, notamment en portée, et se doter d'une capacité mer-sol.

1.3 – Des facteurs de fragilisation de la dissuasion nucléaire apparaissent néanmoins

Soutenue par 123 Etats sur les 177 ayant pris part au vote, une résolution autorisant l'entrée en négociation d'un traité d'interdiction des armes nucléaires a été adoptée en 2016 lors de l'assemblée générale des Nations unies. Les négociations ont débuté en mars 2017 avec pour objectif d'aboutir à un instrument juridiquement contraignant visant à interdire les armes nucléaires en vue de leur totale élimination. Cette démarche est historique et pourrait se révéler un paramètre structurant de la sécurité internationale pour les prochaines années. Il faut en effet s'attendre à voir apparaitre un instrument, dont la portée reste à définir, condamnant les armes nucléaires et les politiques de dissuasion. En parallèle de cette initiative politique, des oppositions se manifestent aussi sur le terrain moral et religieux. Le pape François s'est ainsi posé à plusieurs reprises en contempteur de la dissuasion nucléaire. Dans un discours prononcé en décembre 2014 à Vienne lors d'une conférence organisée par le mouvement des « conséquences humanitaires » à l'origine de la résolution des Nations unies, il indiquait que « *la dissuasion nucléaire et la menace de la destruction réciproque assurée ne peuvent pas être la base d'une éthique de la fraternité et de la coexistence pacifique* ». L'année suivante, à l'occasion du 70° anniversaire du bombardement d'Hiroshima, il réitérait cet avis et soulignait qu'il était « *urgent de travailler à un monde libre d'armes nucléaires* ».

L'agrégation de considérations morales au débat stratégique porte en elle le germe d'une fragilisation du soutien des opinions publiques aux politiques de dissuasion. Or, ce risque apparait au moment où se

profile dans les démocraties dotées de moyens nucléaires militaires la nécessité de mobiliser d'importantes ressources financières pour en assurer le maintien en condition, la modernisation et le renouvellement.

Sur un plan opérationnel, la vulnérabilité potentielle des forces nucléaires pourrait s'accroître dans un monde où se déploient des défenses anti-missiles et anti-aériennes de plus en plus performantes, où les cyber-attaques se développent et où par ailleurs ne cesse d'augmenter le nombre de sous-marins d'attaque. Le durcissement et l'enfouissement d'objectifs susceptibles de subir une frappe nucléaire (centres de pouvoir, de commandement et de communication, installations de production ou de stockage d'armes de destruction massive…) constituent par ailleurs une tendance qui impose, pour que le mécanisme de dissuasion fonctionne pleinement, de pouvoir frapper avec précision.

2 - Situation en 2030

2.1 – Une certaine continuité dans le panorama général de la dissuasion nucléaire

A l'horizon 2030, **le panorama général de la dissuasion nucléaire ne devrait pas être fondamentalement différent** de celui que nous observons actuellement. L'arme nucléaire demeurera de nature essentiellement politique et la crédibilité des forces la mettant en œuvre continuera de faire leur valeur dissuasive. Pour autant, ce pronostic « conservateur » n'exclue en rien que se produisent des évolutions significatives dans les quinze prochaines années en matière de dissuasion nucléaire.

Au chapitre des invariants stratégiques, la défense antimissile, pas plus qu'un autre moyen militaire, ne se sera imposée en 2030 comme une alternative crédible à la dissuasion nucléaire. La Russie et la Chine seront, comme aujourd'hui, les deux puissances majeures susceptibles de porter atteinte aux intérêts vitaux des Européens dans un contexte où la domination nucléaire des Etats-Unis ne devrait pas être remise en cause, ni même contestée sérieusement comme on a pu l'observer pendant les années de Guerre froide. Washington et Moscou seront de loin les détenteurs des arsenaux nucléaires les plus importants, suivis par les autres pays actuellement détenteurs d'armements nucléaires (Chine, France, Inde, Israël, Pakistan, Royaume-Uni) qui, collectivement, détiendront environ un millier de têtes. L'alliance atlantique devrait toujours être une alliance nucléaire s'appuyant en planification sur les moyens américains et britanniques si Londres mène à son terme le programme de renouvellement de sa flotte océanique. Un ou plusieurs des cinq alliés européens susceptibles de conduire

aujourd'hui des missions nucléaires avec des armes américaines (Allemagne, Pays-Bas, Belgique, Italie, Turquie) pourraient néanmoins s'être désengagés de la mission nucléaire. A l'exception de l'Allemagne, ceux restant impliqués dans cette mission pourront vraisemblablement disposer pour la conduire du *F 35* et d'une version modernisée de la bombe *B 61* dans une version modernisée (*B 61-12*). En Asie, la Corée du Nord, devenue une puissance nucléaire à part entière, continuera d'alimenter une insécurité régionale et sera probablement en mesure d'atteindre les Etats-Unis avec ses missiles balistiques, sauf si Washington parvient à l'empêcher d'une manière ou d'une autre, par la négociation ou la coercition.

Sur le plan capacitaire aussi, la situation ne devrait pas subir de bouleversement. S'agissant des vecteurs, **les missiles balistiques resteront dominants** dans les arsenaux nucléaires, essentiellement en version sol-sol hors d'Occident. La précision et la capacité à pénétrer les défenses des vecteurs seront améliorées tandis que plusieurs pays, Russie en particulier, aligneront des missiles de courte portée destinés à être employés sur le champ de bataille dans une logique de compensation d'une infériorité dans le domaine conventionnel. **L'apparition probable dans les arsenaux des premiers planeurs hypersoniques** libérés par des missiles balistiques à moyenne ou longue portée **pourrait en revanche s'avérer déstabilisante** par le fait que certains pays pourraient les utiliser en version conventionnelle (Etats-Unis) et d'autres en version nucléaire (Chine) créant ainsi un risque de méprise aujourd'hui inexistant.

Pour autant, au-delà de ces données invariantes ou presque, on ne saurait retrouver en 2030 un état général des forces nucléaires figé par rapport à celui d'aujourd'hui. Une première évolution marquante devrait être celle d'une réduction en quantité et, dans une moindre mesure, en qualité de l'écart entre les arsenaux nucléaires des grandes puissances nucléaires (Etats-Unis, Russie, France et possiblement Royaume-Uni) et les autres. Par rapport à la situation actuelle, de nouveaux pays seront probablement en mesure de frapper l'Europe avec un nombre accru, mais néanmoins modeste, de missiles balistiques qui auront par ailleurs gagné en performance. Mais, à l'échéance considérée, l'Europe devrait disposer, face à cette menace, qui restera mesurée, d'une défense antimissile otanienne des territoires et des populations efficace. Cette situation ne sera pas l'apanage de l'Europe, placée en la circonstance largement sous la protection américaine, mais aussi de l'Amérique du Nord, de la Chine et de la Russie, qui disposeront en 2030 de systèmes complets de défenses anti-missiles balistiques que les vecteurs nucléaires envisagés pour dissuader ces pays devront pouvoir pénétrer pour rester crédibles.

Il est par ailleurs vraisemblable que l'évolution des sociétés conduise en 2030 les Etats officiellement dotés à rechercher une maîtrise accrue des effets d'une frappe nucléaire, privilégiant ainsi, dans leur doctrine de dissuasion, l'option de frappes précises sur des centres névralgiques.

L'Iran aura en 2030 activement poursuivi son programme balistique et disposera de missiles capables d'atteindre l'Europe occidentale. Il est possible, qu'à cette échéance, Téhéran, libéré des contraintes

de l'accord P 5+1[3] de 2015, cherche en parallèle à se doter d'armes nucléaires. Cette éventualité, si elle se concrétisait, aurait un fort effet déstabilisateur sur la région, l'Arabie saoudite ne restant sans doute pas inerte face à ce basculement stratégique. Le risque d'un effondrement du régime de non-prolifération nucléaire serait alors maximal. On observerait vraisemblablement dans cette hypothèse une augmentation du nombre des arsenaux dans un contexte d'instabilité généralisée.

Pour compléter le tableau, il ne faut pas exclure d'ici 2030 la conduite par les Etats qui n'ont pas démantelé leurs installations *ad hoc* **de quelques essais nucléaires**. Ce pourrait être le fait des Etats-Unis dans une logique de sécurité, en cas de découverte d'un grave défaut sur les têtes en dotation, de la Chine pour accéder à des formules robustes, de la Russie, de l'Inde et du Pakistan pour concevoir des armes nouvelles.

2.2 – Les forces nucléaires occidentales à l'aube d'un renouveau

La cinétique des grands programmes d'armement, en particulier de ceux participant à la dissuasion, est lente. Cette caractéristique permet de disposer dès maintenant d'une vision assez précise des moyens dont seront dotées vers 2030 les forces nucléaires occidentales. On sait ainsi que, dans la première moitié de la décennie 2030, les marines américaine, britannique et française s'apprêteront à mettre en service un nouveau type de sous-marin lanceur d'engins (SNLE) de manière quasi simultanée. La période marquera plus généralement pour les pays du P3 (Etats-Unis, France, Royaume-Uni) le remplacement d'une génération de moyens par une autre.

a) Etats-Unis

Le premier des 14 SNLE « *Ohio* » arrivant en fin de vie en 2027, un nouveau SNLE baptisé « *Columbia* » devra être mis en service en 2029 afin de maintenir un format de flotte opérationnelle à 12 navires. Ce sous-marin se caractérisera par une configuration à 16 tubes (24 tubes sur les « *Ohio* ») et le choix d'une chaufferie nucléaire qui ne nécessitera pas de changement du combustible pendant toute la durée de vie prévue pour le navire (42 ans). Le Congrès évalue le coût du programme pour 12 sous-marins à environ 100 Md$. Les missiles *Trident IID5*, déjà embarqués sur les « *Ohio* », devraient être prolongés jusqu'en 2042.

Les 400 *Minuteman III* de la composante terrestre américaine sont actuellement modernisés afin de rester en service jusque dans la décennie 2030. Au-delà de cet horizon, plusieurs options sont envisagées mais la plus crédible semble être celle de la mise en service d'un nouveau type d'ICBM tiré depuis un silo. Pour que celui-ci soit opérationnel en 2030, l'USAF estime qu'un nouveau programme devra être lancé en 2018.

S'agissant de la composante aéroportée, il est prévu de mettre en service vers 2025

3 - Etats-Unis, Russie, Chine, Royaume-Uni, France et Allemagne.

un nouveau bombardier stratégique furtif (*B 21*) capable d'emporter un nouveau missile de croisière nucléaire (*LRSO*[4]) attendu pour 2028. La programmation prévoit également de moderniser la flotte de *B 52H*, pour qu'elle puisse durer jusque vers 2040 et la rendre compatible avec l'emport du *LRSO*, et d'adapter les *B 2* à l'emport de nouvelles armes nucléaires (*B 61-12* et *LRSO*).

b) Royaume-Uni

Le Parlement britannique a approuvé en 2016 le renouvellement des moyens de la dissuasion réunis dans une unique composante océanique. Les nouveaux SNLE de la classe « *Dreadnought* » devraient en principe remplacer à partir de 2030 les actuels « *Vanguard* ». Le compartiment missile sera commun au « *Dreadnought* » et au « *Columbia* » américain.

Selon le ministère britannique de la défense, le programme « *Dreadnought* » devrait mobiliser 40 milliards d'euros sur 20 ans (avec une provision pour risques évaluée en 2015 à 11 milliards d'euros).

En vertu des accords de Nassau (1963), des missiles américains *Trident* seront embarqués à bord des SNLE de la *Royal Navy*. Ces missiles emporteront, au moins jusqu'à la fin de la décennie 2030, les têtes nucléaires britanniques actuellement déployées.

La future flotte des quatre « *Dreadnought* » maintiendra une permanence à la mer d'un SNLE équipé d'un maximum de 8 missiles opérationnels emportant 40 têtes. Le nombre de têtes opérationnelles ne dépassera pas 120 têtes nucléaires, tandis que le stock global d'armes ne dépassera pas 180 à partir du milieu de la décennie 2020.

c) France

En 2030, la deuxième génération des moyens de la dissuasion nucléaire française articulée autour de deux composantes, océanique et aéroportée, approchera de sa fin de vie. Le plus ancien des quatre SNLE actuels devrait être remplacé à partir de 2030 pour assurer une permanence à la mer, tandis que le couple *Rafale-ASMPA* de la composante aéroportée sera opérationnel jusqu'en 2035. Au-delà de ces échéances, le maintien des deux composantes dans une logique de complémentarité non hiérarchisée est prévu.

S'agissant de la composante océanique, la troisième génération de SNLE devrait schématiquement couvrir la période 2030-2080. Une flotte de quatre sous-marins, proches dans leur tonnage des SNLE actuels et emportant une version évoluée du missile *M 51*, est prévue.

La composante aéroportée pourrait à partir de 2035 mettre en œuvre un missile hypersonique emporté par un avion de combat, un porteur lourd ou un drone furtif. Une orientation sur ce point est attendue à l'horizon des cinq prochaines années.

4 - *LRSO : Long Range Stand Off.*

2.1 – Des vecteurs nucléaires confrontés à des défis plus robustes

Alors qu'actuellement, cinq pays disposent d'une composante sous-marine de dissuasion nucléaire (Etats-Unis, Russie, Chine, France, Royaume-Uni), il y en aura, à l'horizon 2030, sept (Inde, Israël) et peut-être jusqu'à neuf (Corée du Nord, Pakistan). Les sous-marins lanceurs d'engins seront donc plus nombreux et probablement confrontés, davantage qu'aujourd'hui, aux performances des moyens de lutte anti sous-marine et à l'accroissement du nombre de sous-marins d'attaque, tout particulièrement dans l'océan Indien et dans le Pacifique. Les vecteurs aériens seront, comme depuis les origines de la dissuasion, confrontés à des défenses anti-aériennes et des chasseurs particulièrement efficaces. La multiplication des radars de veille lointaine et la mise en réseau de ces systèmes défensifs exigeront, selon un schéma traditionnel, un haut degré de performance de la part des composantes aéroportées de la dissuasion.

Si les SNLE évolueront en 2030 dans un environnement plus contesté, ceux d'entre eux propulsés par une chaufferie nucléaire seront toujours furtifs à cette échéance. Le concept de « mer transparente », selon lequel les SNLE perdraient leur furtivité, n'a pas de sens à l'échéance de 2030. L'idée, çà et là avancée, d'une détection des SNLE par celle des neutrinos émis par leurs chaufferies nucléaires apparait en particulier irréaliste à cet horizon. Les neutrinos sont des particules nucléaires produites en quantité sensiblement égale à celle des neutrons dans un réacteur nucléaire. Alors que ces derniers restent confinés dans le réacteur, la quasi-totalité des neutrinos s'échappe vers l'extérieur et parcourt une distance immense à l'échelle mondiale, d'où l'idée de détection évoquée plus haut. Ces particules complexes ont été détectées une première fois en Californie au début des années 2000 et le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) les étudie depuis. Cet organisme considère envisageable de détecter d'ores et déjà quelques neutrinos en se plaçant à proximité immédiate d'un sous-marin à propulsion nucléaire immobile, et ce avec un appareillage complexe. En revanche, le CEA considère totalement impossible aujourd'hui et pour longtemps encore de réaliser cette détection en ambiance opérationnelle sur un sous-marin en pleine mer.

En Asie, la Chine et l'Inde disposeront en 2030 de défenses anti-missiles balistiques (DAMB) indigènes capables de prendre à partie des vecteurs nucléaires. Sur un plan régional, l'équation stratégique qui lie ces deux pays avec le Pakistan, qui devrait avoir pris du retard en matière de DAMB, s'en trouvera nécessairement affectée. Au-delà, vouloir dissuader Pékin imposera de disposer des moyens capables de pénétrer avec certitude sa DAMB. Les Etats-Unis continueront aussi de déployer en Asie des moyens défensifs de cette nature pour leur propre compte (bases militaires, groupe aéronaval…) ou dans le cadre des garanties de sécurité que Washington apporte à ses alliés asiatiques (Japon, Corée du Sud, Taïwan). Ils le feront aussi sur leur territoire en les tournant vers l'Asie ce qui poussera une Chine à la recherche d'une garantie de frappe en second à rendre plus nombreux et plus performants ses vecteurs nucléaires.

Vu de Moscou, la présence de défenses anti-missiles balistiques multicouches aux Etats-Unis et sur le territoire des alliés en Europe devrait continuer d'être un irritant malgré les efforts entrepris sur le plan diplomatique et les réalités techniques de ces systèmes, qui ne sont pas de nature à pouvoir neutraliser les missiles stratégiques russes. Plus qu'une considération stratégique, il y a sans doute dans l'opposition ferme des Russes aux initiatives des alliés en matière de DAMB une part de frustration issue du déclassement militaire subi après l'effondrement de l'Union soviétique. Quoi qu'il en soit, Moscou aura produit les efforts nécessaires pour disposer également en 2030 d'une DAMB cohérente et efficace qui devra être prise en compte par les dissuasions occidentales.

2.4 – Débat moral et forme non nucléaire de dissuasion

Durant la Guerre froide, le Vatican a, en quelque sorte, mis sous le boisseau ses convictions profondes vis-à-vis de la dissuasion nucléaire. L'Eglise catholique a considéré, au vu de la menace représentée par l'Union soviétique communiste, qu'elle pouvait, au moins tant que cette menace perdurait, tolérer, sinon approuver explicitement, la rhétorique de la dissuasion nucléaire. La déliquescence du bloc soviétique et de ses alliés du Pacte de Varsovie a changé la donne dans les années quatre-vingt-dix et a libéré la parole des autorités catholiques qui ont aligné leur position sur celle de l'Eglise protestante pour condamner la dissuasion. C'est dans ce contexte qu'a pu prospérer, au-delà des enceintes religieuses, l'idée d'une interdiction totale des armes nucléaires qui pourrait entamer, dans les prochaines années, le soutien des peuples aux politiques de dissuasion nucléaire. Pour autant, à l'horizon 2030, une forme de résurgence de la menace russe vis-à-vis de l'Occident et la montée en puissance teintée de nationalisme de la Chine devraient contribuer à réinstaller un sentiment de vulnérabilité dans les sociétés occidentales qui devrait aller dans le sens d'un soutien plus ferme qu'aujourd'hui à la dissuasion nucléaire.

En 2030, il sera, selon toute vraisemblance, possible d'atteindre les intérêts vitaux d'un pays par le biais de cyberattaques. Dès lors, la question de la place de la dissuasion – nucléaire ou non – vis-à-vis de ce péril devra être traitée. L'écueil de la difficulté à attribuer ces attaques devra avoir été levé, ce que l'on peut supposer, pour que puisse jouer dans le cyberespace la grammaire de la dissuasion. D'ici là, un effort collectif devrait avoir été mené qui pourrait avoir débouché en 2030 sur une définition partagée de ce qu'est un « comportement inacceptable » dans le cyberespace.

3 - Scenarii alternatifs

3.1 – Le Royaume-Uni renonce à la dissuasion nucléaire

Avec la sortie du Royaume-Uni de l'Union européenne, la perspective d'une indépendance écossaise devient plus crédible. Les autorités écossaises ayant clairement indiqué leur souhait de ne plus accueillir sur leur territoire la force sous-marine stratégique britannique, Londres devrait soit recréer à grand frais en Angleterre une nouvelle infrastructure pour ses sous-marins nucléaires, soit s'appuyer sur les moyens américains, soit renoncer à la mission de dissuasion. Dans cette dernière hypothèse, la dissuasion française, devenue la seule dissuasion nationale en Europe, deviendrait plus exposée. Sa singularité pourrait susciter une dynamique de remise en cause ou au contraire de valorisation. En cas d'abandon britannique de la dissuasion, la coopération avec Londres dans le domaine de la simulation, établie par les accords de Lancaster House de 2010, cesserait et la France devrait compenser la perte de la part financière versée par les Britanniques dans cette coopération.

3.2 – Une Russie en faillite économique ou devenue démocratique

Frappée successivement par la crise économique et financière de 2008, puis par la baisse des prix du pétrole et les sanctions décrétées après l'annexion de la Crimée en 2014, l'économie russe pourrait s'effondrer d'ici 2030. Celle-ci est en effet affectée par des fragilités structurelles, en particulier une corruption endémique et une extrême dépendance aux exportations de matières premières, qui pourraient jouer sous l'effet de stimuli relativement modérés. Dans cette hypothèse, le plan de modernisation de l'appareil militaire lancé par Vladimir POUTINE dans la décennie 2010 ne serait pas mené à son terme et le simple maintien en condition opérationnelle des forces ne pourrait même être assuré. La dissuasion russe s'en ressentirait avec l'abandon de toute velléité de permanence à la mer des sous-marins lanceurs d'engins et une sous-activité de l'aviation stratégique. La défense anti-missile dans toutes ses fonctions (alerte avancée, veille, interception) se trouverait très dégradée. La crise économique pourrait engendrer une déstabilisation du régime qui serait amené à réprimer durement les manifestations populaires. On reviendrait, sur le plan stratégique, à une situation comparable à celle ayant suivi l'effondrement de l'Union soviétique, avec une réduction de la menace militaire russe. Certaines puissances nucléaires occidentales pourraient alors revoir le niveau d'ambition de leur dissuasion ; la dimension nucléaire de l'OTAN pourrait être aussi remise en cause.

Un autre scénario possible à l'horizon 2030 est celui d'une évolution politique franche de la Russie en direction de la démocratie. Cette nouvelle trajectoire politique russe serait plus favorable aux intérêts occidentaux et ouvrirait la perspective d'un partenariat stratégique entre Moscou, l'Europe et les Etats-Unis. Cette évolution vers des relations apaisées entre la Russie et le monde occidental viendrait affaiblir la justification de la dissuasion nucléaire, en particulier en Europe, et renforcerait la dynamique d'interdiction des armes nucléaires fondées sur des arguments moraux, religieux et humanitaire. A tout le moins, la question d'une diminution des arsenaux nucléaires en Occident s'ouvrirait dans cette hypothèse, a fortiori si aucune nouvelle menace sérieuse n'était perçue. Certains gouvernements occidentaux pourraient vouloir « toucher les dividendes de la paix ».

3.3 – Le régime de Pyongyang disparait ou est déclassé

Le scénario le plus probable à l'horizon 2030 est celui de deux Corées avec une Corée du Nord totalitaire, nucléaire et représentant une menace régionale. Toutefois, il ne peut être exclu que le régime actuel, comme tout régime dictatorial, soit renversé ou ne s'effondre sur lui-même. Un affaiblissement du soutien apporté par Pékin à Pyongyang accroitrait significativement la probabilité d'occurrence d'un tel scénario. La réalisation de cette hypothèse constituerait un facteur important d'apaisement de la situation stratégique en Asie.

De même, on ne peut écarter l'hypothèse d'actions préventives sur le potentiel nucléaire militaire nord-coréen qui, nonobstant leurs risques, déclasseraient néanmoins le régime de Pyongyang sur le plan stratégique.

5

Terrorisme et menaces NRBC : vers un terrorisme technologique ?

L'essentiel

Le niveau de menace terroriste reste significativement élevé du fait de l'action continue d'*Al Qaïda* et des capacités réunies par *Daech*. Le recours à des modes d'actions de plus en plus variés (maîtrise des technologies) et violents, en application d'une doctrine globale de conquête, font du terrorisme international d'inspiration jihadiste une menace difficile à contrer.

Dans l'optique d'accroître encore leur potentiel de nuisance, les groupes terroristes affirment leur volonté d'acquérir tout type de substances nucléaire, radiologique, biologique et chimique (NRBC) susceptibles d'aggraver les conséquences d'un attentat. Cette évolution de la menace, qui inclut des effets potentiels de déstabilisation extrêmement grave sur notre société, doit être prise en compte dès maintenant pour être en mesure de la parer.

Notre pays met en œuvre des dispositifs d'alerte, de prévention, de protection et d'intervention adaptés. La menace NRBC et les risques associés nécessitent la prise en compte dans leurs spécificités et un renforcement adapté de la réponse.

Les attentats perpétrés en France et en Europe depuis 2015 font du sol européen un théâtre ciblé de l'action du terrorisme international. Bien que l'Europe ait déjà connu des vagues terroristes, notamment dans les années quatre-vingt puis quatre-vingt-dix pour la France, et au début des années 2000 pour l'Espagne et le Royaume-Uni, la combinaison de modes opératoires nouveaux, leur répétition, l'implication accrue d'acteurs locaux et le nombre élevé de victimes sont inédits. L'action terroriste est ainsi aujourd'hui perçue par nos compatriotes comme la principale menace, notamment sur le territoire national.

A la suite des attentats du 11 septembre 2001, l'Union européenne (UE) a défini le terrorisme comme « un acte commis dans le but de gravement intimider une population, ou de contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque, ou de gravement déstabiliser des structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou d'une organisation internationale »[1].

La France a de son côté largement légiféré depuis 1986, évitant cependant de créer un régime dérogatoire, définissant le terrorisme comme une « circonstance aggravante » de toute infraction commise « intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur » d'une part, et d'autre part en introduisant dès 1996 l'infraction d'association de malfaiteurs en vue de la préparation d'actes de terrorisme permettant de démanteler les groupes avant tout passage à l'acte[2].

1 - Article 421-2-1 et 421-6 du code pénal.

2 - Article 421-2-1 et 421-6 du code pénal.

Le niveau de menace terroriste a significativement augmenté du fait de celle portée de façon continue par *Al Qaïda*, conjuguée à l'essor de *Daech*. La structuration de la scène jihadiste autour de deux pôles rivaux a contribué à une surenchère terroriste au niveau mondial, rendant la menace à la fois plus complexe à appréhender et à contrer. Les attentats de 2015 ont marqué un tournant tant par leurs intentions que par leur multiplication, la France étant explicitement désignée comme un objectif prioritaire pour les jihadistes.

Dans le même temps, la volonté manifeste de certains groupes terroristes d'acquérir tout type de substances nucléaire, radiologique, biologique et chimique (NRBC) afin de réaliser des armes qui seront présentées comme des armes de destruction massive fait l'objet d'une acuité particulière. Elles trouveraient leur place dans une panoplie destinée à décliner un large éventail d'attaques rudimentaires, technologiques ou systémiques.

La France dispose des compétences et des moyens lui permettant de comprendre et de faire face à la menace. Mais les forces qui sont à l'œuvre sont multiples : dynamique politique des groupes terroristes, diffusion des connaissances techniques, capacité de réaction des partenaires. Face à ce constat, la capacité de la France à faire face à une menace terroriste renforcée à l'horizon 2030, capable de décupler ses capacités de nuisance via le recours à des substances NRBC, est posée.

1 - Etat des lieux en 2017

1.1 – Une menace terroriste durablement très élevée pour la France et l'Europe

La structure et les fragilités de la société française ainsi que la fermeté de l'engagement de la France dans la lutte contre le terrorisme la désignent comme une cible même si notre pays n'est pas le seul visé en Europe, comme en témoignent les attentats de Bruxelles (22 mars 2016), Berlin (19 décembre 2016), Londres (22 mars 2017, Stockholm (7 avril 2017) et Paris (20 avril 2017). La propagande entretenue contre notre pays incite à commettre des attentats planifiés ou des attaques spontanées contre nos ressortissants et nos intérêts. Elle s'est traduite par la vague d'attentats qui a frappé la France en 2015 et 2016 et la préparation d'attentats déjoués (17 au cours de l'année 2016).

Cette menace s'inscrit dans la durée, *Daech* pouvant recourir à un vivier opérationnel de partisans sur le sol européen, coordonnés à distance depuis le Levant. Par ailleurs, si le flux de combattants français partant rejoindre la « terre du jihad » s'est réduit au cours de l'année 2016, l'organisation terroriste a su adapter sa propagande en incitant ses partisans à agir isolément sur

le sol français. Efficacement relayés par les réseaux sociaux ainsi que par la diffusion de magazines et de vidéos glorifiant l'acte kamikaze, ces appels ciblent la mouvance endogène afin de la mobiliser pour la commission d'attaques. Le recours aux modes d'action peu élaborés constatés récemment (Magnanville, Saint-Etienne du Rouvray, Nice, Berlin, Londres, Stockholm) est la marque de fabrique de cette forme de terrorisme.

1.2 – La menace extérieure

La structuration de la scène jihadiste en deux pôles rivaux contribue à une surenchère de la menace terroriste au niveau mondial. Celle-ci s'exprime à travers la volonté de ces groupes d'étendre leur zone d'influence, profitant de l'effondrement ou de la faiblesse des Etats, de la porosité de leurs frontières et de l'absence de contrôle pour s'implanter dans des zones de non-droit au Sahel (Nord-Mali), en Afrique du Nord (Libye), au Levant (Irak, Syrie), dans la péninsule arabique (Yémen), jusqu'à la Corne de l'Afrique, ainsi que dans le sous-continent indien et l'Afghanistan où *Daech* (*wilaya du Khorassan*) s'est récemment implanté.

Au Sahel, la menace terroriste s'est notamment illustrée par les attaques d'ampleur menées à Bamako en novembre 2015, à Ouagadougou en janvier 2016, et en Côte d'Ivoire en mars 2016, ainsi que par une multiplication des actions au Mali contre les forces de défense et de sécurité maliennes[3] et les forces françaises et internationales (forces *BARKHANE* et forces de la mission *MINUSMA* des Nations unies).

En Libye, comme au Levant, en dépit de pertes territoriales et humaines croissantes, les combattants jihadistes disséminés maintiennent une réelle capacité de projection de la menace vers les pays voisins mais également l'Europe.

Au second plan aujourd'hui sur la scène du terrorisme à l'encontre des intérêts occidentaux, l'Afghanistan demeure une source de préoccupation. La récente implantation de *Daech* et son expansion pourraient permettre à l'organisation de se reconstituer un refuge dans un pays qui était déjà un sanctuaire pour *Al Qaïda*. A plus long terme, le terrorisme fondamentaliste pourrait établir ses bases dans l'extrême Sud des Philippines et de certaines parties du territoire indonésien. Les Maldives, les Seychelles, et à une toute autre échelle le Bangladesh, sont également des sujets de vigilance.

3 - Le 18 janvier dernier le groupe *Al Mourabitoune* a frappé les éléments des forces armées maliennes et les troupes de la Coordination et de la Plateforme, réunis à Gao en vue de conduire leur première patrouille mixte. Cet attentat-suicide, qui a tué 84 hommes, a visé directement le processus de l'Accord de paix et de réconciliation.

1.3 – La course aux armes de destruction massive

Les groupes terroristes cherchent activement à se doter de moyens nucléaires, radiologiques, biologiques ou chimiques, pour accréditer l'idée qu'ils disposent d'armes de destruction massive.

Pour chacun des types de substances concernés, des exemples existent qui laissent deviner une stratégie de développement vers un terrorisme à plus fort contenu technologique, au-delà des armes rudimentaires telles que celles de petit calibre ou les explosifs. Les armes de destruction massive sont l'une des conséquences du progrès technologique dont l'Occident est le berceau. Pour un terroriste, laisser penser que l'on dispose de moyens dont la possession était l'apanage des seuls Etats et que l'on peut les retourner contre leurs inventeurs constitue en soi un véritable enjeu stratégique.

Les centrales de Tihange et de Doel, le *Centre d'études nucléaires* (CEN) de Mol et l'*Institut national des radioéléments* de Fleurus ont aussi été à diverses reprises cités depuis 2014 dans le cadre d'enquêtes sur la menace terroriste jihadiste en Europe occidentale.

Des tentatives de récupération de matière fissile sur le marché noir en Europe de l'Est par *Daech* ont par ailleurs été révélées en 2016 par la police bulgare. En outre, *Daech* aurait tenté de se procurer des sources radiologiques utilisées à des fins médicales pour réaliser des bombes sales. Enfin, ce même groupe a mis en œuvre une capacité de production et de vectorisation de l'ypérite (ou gaz moutarde) lors des combats en zone syro-irakienne. En revanche, il n'est pas parvenu à exporter de tels produits vers l'Europe.

Les substances NRBC employées sur les théâtres de conflit par *Daech* n'ont pu servir jusqu'à présent qu'à la confection d'armes tactiques, destinées à déstabiliser l'adversaire par une action avant tout psychologique et désorganisatrice. Ces armes n'ont pas encore permis d'atteindre l'effet de masse recherché. Cependant, forts de cette expérience, on peut craindre une exportation de savoir-faire par *Daech*. Le but recherché serait l'effet de panique des populations et de désorganisation des sociétés.

Les groupes terroristes ont par ailleurs développé une maîtrise des usages d'Internet, dont ils se servent non seulement pour leurs opérations de propagande et de recrutement, mais aussi pour le transfert et la captation des connaissances nécessaires au développement et à la fabrication d'armes (les intangibles).

1.4 – Nos moyens de protection contre la menace NRBC

Dans le domaine de la défense, la menace NRBC n'est pas nouvelle. La défense NRBC suit une démarche prudentielle : la faible probabilité de survenue d'une attaque est à rapprocher de ses conséquences potentiellement désastreuses. Cette assurance coûte entre 1 et 3 % de l'effort global de défense (équipements, effectifs et R&D). La défense NRBC ne se limite pas à l'équipement et à la protection des forces combattantes. Elle revêt un aspect de souveraineté en permettant à l'Etat français de disposer d'une autonomie d'appréciation des situations NRBC, comme peu d'autres Etats en disposent.

L'expérience du ministère de la défense bénéficie aux autres acteurs, comme par exemple la sécurité civile. Le centre national civil et militaire de formation et d'entraînement NRBC-E[4], dont la mission est d'améliorer, en appliquant les doctrines nationales, la capacité de réponse des services de l'Etat aux menaces NRBC, est un exemple de coopération civilo-militaire réussie et rendue nécessaire par l'évolution du contexte sécuritaire.

La réponse à la menace terroriste ne peut être qu'interministérielle. Progressivement en effet, la protection du territoire et de la population a pris plus d'importance. Issu en 2010 des plans Piratox (terrorisme chimique), Biotox (terrorisme biologique) et Piratome (terrorisme nucléaire ou radiologique), le plan gouvernemental « NRBC » a été récemment révisé. Cet outil d'aide à la décision au profit du Premier ministre recense l'ensemble des mesures permettant de gérer une crise de nature NRBC.

Le programme interministériel de R&D contre les menaces terroristes NRBC-E, conduit par le commissariat à l'énergie atomique et aux énergies alternatives, est devenu dix ans après son lancement une référence en matière de développement de produits pour lesquels un besoin opérationnel a été identifié. Citons par exemple le développement en urgence d'un test de diagnostic rapide du virus *EBOLA* ou celui d'un système miniaturisé de prélèvement et de concentration de gaz.

Les besoins devraient croître de manière régulière et conduire au développement d'une ou plusieurs structures de l'Etat compétentes en matière de soutien à la recherche et technologie, de recueil des besoins, de spécification et d'acquisition d'équipements spécialisés. De tels investissements devront s'inscrire durablement dans le budget de l'Etat. A cette fin, dans le domaine de la lutte contre le terrorisme et de sa prévention, l'Etat pourrait s'inspirer des outils de programmation financière pluriannuel développés pour la défense.

Avec le maintien durable d'efforts en de nombreux domaines, la France dispose d'atouts technologiques mais aussi historiques, administratifs, industriels et commerciaux pour lui permettre de faire face au développement éventuel d'un terrorisme NRBC.

Cependant, la technologie ne constitue que l'un des éléments de la réponse. Le comportement des populations – qui ne connaissent plus la guerre – en situation de stress aggravé et durable, constitue un enjeu sociétal susceptible d'affecter directement l'organisation politique mais aussi administrative des sociétés européennes, et donc leur résilience.

4 - NRBC-E : Nucléaire, radiologique, biologique, chimique et explosif.

2 - Situation en 2030

2.1 – La persistance du terrorisme

L'intensité des crises actuelles ne laisse pas augurer d'amélioration de la situation du terrorisme international. L'éradication de celui-ci s'inscrit dans le long terme. La fragilité durable de certains Etats du Sahel, d'Afrique du Nord et de l'Ouest ou du Moyen-Orient, le chaos sécuritaire et politique du « Sunnistan » syro-irakien ne seront pas surmontés d'ici 15 ans. Il en va de même de l'expansion analogue du phénomène jihadiste. L'absence de perspectives solides de développement économique, susceptibles de distraire les franges les plus fragiles de la population mondiale de la spirale de la radicalité, nourrira encore le terrorisme. **La menace terroriste devrait se maintenir jusqu'à l'horizon 2030.** De nouvelles dégradations de la situation sécuritaire dans les zones de crise, notamment en Afrique de l'Ouest et du Nord, pourraient même accroître le niveau de la menace terroriste pour la France et l'Europe.

Lorsque *Daech* perdra son assise territoriale au Levant, il se confondra dans la nébuleuse des organisations terroristes. Sa capacité organisationnelle sera diminuée mais ses autres dimensions perdureront sans doute. Au-delà de la doctrine islamiste, *Daech* s'adresse à tous ceux, qui d'une manière ou d'une autre, peuvent vouloir combattre nos sociétés. Le mouvement devrait ainsi conserver plusieurs années encore toute son attractivité.

Les facteurs qui rendent aujourd'hui l'Europe vulnérable devraient persister. Les problématiques d'intégration de communautés d'origine étrangère, la proximité géographique avec le Moyen-Orient et l'Afrique et la poursuite de ses engagements extérieurs en seront les causes. D'ici 2030, nos sociétés pourraient ainsi subir d'autres attaques terroristes de la part de nouveaux acteurs radicaux.

2.2 – La mise en œuvre d'armes NRBC

Le recours par les organisations terroristes aux modes d'action peu élaborés devrait se poursuivre, reposant sur la fanatisation des esprits et l'accès facile aux armes de contrebande ou aux explosifs. **Un saut technologique de ces organisations vers des armes plus élaborées est néanmoins tout à fait concevable.** D'ici 2030, les groupes terroristes pourraient chercher à recruter des experts NRBC, d'autant plus que le bagage scientifique et technique des combattants de demain devrait s'accroître (lors de la dernière vague de combattants partis rejoindre les rangs de *Daech* au Levant, de nombreux ingénieurs et informaticiens ont été signalés). L'inscription à des cours en ligne de jeunes, grâce au développement des *Massive Open Online*

Courses (MOOCS), désirant s'engager dans le jihad leur permettra vraisemblablement d'accéder aux connaissances techniques indispensables à la fabrication d'armes NRBC.

En décembre 2016, l'AIEA a rappelé que le **vol de matières nucléaires** ou radiologiques et l'attaque directe des sites de production électronucléaire constituaient les deux volets du terrorisme nucléaire. La bombe à dispersion de matières radioactives (qui mélange explosifs traditionnels et produits radioactifs, dite bombe sale) est particulièrement dangereuse, mais lesdites matières (médicales et industrielles, pièces irradiées ou déchets de centrales) font l'objet d'un contrôle étroit qui rend leur possession difficile. La protection des 58 réacteurs français revêt donc une importance toute particulière.

Une **utilisation d'armes chimiques sur le territoire national** (sur le modèle de la secte *Aum* à l'origine d'un attentat au gaz sarin dans le métro de Tokyo en 1995) par des groupes jihadistes ou d'autres radicaux pourrait avoir de lourdes conséquences. La fabrication de substances chimiques nocives de qualité moyenne ne requiert en effet pas de moyens particulièrement difficiles à acquérir ou à opérer.

Pour ce qui concerne les **mésusages des applications de la biologie,** le développement de laboratoires de confinement biologique à travers le monde pour de louables motifs d'ordre sanitaire pose la question de la sécurité de la conservation et du transport des souches. Un candidat au martyr pourrait être infecté d'une ou plusieurs maladies contagieuses et passer les contrôles sanitaires aux frontières sans difficulté en période d'incubation. L'amélioration des techniques de construction de génomes par biologie de synthèse pose par ailleurs la question de la possibilité de recréer des microorganismes déjà existants ou ayant existé dans la nature, notamment des virus dont la virulence et la contagiosité pourraient présenter de réels risques pour la sécurité sanitaire des populations (comme celui du virus de la variole et du virus Ebola). Le délai d'exécution est de plusieurs semaines, et le coût diminue rapidement. La multiplication des sociétés privées maîtrisant ces technologies pour produire « à façon » des gènes de synthèse, ainsi que le développement des *Fablab* et autres mutualisations/productions de recherche spontanée et plateformes coopératives, pose une vraie question de sûreté et de prolifération potentielle. De plus, les séquences des virus pathogènes, comme celui du virus de la variole et du virus Ebola, sont accessibles sur des bases de données publiques.

De manière plus transversale, le développement de la **fabrication additive (impression 3D) offre plusieurs champs d'application pour le terrorisme.** Ainsi, selon la presse spécialisée, un camp de réfugiés en Syrie a été frappé par une mini bombe dont l'expertise a révélé qu'une partie de ses composants avait été réalisée au moyen d'imprimantes 3D, *via* des modèles numériques conçus par des sympathisants occidentaux et qui avaient été téléchargés depuis Internet.

2.3 – Le cas particulier d'un acte de terrorisme radiologique et nucléaire

Le terrorisme radiologique au moyen d'une bombe sale est un scénario certes catastrophique mais identifié et gérable. Il repose sur la dissémination de matières radioactives présentes dans certaines sources radiologiques (instrument d'imagerie médicale et certains composants présents dans les balises de navigation aérienne d'ancienne génération). Des vols de ce type de source ont eu lieu. Pour autant, **les conséquences d'attentats réalisés avec ces sources demeureraient limitées** et pas foncièrement plus spectaculaires que celles d'attentats perpétrés avec des substances chimiques toxiques, au demeurant plus accessibles et aisées à employer.

Un acte de terrorisme nucléaire utilisant une arme dérobée dans un arsenal mal surveillé serait d'une toute autre portée, tout en étant beaucoup moins probable et complexe à perpétrer. Gardons en mémoire, sans sombrer dans le sensationnalisme, que la possibilité d'égarer des armes n'est pas une fiction. En 2007, six armes nucléaires américaines ont échappé pendant 36 heures à tout contrôle gouvernemental et l'on se souvient que le général russe Alexandre LEBED avait signalé que son pays avait perdu la trace de certaines armes portables fabriquées dans les années 1970. Aujourd'hui, la sécurisation de l'arsenal pakistanais fait notamment l'objet de préoccupations.

2.4 – Le potentiel de désorganisation de la société

La nature duale des nouvelles technologies induit des fragilités inédites, voire des risques de rupture stratégique difficilement prévisibles. Même si les évolutions technologiques, particulièrement rapides, rendent difficile une évaluation précise de ce qu'elles pourront être dans 15 ans, l'utilisation du cyberespace pour l'attaque terroriste d'infrastructures vitales doit être envisagée comme un mode d'action probable. Il est possible que des acteurs terroristes entreprennent des actions pouvant viser le vol ou la destruction de données, l'attaque directe de sites Internet gouvernementaux ou privés (déni de service ou défiguration de sites) et la commission d'attentats par le dérèglement des logiciels de fonctionnement d'infrastructures critiques (métros, aéroports, hôpitaux, bourses, etc.).

Conjuguées à des armes NRBC destinées à semer l'effroi chez les citoyens, des actions de grande envergure endommageant les réseaux essentiels seraient susceptibles de paralyser la société, d'affecter l'activité économique et la permanence même du service public. Parmi les conséquences possibles, un épuisement de la société pourrait accroître le besoin de sécurité dans des proportions favorisant l'avènement de régimes autoritaires.

3 - Enjeux pour la France et pour l'Europe

3.1 - Concilier, sur le moyen / long terme, renforcement sécuritaire et préservation de l'Etat de droit

Confronté à une menace terroriste polymorphe et au fort impact psychologique des actions commises, l'Etat pourrait être amené à consolider sa législation et à renforcer le champ répressif. Dans ce contexte au regard des impératifs démocratiques, le maintien par le Gouvernement d'un équilibre entre liberté et sécurité acceptable par la population constituera le cœur de la relation citoyen-gouvernement.

Si la France dispose aujourd'hui d'un arsenal juridique renforcé[5], le gouvernement a également adopté dès 2014 un plan de 80 mesures destinées à lutter contre le terrorisme et la radicalisation, assorti de nouvelles mesures en mai 2016. Des mesures novatrices de police administrative (accès ou sortie du territoire, contrôle des sites web faisant l'apologie du terrorisme, etc.) ont également été introduites en droit français et des plateformes d'assistance aux victimes de la radicalisation à l'instar de « *Stop-djihadisme* » ont été créées.

Pour faire face à la menace terroriste, le recours accru aux technologies de surveillance constitue une option crédible. Pour tirer les bénéfices économiques et technologiques de ce besoin, la France devrait mettre en place une véritable politique de développement de ses industries de sécurité. Elle dispose en la matière d'avantages technologiques qu'elle pourra valoriser auprès d'autres pays confrontés aux mêmes défis.

3.2 - Un effort déterminé de priorisation est nécessaire

La lutte contre le terrorisme passe sans doute par une prise en compte globale au niveau européen et en lien avec nos autres partenaires internationaux. Elle doit aussi continuer d'envisager que le terrorisme radical aura un jour accès à des armes non conventionnelles, ne pas cesser d'œuvrer à l'organisation de ses services pour mieux appréhender les menaces NRBC et travailler de concert avec ses partenaires majeurs pour organiser la réponse à un tel scenario.

Ainsi, les efforts devront être poursuivis pour permettre l'adaptation de la législation et de la réglementation, la mise en œuvre de solutions technologiques adaptées à l'évolution de la menace, dans le cadre d'une coordination renforcée avec nos partenaires y compris pour la conduite des opérations extérieures.

5 - En dehors de la loi de lutte contre le terrorisme du 23/01/2006, la France a renforcé son dispositif législatif face aux nouvelles formes de menaces depuis 2013, par l'adoption de quatre nouvelles lois plus répressives, et d'application plus étendue.

4 - Scenario alternatif : attentat NRBC de grande ampleur par les groupes terroristes

La maîtrise des nouvelles technologies et les progrès des recherches scientifiques permettent à des groupes terroristes de disposer du savoir-faire nécessaire pour fabriquer des armes non conventionnelles puissantes et de franchir un seuil capacitaire en termes de modes d'actions.

Ces évolutions se concrétisent par une attaque terroriste majeure à caractère non conventionnel sur le territoire national. Une telle attaque, par son ampleur, désorganise le fonctionnement de l'Etat (saturation des centres de soin, surmobilisation des services de sécurité, difficulté de gestion des mouvements de population, etc.) et entraîne des conséquences économiques et environnementales durables (chute du tourisme, diminution de l'activité économique, pollutions, etc.). Cette situation conduit au renforcement des forces et des moyens de sécurité intérieure appelant une réallocation des ressources de l'Etat au détriment d'autres priorités ainsi qu'un appel à la solidarité des pays de l'Union européenne pour renforcer l'action militaire contre les foyers terroristes.

Parallèlement, les groupes terroristes utilisent leurs nouvelles capacités de destruction de masse pour imposer un nouveau rapport de force avec les Etats des zones où ils sont implantés (Afrique de l'Ouest et du Nord, Sahel, zone syro-irakienne notamment). Dans l'impossibilité de lutter efficacement contre ces groupes, ces Etats sont déstabilisés, entrainant le basculement de régions entières dans l'orbite terroriste. ●

6

Frontières passoires ou frontières intelligentes

L'essentiel

La sécurisation des frontières en France et en Europe doit tenir compte des réalités géographiques et assurer un traitement fluide des passages, nécessaire au bon fonctionnement de l'activité économique, tout en veillant à la sécurité du territoire et au contrôle des migrations. Contesté du fait de la montée des populismes et de la tentation de certains Etats de faire cavalier seul, l'espace Schengen demeure pourtant un périmètre pertinent. Les technologies de détection, combinées à une volonté politique de préserver la construction commune ainsi qu'à des modifications limitées du traitement juridique des franchissements illégaux, peuvent assurer la police d'accès attendue des citoyens sans entraver la facilité de circulation et les libertés nécessaires à leur bien-être.

La fin de la Guerre froide et la mondialisation avaient donné l'image d'un monde ouvert. L'Union européenne, construite autour de quatre libertés fondamentales pour la circulation des personnes, des biens, des services et des capitaux, a, dans sa phase d'expansion et de consolidation des années 1990-2000, mis en place le système de suppression des contrôles aux frontières intérieures entre les signataires des accords dits de « Schengen ». Cependant, les phénomènes de vagues migratoires spectaculaires de l'été 2015, assortis d'images de l'afflux de réfugiés venus de Syrie ou d'Afrique subsaharienne depuis la Turquie ou l'Afrique du Nord, ont amené des critiques aigües de ce système. La conjonction de ce phénomène avec l'intensification du terrorisme jihadiste en Europe et l'amalgame souvent fait entre les deux sujets ont remis la question des contrôles aux frontières nationales au cœur du débat public.

Dans ce contexte, l'enjeu pour la gestion du contrôle et de la sécurité des frontières en Europe est de parvenir à préserver les « quatre libertés », tout en assurant la stabilité et la sécurité des Etats. Cela se traduit par la nécessité, d'une part, de contrôler et de surveiller afin de détecter et filtrer les personnes et, d'autre part, de préserver la fluidité des passages.

Le contrôle des frontières doit, par ailleurs, être concilié avec le respect des libertés individuelles qui bénéficient d'un haut niveau de protection en droit national et européen. Les textes et la jurisprudence, aussi bien nationaux qu'européens, ont dessiné un cadre complexe mais précis qui s'applique à l'élaboration et l'utilisation de fichiers ainsi qu'à la prise en compte de l'enjeu de protection de la vie privée dans l'étude de nouveaux systèmes ou moyens de surveillance et de contrôle des frontières.

1 - Etat des lieux en 2017

1.1 – Les enjeux à l'échelle de l'Europe

Corollaire des conflits, les migrations de populations devraient également s'amplifier dans les prochaines années en raison des modifications climatiques et des dynamiques démographiques. Selon les Nations unies, le changement climatique pourrait ainsi provoquer le déplacement forcé de 250 millions de personnes à l'horizon 2050.

Les frontières à l'Est de l'Europe sont actuellement peu perméables aux flux de réfugiés, la Russie agissant comme un obstacle à l'immigration irrégulière. Par endroits, la frontière entre la Slovaquie et l'Ukraine dispose, par exemple, de cameras tous les 150 mètres. Ces frontières sont, cependant, un lieu de passage important pour les trafics et sont sous surveillance particulière.

Passages historiques pour l'immigration venue d'Afrique de l'Ouest, Gibraltar et les enclaves espagnoles de Ceuta et Melilla font, depuis le début des années 2000, l'objet d'une vigilance accrue des autorités espagnoles, en collaboration avec le Maroc, ce qui a entraîné une diversification des voies de passage et un relatif tarissement des flux. Ceux-ci se sont déplacés vers l'Est, accompagnant les révolutions arabes et les conflits en Libye ou en Syrie. Ainsi, avec le chaos libyen, Lampedusa devient la nouvelle porte d'entrée pour l'immigration africaine[1] et nord-méditerranéenne qui peut prendre la mer sans contrainte, en espérant atteindre les rivages européens ou, plus sûrement, être recueillie par les forces de sécurité européennes. La guerre en zone syro-irakienne pousse, par ailleurs, les réfugiés et migrants vers les îles du Dodécanèse, situées à quelques kilomètres de la Turquie. Selon l'organisation internationale des migrations et le haut-commissariat de l'ONU pour les réfugiés (HCR), plus d'un million de migrants sont entrés dans l'Espace Schengen en 2015 par voie terrestre et maritime en provenance principalement de Syrie, d'Erythrée et d'Afghanistan, ce chiffre étant retombé à 360 000 pour l'année 2016.

Le premier enjeu, pour l'Espace Schengen, est de pouvoir filtrer les personnes grâce à un dispositif de surveillance efficace pour interdire aux malfaiteurs et migrants illégaux de franchir ses frontières extérieures. La réalisation de ce défi impose une identification systématique des personnes et des biens, en amont et avec un faible taux d'erreur. Si le filtrage est réellement efficace aux frontières extérieures de l'espace Schengen, la liberté de circuler à l'intérieur doit être très large, y compris à travers les anciennes frontières des Etats. Ceci n'exclut pas l'existence de contrôles mobiles[2], transparents pour le voyageur mais efficaces pour lutter contre les quelques infiltrations résiduelles.

1 - Déjà en 2011, sur les 60 000 immigrants arrivés à Lampedusa, seuls 4 000 étaient originaires d'Afrique de l'Ouest soit une baisse sensible par rapport aux années précédentes, principalement en raison de l'attractivité économique plus faible de la zone européenne.

2 - Contrôles mobiles dans la logique de « défrontiérisation » (de *bordering*).

Le deuxième enjeu pour l'Europe est de préserver la fluidité des échanges aux frontières pour ne pas construire une Europe forteresse, mais ouverte avec vigilance aux personnes et biens participant à son essor, sans pénalisation du commerce international. La réalisation de ce défi impose de ne pas freiner les flux et donc d'étaler les contrôles tout en privilégiant des systèmes rapides aléatoires sans files d'attente.

Ceci doit être concilié avec le respect des droits fondamentaux et de l'intimité des personnes. Cet impératif implique de trouver le juste milieu entre un traçage judicieux nécessitant le croisement des différentes bases de données judiciaires internationales et la collecte de données des voyageurs et le respect des droits fondamentaux de ceux-ci. Il incite à veiller à ce que chaque développement et croisement de fichiers envisagé s'effectue dans un environnement respectant strictement la finalité des fichiers utilisés et le principe de proportionnalité et tienne compte également des risques de piratage de telles données qui constituent des informations potentiellement discriminantes pour les individus.

A cette fin, les Européens et la France doivent pouvoir tirer parti des technologies afférentes à la sécurité, domaine dans lequel la France excelle. Cette dernière doit profiter de ce mouvement à l'échelle de l'Europe pour en retirer des bénéfices économiques.

1.2 – Le contrôle des passagers

Le contrôle du franchissement à la frontière doit permettre d'identifier, au milieu du flux massif et régulier des citoyens et étrangers en situation régulière, les entrées irrégulières ou indésirables car présentant une menace pour l'ordre public. Les modalités du contrôle sont distinctes selon qu'ils s'agissent des contrôles aux points de passages identifiés (terrestres, portuaires et aéroportuaires) ou de tentatives de franchissement irrégulier des frontières maritimes ou terrestres.

a) Dans l'espace « Schengen »

- **Cadre général**

En 2015, plus de 50 millions de ressortissants de pays tiers se sont rendus dans l'UE. Actuellement, l'entrée et la sortie des ressortissants de pays tiers aux frontières extérieures de l'UE ne donnent lieu qu'à l'apposition d'un cachet sur leur document de voyage. Le temps passé sur le territoire de l'UE doit être calculé manuellement, ce qui ralentit la procédure et induit un risque de falsification.

En février 2013, la Commission a fait une première proposition pour un système Entrée/Sortie permettant de comptabiliser la durée des séjours et donc le nombre d'étrangers présents à un moment donné dans l'espace Schengen. Dans un avis du 19 juillet 2013, le Contrôleur européen de la protection des données avait considéré que le système Entrée/Sortie dans l'UE proposé par la Commission et fondé sur des données biométriques était « coûteux, insuffisam-

ment justifié et intrusif ». Un nouveau projet présenté en avril 2016 réduit « significativement » le nombre de données conservées, de 36 à 26. Au lieu de dix empreintes digitales, la nouvelle proposition prévoit le relevé de quatre empreintes digitales et de l'image faciale comme identifiants biométriques. Ces éléments d'apparence anecdotique sont révélateurs du conflit persistant entre la logique de sécurité et de contrôle migratoire et celle de la libre circulation et de la protection des données à caractère personnel.

- **Actions destinées à améliorer la gestion communautaire des frontières**

La Commission européenne a proposé, en 2014, le train de mesures « Frontières intelligentes » qui comprend principalement deux règlements. Le premier vise à lutter contre la migration irrégulière en établissant un système apportant fiabilité et rapidité pour calculer la durée de séjour autorisée de chaque voyageur et pointer les dépassements. Le second facilite le franchissement des frontières par des habitués en établissant un programme d'enregistrement des voyageurs (*Registered Traveller Programme* - RTP) qui annonce le contrôle biométrique aux frontières de l'UE. Dans le cadre de « Frontières intelligentes », la France a contribué à cette construction et mené, en 2015, des expérimentations en matière de biométrie à partir de l'iris, d'empreintes digitales et de la reconnaissance faciale.

b) Cadre légal

Le cadre légal des contrôles des passagers dans l'espace Schengen est contraint.

En Europe, les stipulations de l'accord de Schengen de 1985 ainsi que la convention d'application signée en 1990 et entrée en vigueur en 1995, ont été intégrées dans le droit communautaire par le traité d'Amsterdam en 1997 puis modifiées en 2007 par le traité de Lisbonne. Elles forment désormais le titre V du traité sur le fonctionnement de l'Union européenne (pour les principes), complété par le Code frontières Schengen (pour les modalités d'application). Le contrôle aux frontières intérieures de l'espace Schengen est supprimé par principe (sauf rétablissement, qui doit être temporaire). Cette suppression est théoriquement compensée par le renforcement du contrôle des frontières extérieures et de la coopération policière et judiciaire, ainsi que par la possibilité de procéder à des contrôles non frontaliers. Le respect de ces règles s'effectue sous le contrôle de la Commission et de la Cour de justice de l'Union européenne (CJUE).

L'amélioration de la coopération européenne doit notamment être permise par les échanges de données : fichier SIS (Système d'information Schengen), fichier sur les dossiers des passagers (PNR – *Passenger Name Record*) pour le transport aérien. Toutefois, là encore, les limitations politiques et juridiques sont nombreuses. Ainsi, le projet de directive a suscité les réticences de certains Etats membres et n'a pu être adopté que dans un contexte de menace terroriste élevée (tragédie du Bataclan, en novembre 2015).

Dans ce domaine, les questions sont parfois mal posées : ce n'est pas tant le

traitement des données (nécessaire) qui devrait poser question que le contrôle de ces traitements. Le juste équilibre entre le respect des libertés individuelles (fichiers) et l'exigence de protection des populations y occupe une place évidemment centrale. La difficulté de faire évoluer les règles, la crispation forte contre les améliorations techniques des outils de coopération policière et les potentielles dérives de l'interprétation de certaines conventions affaiblissent la capacité de maîtrise des Etats. Elles aboutissent à figer le paysage juridique qui, faute de répondre aux attentes des opinions publiques, risque de voler en éclats.

c) En France

En France, le contrôle de l'identité est principalement régi par le code de procédure pénale (article 78-1 à 78-6). Il est soumis au contrôle du juge judiciaire.

Réglementairement, le contrôle aux frontières extérieures de l'espace Schengen s'effectue par présentation du passeport ou de la carte d'identité à un agent qui vérifie la régularité du document, du visa éventuel et la correspondance entre le voyageur et sa photographie. Ce n'est qu'en cas de doute qu'un contrôle de seconde ligne peut comporter le prélèvement des empreintes digitales pour les comparer aux données éventuellement enregistrées dans des fichiers. Or, le faible niveau d'interopérabilité des dispositifs biométriques utilisés dans l'espace Schengen ne permet pas d'accéder simplement aux empreintes digitales des documents délivrés par d'autres Etats, ce qui réduit l'efficacité des contrôles[3] (même si, depuis octobre 2015, des données biométriques sont enregistrées lors de la délivrance de visas pour l'espace Schengen et sont accessibles pour l'ensemble des Etats parties à l'accord).

Afin de pouvoir concentrer les moyens humains sur le contrôle des étrangers, de nouveaux sas de contrôle automatisés et compatibles avec les passeports biométriques français (PARAFE) ou ceux des citoyens européens s'étant enregistrés au préalable ont été introduits. Ces sas ont la capacité de lire la puce RFID (*Radio Frequency Identification Device* pour identification par radio fréquence) du passeport, stockant la photographie numérisée du porteur et les empreintes digitales issues de deux doigts. Cette procédure s'appuie donc sur l'exploitation de données biométriques monomodales pour obtenir l'identification et l'authentification[4]. Il est à relever qu'aujourd'hui, un citoyen français utilisant PARAFE fait donc l'objet d'un contrôle biométrique alors que le contrôle par la police de l'air et des frontières est purement visuel.

Pour les contrôles frontaliers terrestres entre les points de passage et sur le territoire, en dehors de quelques dispositifs de vidéosurveillance qui équipent les aéroports et quelques gares et postes frontières, aucun dispositif d'observation automatique et permanent ne permet la détection, la reconnaissance et l'identification des personnes franchissant la frontière, l'ensemble des frontières terrestres de France métropolitaine étant partagé avec des pays de l'espace Schengen. Cette situation est, au demeurant, antérieure à la mise en place des accords de Schengen, les contrôles douaniers des personnes aux frontières terrestres revêtant alors un carac-

3 - Sénat, « *Biométrie, mettre la technologie au service du citoyen* », 5 septembre 2016.

4 - L'identification est une procédure qui permet de connaître l'identité de l'individu. A partir d'un échantillon biométrique fourni, on répond à la question « Qui est cette personne ? ».

tère aléatoire, et aucune frontière terrestre n'étant par ailleurs clôturée.

Le seul point de contrôle durci en France est le passage vers le Royaume-Uni (périmètre sécurisé de Sangatte ; contrôle de type aéroportuaire à l'embarquement dans les gares *Eurostar* et les navettes *Eurotunnel*). On y observe un phénomène d'entonnoir où se concentre la majeure partie des flux illicites de personnes qui n'ont fait que transiter par l'espace Schengen dans l'espoir de se rendre au Royaume-Uni. La gestion de ce point est au demeurant fortement portée, au plan financier, par le Royaume-Uni dont la politique migratoire est concernée au premier chef.

S'agissant de l'outre-mer, deux situations spécifiques méritent l'attention :

- la Guyane est le seul territoire français ayant des frontières terrestres avec des Etats n'appartenant pas à l'espace Schengen (si l'on excepte la frontière délimitant la partie française de l'île de Saint Martin de celle appartenant aux Pays-Bas, cette section du territoire de l'île ne faisant pas partie de l'Union). Le problème migratoire qui existe à la frontière avec le Brésil, le long de la rivière Oyapoc et avec le Suriname est néanmoins d'ampleur limitée[5] ;
- le département de Mayotte, seul point du territoire français qui connaisse des entrées massives par la mer d'un flux illicite via des embarcations de fortune, subit, *a contrario*, une considérable pression migratoire en provenance des Comores. La situation politique très détériorée aux Comores, et à Anjouan en particulier, crée une dynamique de départs. Les vulnérabilités de l'état civil mahorais et la porosité des liens familiaux avec le reste de l'archipel facilitent un mouvement difficile à contrôler.

5 - La situation étant plus difficile en matière de contrebande illicite et d'orpaillage illégal.

2 - Situation en 2030

2.1 – Contexte général

E**n 2030, les vagues de réfugiés successives aux frontières Sud et Sud-est de l'Europe** dues au délitement d'un certain nombre de pays et au mouvement de populations fuyant le conflit syrien, à la professionnalisation des trafiquants et à l'accroissement concomitant des actes de terrorisme **auront entraîné un durcissement significatif des contrôles individuels.** Dans le prolongement du train de mesures « Frontières intelligentes » et pour répondre à une demande de sécurisation croissante des citoyens, les frontières extérieures de l'Union européenne auront été renforcées et les systèmes biométriques partagés permettant de croiser plusieurs signatures et de stocker les données captées pourront avoir été autorisés. En 2030, **les citoyens extra-communautaires constitueront le tiers du milliard de voyageurs qui franchiront annuellement les frontières extérieures de l'UE,** si l'on extrapole les données de la Commission européenne pour 2025. Ce scénario (comprenant le maintien de l'espace Schengen) n'est viable que sous la condition d'un durcissement, à la fois légal et matériel, du blocage des tentatives de franchissement irrégulier en mer Egée et dans l'ensemble de la Méditerranée.

2.2 – Des contrôles automatisés aux points de passage

Pour l'ensemble des personnes en transit ou entrantes, toutes les opérations de contrôle sont dématérialisées. Le passager qui aura fait les démarches de pré-approbation est enregistré hors guichet à partir de son téléphone portable équipé d'un logiciel spécifique distribué par des agences autorisées[6]. Les informations codifiées afférentes à son trajet sont exploitées à des fins de gestion et de sécurité et les systèmes des compagnies aériennes sont interfacés avec celui de la gestion administrative de la frontière.

La vérification d'identité s'appuie sur le relevé par un capteur des empreintes digitales mais aussi la captation d'autres éléments biométriques (iris, réseau de veines, attitude, forme du visage, l'utilisation de l'ADN n'étant pas encore possible en raison des délais de traitement). La multi-biométrie, basée sur la combinaison de plusieurs biométries, offre une précision d'excellente qualité limitant le risque d'erreur et de fausse alerte ainsi qu'une robustesse au regard du vieillissement. Ces diverses signatures biométriques sont récoltées par des détecteurs spécifiques, répartis sur l'itinéraire à des passages obligés et explicitement signalés (couloir intelligent ou sas de type PARAFE), et comparées en temps réel avec les données stockées par le passager dans son smartphone lors de sa pré-approbation.

6 - La pré-approbation permet de délocaliser le contrôle pour alléger la procédure d'enregistrement ou de franchissement de frontière.

En temps réel, les données judiciaires du passager font l'objet d'une interrogation des bases nationales et européennes (EUROPOL, pays membres) et internationales, sous le contrôle d'une agence européenne créée à cette fin afin de confirmer son accès. Avant leur arrivée à la frontière ou l'aéroport, certains passagers à risque font l'objet d'une attention particulière sur la base de renseignements issus de services chargés de la prévention ou d'une analyse de leur identité numérique calculée[7]. **Les personnes en situation illégale, signalées par les bases de données ou par leur comportement,** sont interceptées par un personnel suffisamment nombreux, bien formé et rendu disponible par le traitement automatique des contrôles.

Le passage devant un scanner corporel permet la détection automatique d'objets sous les vêtements et permet de contrôler les bagages de cabine. **La vidéosurveillance, omniprésente dans tous les points de contrôles et sur de nombreux points de passage frontaliers, est centralisée** au profit des services de sûreté ou de sécurité, libérés des tâches de service traditionnelles et prêts à affronter l'imprévu. Les caméras équipées de logiciels « intelligents » analysent les faits et gestes pouvant trahir un comportement ou un objet suspect. La mise en place de l'ensemble de ces dispositifs repose sur le développement d'une robustesse aux attaques cybernétiques.

2.3 – Entre les points de passage, une nouvelle frontière sous surveillance technologique

Un scénario à 15 ans ne devrait pas laisser de place à des ruptures technologiques majeures. En revanche, on peut envisager une accélération de la miniaturisation et surtout de l'interconnexion des technologies et des systèmes. La sécurité de la frontière résidera sur une connaissance quasi parfaite des franchissements, par la multiplication des dispositifs de surveillance garantissant une détection, une reconnaissance, une identification systématique des contrevenants. L'efficacité recherchée est atteinte par l'utilisation de systèmes multi-capteurs tirant parti de la complémentarité de :

- capteurs passifs acoustiques ou sismiques omnidirectionnels permettant l'alerte ;
- capteurs passifs optroniques, images ou vidéo permettant la reconnaissance et l'identification tout temps et la collecte de preuves ;
- capteurs infrarouges opérant et radar tous temps ;
- capteurs olfactifs.

Ce système, au sol mais aussi aérien à base de drones ou de ballons voire de satellites, est complété par des patrouilles de capteurs aéroportés de tous types. L'ensemble de ces technologies existe déjà, mais est rendu opérationnel par une baisse notable des coûts, permettant leur installation systématique et le croisement de leurs informations en temps réel et en réseau.

La détection au passage de la frontière facilite le contrôle rapide des franchissements en dehors des points de passage officiels.

7 - L'identité numérique (IDN) relie l'individu à des traces sur le net, elle comprend l'identité déclarative (nom, date de naissance, etc.), l'identité agissante renseignée par les activités de l'individu sur le net, enfin l'identité calculée qui résulte d'une analyse de la précédente.

3 – Enjeux pour la France et pour l'Europe

Il faut mettre en regard le développement des technologies et leur acceptabilité sociale et politique en matière de libertés publiques. Les technologues, dans leurs catalogues toujours plus fournis, proposent des moyens d'intrusion physiques et sociaux toujours plus performants. Mais si le citoyen, depuis le 11 septembre 2001, a en partie accepté de rogner sa liberté au profit de sa sécurité, il n'en demeure pas moins qu'il existe aussi des barrières psychologiques et légales. La question de la mise en place de scanners intégraux dans les aéroports en service aux Etats-Unis, mais pas en France, en est une bonne illustration. Le débat doit donc s'établir entre le citoyen, ses représentants et l'administration, sachant par ailleurs que la technologie peut aider à donner corps à des politiques fondées sur des choix publics solides, mais est impuissante à compenser l'absence de tels choix.

3.1 – Les axes d'efforts politiques

Un point essentiel pour la France comme pour ses partenaires est et demeurera politique : c'est la nécessité de réaffirmer la robustesse de la solution de contrôle qu'apportent l'espace et les mécanismes de Schengen et d'en convaincre la population.

S'agissant de la pertinence de l'espace lui-même, la démonstration factuelle est simple : ce que peut se permettre le Royaume-Uni du fait de son insularité (forte limitation du nombre de points d'entrée ; mers difficiles ne permettant pas le passage par des embarcations de fortune), n'est absolument pas accessible aux 25 Etats continentaux de l'Union. Le passage clandestin à leurs frontières terrestres ne rencontre aucun obstacle géographique incontournable. De fait, l'espace Schengen a renvoyé la frontière extérieure sur des obstacles qui n'existaient pas à l'intérieur : obstacle géographique de la Méditerranée au Sud, obstacle politique à l'Est, qu'il s'agisse de la frontière gréco-turque fortifiée ou de l'immense tampon constitué par l'espace russe.

Convaincre politiquement les opinions de la pertinence des mécanismes du traité est par nature une tâche beaucoup plus complexe. En termes de positionnement politique, elle passe par la démonstration d'une volonté collective de durcir les points de fragilité de la frontière extérieure (essentiellement les îles grecques du Dodécanèse, le canal de Sicile et la frontière terrestre bulgaro-turque), la modification du régime des interceptions en mer ou à l'accostage se traduisant par un principe de non-admission et la mise en place d'une politique de répression de l'action des trafiquants. Si ces éléments politiques sont mis en œuvre – et ils sont nécessaires pour écarter la tentation du repli sur un contrôle aux frontières nationales largement irréaliste – la technologie peut ensuite offrir des solutions de contrôle effectif.

3.2 – Les axes d'efforts techniques

Le comité de la filière industrielle de sécurité (CoFIS), mis en place par le Premier ministre en 2013 et dont le co-pilotage a été confié au secrétariat général de la défense et de la sécurité nationale et à la direction générale des entreprises, a pour ambition de développer des solutions de sécurité efficaces et innovantes au moyen d'un dialogue public-privé enrichi. Dans ce cadre, le CoFIS a identifié différentes technologies de rupture qui permettront aux industriels français de proposer des solutions visant à renforcer la sécurité des frontières. Ces technologies visent en particulier :

- les outils de prédiction et d'analyse des comportements à travers les développements du *big data* et de l'intelligence artificielle. La capacité de disposer d'outils de confiance, sinon souverains, sera un élément clé pour permettre le déploiement de telles solutions en apportant à nos concitoyens la garantie du respect de leurs droits ;
- les traitements des flux vidéo à travers l'introduction du « *deep learning* », de la gestion coopérative 4D « sans couture » intérieur/extérieur et des systèmes « tout video » basés sur l'intelligence artificielle coopérative avec apprentissage. Ces nouvelles technologies vont rapidement être disponibles pour le traitement des foules, la reconnaissance des individus en mouvement et des comportements suspects ou des objets dissimulés mais aussi pour l'identification de mouvements anormaux lors de surveillance de zones étendues, comme par exemple la circulation maritime à proximité des côtes ;
- la surveillance des zones étendues et peu peuplées ainsi que les espaces maritimes à travers la robotique et le vol en essaim de drones. En s'appuyant sur des détecteurs optiques et infra-rouges de plus en plus miniaturisés et performants, l'utilisation de plateformes volantes collaboratives permettra une couverture permanente et exhaustive de zones au relief complexe, difficilement accessibles ou très étendues et seront capables de discriminer les déplacements autorisés et de suivre les déplacements suspects ;
- l'identification des personnes à travers la multi biométrie. L'amélioration des performances des outils de reconnaissance faciale dans une foule ou en faible luminosité mais aussi les analyses large spectre en temps quasi réel sur le terrain permettront de compléter les outils de vérification d'identité ;
- l'identification physique des personnes dans le contexte de l'identité numérique. Les outils d'identité numérique qui permettront l'enrôlement à distance, sécurisé et simplifié, en particulier dans les systèmes informatiques des compagnies aériennes, devront offrir une confiance suffisante pour être intégrés avec les systèmes régaliens d'identité.

Le déploiement de ces technologies nécessitera un effort important, tant sur le plan financier qu'organisationnel, les technologies ne pouvant prendre leur pleine mesure que dans un contexte opérationnel cohérent. Pour cela, il est nécessaire de structurer la démarche de recherche et développement pour répondre aux enjeux technologiques, mais aussi juridiques, dans une approche interministérielle pour pouvoir prendre en compte efficacement les attentes légitimes de nos concitoyens. Cette démarche, qui pourrait s'appuyer sur les groupes de travail « expression du be-

soin » et « recherche et innovation » du CoFIS, devrait aussi pouvoir disposer d'une structure interministérielle dotée d'un budget lui permettant de faire émerger les solutions technologiques nécessaires, puis, selon les cas, être capable de conduire la réalisation et le déploiement de projets d'ampleur nécessitant une maîtrise d'ouvrage stable, pérenne et professionnalisée sur la thématique de la sécurité.

3.3 – Les axes d'efforts administratifs

- Consentir un effort financier. La mise en place de dispositifs de surveillance de cette ampleur exige un effort financier significatif. L'enseignement des initiatives américaine et canadienne en matière de frontières intelligentes démontre que les demi-mesures sont sources d'inefficacité car toute défaillance locale et ponctuelle invalide l'ensemble du système. Le coût est à examiner au regard du coût de la gestion des personnes entrées illégalement. Enfin, un retour sur investissement peut bénéficier au pays à travers le succès des innovations proposées par les industriels nationaux. Pour des raisons d'économies d'échelle, cet effort devrait être européen plutôt que national (duplication des efforts de R&D industriels) et être déployé à l'extérieur d'un périmètre mutualisé plutôt que dupliqué de façon redondante sur toutes les frontières intérieures de l'Union. L'évolution de la technologie, à cet égard, a plutôt tendance à confirmer la pertinence de la logique Schengen.
- Réaliser une véritable interopérabilité des systèmes des Etats membres. La crédibilité des systèmes de surveillance nécessite une interconnexion des différents dispositifs nationaux, européens et même internationaux.
- Développer la coopération entre douane et métiers de la logistique, du voyage et du transport. La douane, mettant à profit les nouvelles techniques de surveillance, doit privilégier des procédures de contrôle facilitant la fluidité des flux logistiques.
- S'adapter au cadre juridique et le faire évoluer. Il s'agit d'évaluer le ratio libertés publiques/sécurité au regard de la menace (notamment dans sa dimension technique) ; si l'on reste dans le cadre défini par les accords de Schengen, une harmonisation ou, *a minima*, un rapprochement des différents modèles juridiques s'avère indispensable pour en garantir l'efficacité. Si ce scénario de référence laisse envisager une demande accrue de sécurité, il implique que l'on aille vers un allégement des normes de protection des libertés publiques et individuelles tout en définissant et préservant le socle minimal de liberté et de préservation de la confidentialité de la vie privée de chaque individu. Le dialogue qu'implique la recherche de cet équilibre doit être mené entre les citoyens, le législateur et les autorités politiques, au moins au niveau européen.
- Former efficacement les personnels. L'efficacité de ces matériels repose aussi sur l'excellence de la sélection et de la formation des personnels.

4 – Scenarii alternatifs

Le scénario de référence est sous-tendu par deux variables : l'utilisation intensive de données biométriques et le respect des droits de l'Homme (au sens de la Déclaration universelle) dans un environnement technologique et humain en profonde transformation. En conséquence, deux scenarii alternatifs pourraient remettre en question l'évolution envisagée précédemment :

4.1 – Des limitations législatives

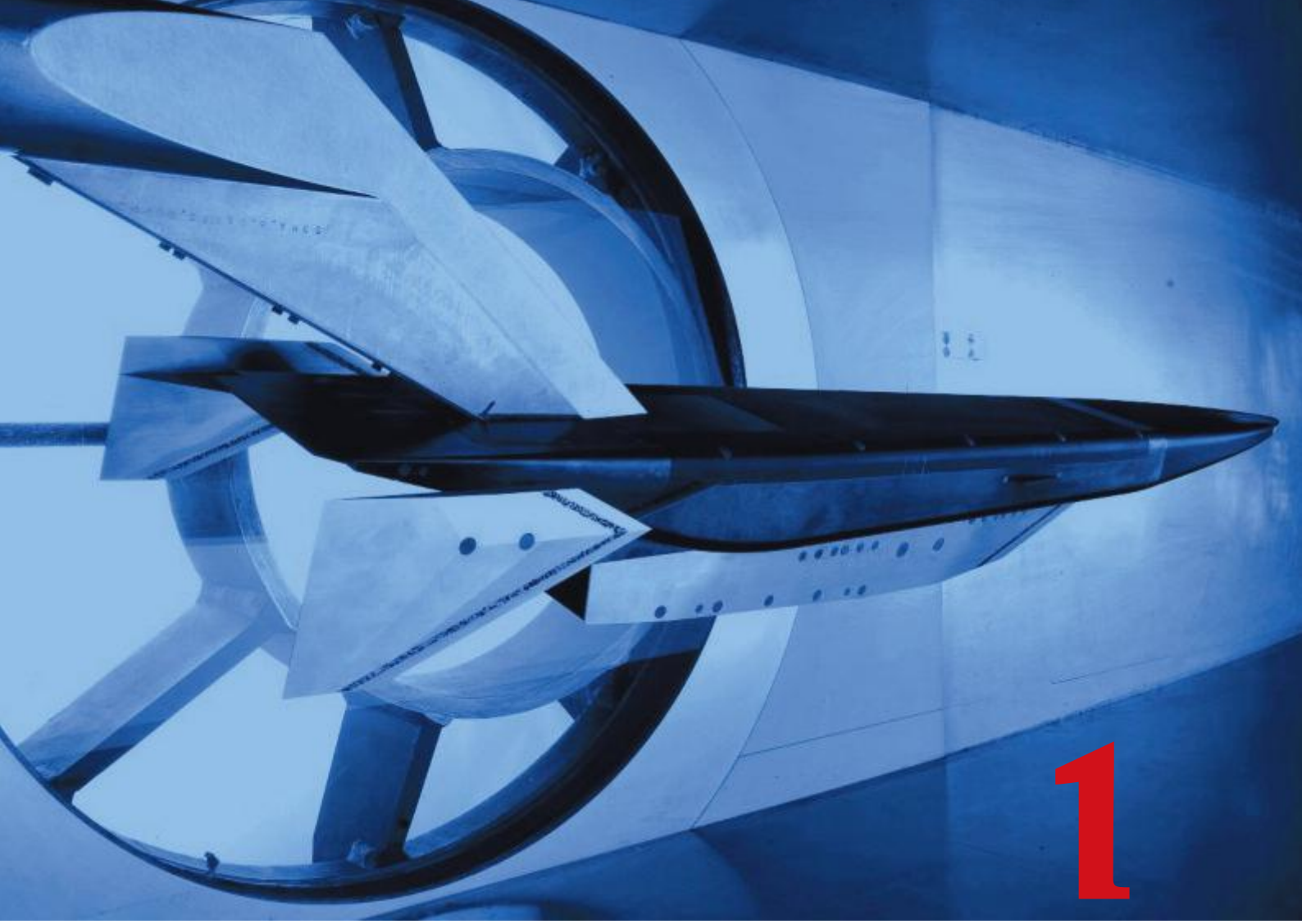
Un premier scénario se fonde sur des limitations induites par un cadre législatif qui privilégie le respect de l'intimité des voyageurs en s'interdisant l'usage des données biométriques au-delà de ce que la CNIL autorise aujourd'hui en France, c'est-à-dire uniquement les empreintes digitales, proscrivant de ce fait les systèmes multimodes et limitant l'utilisation des données recueillies dans le temps. Cette limitation « éthique » diminue fortement l'efficacité des systèmes d'identification et d'authentification des passagers et induit des délais supplémentaires dans les processus de franchissement de frontières.

4.2 – Une saturation des systèmes de gestion

Un autre scénario envisage une saturation des dispositifs de gestion des zones frontalières sous l'effet de déplacements massifs de populations en raison notamment de l'explosion démographique, des conséquences du réchauffement climatique ou de la pauvreté des pays sahéliens et/ou d'une déstabilisation algérienne. Ces flux massifs mettent en échec les systèmes technologiques en saturant leur capacité de traitement et conduisent à la militarisation des frontières extérieures de l'Union au-delà de Schengen et, le cas échéant, des frontières intérieures si cette première ligne s'avérait inefficace.

Partie 2

Ruptures technologiques – ruptures stratégiques



1

Les missiles et vecteurs hypervéloces, nouveaux déterminants des puissances ?

L'essentiel

La France possède des compétences dans le domaine des missiles de croisière, en particulier pour le développement de sa composante nucléaire aéroportée, et conduit des études sur la propulsion hypersonique. Compte tenu des ruptures potentielles qu'introduirait le développement des armements hypersoniques, en termes d'emport de charges conventionnelles ou nucléaires comme de déni d'accès et de l'intérêt qu'y portent la Russie, la Chine et les Etats-Unis, notre pays, afin de ne pas se faire distancer et ne pas engendrer un déséquilibre avec les pays dotés, doit maintenir *a minima* son investissement et poursuivre ses recherches.

Un armement est dit hypersonique lorsqu'il se déplace à une vitesse supérieure à Mach 5, soit cinq fois la vitesse du son.

L'aérodynamique et la thermodynamique des mobiles hypersoniques doivent être envisagées sous un angle nouveau, tandis que leur production nécessite le développement de nouvelles technologies, en particulier en matière de protection thermique et de propulsion.

Les armements hypersoniques se classent en deux catégories :

- celle des planeurs accélérés par un missile balistique mais qui réalisent l'essentiel de leur vol après séparation selon une trajectoire non balistique ;
- celle des missiles de croisière à propulsion aérobie[1] volant à une altitude de 30 à 40 kilomètres. Ces engins peuvent atteindre le seuil de l'hypersonique grâce à un statoréacteur[2] mais ne peuvent se déplacer de manière entretenue en régime hypersonique que par le biais d'un super-statoréacteur[3].

Sur le plan militaire, l'apparition d'armements hypersoniques[4] marque une rupture pour plusieurs raisons :

- leur vitesse, à la condition qu'elle soit associée à des manœuvres, disqualifie les capacités actuelles d'interception des défenses adverses ;
- ces armements offrent une capacité de frappe extrêmement réactive à des portées très supérieures à celles des systèmes actuels, à l'exception bien sûr des missiles balistiques qui n'ont cependant pas leur souplesse d'emploi ;
- ces armements peuvent faire peser à tout moment et à toute distance une menace instantanée de frappe conventionnelle, voire nucléaire.

Les vecteurs hypersoniques restent encore très immatures et les premières mises en

1 - Combustion par l'oxygène de l'air.

2 - Moteur à propulsion aérobie sans compresseur et sans turbine, la compression du flux d'air nécessaire à la combustion étant assurée par la présence des ondes de chocs. L'écoulement d'air dans la chambre de combustion reste subsonique. La plage de fonctionnement d'un statoréacteur est comprise entre Mach 1 et environ Mach 5. (*Ramjet* en anglais).

3 - Lorsque la vitesse de l'engin dépasse Mach 5, l'écoulement d'air dans la chambre de combustion devient supersonique, on parle alors de super-statoréacteur (*scramjet* en anglais, pour *supersonic combustion ramjet*).

4 - *Stricto sensu*, les têtes des missiles balistiques relèvent de cette catégorie lorsqu'elles rentrent dans l'atmosphère mais le caractère prédictif de leur trajectoire conduit à ne pas les évoquer ici.

service opérationnelles ne devraient pas intervenir avant plusieurs années et ce, avec de probables limitations en termes de charge utile, d'autonomie de navigation et de précision terminale. A l'horizon 2030, toutefois, il fait peu de doute que des armements hypersoniques figureront dans les arsenaux de plusieurs puissances. La France elle-même envisage d'en disposer pour la composante aéroportée de sa dissuasion nucléaire à partir de 2035. A cet égard, considérant la rupture stratégique que constituera l'apparition de ces armements, la question de leur emploi dans un domaine conventionnel ou de leur inclusion dans un système de dissuasion nucléaire devra faire l'objet de réflexions eu égard aux risques de méprise que leur tir pourrait engendrer.

Au regard des performances de ces missiles, la question de l'efficacité et de la politique de développement des systèmes de DAMB dans leur configuration actuelle pourrait être remise en question.

1 - Etat des lieux en 2017

Outre la France, quatre pays disposent de programmes visibles de recherche et de développement en matière d'armements hypersoniques : les Etats-Unis, la Chine, la Russie et l'Inde.

Les Etats-Unis disposent des programmes les plus ambitieux, initiés avec le projet de *Conventional Prompt Global Strike* (CPGS) de frappe intercontinentale sur court préavis. Lancé en 2001, il était initialement défini comme un système de contre-prolifération, mais apparaît désormais comme un moyen de contrer les capacités de « déni d'accès ». Sa nature purement conventionnelle est désormais bien ancrée.

Le Département de la défense américain (DoD) a consacré environ 196 millions de dollars en 2016 à ces programmes, soit 20 % des crédits de *Science & Technology* (S&T) sur les plates-formes aériennes ou 2 % de l'ensemble de ses dépenses S&T. Ce montant devrait connaître une hausse significative ces prochaines années.

Dans le domaine des planeurs hypersoniques, deux programmes sont en cours :

- l'*Advanced Hypersonic Weapon* (AHW) de l'*US Army* visant 6 000 km de portée. Un essai a été réussi fin 2011 sur 3700 km (2 300 km de plané hypersonique) ; un second a échoué en 2014 (défaillance du lanceur). De nouveaux essais sont programmés pour 2017 et 2019, possiblement à partir d'une plate-forme navale, ce qui pourrait indiquer un rapprochement entre *Navy* et *Army* sur ce programme ;
- le programme de planeur *Tactical Boost Glide* (TBG) de la *DARPA* à vocation régionale (portée de l'ordre de 1 500 km). Ce programme capitalise sur les acquis du programme *FALCON HTV 2* qui visait une portée de 37 000 km avec des manœuvres dans le plan horizontal sur la moitié de

cette distance (deux essais ratés en 2010 et 2011).

Dans le domaine des missiles de croisière hyper-véloces, l'*US Air Force* conduit, depuis 2012, le programme High-Speed Strike Weapon (HSSW) au sein duquel le missile de croisière *Hypersonic Air Breathing Weapon Concept* (HAWC) est développé avec une perspective de mise en service opérationnelle vers 2020 (objectif probablement très ambitieux). Le HAWC prend la suite du programme de démonstrateur *X 51 Waverider* qui a réussi en 2013 un vol à la vitesse de Mach 5,1 pendant 3 minutes et demi. En 2004, la propulsion par super-statoréacteur avait déjà connu une avancée importante lorsque la *NASA* était parvenue à faire voler pendant 10 secondes son *X-43* à près de Mach 10.

La Chine développe de son côté le planeur hypersonique *DF ZF* (initialement appelé *WU 14*). Le système aurait été testé avec succès à sept reprises depuis 2014. La portée semble ne pas excéder 2 000 km. La vitesse se situerait entre Mach 10 et Mach 5 en fin de phase planée. Un missile de croisière à super-statoréacteur serait également développé dans un design proche du *X-43* américain.

La Russie poursuit le développement de deux projets :

- le missile antinavire hypersonique *3M 22 Tsirkon*, possible évolution de portée allongée du *BrahMos II* co-développé avec l'Inde, qui pourrait être produit dès 2018 ;
- le planeur hypersonique *Yu 71* destiné aux forces stratégiques. Testé depuis 2004, sur des distances n'excédant pas 6 000 km jusqu'à présent, l'engin aurait atteint Mach 15 après avoir été libéré par un missile balistique *Sarmat*.

L'Inde co-développe avec la Russie le missile de croisière à super-statoréacteur *BrahMos II*, dont l'objectif de performances est d'atteindre une vitesse comprise entre Mach 5 et Mach 7 et une portée de près de 300 km, à savoir la limite du régime de contrôle de la technologie des missiles (MTCR).

La France dispose de son côté d'une longue expérience dans le domaine des missiles de croisière à statoréacteur, ayant fait le choix de ce type de propulsion pour sa composante nucléaire aéroportée dès les années 1980, avec la mise en service de l'*ASMP* (Air-Sol Nucléaire Moyenne Portée) en 1986, remplacé par l'*ASMP-A* (Air-Sol Moyenne Portée Amélioré) en 2009. Elle est, à ce jour, le seul pays avec la Russie à avoir mis en service opérationnel des armements dotés de ce type de propulsion. Elle conduit des études sur la propulsion hypersonique dans le cadre du renouvellement de la composante nucléaire aéroportée (*ASN 4G*, Air-Sol Nucléaire de 4ème génération).

2 - Situation en 2030

2.1 – Les facteurs favorisant ou entravant le développement des armements hypersoniques

a) Les facteurs stratégiques et opérationnels

L'environnement géopolitique favorise le développement des armements hypersoniques. Les antagonismes stratégiques croissants entre grandes puissances impliquent en effet un « durcissement » des développements capacitaires. Dans ce contexte, l'armement hypersonique présente un intérêt indéniable car il permet de surclasser, par la vélocité et la manœuvre, des défenses antiaériennes et antimissiles de plus en plus performantes. Dès lors, les systèmes hypersoniques pourraient être des vecteurs privilégiés pour les missions suivantes :

- dissuasion nucléaire ;
- frappes stratégiques conventionnelles ;
- déni d'accès et interdiction de zone (*Anti Access / Area Denial* ou A2/AD), à la fois en tant que moyen offensif, pour pénétrer une zone réputée « interdite », de plus à des distances nettement plus éloignées de la menace, et en tant que moyen défensif susceptible d'établir une situation de cette nature en repoussant au loin, les moyens offensifs adverses.

La France, la Russie et la Chine semblent désigner la dissuasion nucléaire comme mission privilégiée pour des armements hypersoniques. Les Etats-Unis écartent à ce stade cette perspective et envisagent leur emploi pour des frappes stratégiques conventionnelles sous faible préavis (frappe préemptive face à l'imminence d'un tir nucléaire par exemple) ou dans le cadre d'une stratégie de compensation (*Offset Strategy*), visant à surmonter l'A2/AD.

La Chine, la Russie, et l'Inde avec une moindre ambition, **semblent s'orienter également vers l'utilisation d'armements hypersoniques afin d'interdire de vastes étendues maritimes.** Avec un dérivé opérationnel du planeur *DF ZF*, d'une portée de 2 000 km, Pékin serait en mesure de contrôler la plupart des lignes de communications maritimes en Asie et de menacer notamment la base américaine du pacifique à Guam.

b) Le facteur technologique et la plus-value capacitaire

Dans les systèmes de forces des grandes puissances, une technologie innovante, *a priori* intéressante, peut peiner à se concrétiser faute d'apporter une plus-value capacitaire réelle lorsque les planificateurs et les responsables budgétaires la comparent avec les combinaisons alternatives de moyens moins coûteux ou moins risqués. Les analyses accompagnant le développement des programmes américains montrent qu'il en est ainsi pour le CPGS lorsqu'on le compare aux moyens plus classiques de la puissance aérienne. Nombre de missions initialement prêtées aux armements hypersoniques (ciblage

d'opportunité d'objectifs mobiles, suppression des défenses antiaériennes) demeurent réalisables par d'autres moyens plus classiques, en fonction des configurations opérationnelles.

En France, l'adoption pour la composante nucléaire aéroportée de la propulsion hypersonique pourrait ouvrir la voie du choix d'une propulsion supersonique classique (statoréacteur) **pour le renouvellement des missiles de croisière et antinavires conventionnels** (programme *FMAN/FMC*[5]), le cas échéant, en coopération franco-britannique. La France a en effet toujours recherché jusqu'à présent une différenciation tangible entre armements nucléaires et conventionnels. Cette discrimination pourrait cependant être reconsidérée s'agissant du haut du spectre dans les missiles conventionnels.

Sur le plan technique, le développement des armements hypersoniques se heurte cependant à certaines difficultés :

- celle en premier lieu de la tenue des matériaux de revêtement aux très hautes températures générées par l'écoulement dynamique à fort Mach autour de la cellule ;
- celle de la maîtrise de la combustion en régime supersonique pour les armements autopropulsés ;
- celle de la précision à l'impact qui passe par un guidage terminal à la fois « résilient » à l'hypervélocité et satisfaisant sur le plan militaire (discrétion et autonomie) ;
- celle de la tenue des équipements à l'important régime vibratoire engendré par les phases de très fortes accélération et décélération au cours du vol ;
- celle de la compatibilité de leur géométrie avec un emport par un aéronef ou un missile porteur lorsqu'il s'agit de planeur hypersonique.

Les vecteurs hypersoniques sont toutefois porteurs d'avancées incontestables, lorsqu'on considère leur aptitude à compliquer la tâche des défenses antimissiles, mais aussi leur vélocité, à savoir :

- la capacité à frapper des objectifs de haute valeur situés dans la profondeur du dispositif de défense adverse (radars, postes de commandement, etc.), que les autres types de missiles, plus vulnérables, ne peuvent atteindre ;
- la capacité à frapper des objectifs identifiés (fixes ou mobiles) sur court préavis selon des principes de foudroyance et/ou de frappes préemptives.

Sous réserve de posséder un dispositif de ciblage suffisamment précis et dynamique, **l'armement hypersonique pourrait donc offrir une solution susceptible de démultiplier significativement la capacité d'interdiction conventionnelle,** en complément d'autres moyens. L'entrée en premier et la bataille pour la supériorité aérienne devraient pleinement profiter de l'apport de ces armements.

c) Le facteur institutionnel

L'histoire de l'innovation militaire montre que la plus-value capacitaire offerte par une technologie innovante qui se fonde sur la maturation et la rentabilité de cette technologie ne va pas de soi. Le décideur public a tendance à préférer l'amélioration de l'existant à l'introduction d'une innova-

5 - Futur Missile Anti-Navire / Futur Missile de Croisière.

tion radicale car celle-ci nécessite de consentir des investissements initiaux importants, sans pour autant se concrétiser tout de suite en une capacité opérationnelle. La culture institutionnelle représente un prisme important. Elle permettra ou non à une technologie de convaincre, au-delà du cercle des chercheurs qui l'auront conçue. C'est sa bonne appréhension par la communauté opérationnelle qui déterminera le soutien, ou le blocage, au niveau des arbitrages budgétaires. Les premiers retours d'expérience positifs ont en général l'effet d'un accélérateur.

Il est difficile de juger de l'application de ce référentiel pour les cas russe et chinois. Notons cependant que les armements hypersoniques semblent se fondre assez facilement dans les cultures chinoise et russe de projection de puissance et d'interdiction fondée sur l'emploi de missiles plus que sur l'engagement de plates-formes (avions, drones, navires, etc.).

Aux Etats-Unis, la stratégie de l'*US Air Force* considère l'hypersonique comme l'un des cinq « *game changers* » technologiques de la puissance aérienne, à terme. Cela étant, les aléas du CPGS ont fait dire à certains observateurs que **les armements hypersoniques constituaient une « technologie à la recherche d'une mission ».** La réorientation du CPGS en concept réduit aux opérations de théâtre ou à des missions sub-stratégiques est un facteur d'évolution encore mal appréhendé.

d) Le facteur budgétaire

Même si les vecteurs hypersoniques recueillent un soutien institutionnel réel, encore faut-il que les armées disposent de marges de manœuvre budgétaires permettant de les financer. A cet égard, **le pays le mieux disposé est probablement la Chine,** étant donné la vigueur de son effort d'armement depuis deux décennies, mais aussi son intérêt pour les technologies de rupture.

La marge de manœuvre des Américains est plus limitée. L'*US Army* est en phase de restauration de sa disponibilité opérationnelle qui affecte durablement sa stratégie de modernisation, laquelle a d'autres priorités que les armements hypersoniques. L'*Air Force* consacre certes une bonne place à ces équipements dans ses visions prospectives, mais doit absorber le coût de ses grands programmes (*F-35* en tête), au même titre que la *Navy*. Cependant, la recherche d'instruments offrant un effet stratégique tout en permettant d'opérer sous le seuil nucléaire est un élément de nature à favoriser le financement rapide d'une capacité hypersonique américaine.

La situation est sans doute moins favorable en ce qui concerne la Russie. Ses plans de modernisation lancés dans les années 2009/2010 apparaissaient déjà difficilement atteignables avant la crise économique qui l'affecte depuis deux ans. La maturation des programmes antinavires laisse cependant augurer qu'elle est en mesure de consacrer les fonds nécessaires à une capacité ponctuelle en la matière. Les perspectives de développement sont plus difficiles à évaluer pour les systèmes stratégiques à vocation probablement nucléaire, du fait de la disponibilité de systèmes d'armes efficaces et plus simples à moderniser. Toutefois, la Russie peut capitaliser sur des recherches entamées il y a une cinquantaine d'années (têtes manœuvrantes et planeurs), qui expliquent les avancées du programme *Yu-71*.

A l'horizon 2030 considéré ici, les avancées de l'Inde dans le domaine des armements hypersoniques devraient rester marginales.

2.2 – Conséquence : scénario de référence

Compte tenu de ces différents paramètres, les développements opérationnels d'armements hypersoniques devraient demeurer limités à l'horizon 2030. Ils présupposent en premier lieu une maturation rapide des technologies *ad hoc* dont le coût d'acquisition devra rester acceptable et, en second lieu, des efforts de défense restant au moins équivalents à ceux actuellement constatés.

Dans de telles circonstances, **la Chine devrait disposer à l'horizon 2030 d'une capacité opérationnelle de déni d'accès et d'interdiction de zone (A2/AD).** Une capacité initiale pourrait même apparaître dès le début de la prochaine décennie. En complément de ses moyens balistiques (missiles *DF 21*), ses planeurs hypersoniques renforceraient substantiellement sa stratégie A2/AD. Le déploiement de tels systèmes imposerait aux Etats-Unis un effort de modernisation des défenses antimissile de ses infrastructures fixes (Guam) et de ses moyens navals situés à portée des vecteurs hypersoniques chinois. A défaut, le déploiement des moyens américains les plus sensibles (groupe aéronaval) devrait être déporté à l'arrière pour échapper à cette nouvelle menace sans parade.

Pour notamment contrer ce développement, **les Américains pourraient disposer au cours de la décennie 2020 d'un système conventionnel de théâtre.** Une fois mis en service, le concept d'emploi de ces vecteurs serait étendu, au gré des opérations, au traitement d'objectifs de haute valeur ou contre lesquels est recherché un effet de foudroyance.

La Russie devrait concentrer son investissement dans la lutte antinavire et mettre en place l'architecture nécessaire à la mise en œuvre opérationnelle du *Tsirkon* dans le courant de la prochaine décennie. Le missile se déclinerait en versions navales et aéroportées, mais aussi en batteries côtières, dans un contexte marqué par le développement de moyens de défense navals devenant crédibles contre les vecteurs supersoniques. Cet armement pourrait être exporté vers des puissances régionales alliées de la Russie. L'avenir du planeur hypersonique *Yu 71* à vocation stratégique est plus incertain, sous l'effet combiné des contraintes budgétaires et de l'existence prévisible, à l'horizon considéré, de corps de rentrée manœuvrants sur les missiles balistiques russes.

3 - Enjeux pour la France et pour l'Europe

Le scénario de référence proposé ci-dessus aurait des implications directes assez limitées pour la France et ses alliés européens, mais des effets indirects significatifs :

- le durcissement des défenses des Etats potentiellement ciblées par les armes hypersoniques pourrait avoir un impact sur la capacité de pénétration de nos forces nucléaires et induirait une modernisation à hauteur de ce durcissement ;
- nos forces projetées dans des zones possiblement placées à portée de systèmes A2/AD hypersoniques, dont l'exportation doit être envisagée, conduiraient à renforcer leur protection ;
- la vulnérabilité de nos forces navales, déjà confrontées aux missiles supersoniques, serait encore accrue. L'existence d'hypersoniques air-mer, mer-mer et sol-mer devrait être prise en compte sur le plan opérationnel.

4 - Scenarii alternatifs

4.1 - Un scénario minimaliste

Le scénario minimaliste se fonde sur un contexte d'efforts de défense nettement plus contraints par une conjoncture économique et financière fortement dégradée sur le temps long. Dans ce contexte, les budgets manquent pour franchir le pas de la R&D vers des programmes opérationnels. Les priorités se concentrent sur les instruments classiques de la dissuasion nucléaire, sur la préservation des principaux programmes conventionnels et sur un investissement de compensation accru dans les capacités moins onéreuses de guerre électronique et de cyber.

Des systèmes hypersoniques ne sont déployés qu'en très faible quantité par les Etats-Unis, la Chine et la Russie. Le paysage stratégique n'est pas significativement modifié et seules des limitations ponctuelles sur les interventions extérieures pourraient devoir être gérées.

4.2 – Un scénario maximaliste

Le scénario maximaliste envisage à l'horizon 2030 une maturation accélérée à un coût contenu des technologies de l'hypervélocité entraînant un déploiement conséquent de systèmes.

Dans ce scénario, les Russes et les Chinois disposeraient en quantités substantielles de missiles antinavires hypersoniques de plusieurs milliers de kilomètres de portée qu'ils auraient exportés vers plusieurs puissances régionales. Cette prolifération aurait pour corollaire de s'accompagner d'un déploiement de drones de renseignement de théâtre et d'architectures de transmission de données. Elle aurait pour effet d'exposer à un risque important les marines de guerre.

La Chine et la Russie mettraient également leurs capacités hypersoniques de plus longue portée, mais aussi leurs capacités ISR[6], à disposition d'alliés. Cette mise à disposition serait porteuse de deux risques, car elle induirait :

- une capacité d'accès aux théâtres fortement dégradée pour les puissances militaires occidentales ;
- un risque de frappe de précision ponctuel opéré par le ou les pays ciblé(s) par une éventuelle intervention. Cette capacité jouerait un effet dissuasif.

Les Américains disposeraient dans leurs forces de planeurs et de missiles de croisière hypersoniques dont l'emploi s'appuierait sur des capacités C4ISR[7] exploitant pleinement les révolutions spatiales et cybernétiques en cours. Le risque d'un franc découplage capacitaire avec leurs alliés serait alors maximum. Il pourrait conduire, au sein de l'OTAN, au décrochage d'une majorité de puissances militaires européennes, contraignant à reformuler les coopérations dans le sens d'une complémentarité plus systématique.

Dans ce scénario, la France serait moins exposée que bon nombre d'Etats européens compte tenu de son avance technologique dans le domaine de l'hypervélocité. Elle prendrait la voie de la propulsion hypersonique pour sa composante nucléaire aéroportée et renforcerait également considérablement ses capacités de frappe conventionnelle dans la profondeur, en s'appuyant sur de nouveaux vecteurs conventionnels propulsés par statoréacteurs hautes performances (au-delà de Mach 4) ou adoptant également la propulsion hypersonique si des raisons financières ou industrielles incitaient à rechercher dans le haut du spectre une certaine communauté entre missile nucléaire et missile conventionnel.

6 - En anglais, *Intelligence, Surveillance, Reconnaissance*.

7 - En anglais, *Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*.

2

Militarisation et insécurisation de l'espace

L'essentiel

La multiplication des acteurs spatiaux, l'évolution des technologies et l'apparition de nouvelles menaces spatiales doivent conduire la France à poursuivre et à accroître significativement son rôle dans ce domaine. Cela doit se traduire à la fois par la promotion d'instruments de régulation nationaux et internationaux adaptés aux nouvelles conditions d'exploitation de l'espace, par l'acquisition de réelles capacités d'évaluation de la menace et par l'adoption de mesures de protection adaptées.

L'utilisation militaire croissante de l'espace en fait un enjeu stratégique majeur, l'espace jouant un rôle de multiplicateur de force pour les capacités militaires conventionnelles de tout pays souhaitant développer une politique de puissance.

L'espace civil constitue également un enjeu stratégique par ses implications économiques et sociétales. Le déploiement des satellites reste déterminant pour l'accès à l'information. C'est le cas notamment des satellites de télécommunications, dont le développement permet de connecter tous les points du globe, ainsi que des satellites de géolocalisation, qui donnent un accès direct à une référence temporelle et à une position très précise. Il en est de même des satellites d'observation qui permettent une surveillance permanente de la planète au service de la météorologie, de l'océanographie, de la cartographie, de la surveillance de l'évolution climatique, ainsi que pour des applications de sécurité civile telles que l'organisation des secours en cas de catastrophes majeures.

Alors que le nombre d'acteurs privés et publics agissant dans l'espace extra-atmosphérique s'accroît continûment, les risques et les menaces dans ce nouveau milieu de confrontation se démultiplient. D'ores et déjà s'affichent des velléités d'action militaire dans l'espace, tandis que s'y déroulent des opérations qui laissent peu de doute sur leur finalité réelle.

Il ne s'agit plus de savoir si des moyens militaires seront capables d'interagir dans l'espace à l'horizon 2030, mais plutôt de s'interroger sur les voies et moyens susceptibles, à cette échéance, d'apporter de la sécurité aux opérations spatiales. Le développement d'un véritable volet spatial dans nos politiques de défense et la mise en place d'une réglementation par le droit international sont les deux leviers disponibles pour parvenir à cette fin.

1 - Etat des lieux en 2017

Le thème de la sécurité de l'espace a pris une importance croissante depuis la fin de la Guerre froide. Tant que celle-ci durait, bien que des armes anti-satellitaires (ASAT) fussent testées du côté américain comme du côté soviétique, elles ne furent jamais déployées opérationnellement et un principe de retenue s'appliquait. Les satellites étaient pour l'essentiel soit américains, soit soviétiques, et pouvaient être considérés comme invulnérables, ce qui offrait d'intéressantes perspectives militaires. Cette situation a désormais cessé d'être.

En premier lieu, l'effondrement du bloc soviétique a mis fin à une certaine parité entre les deux grandes puissances spatiales, laissant les Etats-Unis occuper une position dominante (budget, nombre de satellites en orbite, missions remplies, etc.). Cette suprématie américaine, liée à la multiplication des usages civils de l'espace, a créé une dépendance qui a conduit à une perception de vulnérabilité. La commission Rumsfeld, créée en 1999 pour « évaluer l'organisation et la gestion des activités spatiales comme soutien à la sécurité nationale » et qui a rendu ses conclusions à la veille de l'entrée en fonction de l'administration Bush, évoquait à cet égard la perspective d'un « Pearl Harbor spatial ». Elle recommandait de « poursuivre vigoureusement l'acquisition des capacités assurant que le Président soit en mesure de déployer des armes dans l'espace ». En 2006, alors que les capacités spatiales russes étaient en forte dégradation, Washington a adopté une politique pour l'espace qui prenait en compte explicitement les préoccupations militaires[1]. Aujourd'hui, les Etats-Unis détiennent une position de domination absolue s'agissant de sécurité spatiale. Ils disposent d'une gamme complète et performante de moyens de surveillance de l'espace et de systèmes (au sol et dans l'espace) visant à dénier à une force hostile toute utilisation de l'espace. Après être passé du concept d'espace « sanctuarisé » aux concepts de « *Space control* » et de « *Space dominance* », qui caractérisent aujourd'hui la doctrine militaire spatiale des Etats-Unis, Washington ne renie pas l'éventualité d'une guerre dans l'espace sur le principe de la légitime défense et via l'introduction implicite de la notion de frappe préventive. Dans cette perspective, un travail important de réflexion est actuellement en cours à l'initiative de l'*Institute of Air and Space Law* de l'université de McGill, sur les règles d'engagement possibles dans l'espace.

La domination américaine n'a toutefois pas empêché l'émergence de nouveaux acteurs ayant l'ambition de maîtriser toute la chaîne du spatial, notamment sa dimension militaire, et entrant en compétition avec les Etats-Unis. C'est tout particulièrement le cas de la Chine qui n'a pas fait mystère de ses intentions en procédant, en janvier 2007, à la destruction d'un de ses vieux satellites météorologiques en orbite à 800 km grâce à l'utilisation d'un véhicule d'interception à énergie cinétique mis en orbite par, selon toute vraisemblance, un missile dérivé d'un missile balistique. Ce tir a généré une importante et durable pollution d'une orbite très occupée en y dispersant des milliers de débris. Une année plus tard, Washington, ayant bien perçu

1 - « Les Etats-Unis prendront les mesures qu'ils estimeront nécessaires pour protéger leurs capacités spatiales, répondre aux interférences, et, si besoin est, interdire à tout adversaire l'utilisation de moyens spatiaux hostiles aux intérêts américains ». « Le Secrétaire à la Défense développera les capacités, les plans et les scénario d'emploi pour assurer une liberté d'action dans l'espace, et la dénier sur ordre à tout adversaire ».

le message chinois, y répondait en détruisant un de ses satellites en perdition à une altitude de 247 km au moyen d'un missile *SM 3* modifié tiré d'une frégate. Quelques mois plus tard, le chef d'état-major de l'armée de l'air chinoise estimait « historiquement inévitable » une compétition entre forces armées dans l'espace et jugeait « impératif » que la Chine y développe des moyens offensifs et défensifs. Depuis, Pékin conduit de nombreuses opérations spatiales à vocation militaire et conduit des programmes d'équipements susceptibles d'opérer de manière offensive dans l'espace comme l'avion spatial *Shenlong* qui n'est pas sans rappeler le *X 37B* américain[2].

Les évolutions technologiques considérables qui concernent le secteur spatial depuis une quinzaine d'années ont aussi changé la donne (ère du *New Space*). La miniaturisation des satellites (mini, voire microsatellite) de très haute performance[3], l'arrivée sur le marché de lanceurs à bas coût, voire réutilisables, l'émergence d'acteurs privés, sont autant de facteurs qui renforcent la compétition et les rapports de force dans l'espace et sur Terre.

Ces évolutions, qui portent la marque d'une compétition parfois vive, fragilisent le « Traité de l'espace » de 1967 qui fixe les principes régissant les activités des Etats en matière d'exploration et d'utilisation de l'espace extra-atmosphérique. Aujourd'hui, la sécurité de l'espace englobe une large palette de questions qui recouvrent pour l'essentiel deux grandes catégories de préoccupations portant sur l'environnement spatial (débris, météo spatiale, encombrement des orbites) et sur l'usage des moyens spatiaux (militarisation, arsenalisation de l'espace). Des enceintes distinctes traitent de ces deux volets de la sécurité dans l'espace (Conférence du désarmement et COPUOS[4]) et l'on constate une paralysie des négociations internationales dans l'un et l'autre format, le nombre croissant d'acteurs et l'inégalité de leur poids respectif n'incitant personne à une attitude coopérative, alors que la plupart des experts convergent sur une quasi-inéluctabilité d'affrontements dans l'espace. En effet, les satellites sont à la fois des moyens essentiels pour les Etats et des cibles vulnérables, le tout loin du sol, c'est-à-dire avec une relative impunité et une difficulté d'attribution de l'acte hostile.

En France, si le Livre blanc sur la défense et de la sécurité nationale de 2013 a bien identifié ces enjeux et la dimension stratégique qu'ils revêtaient[5], force est de constater le décalage entre les ambitions affichées et la faiblesse des moyens consacrés à la sécurité des moyens spatiaux nationaux.

2 - Le *X 37B* est un avion spatial mis en œuvre par l'*USAF* qui évolue en orbite basse (moins de 1 000 km, typiquement vers 400 km). Doté d'une soute et manœuvrant, il est capable de placer une petite charge utile en orbite et d'inspecter, voire de récupérer des satellites. Il a volé pour la première fois en 2010.

3 - Ce qui est vrai pour les satellites ne l'est pas encore pour les lanceurs. Le seul acteur privé actuel, *SPACE X*, est adossé à la *NASA* et à l'*US Air Force* pour le développement de ses lanceurs.

4 - *Committee on the Peaceful Uses of Outer Space*.

5 - « Avec la multiplication des débris spatiaux et l'apparition de possibilité d'agressions directes sur des satellites, la protection de l'espace extra-atmosphérique constitue désormais un enjeu majeur au regard de l'importance des services et des missions auxquels pourvoient les moyens spatiaux. La France soutiendra les travaux internationaux visant à promouvoir le développement durable de l'espace. Elle maintiendra l'effort de développement des capacités relatives à la surveillance de l'espace afin de préserver une autonomie d'appréciation de la situation spatiale. Une approche européenne sera favorisée sur ce sujet d'intérêt partagé en tirant partie des moyens existants comme le radar *GRAVES* et en développant de nouveaux projets concrets. Un schéma directeur organisant la mission de surveillance de l'espace et les différents acteurs y concourant sera établi. Les infrastructures terrestres d'exploitation des systèmes spatiaux feront l'objet d'une protection renforcée ». (Livre blanc sur la défense et la sécurité nationale 2013 – page 103).

2 - Situation en 2030

L'hypothèse la plus vraisemblable repose sur un renforcement à l'horizon 2030 des politiques de défense dans l'espace, au détriment de l'élaboration de normes et de réglementations internationales aux fins de sécurisation de l'espace. En 2030, les Etats-Unis, la Chine et la Russie entretiendront probablement dans l'espace un rapport de force et devraient ainsi mettre en œuvre une politique spatiale militaire incluant un volet offensif et un volet dissuasif. Il est vraisemblable qu'il n'y aura pas, à cet horizon, d'engagement coopératif de ces Etats dans la négociation de règles de sécurité collective. Pour les grandes puissances ne reniant pas une dimension militaire affirmée dans leur politique spatiale (Etats-Unis, Russie et Chine principalement), la sécurité spatiale ressemble peu ou prou, à l'horizon 2030, à la course aux armements nucléaires des débuts de la Guerre froide avant l'adoption du TNP.

S'agissant des évolutions du droit international de l'espace, l'irréductibilité des positions russe, chinoise et américaine en matière de réglementation relative à l'arsenalisation de l'espace **gèle, dans le scénario envisagé, tout processus collectif de sécurisation de l'espace.** L'opposition se renforce entre pays souhaitant un régime contraignant, dans une perspective de contrôle des armements et pays valorisant la notion de « comportement responsable », renvoyant à la responsabilité nationale de chaque pays et aux mesures de transparence et de confiance. **Ainsi perdure le blocage dans les enceintes multilatérales chargées de ces questions.**

Les politiques de défense dans l'espace se renforcent en se déclinant selon plusieurs approches, non exclusives l'une de l'autre :

- durcissement des satellites et des infrastructures au sol, notamment sur le plan de la cybersécurité ;
- développement de satellites manœuvrants capables de se soustraire à une menace ;
- développement d'architectures de systèmes spatiaux utilisant des constellations de microsatellites, voire des systèmes en briques distinctes afin d'améliorer la résilience en cas d'attaque (associées à une capacité de remplacement rapide) ;
- défense active des moyens en orbite avec des moyens offensifs ;
- menace de représailles (politique déclaratoire et moyens associés).

Les Etats-Unis devraient adopter une stratégie de riposte graduée. Dans cette perspective, ils continueraient à fournir l'effort le plus important en matière de développement de programmes antisatellites, fragilisant ce faisant, jusqu'à le mettre en péril, le « Traité de l'espace » de 1967. Les Américains demeureraient à la fois ceux qui redoutent le plus les menaces d'actions offensives contre leurs satellites – qu'elles s'expriment du sol ou de l'espace –, et ceux qui disposent des moyens offensifs les plus importants. Matérialisant concrètement leur *National Space Security*

Strategy, les Etats-Unis pourraient déployer dans l'espace des systèmes d'armes aux fins de légitime défense, de dissuasion par représailles et de frappe préventive. La Russie et la Chine, entendant être considérées à l'égal des Etats-Unis, pourraient aussi développer une politique de puissance dans l'espace.

La surveillance de l'espace restera la pierre angulaire de la sécurité spatiale dans ses trois fonctions : détection, identification, suivi. Il s'agira de savoir précisément ce que font les autres pays, d'avoir un support indispensable aux ASAT (ciblage notamment) et de pouvoir détecter des menaces éventuelles. La Russie et la Chine auront modernisé et développé leurs capacités de surveillance, tandis que l'Inde pourrait privilégier le partage de données SSA (*Space Situational Awareness*) avec les Etats-Unis et conduire une politique d'intégration de moyens étrangers (japonais, européens...) *via* une politique de coopération active.

3 – Enjeux pour la France et pour l'Europe

Une position passive de la France et de l'Europe serait contre-productive, sauf à accepter de perdre toute crédibilité en tant qu'acteur sur la scène spatiale internationale ce qui semble inenvisageable. Deux options sont possibles :

- développer une politique de défense dans l'espace ;
- adopter une position de médiateur visant à limiter le développement/déploiement de moyens contre-spatiaux.

Dans les deux options, souveraineté et autonomie d'appréciation devront être les deux piliers de notre politique. Cela implique que la France et l'Europe se dotent de réelles capacités afin d'évaluer les menaces qui visent leurs satellites et de prendre les mesures de protection adaptées. La France, qui a un rôle de pionnier dans le domaine de la SSA et dispose d'ores et déjà de capacités dans ce domaine, devrait continuer à sensibiliser ses partenaires européens sur ces questions et en particulier rechercher avec l'Allemagne (dont les moyens nationaux sont complémentaires), la construction d'une dynamique commune.

3.1 – La France s'engage dans une politique de défense de l'espace

Une première option pour l'Europe consisterait à participer à la dynamique globale de rapport de force entre Etats observée dans l'espace et de développer en conséquence une politique de défense spatiale. La France et les Européens devraient dans cette hypothèse se doter en priorité de moyens indépendants robustes de surveillance spatiale, ce qui impliquerait notamment de tenir le calendrier de rem-

placement du système Graves, de développer les moyens d'observation associés et d'accroître l'interopérabilité avec les autres capacités européennes, notamment allemandes.

La France devrait, de plus, se doter d'instruments de représailles et d'une politique déclaratoire en rapport. Ceci nécessiterait un choix politique de rupture, qui devrait être traduit rapidement dans la programmation militaire, compte tenu des délais de développement de tels systèmes. Le lancement d'un tel programme en commun avec des partenaires européens pourrait naturellement être envisagé. Des effets d'annonce sur les briques technologiques existantes en matière de moyens antisatellites (brouillage par exemple) pourraient être utilisés.

3.2 – L'Europe et la France privilégient la négociation internationale pour sécuriser l'espace

La seconde option pour la France et pour l'Europe consisterait à adopter une position de médiateur en limitant le développement/déploiement de moyens contre-spatiaux. Acteurs de l'élaboration de normes et de réglementations internationales, déclinant une approche soft-power, elles renforceraient leurs positions en devenant force de proposition. Utilisant les instruments de la diplomatie, elles tenteraient de réunir les positions parfois éloignées de la communauté internationale, notamment en travaillant et en réfléchissant sur les conditions nécessaires pour élaborer un droit de la guerre dans l'espace. Pour soutenir cet effort diplomatique, l'Europe devrait toutefois assurer son autonomie stratégique en se dotant d'un outil spatial militaire commun qui pourrait, dans un premier temps, résulter de la fédération et de l'interopérabilité des moyens nationaux. En outre, le développement de programmes militaires spatiaux en Europe et en France pourrait bénéficier d'une coopération accrue avec les opérateurs civils (privés ou publics). Être un acteur crédible en matière d'espace militaire renforcerait cette position d'acteur médiateur. L'épisode infructueux du code de conduite sur l'espace exo-atmosphérique, porté par une Europe au rôle spatial timide face à une Chine au caractère plus agressif, a démontré l'importance de ce point.

Sous réserve que les efforts nécessaires aient été engagés par la France et l'Europe pour peser comme puissance spatiale, il faudrait dans cette hypothèse que la période d'ici 2030 soit mise à profit pour poser les jalons d'un futur instrument de régulation. Le choix du moment et des termes pour assembler les éléments menant à cette initiative sera délicat (le risque étant qu'une telle initiative apparaisse dupliquer dans sa substance le projet PAROS traditionnellement porté par la Russie et la Chine contre les intérêts américains au sein de la Conférence du désarmement).

En termes de contenu, l'initiative, qui devra être progressivement alimentée d'ici à

2030, visera à faire évoluer le droit de l'espace et à l'adapter aux nouvelles conditions de son exploitation telles que l'ouverture aux acteurs privés, la multiplication du nombre de petits satellites et des petits lanceurs, la croissance rapide du club des Etats possesseurs de moyens spatiaux, en recherchant un nouvel équilibre suivant trois axes :

- la non-appropriation de l'espace ;
- le bannissement des armes dans l'espace ;
- l'engagement à ne pas créer de débris dans l'espace.

En cas de fort durcissement des relations internationales spatiales (rigidification des politiques déclaratoires des grandes puissances, suivies par les puissances spatiales émergentes), la France et l'Europe devraient alors changer de posture et s'engager dans une politique de défense spatiale envisageant l'utilisation de moyens de défense, comme le brouillage, le laser au sol ou encore la cyberdéfense.

4 - Scenarii alternatifs

4.1 – Une réglementation internationale qui se renforce avec la conclusion d'un traité de non-déploiement d'armes dans l'espace dans un contexte de détente des relations internationales spatiales

La proposition russe effectuée lors de la 59ème session du *Committee on the Peaceful Uses of Outer Space* (COPUOS) de juin 2016, consistant à créer une plate-forme d'informations alimentée tant par les Etats que par les acteurs privés, est acceptée. Sur cette base, un catalogue public précis et exhaustif des objets en orbite est créé.

La mise en œuvre de cette initiative ouvre la voie à des négociations entre puissances spatiales pour moderniser le droit de l'espace et l'adapter aux nouvelles conditions de son exploitation telles que l'ouverture aux acteurs privés, la multiplication du nombre de petits satellites et des petits lanceurs, la croissance rapide du club des Etats possesseurs de moyens spatiaux, etc.

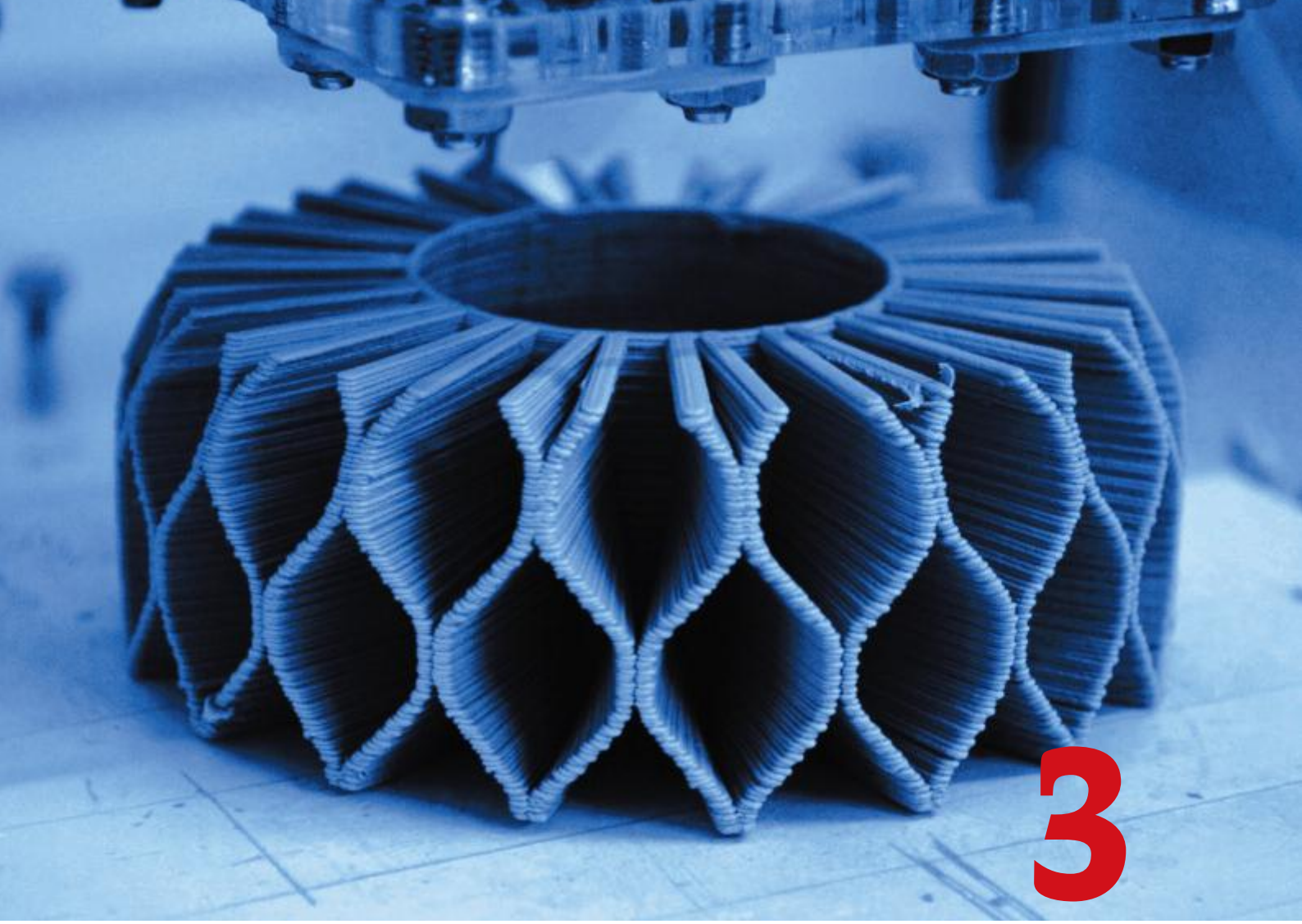
Sur ces nouvelles bases communes, l'élaboration d'un traité de non-prolifération des moyens ASAT et de non-déploiement d'armes dans l'espace est enclenchée. Des mesures de contrôle telles que l'accès transparent aux infrastructures spatiales nationales, la mise en place d'une surveillance spatiale internationale, la création d'une organisation internationale unique pour couvrir tous les aspects de la sécurisation de l'espace, peuvent dès lors être mises en débat, les mesures de confiance devant désormais garantir la sécurité des Etats.

4.2 – Un durcissement majeur des relations internationales spatiales amène l'Europe à renforcer sa position en matière d'antisatellites et d'armes dans l'espace

Le déploiement d'armes dans l'espace est acté et l'officialisation de l'emploi d'armes antisatellites est avérée. Les politiques déclaratoires des différentes puissances spatiales n'excluent pas une montée aux extrêmes en cas de conflit. Les puissances spatiales émergentes suivent la même voie.

La prise de conscience par l'Europe de ses responsabilités et de la nécessité d'avoir un argumentaire solide pour accroître sa crédibilité internationale, notamment vis-à-vis des Etats-Unis, l'amène à se recentrer sur le développement d'un réseau renforcé de surveillance spatiale complétement autonome dans lequel la France joue un rôle de premier plan. Cette montée en puissance d'un système de surveillance spatiale permet d'apprécier les risques et d'adopter des solutions adaptées. Dans ce cadre, la France et l'Europe s'engagent dans une politique de défense spatiale qui envisage l'utilisation de moyens de défense, comme le ou les lasers au sol.

L'autorisation des mesures de dissuasion par menace de représailles conduit à des relations tendues entre Etats-membres de l'UE. La France doit convenir, au plan national, de mesures techniques et doctrinales pour encadrer les évolutions de la posture européenne.



3

La révolution de l'impression 3D

L'essentiel

La fabrication additive ouvre de nouvelles perspectives qui représentent autant d'enjeux dans les différents secteurs pour lesquels cette nouvelle technologie apportera des solutions innovantes. Elle ouvre des perspectives aux armées en termes de logistique, notamment pour la réparation rapide des matériels. Elle fait parallèlement apparaître de nouvelles menaces, compte tenu des facilités offertes pour des activités de prolifération et la fabrication d'armes par des acteurs non étatiques.

La France doit continuer à être un acteur de cette innovation, tout en contribuant à encadrer son développement afin que celui-ci soit cohérent avec les différents régimes de contrôle, les traités d'interdiction en vigueur, les règles d'exportation et les embargos.

L'impression 3D fait référence à un processus de fabrication dit « additif », connu également sous l'acronyme anglo-saxon « AM » pour « *Additive Manufacturing* ». La fabrication additive est définie comme le procédé de mise en forme d'une pièce par ajout de matière, à l'opposé de la mise en forme traditionnelle par enlèvement de matière (usinage). L'impression tridimensionnelle recouvre en pratique plusieurs types de technologies, mettant en œuvre des matériaux très divers tels que les polymères thermodurcissables ou thermoplastiques, le bois (papier), les métaux (titane, chrome-cobalt) et les matériaux céramiques industriels ou structurés[1].

Le développement des technologies liées à l'impression 3D a débuté dans les années 1980. Toutefois, ce n'est que depuis quelques années que sa commercialisation, potentiellement exponentielle, incite les observateurs à parler de nouvelle « révolution industrielle », comparant l'émergence de l'impression 3D à la genèse de l'Internet.

En dépit de l'intérêt qu'elle suscite, le niveau de maturité de cette technologie doit être relativisé. Elle reste en effet à ce stade une capacité émergente pour laquelle, malgré des annonces spectaculaires, le passage à la production de masse se fait toujours attendre.

Les principaux usages actuels de l'impression 3D s'opèrent au niveau des industriels généralistes des secteurs aéronautique, automobile, de la santé et, dans une moindre mesure, de la défense, qui intègrent la fabrication additive dans leurs processus[2]. A ce titre, cette méthode est essentiellement utilisée comme aide à la conception (prototypage, réalisation de modèles de présentation) ou pour produire des pièces fonctionnelles (pièces neuves,

1 - Les sept principaux procédés suivants y sont associés : photopolymérisation en cuve, projection de matière, projection de liant, fusion sur lit de poudre, extrusion de matière, dépôt de matière sous flux d'énergie dirigée et stratification de couche.

2 - Coopération sur la stéréolithographie entre *RENAULT*, *PEUGEOT* et *DASSAULT AVIATION* dès la fin des années 1980.

réparation de pièces endommagées) et des outillages pour la production (moules, outils). Le recours le plus important à ce procédé reste la maintenance, pour laquelle cette technologie est appliquée pour le remplacement en petites séries de pièces qui ne sont plus fabriquées ou pour lesquelles le transport n'est pas rentable.

Dans le secteur de la défense, les industriels pourraient tirer de nombreux bénéfices de l'impression 3D et ce, bien au-delà de la seule possibilité de créer des armes rustiques par fabrication additive, comme dans le cas de l'affaire « Cody WILSON », fortement médiatisée, qui a fait planer le spectre d'une production de masse d'armes à domicile[3].

Toutefois, il est d'ores et déjà possible d'identifier quatre impacts potentiels de l'impression 3D sur les enjeux de sécurité et de défense, à savoir :

- **une remise en cause des équilibres industriels** actuels dans une gamme d'activités allant de la chimie et la biologie à la santé en passant par les industries traditionnelles, du fait de l'émergence d'un marché spécifique (production de machines d'impression ; production de produits et de pièces *ad hoc*) et de la modification des rapports de compétitivité ;
- **la mise à disposition de la défense** de nouveaux moyens logistiques, notamment dans le domaine de la cartographie du champ de bataille, de la maintenance et de la médecine de guerre ;
- **l'apparition d'un risque nouveau** de prolifération des armes de destruction massive, par la création de voies possibles de contournement des contrôles d'acquisition de matériels sensibles ;
- **l'émergence de modes opératoires nouveaux pour les terroristes,** la 3D, technologie potentiellement plus accessible, leur permettant à terme de créer facilement eux-mêmes des objets dont l'acquisition est aujourd'hui complexe.

3 - Nom du jeune Américain ayant réalisé un pistolet rustique par fabrication additive. La publicité donnée à cette affaire par les médias a entraîné une inquiétude visible de l'opinion publique et des pouvoirs publics.

1 - Etat des lieux en 2017

S'il est aujourd'hui trop tôt pour parler de « quatrième révolution » avec certitude, l'impression 3D apparaît toutefois clairement comme une technologie détenant un potentiel de rupture[4].

1.1 - Les acteurs

a) Cartographie des Etats moteurs en matière de R&D sur l'impression 3D

- Les Etats-Unis

Les Etats-Unis se sont lancés les premiers dans la course à la 3D et à la fabrication additive. La première société, *3D SYSTEMS*, a été créée en 1986. Vingt ans plus tard, le président OBAMA en fit une priorité politique en engageant plusieurs programmes *via* « *We can't wait !* », puis « *Join the Revolution now !* » dans les secteurs de la recherche et l'industrie. L'ambition du président américain était la mise en place d'un réseau national d'innovation en matière de procédés de fabrication (NNMI). Un milliard de dollars aurait été consacré à la formation et deux milliards aux investissements. Entre 2010 et 2014, 700 000 emplois auraient été créés dans le secteur.

- La Chine et l'Asie-Pacifique

La Chine a engagé une réflexion en 2012 sur l'impression 3D. Pour Pékin, cette démarche répondait à l'origine à deux enjeux majeurs : se repositionner face aux relocalisations occidentales et au déplacement de la concurrence manufacturière à bas coût en Asie du Sud-est d'une part, et maintenir sa compétitivité industrielle vis-à-vis des Etats-Unis d'autre part.

Les efforts de recherche consentis par la Chine s'inscrivent dorénavant dans la stratégie économique et sociale chinoise de long terme. Elle s'attache à consolider son secteur industriel à partir de ses trois champions (*TIERTIME*, *FARSOON*, et *SHINING 3D*) tout en développant la R&D et le secteur particulièrement porteur des imprimantes personnelles.

Le Japon s'est intéressé très tôt à la fabrication additive, commercialisant ses premières machines dès 1988. Le gouvernement japonais considère la fabrication additive comme une technologie clé et a mis en œuvre depuis 2013 de nombreuses initiatives devant lui permettre de disposer de fondations saines pour exploiter la fabrication additive métallique[5] et favoriser l'innovation associée[6]. D'autres Etats asiatiques (Singapour, Corée du Sud, Australie) ont également développé des plans nationaux de recherche et de développement, mais qui restent à un niveau moins avancé.

4 - Elle a notamment inspiré la mise en place de « *FabLab* », afin de favoriser l'innovation et de permettre au grand public de s'approprier ces technologies.

5 - *Technology research association for future additive manufacturing*.

6 - *Strategic innovation promotion program*, d'une durée de 5 ans.

- **Israël**

Pays dynamique dans le domaine des nouvelles technologies, Israël l'est également en matière d'impression 3D et ce, sans bénéficier d'intervention étatique spécifique. Les sociétés mixtes israélo-américaines comme *STRATASYS* jouent un rôle majeur au niveau mondial, alors que dans le domaine de la recherche, le *TECHNION* d'Haïfa est à la pointe.

- **Europe**

Le potentiel industriel de l'impression 3D n'a pas échappé aux Etats européens disposant déjà de capacités industrielles importantes. Ainsi, l'Allemagne s'est lancée dans la course via le plan « Industrie 4.0 » dès 2012 en s'appuyant sur le réseau des *Fraunhofer*, dont une partie est consacrée à la R&D sur les techniques manufacturières. Le Royaume-Uni s'est également investi dans ce secteur dès 2012, *via* son programme triennal « *High Value Manufacturing* », dont la fabrication additive manufacturière était l'une des thématiques d'étude.

Première à s'être lancée dans la recherche 3D dans les années 1980, la France n'a pas su capitaliser sur son avance. Les nombreuses initiatives actuelles d'industriels[7], d'écoles d'ingénieurs[8] ou de régions[9] animent et cherchent à structurer un secteur dont le développement reste naissant. Le plan « Usine du futur », lancé en 2015, attribue une place modeste à la fabrication additive, également identifiée par la Direction générale des entreprises (DGE) du ministère de l'économie et des finances comme l'une des 47 technologies clés listées dans le rapport « Technologies 2020 ».

Sur le plan communautaire, la fabrication additive est présente dans le programme de recherche de l'Union européenne « Horizon 2020 » et 88 projets, touchant les domaines les plus divers, ont été lancés entre 1991 (PCRD) et 2013. Elle n'est, cependant, qu'une priorité européenne parmi d'autres.

b) Les équipements et les sociétés

- **Parcs installés, production et vente de machines par région du globe**

Les Etats-Unis détiennent 40 % des machines d'impression 3D à usage industriel dans le monde. Le reste des machines de ce type se répartissent à parts sensiblement égales entre l'Europe (28 %) et la région Asie-Pacifique (27 %)[10]. En 2016, l'Europe accueillait le plus grand nombre de sociétés productrices de machines (47 %), devant l'Asie (Chine à 17 %, Japon à 12 % et Corée du Sud à 7 %), les Etats-Unis (15 %) et Israël (2 %). La répartition des ventes par région du globe évolue très rapidement. En 2015, Israël était le principal fournisseur (41 %) devant l'Europe (32 %), les Etats-Unis (17 %) et l'Asie (10 %).

La tendance récente est à une montée en puissance de l'Asie et de l'Europe sur le marché. Une forte croissance du développement des technologies métalliques, supérieure à celle des machines mettant

7 - Exemples : projet *SOFIA* impulsé par *FIVES - MICHELIN Additive Solutions Joint-Venture*, « *Initiative 3D* » de l'*IPC* ou Centre technique industriel de la plasturgie des composites, centre de recherche et technologie *SAFRAN TECH* inauguré en janvier 2016 par *SAFRAN Additive Manufacturing*.

8 - Exemple : *Institut Carnot M.I.N.E.S.*

9 - Exemple : plateforme *CETIM-CERTEC*.

10 - Chine (9,5 %), Japon (9,4 %), Corée du Sud (2,9 %) et Taïwan (1,6 %).

en œuvre des polymères, est notée sur l'ensemble du globe depuis 2015. Cette dynamique n'est pas neutre s'agissant d'intérêts de défense, puisque l'un des premiers secteurs utilisateurs des procédés de fabrication additive métallique est celui de l'aéronautique, dont le caractère dual est très affirmé.

- **Sociétés productrices de machines**

Le rapport *Wohlers*[11] de 2016 identifie 62 sociétés majeures productrices d'imprimantes 3D (un plus grand nombre de sociétés de services exploitent par ailleurs ce procédé).

STRATASYS (société américaine comptant depuis décembre 2012 une branche israélienne) et *3D SYSTEMS* (société américaine qui a racheté à 80 % la société française *PHENIX SYSTEMS*) dominent le marché de la production. Elles sont défiées par trois sociétés européennes : *ENVISIONTEC* (Allemagne), *MCOR* (Irlande) et *EOS* (Allemagne). Les autres entreprises se partagent le reste du marché. Les sociétés françaises actives dans ce domaine sont principalement *PRODWAYS* (groupe *GORGE*), *BEAM*, *PHENIX SYSTEM* (filiale de *3D SYSTEMS*) et *3D CERAM*.

- **Matières premières et pays producteurs**

L'impression 3D nécessite des matières premières, dont la disponibilité conditionne la capacité d'imprimer. Les principales matières utilisées sont : des photopolymères (46 %), des poudres polymères (25 %), des filaments (15 %) et des poudres métalliques (11,5 %).

Les constructeurs de machines sont, dans la majorité des cas, les principaux fournisseurs des matières d'impression. Il en existe de très nombreux aux Etats-Unis, en Europe (Allemagne, Italie, Royaume-Uni, Belgique, France), en Asie (Chine, Japon) et au Moyen-Orient (Arabie saoudite). A ce jour, il n'existe pas de contrôle dédié, ce qui pourrait à terme ouvrir une possibilité de contournement des régimes de contrôle de certaines technologies sensibles (groupes de fournisseurs contrôlant les biens nucléaires, biologiques, chimiques, liés aux missiles et aux armements).

- **Ensembliers et sous-traitants**

Des entreprises, qui comptent parmi les plus importantes au monde, développent déjà des unités de fabrication additive, que ce soit dans le secteur aéronautique (*AIRBUS, SAFRAN, GENERAL ELECTRIC, BOEING, DASSAULT*), le secteur automobile (*BMW, FORD*) avec ses sous-traitants (*MICHELIN* qui se trouve en pointe), mais aussi dans les domaines de la chimie et de la santé (reconstitution de tissus, d'os, etc.).

Pour les ensembliers, comme pour les sous-traitants, les gains de productivité peuvent être considérables sous l'effet de deux facteurs :

- l'accélération, parfois très significative, du rythme de production qui entraîne une baisse des coûts de celle-ci pouvant aller jusqu'à 75%[12] ;
- la diminution des délais nécessaires au développement et à l'expérimentation de solutions ou de produits viables, également source importante de réduction de coûts.

11 - Le *Wohlers 2016* appuie ses résultats sur les réponses apportées par 62 producteurs de machines et 98 fournisseurs de services.

12 - *SNECMA* va imprimer ses injecteurs de moteurs de la fusée *Ariane* en deux semaines au lieu de neuf mois.

Le secteur de la fabrication additive se caractérise aussi par le développement d'entreprises qui peuvent réaliser à façon des impressions sur la base d'une description logicielle du produit ; il s'agit là aussi d'une flexibilité pouvant affecter l'efficacité des régimes de contrôle.

1.2 – Le marché : des perspectives de développement importantes

La 3D et la fabrication additive représentent un marché émergent. Les hypothèses de travail laissent entrevoir des possibilités exponentielles de croissance dans de très nombreux domaines (bien au-delà de ce qui est exploité aujourd'hui) : production, approvisionnement, flux logistiques, stockage, inventaires des stocks.

Deux types d'investissement en impression 3D existent, dont les effets diffèrent fondamentalement : les investissements orientés vers des imprimantes de taille réduite fonctionnant essentiellement à partir de matières plastiques dont le prix (quelques milliers de dollars) baisse continûment, et ceux qui sont orientés vers des machines travaillant sur des métaux et alliages extrêmement complexes dont le coût peut atteindre plusieurs millions de dollars.

Le marché des imprimantes 3D, quel qu'en soit le type, est en progression constante. Alors que seule une dizaine de machines industrielles avait été vendue à la fin des années 1990, la barre des 5 000 unités a été franchie en 2010 pour atteindre 8 000 en 2012, et 13 000 en 2014[13]. Les ventes aux particuliers d'imprimantes de type *RepRap* sont en hausse constante (35 000 exemplaires vendus jusqu'en 2012 ; 140 000 entre 2012 et 2014). La vente de matériaux *ad hoc* (poudre de titane et autres poudres métalliques) suit cette tendance. Sur le plan financier, plusieurs rapports (*Market Research Reports, Wolhers*, IHS) prévoient une croissance forte, tant au niveau des zones de production historiques que des pays émergents. Pour ces derniers, le marché pourrait augmenter de 20 % d'ici 2020. Le rapport *Wolhers* souligne que la fabrication additive a engendré 4,5 milliards de chiffre d'affaires en 2014, 7 milliards en 2016, puis 12,5 en 2018 et 20 milliards de dollars en 2020. *IHS*, qui prend en compte tous les aspects de la 3D, des machines aux pièces détachées et autres produits, avance le chiffre global de 35 milliards pour 2020 tandis que *MCKINSEY* l'estime à 550 milliards de dollars à l'horizon 2025. Le passage dans le domaine public de nombreux brevets pourrait accélérer le phénomène.

Les secteurs de la défense et de l'aérospatial sont très actifs, à l'image d'*AIRBUS* qui a récemment annoncé son intention d'imprimer en 3D la moitié de sa flotte à terme.

13 - Aux Etats-Unis, la vente d'imprimantes industrielles représentait déjà en 2014 un tiers du volume des ventes de robotique et automation industrielles, certaines estimations prévoyant un accroissement de cette proportion à plus de 40 % d'ici quatre ans.

1.3 – Verrous technologiques et difficultés structurelles

Le premier facteur freinant le développement de la fabrication additive est le coût de celle-ci. Les imprimantes industrielles accroissent leurs performances mais au prix d'un renchérissement du prix d'achat. A titre d'exemple, le coût d'une imprimante à frittage laser pour le métal peut aller de 500 000 à plusieurs millions de dollars. Le prix des matières premières est lui aussi particulièrement élevé.

La complexité du fonctionnement des machines peut également constituer un facteur capable de freiner la généralisation à court terme de cette technologie (logiciels hyperspécialisés).

La qualité finale des objets produits nécessite encore d'être perfectionnée. Des opérations de finition (traitements thermiques, usinage, etc.) sont dans la plupart des cas encore nécessaires pour finaliser les pièces. Les problèmes de fiabilité et de confiance peuvent aussi freiner l'utilisation de cette technologie pour les productions « stratégiques », mais aussi pour certaines pièces et produits de haute technologie.

1.4 – Impact sur la dimension militaire de la défense : maintenance et logistique

Dans le domaine militaire, l'un des aspects les plus attrayants de l'impression 3D, et probablement le plus porteur, est sa faculté de réparation des matériels d'ancienne génération dont la production en série a cessé. L'armée de l'air israélienne a, par exemple, utilisé ce processus pour la maintenance de ses appareils (« *Aerial Maintenance Unit* » - AMU).

Par ailleurs, au « juste besoin » pourrait se substituer la « juste offre », si l'implantation d'imprimantes 3D se généralisait sur les théâtres d'opérations. L'armée américaine est en train d'expérimenter cette solution en mer[14], ainsi qu'à terre via des laboratoires expéditionnaires. L'*US Army* envisage même de fabriquer des rations par ce biais.

La fabrication additive peut aussi être un moyen d'appui aux forces (reconstitution cartographique en 3D ; fabrication de matériel léger ou rare, *ad hoc*). Ainsi, le commandement des opérations spéciales de l'armée américaine a fait construire huit usines mobiles qui peuvent rentrer dans des conteneurs de transport standards.

14 - Le *RETEX* semble positif en ce qui concerne pour le moment des pièces simples (couvercles de réservoirs d'huile et seringues par exemple à bord de l'*USS Essex*).

2 - Situation en 2030

2.1 – L'industrie du futur ? La lutte pour la prééminence

La fabrication additive constitue une nouvelle révolution industrielle. Les efforts conjugués de programmes nationaux ambitieux et financièrement étayés accompagnent l'effort industriel privé. Si les tendances actuelles se poursuivent et si aucune politique spécifique n'est mise en œuvre, **le développement de la fabrication additive tournera autour de trois pivots : les Etats-Unis, la Chine-Asie élargie et l'Allemagne.**

La France risque d'être distancée par ses concurrents et de demeurer productrice d'innovations majeures dans de nombreux domaines sans être capable d'en assurer la transformation industrielle. Le rachat de jeunes entreprises françaises performantes par les « Majors » du secteur est le signe à la fois du dynamisme de la recherche dans notre pays et de sa faiblesse structurelle dans le passage à l'industrialisation. **La France pourrait cependant conserver une place dans le secteur des poudres,** déjà fortement concurrentiel.

2.2 – Terrorisme, guérilla et prolifération : produire et agir « rustique »

Le développement des « FabLab », notamment dans les domaines chimique et biologique, facilite l'accès à des vecteurs d'attaque potentiels (couteaux passant les portiques de sécurité, par exemple ; voire armes de poing – *cf.* Affaire Cody WILSON).

Ils ouvrent également la voie à la fabrication d'engins (drones, par exemple), **« rustiques »** ou pas, pouvant offrir un avantage tactique à un adversaire asymétrique. Le cyber-sabotage des logiciels d'impression 3D est aussi un risque réel[15].

Ainsi, la dissémination de la technologie 3D pourrait devenir un véritable avantage pour un ennemi imaginatif, lui permettant de produire des armes certes « rustiques » ou de qualité intermédiaire, mais capables de produire des effets ponctuels de déstabilisation de théâtre, de dissémination de la menace terroriste et de participer à la prolifération des armes de destruction massive.

15 - Voir : V. BOULANGER, « *L'impression 3D: la nouvelle arme des terroristes ?* », www.additiverse.com, 13 septembre 2014.

3 - Enjeux pour la France et pour l'Europe

3.1 – Un potentiel de relance industrielle et technologique qui devra être encadré

a) Enjeux

Le développement de la fabrication additive offre un champ considérable de croissance au travers des gains de productivité qu'il permet. Tous les secteurs de production sont concernés mais l'enjeu réel réside dans la capacité de passer au stade de l'industrialisation.

Aujourd'hui en Europe, seule l'Allemagne semble disposer des moyens permettant de gérer cette montée en puissance. En France, la mise en œuvre d'une politique ambitieuse, telle que celle défendue dans le rapport CCI Paris-CGARM (17 recommandations), constituera un enjeu majeur. Comme indiqué plus haut, le programme européen « Horizon 2020 » et son prédécesseur n'ont pas spécifiquement individualisé les technologies de fabrication additive parmi les technologies capacitaires clés (KETs).

Même si la fabrication additive n'est pas encore l'industrie de demain, il n'en demeure pas moins qu'elle représentera un secteur industriel et commercial important dans les années à venir.

b) Risques

Les risques liés au développement de l'impression 3D sont multiples : piratage des droits d'auteur ; contrefaçons de luxe ou d'objets technologiques, etc. Leurs conséquences exposeront l'individu comme la collectivité (accidents provoqués par des pièces détachées à bas coût et défectueuses insérées dans des engins routiers, ferroviaires ou volants, des usines chimiques ou des centrales nucléaires par exemple). Ce constat appelle une action des pouvoirs publics afin d'encadrer le développement de l'impression 3D, comme le souligne l'exposé des motifs de la proposition de loi intitulée « l'impression 3D et l'ordre public » déposée par la députée Claudine SCHMID, le 28 octobre 2016.

3.2 – L'augmentation des capacités terroristes et militaires des adversaires : adapter la réponse

Au-delà du risque industriel et commercial, les imprimantes 3D posent aussi un problème de défense et de sécurité. Côté menace, la fabrication clandestine de matériel à usage terroriste, de tout ou partie d'armements conventionnels, et des moyens de produire ceux-ci deviendra un important facteur de vulnérabilité.

La situation est également problématique en matière de prolifération. Ce n'est pas tant la production d'armes et matériaux qui est en cause, que les moyens de leur production (pièces détachées, centrifugeuses, etc.). Cette réflexion est valable tant pour les armes que pour leurs vecteurs (missiles notamment).

Par ailleurs, certains de ces nouveaux moyens pourraient permettre de contourner les contrôles et les garanties (*safeguards*) des traités internationaux d'interdiction, ainsi que les embargos. De très nombreux composants dans le domaine nucléaire ou balistique peuvent être ou seront produits en 3D. Pour limiter ce risque, il convient d'envisager de contrôler l'exportation des imprimantes 3D les plus sensibles, c'est-à-dire celles susceptibles d'avoir un impact en termes de prolifération, de même que les logiciels les plus performants et les matières pouvant y contribuer.

Cela implique une réflexion en amont entre alliés sur le niveau et la granularité du contrôle. Tous les régimes sont concernés (*NSG, Groupe Australie, MTCR* et *Wassenaar*) et certains se préoccupent déjà de ce phénomène montant.

Comme l'ont souligné les recherches de KRONIG et VOLPE, la problématique de la prolifération issue de l'impression 3D exige une prise en charge dès maintenant : « *on pourra arguer que les mesures que nous préconisons sont prématurées car les Etats n'ont pas les moyens de construire encore des composants nucléaires. Mais si nous attendons que le futur proliférateur surgisse avec une quantité significative de matière fissile, la communauté internationale, une fois encore, aura agi trop tard* ».

Les industriels ne sont pas non plus restés passifs face à ces menaces potentielles. Ils se mobilisent pour la protection des brevets, la sécurisation des logiciels les plus sensibles et le suivi des matières. Toutefois, compte tenu des potentialités de cette technologie et de son niveau de développement, l'impression 3D ne constitue pas un enjeu stratégique au regard de ce qu'elle est aujourd'hui, mais au regard de ce qu'elle sera demain et du champ des possibles qu'elle ouvre.

4 - Scenarii alternatifs

4.1 – Une supériorité asiatique écrasante

La prise de conscience par la Chine du potentiel que représente l'impression 3D entraîne le lancement par Pékin d'une nouvelle révolution industrielle. Suivie par quelques autres nations asiatiques, la Chine généralise la fabrication additive de haut niveau dans tous les secteurs de production, du stratégique militaire à l'alimentaire.

La mise en œuvre de cette politique pose, au reste du monde et en particulier aux industriels européens, des problèmes de concurrence, causés par une importante baisse des prix à la vente des marchandises. La dynamique asiatique est accrue par une exploitation systématique des brevets et autres propriétés industrielles disponibles. Seuls les Etats-Unis résistent à cette vague en se positionnant au plus haut niveau technologique.

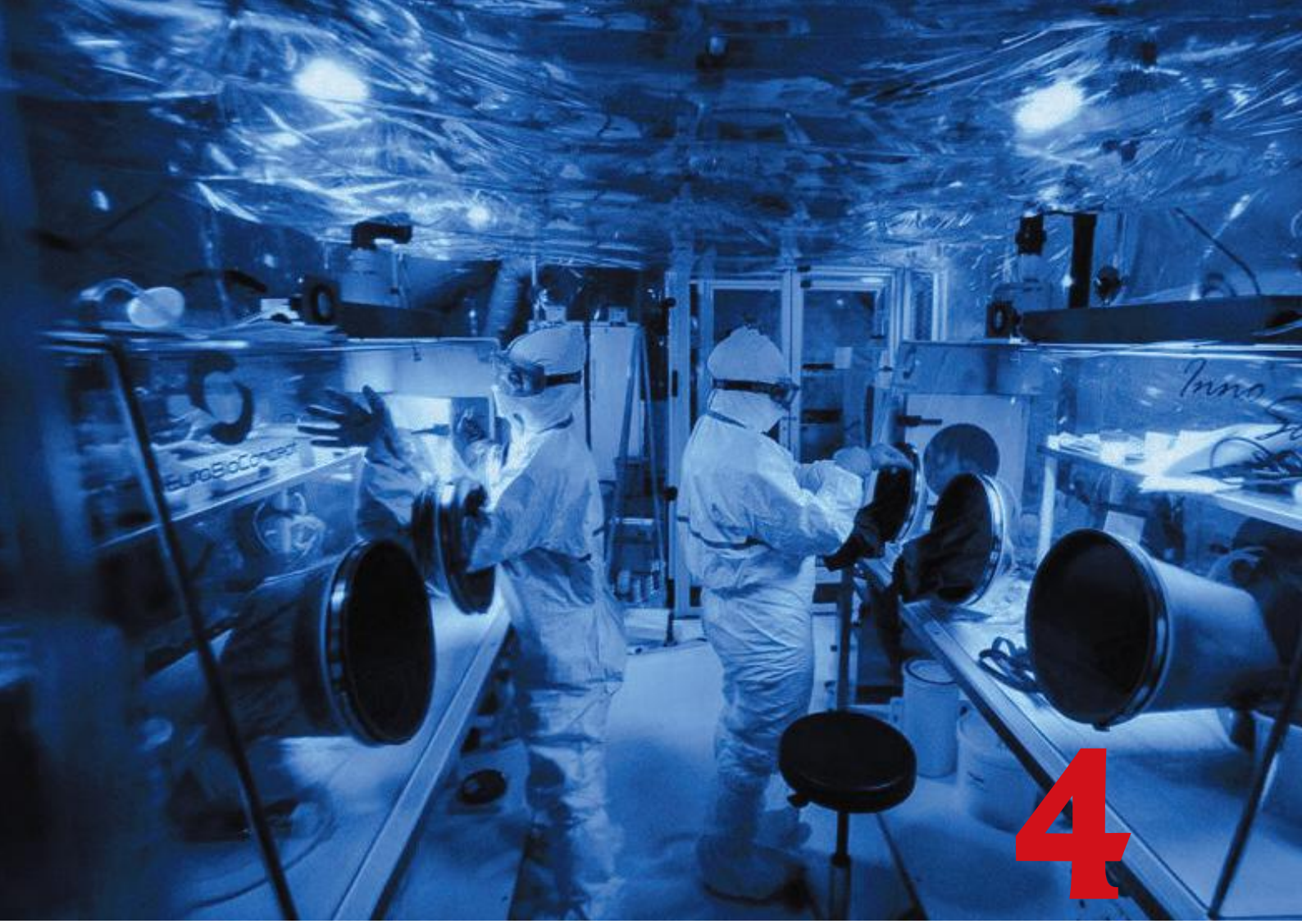
4.2 – Le renforcement militaire d'acteurs non étatiques

La fabrication additive peut accroître la capacité d'un Etat de niveau intermédiaire, d'un Etat sous sanctions, d'un groupe terroriste puissant ou d'un proto-Etat à fort potentiel (modèles *Hezbollah* ou *Daech*) de produire des pièces ou des exemplaires d'objets technologiques, voire des armes, sans aller chercher ces derniers à l'étranger.

4.3 – Un soutien croissant à la prolifération

Le danger à venir ne résiderait pas tant dans l'appétit des proliférateurs classiques, toujours à l'affût de nouvelles facilités, mais toujours sous étroite surveillance, que dans celui des acteurs non étatiques prompts à mettre en œuvre des technologies rustiques capables de provoquer des dommages restreints mais spectaculaires.

Le scénario le plus pessimiste serait celui du développement de capacités nouvelles à même de produire des matériels contribuant à la prolifération nucléaire ou balistique, *via* la production de pièces entrant dans leurs moyens de production ou de pièces détachées. Cette menace vaut aussi pour les dimensions chimique et biologique.



4

La biologie de synthèse : un saut dans l'inconnu

L'essentiel

Les champs d'application de la biologie de synthèse sont nombreux et couvrent des domaines clés (agriculture, énergie, santé, etc.). Ils posent également des questions éthiques (manipulations génétiques, dérives). Aussi, un encadrement et une structuration de cette filière en France paraît dès à présent nécessaire afin d'en appréhender les enjeux et de décider d'une politique française qui, aujourd'hui, n'est pas mise en place.

La biologie de synthèse (ou biologie synthétique) recouvre l'ingénierie de composants et de systèmes biologiques qui n'existent pas dans la nature, ainsi que le remaniement de systèmes biologiques existants pour exécuter des tâches spécifiques (production de médicaments, de biocarburants, de détecteurs d'explosifs, de biomatériaux, etc.). Elle peut être définie comme une nouvelle approche pluridisciplinaire de la biologie.

Cette nouvelle discipline, aux frontières encore floues, résulte de la convergence de connaissances et de techniques issues d'autres disciplines telles que la biologie, la physique, la chimie, les mathématiques, l'informatique, l'automatique et les sciences de l'ingénieur. Elle se différencie des biotechnologies traditionnelles par l'emploi systématique d'outils informatiques et par la conception de systèmes biologiques complexes par ingénierie[1].

Les champs d'application sont multiples et la biologie de synthèse ouvre de nouvelles perspectives dans des domaines aussi variés que l'énergie, l'agro-alimentaire, la santé, les biomatériaux ou encore la chimie. Elle représente ainsi une filière de la bioéconomie en plein essor. Mais ces développements s'accompagnent également de préoccupations éthiques, sociétales, sanitaires, environnementales et sécuritaires (cette technologie étant par essence, duale).

1 - François KEPES, « *Conditions scientifiques et technologiques de l'émergence de la biologie de synthèse* », Médecine / Sciences, Vol. 29, Hors-série n°2 (2013), pp. 13-15.

1 - Etat des lieux en 2017

1.1 – Etats-Unis, Royaume-Uni, France, trois pays qui s'intéressent à la biologie de synthèse

Les Etats-Unis dominent le secteur de la biologie de synthèse au niveau international. Sur la période 2008-2014, ils y ont consacré un budget de recherche de 820 millions de dollars environ, principalement financé par le *Department of Defense*[2] au travers de la *DARPA*[3], son agence de recherche. Le Pentagone est à ce jour la seule structure étatique de défense du monde occidental à intervenir massivement pour structurer le secteur et conserver une avance technologique sur certains éléments clés.

En Europe, ce sont les investissements privés qui dynamisent le développement de la biologie de synthèse. Ils représentent la principale source de financement des *start-ups* qui se lancent dans ce domaine (plus de 207 millions de dollars pour l'année 2015). Le Royaume-Uni est particulièrement volontariste, avec la définition d'une feuille de route en 2012, puis la mise en place, en 2016, d'un plan stratégique visant à renforcer la recherche et accélérer le processus jusqu'à la commercialisation des produits et services[4].

La France se place au troisième rang sur le plan académique, derrière les Etats-Unis et le Royaume-Uni. On y dénombre par ailleurs une dizaine d'entreprises et de start-ups qui exploitent la biologie de synthèse en biotechnologie industrielle, par comparaison avec les quelques 400 entreprises de biotechnologies traditionnelles[5]. S'il n'y a, à ce jour, pas de programmes de financement dédiés au niveau national, certains appels d'offres englobent la biologie de synthèse et l'*Agence nationale de la recherche* (ANR) participe à l'appel à projets transnational sur cette thématique. Dans ce contexte, afin de consolider la position de la France à horizon de 5 à 10 ans, le *Genopôle*, premier bio-cluster français établi à l'initiative de l'Etat et réunissant les principaux acteurs de recherche du secteur, a lancé le projet *GenoBIOS*, qui démarre en 2017 et vise à fédérer et structurer l'innovation en biologie de synthèse sur l'ensemble du territoire national.

2 - *Wilson Center, U.S. trends in synthetic biology research funding*, 2015.

3 - *DARPA : Defense Advanced Research Projects Agency*.

4 - *UK synthetic biology roadmap coordination group, A synthetic biology roadmap for the UK*, 2012.

5 - Campus France, *La recherche en biotechnologie en France*, 2013 et Genopole, *Consolider la biologie de synthèse en France*, 6 décembre 2016.

1.2 – De nombreuses applications potentielles pour la biologie de synthèse

La biologie de synthèse contribue à améliorer la compréhension des processus biologiques et offre la possibilité de développer des solutions innovantes pour répondre à des défis économiques, sociétaux et environnementaux majeurs, comme ceux résultant de :

- la raréfaction des ressources naturelles ;
- la croissance de la population ;
- la pollution de l'environnement par les activités humaines ;
- l'augmentation des besoins de santé liés à l'évolution des modes de vie, au vieillissement de la population ou aux maladies infectieuses.

La biologie de synthèse trouve de nombreuses applications en biotechnologies, ou pour la bioproduction d'intermédiaires pour la chimie, la production de biocarburants, de biopolymères ou de biomatériaux aux propriétés spécifiques, ou pour la mise au point d'outils de bio-remédiation destinés à lutter contre les contaminations environnementales[6]. Elle peut également être exploitée dans le développement de nouvelles approches thérapeutiques ou diagnostiques, par exemple contre les maladies infectieuses ou les cancers. L'une des pistes pour contrer le phénomène d'antibiorésistance repose par exemple sur le développement d'antibiotiques capables de détecter les gènes bactériens responsables des résistances afin de détruire spécifiquement les bactéries dangereuses.

En 2015, plus d'une centaine de produits et d'applications issus de la biologie de synthèse sont déjà sur le marché ou proches de la commercialisation, tous secteurs biotechnologiques confondus. Parmi les applications commerciales et industrielles figurent par exemple la production d'un précurseur de l'artémisinine, substance active utilisée dans le traitement du paludisme, ou celle du propane-1,3-diol, qui sert à la fabrication de « polymères » et de matériaux composites, ainsi que l'emploi d'un outil de diagnostic issu de la biologie de synthèse pour le suivi de patients atteints de viroses multiples.

Parmi les perspectives à plus long terme figure la possibilité de combiner des robots à l'échelle micrométrique avec des micro-organismes obtenus par synthèse, dans l'objectif de développer un biocapteur mobile dans le corps ou de parvenir à une régénération tissulaire ou à la création d'un tissu. Une tout autre perspective est celle de rendre plus accessible l'exploration spatiale, en particulier celle de la planète Mars. Est ainsi notamment envisagée par la *NASA*, qui finance des recherches sur ces sujets, la bioproduction de nourriture, de carburants, de produits pharmaceutiques ou d'autres matériaux, afin de diminuer la charge emportée et donc réduire les coûts, mais aussi améliorer la santé et le confort des astronautes.

6 - Commission biotechnologies de l'Académie des technologies, Biotechnologies blanches et biologie de synthèse, 2015.

1.3 – Un secteur en pleine évolution

La découverte en 2012 de la technologie *CRISPR-Cas9*, par la Française Emmanuelle CHARPENTIER et l'Américaine Jennifer DOUDNA, a constitué un progrès technique significatif en biologie de synthèse. Ce procédé d'édition génomique permet de couper rapidement, simplement et pour un coût modeste l'ADN avec une grande précision, puis d'inactiver ou de remplacer un gène ou d'en modifier l'expression. *CRISPR-Cas9* se présente comme une révolution dans l'ingénierie des génomes et suscite de grandes attentes dans le domaine médical, alors que depuis deux ans, de spectaculaires résultats sont obtenus. Il permet de conférer aux organismes pluricellulaires de nouvelles propriétés. Ainsi, grâce à *CRISPR-Cas9*, des chercheurs américains sont parvenus à améliorer l'acuité visuelle de rats, tandis qu'une autre équipe réussissait à rendre résistante au paludisme une espèce de moustique. Egalement dans le cadre de la lutte contre le paludisme – maladie qui tue plus de 400 000 êtres humains chaque année – une équipe internationale menée par l'*Imperial College* de Londres a réussi au travers d'un « forçage génétique » à rendre stériles des moustiques femelles. Cette recherche, qui bénéficiera des avancées accumulées sur la durée par d'autres équipes, est l'une des voies, à côté de celles développées notamment en recherche sur les applications pacifiques de l'énergie nucléaire, permettant d'envisager l'élimination ou la réduction drastique des populations (qui sont les vecteurs de transmission de la maladie).

L'automatisation et la diminution des coûts de la synthèse de gènes à façon, grâce à des avancées en matière de miniaturisation, de métrologie et de standardisation, devraient continuer à contribuer à l'essor de la biologie de synthèse. L'objectif à terme est de synthétiser des génomes complexes à partir d'une bibliothèque de bio-briques. L'automatisation de la phase de conception, qui permettra depuis un ordinateur de donner des ordres à un automate pour procéder aux opérations d'assemblage, est aujourd'hui une étape limitante dans l'atteinte de cet objectif (la construction de systèmes à très grande échelle nécessitant d'intégrer la complexité des interactions moléculaires à l'échelle du génome). Dans cette perspective, le premier centre automatisé d'ADN, l'*Edinburgh Genome Foundry*, a été lancé à l'été 2016, permettant la conception et la production de brins d'ADN à grande échelle par des procédés entièrement automatisés. L'augmentation des capacités de calcul et de stockage, l'amélioration des outils de modélisation et de simulation, de même que les progrès dans le domaine de l'intelligence artificielle vont également favoriser le recours à la biologie de synthèse dans toute une panoplie de secteurs.

1.4 – Des menaces et des risques

Les aspects éthiques, sanitaires et environnementaux font depuis longtemps partie des préoccupations liées aux biotechnologies en général. La préoccupation sécuritaire liée à la biologie de synthèse, apparue en 2002, s'est fortement accrue depuis quatre à cinq ans : les progrès techniques en la matière pourraient dans un avenir proche rendre des capacités avancées accessibles à un nombre croissant d'acteurs étatiques ou non étatiques, potentiellement malveillants. D'ores et déjà, on peut se procurer sur Internet, pour 150 dollars seulement, un « *Kit CRISPR* » qui permet, à domicile, de modifier génétiquement une bactérie en suivant le mode d'emploi fourni.

La diffusion accidentelle ou intentionnelle d'un micro-organisme obtenu par synthèse, en fonction de ses caractéristiques, pourrait non seulement provoquer la contamination des individus, des animaux, ou des plantes mais aussi celle de l'environnement. Il peut y avoir un risque d'hybridation des micro-organismes avec des espèces naturelles, leur permettant de s'adapter au milieu naturel et d'y proliférer.

Des expérimentations, comme la synthèse d'un virus ayant les caractéristiques biochimiques et pathogéniques d'un poliovirus, l'obtention par génétique inverse d'un virus comportant les huit segments génomiques de la souche de la grippe de 1918 et de virus recombinants comportant certains de ces segments, ou encore la création de la première cellule bactérienne contrôlée par un génome obtenu par synthèse et assemblage capable de s'auto-répliquer, ont alimenté les controverses et rappelé que l'exploitation de la biologie de synthèse n'était pas dénuée de risques, qu'ils soient accidentels ou intentionnels. Dans un rapport de janvier 2017 sur « *les risques associés à un usage dual des techniques de synthèse et de modification programmée des génomes* », le Conseil national consultatif pour la biosécurité (CNCB), comité français chargé de biosécurité, souligne que le nouvel outil de biologie moléculaire qu'est *CRISPR/Cas9* pose la question de la possibilité de recréer *de novo* des microorganismes déjà existants dans la nature, notamment des virus dont la virulence et la contagiosité pourraient présenter de réels risques pour la sécurité sanitaire des populations. A cet égard, le développement de nouvelles technologies dans le domaine de la synthèse de l'ADN et la multiplication des sociétés privées maîtrisant ces technologies pour produire « à façon » des gènes de synthèse, pose une véritable question de sûreté et de prolifération potentielle. La crainte que le virus de la variole puisse être recréé artificiellement a d'ailleurs été l'un des arguments avancés à l'assemblée mondiale de la santé pour reporter la destruction des stocks encore conservés (pour mise au point de contre-mesures médicales).

L'émergence du « *biohacking* », ou biologie participative, doit aussi être prise en compte. Ce phénomène nouveau rassemble des amateurs et des chercheurs qui développent leurs propres projets en biotechnologie en dehors des cadres professionnels traditionnels, dans des laboratoires communautaires, voire chez eux. Cette pratique, reconnue dans les

milieux de la recherche et bénéficiant au demeurant des mécanismes de soutien publics et privés à la recherche, reproduit dans le domaine de la biologie l'état d'esprit et les modes d'organisation d'émulation et de liberté propres au monde du numérique. C'est un véritable changement de paradigme puisque cette biologie participative n'a ni les rigidités du domaine académique, ni ses garde-fous. Aussi suscite-t-elle certaines interrogations quant aux risques de dérives, d'accidents ou d'intrusion et pose le problème de la gouvernance.

C'est dans ce contexte que, dans un rapport déclassifié sur l'état de la menace dans le monde, le directeur national du renseignement américain, James CLAPPER, estimait en février 2016 que les techniques d'édition du génome, en particulier *CRISPR-Cas9*, devaient être considérées comme des armes de destruction massive. Le CNCB considère quant à lui, dans son rapport que le système *CRISPR-Cas9* est un nouvel outil qui, certes, facilite et accélère la manipulation des génomes, et particulièrement des génomes des cellules dotées d'un noyau, mais qui, en l'état de l'art, ne permet pas d'accroitre fondamentalement le risque de prolifération d'armes biologiques.

2 - Situation en 2030

D'ici 2030, le marché de la biologie de synthèse pourrait proposer des milliers de produits et de services.

Les principales applications intéresseraient le domaine de la santé. Des traitements innovants contre les cancers et les maladies infectieuses ou orphelines, et des outils de diagnostic permettant de détecter certaines maladies de façon beaucoup plus précoce, devraient avoir été mis au point. Après des essais cliniques concluants, un nouvel antibiotique ciblant préférentiellement les bactéries porteuses de résistance serait sur le point d'être commercialisé, alors que les résistances aux antibiotiques se sont largement propagées, entraînant une hausse de la mortalité et une augmentation des dépenses de santé.

L'agroalimentaire et la chimie bénéficieraient aussi des avancées issues de la biologie de synthèse, avec la mise au point d'engrais moins polluants et de matériaux biodégradables. De nouveaux matériaux plus solides et plus légers pourraient être mis au point pour l'industrie automobile. Les travaux sur les biocarburants continueraient de progresser, toujours financés pour l'essentiel par les groupes pétroliers. Cependant, malgré des collaborations public-privé et les résultats des programmes d'industrialisation lancés dès le milieu des années 2010, leur utilisation resterait marginale par rapport à celle des énergies fossiles.

S'agissant du secteur de la défense, les innovations pourraient porter sur le développement de matériaux de protection plus robustes et plus légers pour les per-

sonnels et les blindages, **ainsi que de nouveaux matériaux permettant de réduire les signatures thermiques et magnétiques.** Ces innovations pourraient également conduire à la bio-remédiation de milieux contaminés par des explosifs ou autres contaminants liés à l'activité militaire.

Dans un contexte où le phénomène de science ouverte se serait considérablement développé, la biologie participative serait devenue de plus en plus attractive au niveau mondial, avec d'une part, l'implantation d'un nombre croissant de laboratoires communautaires rassemblant des personnes d'horizons très divers et, d'autre part, la multiplication d'initiatives isolées. A l'instar du développement de la technique *CRISPR-Cas9*, **des avancées scientifiques et technologiques permettraient à des amateurs de plus en plus nombreux de se lancer dans des projets de biologie de synthèse.** Ces amateurs feraient valoir que leurs initiatives permettraient le développement de solutions innovantes, souvent à des coûts réduits par rapport aux produits développés par les groupes industriels. Ces évolutions soulèveraient cependant des questions de gouvernance, en lien avec les problématiques d'acceptation sociétale, de sécurité et de sûreté biologiques. Il serait devenu quasiment impossible d'avoir une idée précise du nombre d'initiatives réalisées, alors même que les pratiques diffèreraient considérablement en fonction des associations et des pays. Des cas de dissémination dans l'environnement de micro-organismes de synthèse, aux effets toutefois limités, pourraient avoir été constatés, de même que quelques cas d'expérimentation aux conséquences dramatiques chez des volontaires ayant pris l'initiative de tester sur eux-mêmes leurs inventions en dehors de tout protocole validé.

Ces évolutions modifieraient le panorama de la R&D industrielle dans des secteurs comme l'industrie pharmaceutique ou chimique dans un contexte de forts enjeux économiques et sociétaux. Certains groupes industriels pourraient chercher à développer des partenariats exclusifs avec des laboratoires communautaires, leur apportant un important soutien financier mais exerçant sur certaines équipes des pressions susceptibles de les détourner de la philosophie initiale de leur projet. Certains pays pourraient mettre en place des dispositifs permettant de capter le résultat de ces recherches avec des mesures incitatives financières ou matérielles, voire des mesures plus agressives.

3 - Enjeux pour la France et pour l'Europe

Pour l'Europe, et singulièrement pour la France, le secteur de la biologie de synthèse pourrait constituer à l'horizon 2030 un univers où elles ne disposeraient ni d'une avance technologique, ni d'une capacité de limiter les progrès d'autres acteurs, faute de normes internationales établies ou de bonnes pratiques en matière d'exportation négociées entre les Etats.

Plusieurs axes d'effort pourraient, dans ce contexte, être poursuivis :

- soutenir la structuration de la filière de la biologie de synthèse, de la recherche aux applications commerciales, avec des mécanismes de financement dédiés ;
- assurer une veille stratégique internationale afin d'identifier les orientations scientifiques prometteuses et leurs éventuels impacts pour la société ;
- réaliser une analyse bénéfices / risques périodique afin d'envisager les conséquences des avancées dans le secteur de la biologie de synthèse ;
- promouvoir les initiatives innovantes qui se développent en dehors du cadre institutionnel, en les accompagnant afin de soutenir les processus de valorisation des résultats ;
- garantir une sensibilisation et une éducation des parties prenantes, tant dans le cadre institutionnel qu'en dehors de celui-ci, face aux risques, qu'ils soient de nature accidentelle ou malveillante.

4 - Scenarii alternatifs

4.1 – Scénario 1 : des biocarburants et des produits chimiques remplacent les intermédiaires pétrochimiques à des coûts relativement bas

Une hausse prolongée des prix du pétrole, l'augmentation des besoins mondiaux et des conflits entre Etats perturbant les approvisionnements énergétiques mettent en lumière de façon plus aiguë les risques liés à la dépendance énergétique et incitent certains Etats à développer de manière encore plus décisive des programmes pour mettre au point des sources alternatives. Des biocarburants sont produits à l'échelle industrielle et commencent à représenter une part croissante du marché.

Etats-Unis et Chine ont consenti des investissements massifs et mis en place une stratégie comprenant notamment des mesures incitatives, afin d'attirer les meilleures équipes de recherche au niveau international. Des groupes américains et chinois, bénéficiant par ailleurs de programmes nationaux de soutien, ont

entrepris de racheter progressivement les *start-ups* françaises et européennes impliquées dans la recherche sur les biocarburants et les énergies alternatives. De nouveaux acteurs comme le Brésil émergent par ailleurs et se positionnent sur le marché.

L'essor des biocarburants et le développement de composés chimiques remplaçant les intermédiaires pétrochimiques commencent à diminuer la dépendance à l'égard de ceux-ci. Les pays européens qui ont investi dans ce secteur trouvent là une source d'énergie renouvelable qui leur permet d'être autonomes, de développer leur économie et d'exporter leurs produits tout en préservant leur savoir-faire. Si cet essor génère des tensions et représente un facteur déstabilisant pour les pays très dépendants de l'exportation d'hydrocarbures, il relâche simultanément la pression sur les pays les plus pauvres pour limiter leur empreinte carbone (les biocarburants recyclent le carbone atmosphérique au lieu de libérer le carbone fossile).

D'autres enjeux se dessinent, liés à la conversion des terres pour la production des biocarburants et à un usage intensif d'engrais. Des organisations non gouvernementales et certains partis écologistes s'inquiètent des conséquences environnementales d'une production croissante de biocarburants. Celle-ci n'entre pas en concurrence avec la production de produits alimentaires mais les activistes redoutent qu'elle ne se fasse au détriment des espaces naturels, ou que des micro-organismes modifiés ne se disséminent dans l'environnement avec des effets non maîtrisés comme la destruction d'écosystèmes entiers.

4.2 – Scénario 2 : un virus recréé par biologie de synthèse s'échappe d'un laboratoire de recherche

Des scientifiques qui étudient les conséquences de la fonte du permafrost réussissent à identifier un virus hautement pathogène transmissible par voie aérienne et contre lequel la population mondiale n'est pas immunisée. La séquence génomique de ce virus est disponible sur des bases de données librement accessibles, ce qui permet à plusieurs laboratoires ne répondant pas aux normes les plus strictes en matière de sécurité et de sûreté biologiques d'obtenir ce virus par voie synthétique. A la suite d'un accident dans l'un de ces laboratoires, le virus est disséminé dans l'environnement et plusieurs personnes sont contaminées. Il n'existe aucun traitement efficace et le taux de mortalité est très élevé. Un tel scénario est possible, en dépit de son caractère sensationnaliste. Les conséquences de la crise sanitaire qui s'ensuivrait devraient être gérées dans un monde très ouvert, ce qui n'a pas de précédent.

Sans aller jusque-là, un incident aux conséquences limitées pourrait suffire à renforcer les réactions de rejet sociétal. A titre d'exemple, le Japon n'est toujours pas parvenu à décider de la construction d'un nouveau laboratoire de niveau de confinement 4 depuis que la crise de Fukushima

a détruit, dans l'opinion publique, la confiance accordée aux autorités en matière de sûreté des installations sensibles. Un accident de ce type, même mineur, suffirait à modifier la politique d'exportation des installations de confinement pilotée par le SGDSN et à renforcer l'évaluation bénéfice/risque réalisée préalablement à chaque projet d'exportation en y incluant les risques induits par les progrès de la biologie de synthèse. Un comportement analogue, généralisé à l'échelle mondiale, pourrait affecter les politiques de soutien public à la recherche dans le domaine de la biologie de synthèse. Il n'affaiblirait pas pour autant la curiosité scientifique ni le besoin de secteurs entiers (santé, agriculture, industrie, énergie) en matière d'innovation dans ce domaine. Le risque serait alors que la recherche se poursuive exclusivement dans le cadre du « *biohacking* » ou hors du territoire des Etats les plus régulateurs. La traduction serait un niveau réduit d'activité, mais aussi de contrôle.

5

Comment les neurosciences vont-elles transformer la guerre ?

L'essentiel

L'impact potentiel des neurosciences sur la manière de faire la guerre est identifié et de nombreuses recherches sont en cours. Essentielles en termes de santé, ces avancées vers « l'Homme augmenté » sont parfois déroutantes au plan militaire et éthique. La France et l'Europe doivent les prendre en compte pour maintenir leurs capacités de défense pour la guerre du futur, identifier les priorités afin de ne pas disperser moyens et financements et se préparer à créer les conditions d'une modération des acteurs et d'un encadrement international.

Le système nerveux central et périphérique est le siège de la perception, de la cognition ou de l'action. Les neurosciences recouvrent l'ensemble des disciplines scientifiques et médicales relatives à l'étude de l'organisation et du fonctionnement du système nerveux à différentes échelles. Leur essor, reposant sur une approche interdisciplinaire, a permis de faire considérablement progresser les connaissances sur le cerveau humain, dont l'exploration reste l'un des plus grands défis scientifiques contemporains. Les convergences avec les nano-biotechnologies, les sciences de l'ingénieur et l'informatique favorisent le développement de nouveaux outils et méthodes d'intervention au niveau cérébral. Les neurosciences ouvrent ainsi de nouvelles perspectives pour la recherche biomédicale et clinique, en permettant par exemple le développement de modèles cellulaires et animaux, l'étude des mécanismes physiopathologiques, l'identification de marqueurs biologiques des maladies neurologiques ou psychiatriques, ou encore la mise au point de stratégies thérapeutiques innovantes. Au-delà, elles peuvent également permettre d'envisager le développement à plus ou moins long terme d'applications telles que la mise au point d'ordinateurs plus performants ou de robots dotés d'une forme d'intelligence, mais aussi l'augmentation des performances physiques ou cognitives humaines (« l'Homme augmenté »).

Présentant potentiellement un intérêt tant d'un point de vue civil que militaire, ces applications relèvent souvent du double usage. Certaines de ces avancées, si les perspectives se concrétisent, ont le potentiel de modifier profondément la pratique militaire, voire l'art de la guerre, ouvrant de nouvelles perspectives mais suscitant aussi des questionnements éthiques et créant de nouvelles vulnérabilités.

1 - Etat des lieux en 2017

1.1 – Un contexte propice aux neurosciences

a) L'impact sociétal et économique des maladies cérébrales et du système nerveux

Les affections neurologiques, incluant les maladies neurodégénératives dont la fréquence augmente avec le vieillissement de la population, les maladies psychiatriques et les déficits des organes des sens (vision et audition) affectent une part significative de la population et ont un impact sociétal et économique très important. Les maladies cérébrales et du système nerveux représentent, entre soins curatifs et accompagnement de la dépendance, le poste de dépenses de santé le plus important en Europe, toutes pathologies confondues, soit 800 milliards d'euros par an.

b) De « l'Homme réparé » à « l'Homme augmenté »

Restaurer les capacités affectées par la maladie, le vieillissement ou les accidents ou freiner les processus de dégénérescence ne sont pas le seul objectif. Le défi est également de parvenir à « l'Homme augmenté », capable de dépasser ses limites biologiques grâce à l'amélioration artificielle de ses capacités. Les Américains ont imprimé une dynamique, avec la diffusion au début des années 2000 du rapport dit « NBIC », produit par un *think tank*, le *World Technology Evaluation Center* (WTEC). Il porte en particulier sur l'amélioration des performances humaines par la convergence entre nanotechnologies, biotechnologies, technologies de l'information et sciences cognitives. De même, le mouvement de pensée philosophique transhumaniste prône l'amélioration de l'individu grâce aux sciences et techniques, estimant qu'il devient désormais possible d'intervenir dans la définition biologique même de l'humain. Il met en avant l'idée que l'être humain, loin d'être stable, est en constante évolution et que les avancées technologiques peuvent l'« augmenter ».

1.2 – Les neurosciences, un domaine de recherche qui suscite l'intérêt

a) Des initiatives ambitieuses avec des financements conséquents

En janvier 2013, la Commission européenne a annoncé qu'elle allait financer le *Human Brain Project*, piloté par l'Ecole polytechnique fédérale de Lausanne (EPFL), à la tête d'un consortium international qui rassemble des milliers de chercheurs. Il s'agit de l'un des deux projets de recherche phare de la décennie pour la Commission (l'autre portant sur l'exploitation du graphène). Ce projet, d'une durée de dix ans et doté de près de 1,2 milliard d'euros, a

pour ambition de réaliser une simulation numérique complète du cerveau humain grâce à un supercalculateur et de contribuer à mieux comprendre les maladies neurologiques. Le très ambitieux programme européen n'a cependant pour le moment pas abouti aux résultats escomptés et a fait l'objet de vives critiques, ce qui a conduit à revoir en cours de route sa gouvernance et à envisager comment mieux intégrer les neurosciences cognitives. Le projet est désormais entré en phase opérationnelle avec le lancement de six plateformes collaboratives.

Dans le même temps, l'initiative *BRAIN* (*Brain Research through Advancing Innovative Neurotechnologies*), lancée en avril 2013 par le président américain Barack OBAMA, a réussi à démontrer l'intérêt que pouvait présenter un tel programme. Prévu pour durer une douzaine d'années et doté d'un budget total de 4,5 milliards de dollars, il vise à révolutionner la compréhension du cerveau humain, développer de nouvelles technologies et soutenir la R&D en matière de neurotechnologies. Les financements proviennent de six agences fédérales, dont le *National Institute for Health* (NIH) et la *Defense Advanced Research Project Agency* (DARPA). Ces financements ne représentent cependant qu'une partie des sommes allouées aux neurosciences aux Etats-Unis. Les investissements consentis par le NIH à l'initiative *BRAIN* pour l'année fiscale 2016 n'étaient par exemple que de 150 millions de dollars, pour un budget global en 2015 de 5,7 milliards de dollars dédié aux neurosciences.

Hors d'Europe et des Etats-Unis, d'autres pays conduisent également des travaux de recherche sur le cerveau, comme l'Australie, le Canada, Israël, le Japon, la Nouvelle Zélande ou encore la Chine. Cette dernière a ainsi mis en place un programme de quinze ans visant à mieux comprendre les circuits neuronaux à l'origine des fonctions cognitives et à développer diagnostics et traitements des maladies cérébrales.

b) Une recherche française en neurosciences dynamique

La France se classe au troisième rang européen, derrière le Royaume-Uni et l'Allemagne, et au septième rang mondial pour la recherche en neurosciences, sciences cognitives, neurologie, psychiatrie et organes des sens. Les équipes françaises sont notamment considérées comme en pointe en matière de biothérapies, de thérapies cellulaires et géniques, de neurochirurgie fonctionnelle, mais aussi d'interfaces cerveau-machine. Près de 625 équipes de recherche travaillent dans ces domaines, tous organismes confondus (incluant notamment les universités, le CEA, le CNRS, l'INRIA, l'INRA, l'Inserm ou l'Institut Pasteur). Environ 2 500 enseignants-chercheurs, près de 250 équipes et plus de 80 unités de recherche françaises et laboratoires rattachés à une vingtaine d'écoles doctorales en biologie et sciences de la vie et de la santé sont impliqués dans les recherches portant sur l'organisation et le fonctionnement cérébral. Depuis 2005, l'*Agence nationale de la recherche* (ANR) a financé près de 1 000 projets en neurosciences.

1.3 – De formidables avancées susceptibles d'intéresser la défense

Les stratégies et méthodes permettant d'étudier le fonctionnement cérébral ou de modifier les capacités cognitives sont de natures très diverses, impliquant à la fois des technologies non-invasives ou invasives. Des avancées récentes en matière d'imagerie cérébrale, de techniques de neuromodulation ou d'interfaces cerveau-machine ouvrent de nouvelles perspectives à plus ou moins long terme.

a) Des outils et technologies de plus en plus performants pour l'exploration cérébrale

L'outil le plus performant à l'heure actuelle pour l'imagerie biomédicale reste l'imagerie par résonance magnétique (IRM), avec son dérivé, l'imagerie par résonance magnétique fonctionnelle (IRMf). Développée dans les années 1990, cette dernière est très utilisée dans le domaine des neurosciences, car elle permet d'étudier *in vivo* l'activité neuronale lors d'évènements cognitifs, émotifs, perceptifs ou dans le fonctionnement de la commande des sens et de la motricité. En outre, des avancées majeures sont en train d'être réalisées. L'optogénétique, appliquée aux neurosciences, permet d'observer et contrôler l'activité de groupes de neurones spécifiques, en les rendant sensibles à la lumière. Née au début des années 2000, cette technique, qui combine les apports de l'optique et du génie génétique, peut être considérée comme une révolution technologique majeure. Autre exemple, fin 2015, une équipe de l'*Institut Langevin* (*CNRS, ESCPI* et *INSERM*) a présenté une nouvelle technique d'imagerie microscopique par ultrasons, non invasive et rapide, permettant de voir en profondeur dans les tissus avec une résolution bien supérieure à celle des techniques existantes. La technique doit être évaluée chez l'être humain, après une première phase qui a permis l'observation de l'activité vasculaire du cerveau d'un rat *in vivo*, avec une précision micrométrique et une cadence d'acquisition de 5 000 images par seconde.

b) Le développement des interfaces cerveau-machine

Une série de développements et d'essais cliniques survenus depuis le début des années 2000 a conduit à d'immenses progrès en matière d'interfaces cerveau-machine, avec des applications concrètes qui se profilent, dont certaines présentent un intérêt évident pour les armées ou les forces de sécurité, comme l'illustrent de récents travaux :

- le centre de recherche *Clinatec* de Grenoble travaille sur un exosquelette qui pourrait être contrôlé par une interface transmettant les ordres du cerveau, pour des patients paraplégiques ;
- un essai de quelques minutes réalisé par la société *TEKEVER* en 2015 dans le cadre du programme européen *Brainflight*, qui vise à développer des outils de commande cérébrale pour le secteur aérien, a montré qu'il était possible de piloter un drone par la pensée, le pilote étant muni d'un casque à électrodes détectant l'activité cérébrale. La même année, une patiente paraplégique atteinte d'une maladie neurodégénérative, après avoir

pu commander un bras grâce à des microélectrodes implantées dans son cerveau, a réussi, après reprogrammation du dispositif, à piloter un avion de chasse F-35 en simulateur ;

- une équipe du *Karlsruhe Institute of Technology* (Allemagne) et du *Wadsworth Center* (Etats-Unis) a réussi à restituer des phrases entières pensées en langage naturel, par l'enregistrement des ondes cérébrales par des électrodes intracrâniennes ;
- des chercheurs de la *Duke University* ont publié en 2015 les résultats de deux séries de recherche portant sur la construction d'un dispositif informatique organique à l'aide de plusieurs cerveaux interconnectés, dispositif qu'ils ont baptisé *brainet* (contraction de *brain* et de *network*). Ils ont pu montrer que des singes ou des rats étaient capables de coordonner des signaux cérébraux afin de réaliser une action commune (par exemple, déplacer un bras virtuel pour atteindre une cible, afin d'obtenir une récompense).

La simple énumération de ces évolutions marquantes met cependant en évidence les dilemmes éthiques, autant que les défis scientifiques et technologiques qu'implique le développement de dispositifs opérationnels hors d'un environnement maîtrisé, dans les conditions d'emploi que seraient celles liées à un usage militaire.

1.4 – Une intégration des neurosciences au profit de la défense

L'exploitation des connaissances et techniques relevant des neurosciences dans les armées n'est pas récente, avec l'emploi de substances psychoactives, notamment de stimulants du système nerveux central ou au contraire d'incapacitants, ou encore la mise au point de méthodes de formation et d'entraînement optimisées. Mais il s'agit désormais d'aller plus loin. Pour les forces armées, les recherches actuelles dans le domaine des neurosciences, si elles aboutissent, pourraient participer à la réalisation de plusieurs objectifs, comme :

- la préservation de la santé et de la sécurité des opérateurs militaires ;
- le maintien, voire l'amélioration de leurs performances, notamment en matière d'endurance, de capacités sensorielles, de réactivité, de productivité, de créativité ou encore de résistance au stress.

Ces applications auraient une incidence directe sur les performances individuelles et la capacité opérationnelle.

Parmi les axes de recherche qui suscitent également un intérêt – et soulèvent autant d'enjeux éthiques et sociétaux – figurent l'exploitation des connaissances et technologies relevant des neurosciences, en particulier des techniques d'imagerie cérébrale fonctionnelle, en vue d'évaluer la véracité des informations obtenues lors d'un interrogatoire ou même de déterminer le degré de responsabilité d'un individu, notamment dans le cadre d'expertises judiciaires ou dans le domaine du renseignement.

a) L'exemple américain de programmes innovants et soutenus par la défense

Les avancées dans le domaine des neurosciences rendent désormais possible d'envisager que des applications qui semblaient encore relever de la science-fiction il y a quelques années puissent, à plus ou moins long terme, être mises en œuvre. Aux Etats-Unis, le *Departement of Defense* (DoD) alloue chaque année quelques centaines de millions de dollars pour la recherche dans le domaine des neurosciences, principalement à la DARPA, mais aussi à la *Navy*, l'*Army* et l'*Air Force*.

Les programmes lancés par la DARPA en soutien à l'initiative *BRAIN* illustrent les multiples perspectives et les enjeux posés tant pour la recherche que pour les usages possibles. Elle a ainsi initié un certain nombre de programmes avec des objectifs variés, comme favoriser les processus d'apprentissage en stimulant la plasticité synaptique (*TNT*), restaurer le sens du toucher chez des personnes appareillées (*HAPTIX*) ou permettre le contrôle de machines complexes incluant des prothèses haute performance (*Revolutionizing Prosthetics* ou *RE-NET*).

Le programme *RAM* vise à développer, à des fins thérapeutiques, une interface neurale implantable destinée à extraire des souvenirs existants, mais aussi à faciliter la formation de nouveaux souvenirs chez des personnes ayant perdu les leurs à la suite d'un traumatisme cérébral ou d'une maladie neurologique. Le programme *RAM-Replay* doit quant à lui permettre d'explorer les mécanismes de mémorisation afin d'aider les personnes à se remémorer certains évènements.

Dernier exemple, le programme de R&D *NESD* (*Neural Engineering System Design*) a pour ambition de développer une interface neuronale implantable avec une résolution du signal et une bande passante sans précédent pour le transfert de données entre le cerveau et le monde digital. L'objectif est d'arriver à développer un système pouvant communiquer clairement et individuellement avec jusqu'à un million de neurones dans une région donnée du cerveau, avec un dispositif biocompatible qui ne mesurerait pas plus d'un cm^3 et coûterait environ 10 dollars. Par comparaison, les interfaces neurales qui peuvent actuellement être utilisées chez l'homme reposent sur l'agrégation de signaux provenant de dizaines de milliers de neurones, d'où des résultats imprécis. Parmi les applications potentielles figurent la possibilité de compenser des pertes auditives ou visuelles, mais également de remplacer les lunettes de réalité virtuelle et de permettre l'affichage d'informations dans le cortex visuel perceptibles uniquement par le porteur de l'implant.

Récemment, l'armée de l'air américaine a également testé l'efficacité de la stimulation transcrânienne dite « à courant direct ». Cette expérimentation a montré qu'elle améliorait la vigilance, l'attention, la mémoire de travail et la coordination motrice dans le cadre d'une opération multitâche. L'électrostimulation cérébrale pourrait ainsi présenter un intérêt pour des personnels soumis à des sollicitations multiples et devant rester concentrés sur de longues périodes, comme par exemple les pilotes de drones. Les risques d'un usage répété ne sont cependant pas connus à ce stade.

b) En résumé, quelles applications pour la défense ?

Les applications potentielles des neurosciences pour les forces armées, dont certaines restent à l'heure actuelle très hypothétiques, comprennent :

- le suivi médical individuel des combattants, par exemple la surveillance de l'évolution de la vigilance ou du niveau de stress ;
- la prise en charge médico-psychologique, avec notamment la possibilité de restaurer une fonction après une atteinte à l'intégrité physique, voire psychique (commande de dispositif prothétique, perception de sensations recréées, restauration des souvenirs, etc.) ;
- l'amélioration de la formation et de l'entraînement, y compris en cas de stress ;
- l'amélioration des performances physiques et sensorielles des combattants ;
- le guidage à distance de systèmes d'armes, tels que des robots, des drones ou un exosquelette, par une interface cerveau-machine ;
- l'amélioration des performances cognitives des opérateurs et des combattants, en particulier dans un environnement complexe et avec des sollicitations multiples ;
- l'obtention et l'évaluation d'informations à des fins de renseignement ;
- la mise en réseau de capacités cérébrales afin de pouvoir combiner des compétences individuelles.

1.5 – Des questionnements majeurs et des controverses

S'ils se concrétisent, certains développements pourraient être à l'origine de profonds bouleversements dans les prochaines décennies, sans qu'il ne soit encore possible de déterminer toutes les conséquences au niveau individuel, sociétal ou international. En effet, outre la restauration des capacités, il devient désormais envisageable de pouvoir altérer de façon ciblée des fonctions cognitives telles que la mémorisation ou le processus de prise de décision, en les améliorant ou en les dégradant, voire peut-être un jour de modifier ou créer des souvenirs ou encore d'accéder aux pensées d'un individu. Ces évolutions imposent d'engager une réflexion approfondie sur les questions éthiques, sociétales, juridiques et médicales afférentes, en fonction des applications, qu'elles soient civiles ou militaires, et du contexte d'emploi. Elles soulèvent des questions quant aux conséquences en termes de dignité humaine et de respect de la vie privée, mais aussi de risques d'atteinte à l'identité personnelle et à l'autonomie. En interférant avec les fonctions cognitives, ces avancées s'accompagnent ainsi d'une possible remise en cause des notions de libre arbitre ou de responsabilité individuelle, telles qu'elles sont traditionnellement appréhendées. Enfin, il convient de considérer les risques de détournement à des fins malveillantes.

Au-delà de l'état actuel des connaissances sur le cerveau et son fonctionnement, la complexité de la problématique est aussi

liée à l'interdépendance fonctionnelle avec l'environnement physique et social. Que la modification soit recherchée ou secondaire, il peut y avoir atteinte à l'intégrité physique ou psychique des individus. Sans même chercher à dégrader certaines capacités, il existe un risque que l'amélioration de fonctions cognitives spécifiques se fasse au détriment d'autres. La question de la réversibilité des effets doit également être posée. Il faut de plus considérer la problématique de l'acceptabilité individuelle mais aussi sociétale.

La sécurité des équipements médicaux implantables fait déjà partie des préoccupations majeures pour les acteurs du secteur de la santé. En plus des risques de dysfonctionnement, la vulnérabilité aux cyber-attaques de certains systèmes représente donc une crainte légitime, en particulier s'agissant de ceux qui sont connectés et reçoivent et/ou transmettent des flux de données à distance, et ce d'autant plus s'ils sont invasifs. En prenant pour exemple les travaux de recherche en cours portant sur le développement d'un implant neuronal qui pourrait remplacer les dispositifs externes de réalité virtuelle, des informations altérées pourraient par exemple être transmises directement au niveau du cortex visuel.

2 - Situation en 2030

A l'horizon 2030, un soutien financier substantiel à des programmes de recherche innovants aura permis d'obtenir des résultats concrets, avec une **transition réussie de la recherche fondamentale à des applications concrètes de façon générale mais aussi *a posteriori* dans les forces armées.** Dans le même temps, les recherches relevant des neurosciences bénéficieront des approches collaboratives et interdisciplinaires, permettant la levée de verrous technologiques. « L'Homme augmenté » sera en passe de devenir une réalité.

Les Etats-Unis, comme la Chine, auront investi massivement dans ce domaine. Malgré de fortes réticences au sein de la société civile et d'organisations non gouvernementales, voire du Comité international de la Croix-Rouge, **certains systèmes innovants seront déployés et opérationnels** au sein des forces armées américaines et vraisemblablement, de façon plus limitée, de celles d'autres pays comme la Chine, de la Russie ou Israël. A ce stade, il s'agira principalement :

- d'implants destinés à augmenter l'acuité visuelle ou auditive ;
- de dispositifs d'électrostimulation cérébrale pour les opérateurs exerçant en environnement complexe ;
- d'interfaces cerveau-machine permettant soit d'utiliser des exosquelettes afin d'augmenter les capacités locomotrices, soit de piloter des drones ou des robots pour le déminage des engins explosifs improvisés (IED) ;
- d'outils d'aide aux interrogatoires à des fins de renseignement.

En France, des programmes d'essais d'interfaces cerveau-machine seront également en cours avec en parallèle un débat sur la dimension éthique, avec la difficulté d'arriver à un consensus quant à l'intérêt opérationnel par rapport aux investissements et aux risques supposés. **Les utilisations au sein de nos forces armées en dehors de ces essais resteront limitées** soit à un usage thérapeutique, soit à un emploi par une population militaire restreinte, sur de courtes durées, de dispositifs non invasifs augmentant les capacités sensorielles.

Il est encore difficile d'évaluer l'impact des technologies issues des neurosciences pour les armées dans le cadre d'un conflit armé vers 2030. Les potentialités sont évidentes, mais l'absence de recul, des contextes d'engagement variés et une grande opacité quant à leur utilisation ne permettent pas d'affirmer, à ce stade, qu'elles auront, en 15 ans, induit une transformation majeure de la guerre, contrairement à la robotisation du champ de bataille qui aura continué de progresser en parallèle, avec une tendance croissante à la mise en service de systèmes d'armes de plus en plus autonomes.

Comme pour d'autres domaines tels que la biologie de synthèse, certains scientifiques s'inquiètent des risques de mésusage liés à l'essor des neurosciences et appellent à un moratoire pour certaines recherches. La problématique de la gouvernance est régulièrement débattue et la nécessité de la sensibilisation des scientifiques est un point régulièrement rappelé. Il s'avère pourtant vite extrêmement difficile de concevoir un dispositif permettant le développement d'applications à des fins pacifiques en encadrant les recherches pouvant être détournées, en raison d'une part de la dualité, et d'autre part des enjeux économiques et militaires des neurosciences.

3 - Enjeux pour la France et pour l'Europe

Nous ne nous trouvons pas aujourd'hui dans une situation où les Etats actifs dans les neurosciences sont spontanément susceptibles de s'engager dans un processus de limitation de leur utilisation militaire. Les Etats-Unis estiment bénéficier d'une avance leur permettant d'acquérir des avantages capacitaires durables contribuant à la pérennisation de la supériorité de leurs forces et donc de leur puissance. Les puissances rivales sont lancées dans une action de rattrapage qu'elles estiment pouvoir réussir. En revanche, celle-ci n'est pas aboutie et geler les positions dans leur état actuel n'est dans l'intérêt d'aucune des parties. En clair, s'agissant des applications militaires des neurosciences, nous sommes dans le contexte où nous nous trouvions dans les années soixante en matière nucléaire, avant le lancement de la négociation du TNP : un contexte non coopératif de compétition capacitaire, chaque partie espérant devancer l'autre et étant techniquement fondée à le penser.

Dans un tel contexte, l'opportunité d'une initiative diplomatique française compara-

ble à celle de 1992 qui conduisit à la négociation de la convention d'interdiction des armes chimiques n'apparaît pas évidente. Une telle négociation ne parviendrait pas aujourd'hui à fédérer les principaux pays impliqués dans la filière ; elle risquerait en revanche, sous l'influence des organisations non gouvernementales, de se déplacer d'une logique de contrôle des armements à une logique d'interdiction placée sur le terrain du droit international humanitaire, établissant une norme de nature morale que les Européens suivraient mais pas leurs adversaires. En revanche, l'espace politique existe pour engager un travail dans une logique de groupe de fournisseurs, afin de commencer à constituer un corpus de bonnes pratiques pouvant ensuite être repris dans un cadre multilatéral. Ceci pourrait se faire par extension du *Groupe Australie* en créant par exemple un sous-groupe spécifique dédié aux neurosciences ou à côté de celui-ci. Cette seconde possibilité présenterait l'avantage de pouvoir inclure des pays fournisseurs, tels que la Chine ou le Brésil, qui ne souhaitent actuellement pas être membres du *Groupe Australie*.

Indépendamment de la question de la constitution de moyens offensifs, qui pose des problèmes éthiques a priori difficilement surmontables dans l'état actuel de notre droit et de la sensibilité de l'opinion à ces problématiques, la France doit en revanche travailler à l'acquisition de capacités défensives si elle veut être capable de maintenir la crédibilité de ses forces, voire même leur interopérabilité au sein de l'OTAN. La constitution de capacités défensives sans se doter de capacités offensives symétriques est toutefois un exercice qui connaît ses limites. Comme on peut le voir en matière de protection contre les armes chimiques, on ne sait se défendre que de ce que l'on connait. La dualité du domaine biologique accentue encore cette difficulté. Cela a permis notamment à l'Union soviétique de développer son programme biologique dans les années 70-80 alors même qu'elle avait ratifié la convention d'interdiction des armes biologiques ou à toxines.

Etant donné les enjeux économiques, sociétaux et éthiques liés à l'essor des neurosciences, plusieurs axes d'effort devront alors être poursuivis :

- assurer une veille stratégique au niveau international, afin d'identifier les axes de recherche poursuivis et suivre les résultats concrets ;
- soutenir la filière des neurosciences, avec des mécanismes de financement de l'innovation adaptés, permettant la transition de la recherche fondamentale aux applications, afin notamment d'éviter qu'équipes de recherche et *start-ups* ne soient contraintes de rechercher des investissements étrangers ;
- sensibiliser les scientifiques sur les risques et réfléchir aux questions de gouvernance ;
- mobiliser au service des neurosciences les avantages comparatifs dont notre outil de recherche dispose dans d'autres domaines. C'est en particulier le cas de notre capacité en calcul haute performance, évidemment utile aux projets de cartographies du cerveau mais également nécessaire au développement des dispositifs d'interface neurale par exemple ;
- procéder périodiquement à une analyse bénéfices / risques, en considérant le caractère dual de certains développements, afin de pouvoir anticiper leur impact potentiel, positif ou négatif, à moyen et long terme, et d'y adapter nos moyens de défense.

Un des enjeux pour la France sera de développer le rôle de l'Europe et de ses instruments financiers sur ce secteur :

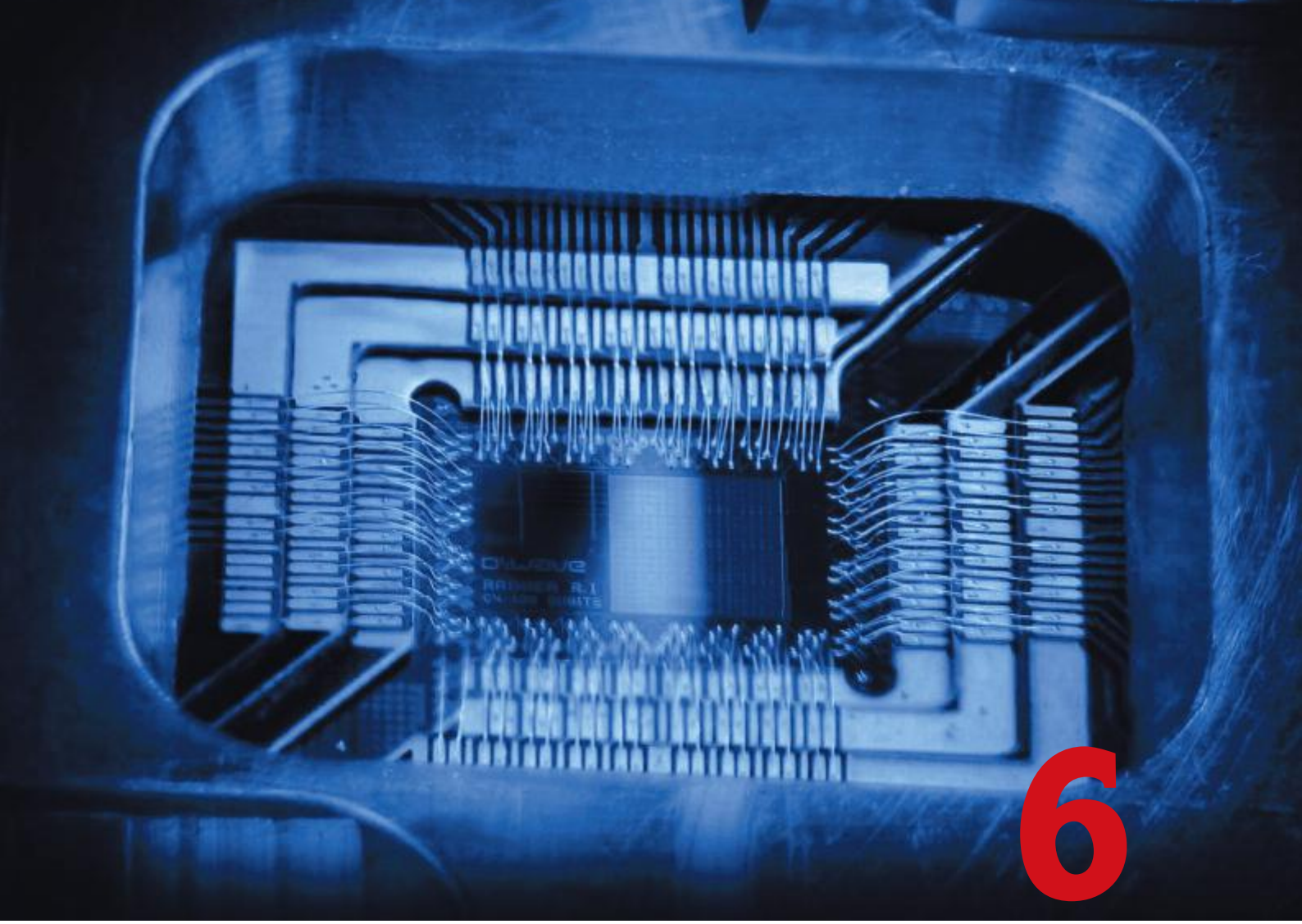
- parce que l'investissement public national restera, sur la période de référence, plafonné et fortement contraint par la concurrence avec les besoins de financement de l'existant et ceux du financement de l'innovation dans les secteurs bénéficiant d'une priorité de politique publique déjà construite (énergies renouvelables) ; c'est sur les aspects connexes à la défense (peu ou pas financés par l'UE) qu'il faudra en priorité l'orienter ;
- parce que les programmes européens d'aide à la recherche, en plus d'être bien dotés, ont l'avantage de faire une place large aux technologies capacitantes (*KETS*) et aux technologies répondant à des défis sociétaux ;
- parce que les programmes européens sont conçus pour ne pas fonctionner en abondement de financements nationaux existants et privilégient les projets interdisciplinaires, de préférence portés par des acteurs non publics, ce qui correspond au profil de développement des dispositifs innovants décrits plus haut.

Enfin se posera, pour la France et l'Europe, en complément du défi de mise au point de dispositifs défensifs, celui de mener une planification de *scenarii* de menaces terroristes et de cartographie des risques cybernétiques, particulièrement élevés dans ce domaine, sur les applications amenant à connecter le vivant à la machine.

4 - Scénario alternatif

Les neurosciences révolutionnent l'art de la guerre suite à la levée d'une série de verrous scientifiques et technologiques par l'investissement massif des Etats-Unis dans les recherches en neurosciences, notamment à des fins militaires mais aussi d'intelligence économique. Les travaux portant sur le contrôle à distance des émotions et des actions, sur l'implantation de souvenirs altérés, ainsi que sur le décodage des pensées et l'appréciation de la véracité des propos, aboutissent et des dispositifs permettant d'intervenir à distance ont été mis au point. Les soldats sont équipés d'interfaces neurales améliorant leurs sens et leur permettant de recevoir directement des informations en temps réel. Les interfaces cerveau-machine permettant de contrôler les drones et d'autres systèmes d'armes sont par ailleurs entrées en service dans les armées. Les neurosciences contribuent ainsi à transformer la guerre, en association étroite avec la robotisation du champ de bataille.

Le déploiement de ces technologies contribue dans un premier temps à asseoir l'hégémonie américaine. Cependant, très rapidement, les tensions géopolitiques s'exacerbent et les Etats-Unis sont régulièrement accusés d'interférer dans les processus électoraux et décisionnels d'autres Etats, en fonction de leurs intérêts. Dans ce contexte, la question de la garantie de la protection des informations et de l'intégrité des processus décisionnels se pose de façon aiguë.



6

La cryptographie est-elle à l'aube de la révolution quantique ?

L'essentiel

Utilisée depuis l'Antiquité, la cryptographie a connu au cours des siècles différentes révolutions, évoluant d'un art à une science avec le développement de l'algorithmie. La cryptographie constitue aujourd'hui une composante essentielle de la protection de la vie privée. Son utilisation se démocratise progressivement alors que le déchiffrement est dorénavant utilisé à des fins judiciaires ou de renseignement.
La place croissante du numérique dans la société et les nécessités de préserver les libertés fondamentales et de garantir la sécurité des citoyens imposent de trouver un équilibre juste entre une large utilisation de la cryptographie et le maintien d'une possibilité d'accéder à des informations chiffrées. Le fragile équilibre actuel pourrait être remis en cause par les ruptures technologiques que seraient l'avènement d'algorithmes et d'ordinateurs quantiques.

Depuis la fin du XX^{ème} siècle, la numérisation des sociétés s'est accélérée. Le numérique, vecteur de croissance et d'innovation, est devenu omniprésent dans la vie quotidienne des citoyens, dans le monde de la recherche, au sein des entreprises, tout autant que dans la conduite de l'action de l'Etat. Cette numérisation est également source de risques. Or, les questions de sécurité conditionnent la confiance dans les produits et services, et constituent un véritable gage de réussite de la transition numérique. Face aux menaces pesant sur la sécurité nationale, notre économie et nos concitoyens, la France a fait de la sécurité du numérique une priorité stratégique, réaffirmée formellement à plusieurs reprises, notamment dans les livres blancs sur la défense et la sécurité nationale et la stratégie nationale pour la sécurité du numérique publiée en 2015.

1 - Etat des lieux en 2017

1.1 - Toujours plus de données à protéger et une cryptographie qui se démocratise

Au premier rang des indispensables outils de protection de l'information figurent les moyens de cryptographie, qui permettent d'assurer un juste niveau de sécurité lors de la transmission, du stockage et de l'accès aux données numériques sensibles. Utilisée depuis l'Antiquité, la cryptographie, longtemps méconnue et réservée à une communauté très restreinte d'utilisateurs, est aujourd'hui largement diffusée,

accessible et aisée dans sa mise en œuvre. Ses applications sont très nombreuses : échanges couverts par le secret de la défense nationale, données de santé ou de professions réglementées, données techniques, commerciales et stratégiques des entreprises, données personnelles des citoyens, etc.

L'usage des moyens de cryptologie, auparavant très encadré réglementairement, tend à se généraliser. Le développement et la diffusion de solutions de sécurité robustes et de confiance est encouragé. La législation française donne explicitement la liberté d'usage de ces moyens, en recherchant un juste équilibre entre la protection des libertés individuelles et la sécurité collective.

1.2 – L'apport de la physique quantique à l'informatique

En s'appuyant sur les principes - parfois déroutants - sur lesquels repose la mécanique quantique, plusieurs physiciens théoriciens ont imaginé, dans les années 1970, le concept de l'ordinateur dit « quantique ». Les ordinateurs traditionnels, du simple ordinateur de bureau au supercalculateur, fonctionnent aujourd'hui avec des transistors et des processeurs, et une base binaire de codage de l'information, les fameux bits, dont la valeur peut être soit 0 soit 1. L'ordinateur quantique, lui, manipule des particules élémentaires, telles que les photons, pour représenter l'information. Ces particules, de taille infinitésimale – de l'ordre de 10^{-22} mètres – ont des propriétés dites « quantiques », en rupture avec l'approche classique déterministe, qui peuvent heurter l'intuition.

Parmi les propriétés importantes, le phénomène de superposition, qui « permet » à une particule « d'être » à plusieurs endroits en même temps, est sans doute le plus structurant. En appliquant cette idée à l'informatique, les pères fondateurs de l'informatique quantique ont cherché à tirer profit de la possibilité, pour une particule, d'être à plusieurs endroits à la fois, pour construire un système qui pourrait effectuer plusieurs calculs en même temps, et non plus simplement en parallèle, ce que font les ordinateurs actuellement.

Ce passage du monde classique au monde quantique est notamment symbolisé par l'utilisation des qbits, pendants quantiques des bits informatiques classiques, qui ne valent plus strictement 0 ou 1 de façon déterministe, mais une superposition de ces deux valeurs, avec des probabilités différentes. Très concrètement, cette approche permet aux systèmes de calcul quantique de voir leur puissance de calcul augmenter de façon exponentielle au fur et à mesure que leur nombre de qbits augmente – là où la croissance des machines classiques était « seulement » linéaire – ce qui laisse entrevoir des opportunités et développements extrêmement intéressants dans de nombreux champs d'application. Ainsi, un ordinateur quantique de 300 qbits devrait avoir une puissance de calcul analogue à celle d'un supercalculateur construit avec

tous les atomes de l'univers. A titre de comparaison, on mettra en regard cet exemple avec l'ambition affichée par la société canadienne *D-WAVE*, qui annonce être en passe de commercialiser – sans toutefois l'avoir démontré à ce jour – un ordinateur quantique contenant 2 000 qbits.

Si l'exemple de *D-WAVE* soulève un certain nombre de doutes au sein de la communauté scientifique, le sujet de l'informatique quantique et de ses différentes applications a été investi par de nombreux acteurs, qu'ils soient gouvernementaux, industriels ou académiques. Ainsi, plusieurs initiatives récentes ont donné une dynamique nouvelle aux réflexions sur la cryptographie dite « quantique » et « post-quantique ». Parmi celles-ci, figurent l'annonce, en mai 2016, par la Commission européenne de la création en 2018 d'un nouveau programme de recherche européen sur les technologies quantiques doté d'un milliard d'euros, ou encore le lancement remarqué, en novembre 2016, par le groupe *ATOS* du premier programme industriel d'informatique quantique en Europe.

Développer et mettre en œuvre un ordinateur quantique fonctionnel, en maîtrisant les particules qu'il manipule, constitue un véritable défi scientifique, technologique et industriel. En effet, on ne sait aujourd'hui manipuler ces entités infiniment petites que dans des conditions de laboratoire très particulières, à des températures et des pressions extrêmement faibles, et par « petites poignées ». Au-delà de la machine elle-même, c'est également tout le champ des algorithmes qui nécessite d'être investi, afin de mettre au point des modes de calcul qui pourront tirer pleinement partie des possibilités offertes par la chose quantique. Si la faisabilité même de cette rupture n'est à ce jour pas acquise, et que les échéances dans lesquelles elle pourrait se produire sont encore très floues, il semble raisonnable de la considérer avec le plus grand sérieux eu égard aux implications majeures qu'elle engendrerait.

1.3 – Cryptographie dite « quantique » : de quoi parle-t-on ?

Si les propriétés quantiques de la matière peuvent être mises à profit pour développer des ordinateurs dits « quantiques », elles ont également plusieurs applications concrètes dans le cadre plus spécifique de la sécurité de l'information numérique.

a) La cryptographie dite « quantique »

La « cryptographie quantique » consiste à utiliser des propriétés issues de la physique quantique, comme le principe de superposition décrit plus haut ou la corrélation des états de deux photons, afin de construire de nouveaux mécanismes de transmission sécurisée d'informations. Elle introduit en particulier la possibilité de transmettre une information sans en protéger la confidentialité de prime abord, mais en garantissant la détection *a posteriori* de toute interception par une tierce partie.

Ces approches, théorisées dans le monde académique depuis le milieu des années quatre-vingt, ne nécessitent pas la mise en œuvre d'un ordinateur quantique, et ont fait l'objet d'un certain nombre d'implémentations concrètes depuis le début des années 2000. Dans le cadre du programme *QUESS*, la Chine a par exemple lancé en 2016 le satellite *MOZI* afin de mener des expériences sur la transmission d'informations à longue distance au moyen de systèmes de cryptographie quantique.

Cependant, la cryptographie quantique ne constitue pas en soi une rupture conceptuelle majeure, dans la mesure où elle ne remet pas en cause la sécurité de la cryptographie classique et ne présente un intérêt significatif que dans certains cas d'usage spécifiques.

b) La cryptanalyse grâce à des ordinateurs quantiques

La sécurité des mécanismes cryptographiques en vigueur repose, dans une large mesure, sur des problèmes mathématiques dits « difficiles ». Ainsi, au regard des puissances de calcul actuelles, une signature cryptographique ou un déchiffrement sont des opérations mathématiquement simples pour qui connaît le secret – la clé – utilisé par l'algorithme mis en œuvre, mais d'une complexité impraticable pour qui ne le connaît pas.

On appelle « cryptanalyse » la démarche consistant à « casser » un message chiffré sans connaitre la clé utilisée lors du chiffrement. La « cryptanalyse quantique », quant à elle, est à ce stade un concept hypothétique, conditionné à la mise au point future d'un ordinateur quantique fonctionnel. Celui-ci, en exploitant des propriétés quantiques lui permettant d'atteindre des puissances de calcul très importantes, pourrait remettre fondamentalement en cause le caractère « difficile » de certains problèmes mathématiques, et notamment la sécurité de constructions cryptographiques cruciales. Des opérations nécessitant en théorie aujourd'hui des milliards d'années de calcul deviendraient ainsi réalisables dans des délais raisonnables.

c) La cryptographie dite « post-quantique » comme moyen de résister à un attaquant doté d'une puissance de calcul quantique

La cryptographie dite « post-quantique » vise à l'élaboration de nouveaux mécanismes cryptographiques, reposant sur des problèmes mathématiques différents et susceptibles de résister à une future cryptanalyse par ordinateur quantique. Il s'agit d'un domaine de recherche relativement ancien mais qui n'a connu un regain d'activité que récemment.

Plusieurs algorithmes de cryptographie issus de ces travaux sont actuellement réputés résistants à une cryptanalyse quantique. Il convient cependant de souligner le manque de maturité de la recherche dans ce domaine : la résistance de ces nouveaux mécanismes, tant face à des attaques « quantiques » que vis-à-vis de techniques de cryptanalyse plus classiques, n'a pas à ce jour été significativement éprouvée, ni même théoriquement démontrée. Par conséquent, et compte-tenu du caractère hypothétique du risque quantique, il n'apparaît pas opportun à ce jour de remplacer les mécanismes cryptogra-

phiques en usage courant par l'un ou l'autre de ces mécanismes émergents.

L'amélioration du niveau de confiance envers ces mécanismes post-quantiques nécessitera une forte implication des équipes de recherche académiques. C'était précisément le but de la compétition internationale lancée par le *NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY* (NIST) américain le 24 février 2016, afin de sélectionner de nouveaux standards cryptographiques post-quantiques. Cette compétition, qui débute à peine, devrait fédérer et dynamiser les efforts de recherche dans le domaine au niveau mondial, pour une durée de trois à cinq ans.

2 - Situation en 2030

Aujourd'hui, **la cryptanalyse et le déchiffrement sont réalisés à partir de deux technologies complémentaires, l'algorithmie et les supercalculateurs,** dont on aperçoit déjà les limites de développement.

L'algorithmie est désormais largement théorisée, et seul l'usage des algorithmes spécifiques à chaque outil de chiffrement peut être optimisé. **Cependant, il est peu probable que cette science en elle-même soit remise en question par une révolution dans les 15 prochaines années.**

Les supercalculateurs, quant à eux, sont en constante évolution et suivent approximativement la loi de MOORE, avec un doublement de leurs capacités tous les 18 mois environ. Ce développement est obtenu essentiellement grâce aux progrès technologiques apportés par l'augmentation de la finesse de la gravure des composants électroniques et la multiplication de ceux-ci. **Cette augmentation continue des performances des supercalculateurs devrait cependant atteindre une asymptote vers 2020,** avec les limites physiques que constituent :

- la consommation électrique et la nécessaire dissipation calorique associée ;
- le seuil « plancher » de la dimension de l'atome pour la taille des gravures, seuil qui correspond en outre aux dimensions où les lois de la physique quantique ne sont plus négligeables devant les lois de l'électromagnétisme « classique », qui régissent la conception actuelle des supercalculateurs.

Prenant acte des horizons finis de ces deux domaines, de nombreuses initiatives, tant dans la recherche que dans le monde industriel, ont été lancées pour développer les ordinateurs quantiques, dont le principe de fonctionnement assurerait *de facto* une puissance de calcul bien supérieure aux supercalculateurs les plus puissants en cours de développement aujourd'hui.

Rien ne permet d'affirmer que le développement d'ordinateurs quantiques sera techniquement possible d'ici 2030. On pourrait bien observer d'ici là l'incapacité de l'ensemble des acteurs de la communauté internationale à surmonter les défis techniques liés au développement

et à la mise en œuvre d'un ordinateur quantique fonctionnel et ce de façon durable.

Toutefois, si le développement de technologies fondées sur la physique quantique demeure relativement incertain, **il constituerait sans aucun doute une rupture majeure** pour notre pays. En effet, l'émergence d'ordinateurs quantiques – indépendamment des immenses défis techniques et financiers que représente leur conception et leur construction – bouleverserait l'environnement numérique **en rendant inopérant de nombreux systèmes de chiffrement contemporains.**

Face à ces constats, il apparaît pertinent de se concentrer à la fois sur la mise au point d'un ordinateur quantique et sur la poursuite du développement des capacités classiques actuelles de cryptologie.

Au regard de ces différents éléments, il pourrait être adopté à ce stade les positions suivantes :

- assurer une veille active sur l'émergence de la technologie quantique et notamment des briques technologiques indispensables à son développement ;
- renforcer le développement d'une cryptologie robuste afin de préserver l'intégrité des instruments stratégiques de l'Etat (dissuasion nucléaire, défense, nucléaire civil, économie, etc.).

3 - Enjeux pour la France et pour l'Europe

Les principaux enjeux de l'avènement de l'ordinateur quantique, pour la France et pour l'Europe, sont de trois ordres :

- un enjeu de souveraineté, résidant dans le maintien de la capacité à protéger correctement les informations sensibles (données relevant du secret de la défense, médicales, personnelles, etc.) ;
- un enjeu technologique, avec la possibilité de capitaliser sur une longue tradition d'excellence scientifique française et européenne, afin de se positionner à la pointe de ce nouveau domaine ;
- un enjeu économique, avec la dynamisation du tissu industriel français et européen sur ces sujets.

Si la France parvenait à maîtriser les technologies permettant de développer et d'opérer des ordinateurs quantiques fonctionnels avant les autres pays, elle jouirait de nombreux avantages dans divers domaines. Dans le domaine scientifique, l'ordinateur quantique fournirait une capacité de calcul dont le potentiel pourrait utilement être exploité par les travaux de simulation, par exemple à des fins d'anticipation et de compréhension de phénomènes naturels et biologiques. Les domaines de la physique nucléaire, de la météorologie et de la biomédecine seraient concernés en particulier. La capacité de cryptanalyse quantique pourrait aussi être mise à profit par les services de renseignement afin de mettre au clair les flux de

données interceptés. L'exportation d'une technologie aussi prometteuse que celle de l'ordinateur quantique, qui devrait nécessairement être encadrés, représenterait enfin un potentiel important de financements pour son exportateur.

A l'inverse, ne pas maîtriser cette technologie alors qu'un autre Etat s'en serait doté serait susceptible de faire peser des risques très sérieux sur la sécurité nationale. La captation puis le décryptage de données sensibles, telles que les informations classifiées ou celles relevant du patrimoine scientifique et technique de l'industrie nationale, pourrait causer des dommages extrêmement graves. Un telle perspective impliquerait notamment :

- sur le plan de la sécurité et de la souveraineté, de devoir mettre en place un plan global de protection des informations, désormais exposées à des attaquants disposant de capacités de calcul quantique, couplé à la mise en œuvre d'un rattrapage capacitaire massif ;
- sur le plan économique, pour les acteurs impliqués dans le domaine, de se repositionner utilement, afin de rattraper le retard induit par l'émergence de solutions concurrentes opérationnelles.

7

Le champ de bataille « 3.0 » : intelligence artificielle, robots, nanotechnologies et armes à énergie dirigée sous l'uniforme

L'essentiel

Les robots et les systèmes autonomes sont déjà présents dans les armées. Ils permettent de préserver des capacités humaines ou de les dépasser. Ils sont capables d'un niveau de précision inaccessible en contrôle manuel. Leurs analyses sont plus rapides et statistiquement plus prédictibles que celles d'un être humain, particulièrement en état de tension nerveuse et physique. Certains de leurs promoteurs n'hésitent pas à attribuer à ceux-ci une « supériorité éthique » par rapport à l'être humain car ils estiment que leur comportement général ne pourrait enfreindre sciemment les règles fixées. En 2030, les robots et systèmes autonomes seront devenus des acteurs ordinaires dans le domaine des opérations militaires. Télé-opérés ou entièrement autonomes, ils agiront dans les champs d'affrontement physiques et le cyberespace. Toutes les configurations seront possibles : seuls, en groupes homogènes ou au sein d'unités mixtes humains-robots.

Les nanotechnologies constituent, par ailleurs, à la fois une révolution industrielle, dans laquelle la France est engagée, et un enjeu majeur pour la défense par leurs nombreuses applications déjà exploitées, envisagées et envisageables ; cette évolution est rapide et irrésistible. Les ruptures technologiques que permettront les applications des nanotechnologies au domaine de la défense auront des incidences certaines sur les équipements et la conduite des opérations.

A l'origine des armes, la puissance de celles-ci était limitée par la force physique de celui qui s'en servait. Au Moyen-âge est intervenue une révolution dans l'art de la guerre, lorsque la poudre a fait son apparition et que la puissance des armes a pu se libérer des limitations humaines grâce à la chimie. Si depuis les progrès ont été nombreux en matière d'armement, c'est bien toujours le principe d'une munition propulsée par une réaction chimique qui demeure. L'apparition dans les unités opérationnelles d'armes à énergie dirigée pourrait bien être l'amorce de la prochaine révolution militaire.

1 - Etat des lieux en 2017

1.1 - Robots et systèmes autonomes : de quoi parle-t-on ?

Les robots et systèmes autonomes[1] sont des objets physiques ou « intangibles » dotés de fonctions complexes comme l'orientation, la navigation, le déclenchement ou l'arrêt d'effecteurs. Un robot peut disposer d'une autonomie complète, partielle, ou nulle. Les systèmes « intangibles » disposant d'autonomie peuvent être des logiciels d'analyse d'image, d'analyse de la parole, d'analyse des attaques informatiques, de diagnostic médical ou simplement d'optimisation.

1 - Il n'existe pas de définition consensuelle de ces systèmes.

En fonction de leur degré d'autonomie, trois types de systèmes sont ainsi définis :

- **le système télé-opéré**, qui est un système piloté à distance par un équipage, *via* des moyens de télécommunication. L'équipage accomplit à distance les mêmes tâches que s'il était embarqué ;
- **le système télé-supervisé**, qui est un système dont certaines tâches (navigation, observation, pointage des capacités de tir) sont automatisées. Grâce à des moyens de télécommunication, un opérateur analyse la situation fournie par les systèmes et contrôle l'exécution des tâches les plus sensibles (pointage et ouverture du feu par exemple) ;
- **le système autonome** qui exécute l'ensemble de ses tâches sans intervention humaine, y compris les plus sensibles, telles qu'elles lui ont été assignées avant le début de sa mission. Toutes les tâches sont automatisées. Un type particulier de système autonome focalise aujourd'hui l'attention ; il s'agit du système d'arme létal autonome (*SALA*) qui est un système robot disposant d'une part d'autonomie plus ou moins développée et qui mène par lui-même, de par sa conception, des missions de destruction. De tels systèmes existent déjà (torpilles, missiles « rodeurs », systèmes de défense).

Certains pays (Etats-Unis, Chine...) nourrissent de grandes ambitions en matière de développement puis d'acquisition de systèmes autonomes. Les avancées observées en matière d'intelligence artificielle crédibilisent ces velléités. Pour autant, sauf rupture technologique majeure, les armes totalement autonomes ou « robots tueurs » ne devraient pas voir le jour avant 20 à 30 années.

1.2 – La robotique militaire, une donnée déjà opérationnelle et qui se développe

Tous les pays producteurs d'armement (Etats-Unis, Russie, Chine, France, Grande-Bretagne, Israël...) proposent aujourd'hui des systèmes d'armes, y compris létaux[2], intégrant des robots ou des systèmes autonomes (suivi de terrain automatique pour avions de combat, systèmes de défense anti-aérienne et anti-missile, missiles de croisière ou « rodeurs », systèmes d'autodéfense de plateformes de combat, mines marines). Sur le plan économique, le marché de la robotique militaire est évalué à 3,2 Md$/an. Il devrait atteindre 10,2 Md$/an en 2021[3]. Par ailleurs, les études capacitaires concluent à l'autonomisation possible de tous les systèmes militaires pour presque toutes les missions : systèmes de renseignement, de surveillance et de reconnaissance, systèmes offensifs et systèmes de commandement. Tous les milieux d'engagement sont concernés. Le potentiel d'accroissement du nombre de ces systèmes s'avère très important.

Aujourd'hui, les avions de combat peuvent évoluer en suivi de terrain automatique et

2 - En général, les systèmes défensifs sont dotés d'un plus large degré d'autonomie que les systèmes offensifs pour lesquels l'ouverture du feu reste soumise à l'autorisation d'un opérateur.

3 - Etude de marché *WINTERGREEN RESEARCH* (2014).

leurs pilotes peuvent se contenter d'autoriser le tir de leur armement selon une séquence que le calculateur principal de l'avion a élaboré et proposé. Dans le domaine du renseignement, les drones aériens sont apparus dès les années 60, mais leur véritable essor date des années 90 avec l'apparition de drones de reconnaissance télé-opérés de longue endurance[4]. Une nouvelle étape a été franchie avec les premières frappes de drones de reconnaissance armés[5] dans les crises des années 2000 ; en parallèle, les Américains lançaient le développement de drones de combat autonomes furtifs[6]. Actuellement, des drones à décollage vertical ou volant en essaim sont à l'essai avec des perspectives opérationnelles prometteuses[7]. L'importance prise par les drones dans les opérations militaires est désormais une évidence que personne ne conteste. Elle se constate tout particulièrement aux Etats-Unis, pays qui consacre chaque année, dans son budget de la défense, environ 5 milliards de dollars à ces systèmes et qui prévoit que ses forces armées puissent en 2019 activer en permanence 90 orbites de drones aériens de surveillance, alors même que la CIA peut déjà en activer une vingtaine. Si Israël a bien perçu le potentiel militaire de ces engins, l'Europe a pris du retard dans le domaine des drones de longue endurance et, malgré plusieurs tentatives manquées de coopération industrielle dans le passé, en est réduite à acquérir sur étagère des matériels américains ou israéliens. Elle semble néanmoins se mobiliser, comme en témoigne le projet *MALE RPAS* (*Moyenne altitude et Longue Endurance Remotely Piloted Aircraft System*) lancé en 2014 et qui devrait aboutir en 2025 à une première livraison aux pays partenaires (France, Allemagne, Italie, Espagne). Des programmes de démonstrateurs d'UCAV furtifs sont en outre conduits par la Grande-Bretagne (*Taranis*) et par un groupe d'industriels européens emmenés par D*ASSAULT AVIATION* (*Neuron*), tandis que l'Europe, en particulier la France, est présente sur le secteur des drones tactiques.

Dans le milieu maritime, les systèmes d'autoprotection autonomes sont apparus sur les navires à partir des années 50. Au cours des années 70, ces systèmes ont été dotés de modes de tir autonomes. Ainsi, les Américains défendent à courte portée leurs plateformes avec le système automatique *Phalanx* qui acquiert sa cible, pointe son canon multitubes et ouvre le feu dans une séquence entièrement automatisée. Dans le domaine du renseignement, de la surveillance, de la reconnaissance et de la guerre des mines d'autres systèmes autonomes sont proposés. L'industriel *THALES* a ainsi récemment présenté un concept de drone mixte de surface et sous-marin, l'*AUSS* (*Autonomous Underwater & Surface System*), qui pourrait conduire un large spectre de missions de manière autonome sur une période de plusieurs semaines.

Dans le domaine des opérations terrestres, des systèmes autonomes sont apparus au milieu des années 2000 avec pour principal objectif de préserver la vie des

4 - Drones israéliens *Hunter* puis *Héron*, drones américains de la famille *Predator*.

5 - *MQ-1 Predator*, puis *MQ-9 Reaper* américains notamment.

5 - Ces développements d'*UCAV* (*Unmanned Combat Air Vehicle*) ont débouché sur une série de vols du démonstrateur *X 47B* entre 2011 et 2015, au cours desquels plusieurs « premières » ont été réalisées pour un drone (premier catapultage et premier appontage en 2013, premier ravitaillement en vol en 2015).

5 - En octobre 2016, trois chasseurs *F 18* américains ont largué à grande vitesse 103 mini-drones qui ont ensuite évolué en essaim mettant en œuvre un processus de décision collective ayant conduit à des adaptations de la formation en vol.

combattants. Depuis lors, des robots et drones sont très largement utilisés, principalement dans des missions d'observation et de déminage[8]. Ils permettent de soutenir l'homme et de préserver sa vie, sa santé et ses forces[9]. Par ailleurs, depuis les années 2010, les systèmes de défense autonomes létaux répondent au besoin de protection des personnels et des biens et à l'interdiction de zones (frontières, zones interdites, infrastructures militaires ou vitales...) face à une menace permanente. Ainsi, depuis 2013, la Corée du Sud a réparti le long de sa frontière avec la Corée du Nord des robots *SGR-A1* développés par *SAMSUNG TECHWIN*. Dotés de capteurs et armés d'une mitrailleuse et d'un lance-grenade, ceux-ci remplissent une mission de sentinelle statique. La fonction d'ouverture du feu, quoiqu'automatisable, demeure néanmoins sous le contrôle d'un opérateur humain distant. Les Israéliens, quant à eux, ont développé un drone terrestre armé nommé *Segev* pour patrouiller le long de leur frontière avec la bande de Gaza. La Chine indique développer des groupes de combat robotisés. Les Russes ne sont pas en reste et auraient déjà déployé une unité robotisée[10] en Syrie pour s'emparer de points clés du terrain[11]. Le robot russe *Volk 2*, télé-piloté, serait capable de tirer en mouvement à une vitesse de 35 km/h avec une excellente précision de tir. L'armée russe l'utiliserait pour protéger ses camions porte-missiles balistiques. Le robot chenillé *Strelok*, capable de se mouvoir en environnement urbain, serait utilisé par les forces spéciales. Les Russes mettraient aussi en œuvre un robot démineur *Ouran-6*, télé-piloté, qui détecterait et neutraliserait tout type de mines. Enfin, le dernier char russe, le *T 14 Armata*, serait équipé d'un système d'autonomisation complète de sa tourelle. En 2025, l'objectif affiché par les militaires russes est d'employer plus de 30 % de systèmes d'armes autonomes et semi-autonomes. Aux Etats-Unis, le commandant du *Marine Corps* a déclaré vouloir équiper chacune de ses sections de *Marines* de mini-drones de reconnaissance et le commandement des opérations spéciales a demandé que lui soit proposé pour évaluation en 2018 un prototype d'exosquelette.

1.3 – Atouts et limites des robots et des systèmes autonomes

Les robots permettent au combattant terrestre de tirer parti des capacités techniques des équipements actuels qui dépendent de capteurs toujours plus performants mais dont la masse est pénalisante en termes de mobilité et d'endurance. Ils disposent généralement d'une mobilité (vitesse, accélération, durée) bien supérieure à la résistance humaine.

Les systèmes télé-supervisés permettent de réduire les pertes et le risque d'effets collatéraux en permettant d'exécuter un « geste technique » parfait et largement dépouillé de tout affect. Ils permettent aussi d'accé-

8 - L'armée américaine aurait acquis plus de 14 000 exemplaires de petits robots de déminage *Packbot* et *Talon* et plus de 11 000 exemplaires des microdrones *Raven*.

9 - La société *BOSTON DYNAMICS* propose ainsi des robots mules (*Big Dog* et *LS 3*).

10 - Equipée de robots *Plateform-M* et *Argo* (1 000 kg, 20 km/h, équipé d'une mitrailleuse et de grenades).

11 - La réalité de ce déploiement fait débat.

lérer le rythme de l'action militaire grâce à une disponibilité quasi-permanente au plus près des combats.

Quant aux systèmes autonomes, leurs atouts sont encore plus nombreux. Un récent rapport américain[12] identifie les domaines opérationnels au sein desquels l'autonomie peut apporter une plus-value notable :

- l'accélération de la prise de décision ;
- le traitement et l'ordonnancement de données en masse ;
- la réaction à des lacunes en matière de transmissions opérationnelles ;
- la gestion de la complexité d'une manœuvre « coordonnée » ;
- les missions dangereuses pour l'homme et la permanence opérationnelle.

On pourrait ajouter à ces atouts, la capacité des systèmes autonomes à jouer un rôle de multiplicateurs d'influence (crainte de l'adversaire, confiance des alliés) et à analyser les expériences dans une logique d'optimisation progressive de leur emploi.

Au rang des limites de ces machines il faut relever leur inaptitude à agir en dehors du domaine d'application prévu et un risque de perte de contrôle du système. La complexité de certaines situations tactiques excède encore leurs capacités d'analyse, générant ainsi des incidents (un *Tornado* britannique et un *F 18* américain ont ainsi été abattus en Irak en 2003 par des missiles anti-aériens américains *Patriot* tirés en mode automatique et un *F 16* a été contraint pour se défendre de tirer sur une batterie de *Patriot*). Les dysfonctionnements sont généralement traités par une adaptation des procédures opérationnelles et des processus de développement et de qualification. Au bilan, aucun retour en arrière vers des systèmes non autonomes n'a été constaté.

La crainte de voir la machine trop s'autonomiser et ainsi de faire perdre de la cohérence à la manœuvre d'ensemble par altération de l'unicité de commandement, conduit aujourd'hui les armées qui disposent de systèmes autonomes à imposer le maintien d'une intervention humaine dans la chaine d'engagement. Cette précaution bride cependant les potentialités de la machine – qui dépassent celles de l'homme – et impose le maintien d'une liaison entre l'opérateur et le système qui constitue une vulnérabilité. Dans un souci d'efficacité opérationnelle et de responsabilité, c'est au cas par cas, au regard des missions à mener par la machine qu'il convient de s'interroger sur le degré d'autonomie concédé à celle-ci. La question du principe de la place de l'homme dans la décision d'ouverture du feu résulte d'une politique d'emploi de l'arme et non de l'arme elle-même.

12 - Rapport sur l' « *Autonomy* » du *Defense Science Board* du *Department of Defense (DoD)* des Etats-Unis d'Amérique (juin 2016).

1.4 – Les nanotechnologies en uniforme

Les nanotechnologies sont un ensemble de technologies émergentes liées à l'échelle nanométrique qui présentent un potentiel de développement industriel sans précédent (l'Europe évoque un marché de l'ordre de mille milliards d'euros). Les bénéfices attendus touchent des domaines variés comme les transports (nouvelle électronique), l'agriculture (pesticides et engrais mieux ciblés), les énergies renouvelables, l'environnement (dépollution, réduction des émissions), l'alimentation (emballages, adjuvants, conservateurs), les technologies de l'information et des communications (miniaturisation, successeurs du silicium), les textiles (vêtements innovants), la chimie durable et la santé. En informatique, en particulier, les nanotechnologies constituent une des voies les plus prometteuses pour miniaturiser les transistors et dépasser les limites du silicium aussi bien en finesse d'intégration qu'en vitesse de traitements. Regroupant le *Laboratoire de photonique et de nanostructures* (LPN) et l'*Institut d'électronique fondamentale* (IEF), le *Centre de nanosciences et de nanotechnologies* (C2N) s'installera fin 2017 à Paris-Saclay. Il développera des axes de recherche stratégique dans les domaines des matériaux, de la nanophotonique, de la nanoélectronique et des nanobiotechnologies appliquées aux micro-nano systèmes.

On estime qu'un quart des investissements consacrés au développement des nanotechnologies seront dédiés à un usage sécuritaire et militaire (détection, protection, capteurs, armes). D'ores et déjà, les nanotechnologies permettent d'accroître les capacités des armes, des munitions, des vecteurs, voire des senseurs et des moyens de protection. C'est ainsi que les blindages se font plus légers et plus résistants, que des revêtements furtifs apparaissent, que des particules ultrafines sont utilisées pour la propulsion et les explosifs et que l'arrivée dans les forces terrestres de microdrones tactiques préfigure un changement significatif de la vision du champ de bataille et partant des modes opératoires des petites unités terrestres combattantes.

1.5 – Les armes à énergie dirigée, du mythe à la réalité

On appelle arme à énergie dirigée, une arme capable de faire se propager vers une cible, à la vitesse de la lumière, un faisceau d'ondes électromagnétiques (laser ou micro-ondes), le cas échéant avec une grande directivité (arme laser).

Les avantages que présentent ces armes sont multiples :

- la fulgurance de leur tir permet de multiples engagements dans des séquences très brèves, y compris contre des mobiles extrêmement rapides ;
- leur puissance pouvant être modulée, elles offrent la possibilité de produire une large gamme d'effets létaux ou non ;

- la directivité de leur faisceau leur assure une très grande précision et une excellente maîtrise des effets du tir (arme laser) ;
- s'affranchissant de toute munition, elles se révèlent économiques[13] et peuvent théoriquement tirer tant que de l'énergie leur est fournie.

a) Les armes laser

Ces atouts théoriques ne peuvent toutefois se traduire par un avantage opérationnel qu'après avoir maîtrisé plusieurs difficultés techniques s'agissant des armes à énergie dirigée utilisant un faisceau laser :

- celle de la capacité à produire dans un environnement opérationnel l'énergie nécessaire au tir (typiquement le triple de la puissance du tir) ;
- celle du refroidissement du laser qui dissipe une grande quantité de chaleur à chaque tir ;
- celle de la gestion en toute sécurité dans une ambiance agressive des réactifs chimiques utilisés pour déclencher le tir dans les lasers chimiques ;
- celle du « *blooming* », phénomène qui tend à disperser dans l'atmosphère l'énergie du faisceau laser.

Au-delà de ces défis technologiques, qui restent à relever pour la plupart, les armes laser resteront à jamais limitées par leur inaptitude au tir indirect.

Parmi les armes à énergie dirigée, les plus matures utilisent un faisceau laser. La Chine et les Etats-Unis apparaissent les plus en pointe dans ce domaine. On se souvient, qu'en 2006, un laser situé en Chine a aveuglé un satellite américain de reconnaissance *Key Hole* et, qu'il y a une dizaine d'années, les Américains ont conduit quelques essais de laser aéroporté anti-missile. Mais, au niveau tactique, outre des systèmes d'autoprotection montés sur aéronefs qui sont déjà largement répandus, les armes laser restent rares dans les unités opérationnelles. Elles ont pourtant fait leur apparition il y a déjà plus de vingt ans. En 1995, déjà, la Chine commercialisait le laser tactique *ZM 87*, présenté comme étant capable d'aveugler temporairement des soldats et les optiques de leurs systèmes de visée et d'observation. Du côté américain, le *THEL* (*Tactical High Energy Laser*), un laser de forte puissance, est parvenu à détruire en vol une salve d'obus de mortier lors d'un essai réalisé en 2004. On observe par ailleurs, depuis 2014, la présence à bord de certains navires de l'*US Navy* d'armes laser capables de détruire à plusieurs kilomètres des missiles, des drones ou de petites embarcations. D'une puissance de 30 kW, cette arme est la première de cette nature à être devenue opérationnelle aux Etats-Unis.

S'agissant des développements en cours, le Pentagone est plutôt taiseux sur ce sujet susceptible d'apporter aux forces américaines un avantage décisif en opérations et les autres pays se montrent particulièrement discrets. Quelques informations ont néanmoins été données qui révèlent l'existence d'un réel effort américain. A la fin des années 2000, la *DARPA*[14], l'agence de recherche du *Pentagone*, et l'*US Air Force* ont ainsi lancé le programme *HELLADS* (*High Energy Liquid Laser Aera Defense System*) avec pour objectif de réaliser une arme laser d'une puissance de 150 kW, dont l'encombrement et la masse seraient divisés par dix par rapport aux standards du début du

13 - Selon l'*US Navy*, le coût d'un tir est de l'ordre de l'euro, alors que celui d'un missile anti-aérien par exemple est de l'ordre du million d'euros.

14 - *DARPA : Defense Advanced Research Projects Agency.*

programme. Avec l'ambition d'obtenir un ratio poids/puissance de 5 kilogrammes par kilowatt, la perspective d'un emport par avion de ce laser apparaît crédible. On sait que des essais du *HELLADS* ont débuté à l'été 2015 sur le champ de tir de *White sands* au Nouveau Mexique. Aujourd'hui, l'*US Air Force* finance deux programmes pour lesquels elle a déjà consacré, avec la *DARPA*, 500 M$. Il s'agit, d'une part, du programme *SHIELD* (*Self Protect High Energy Laser Demonstrator*) qui vise à démontrer, dès 2021, la faisabilité de l'emport d'un laser de moyenne puissance par un chasseur pour son autoprotection[15], et, d'autre part, du programme *DLWS* (*Demonstrator Laser Weapon System*), qui prolonge le *HELLADS* et qui est destiné à la défense sol-air d'une plateforme contre les missiles, les roquettes, les obus de mortiers… L'*US Air Force* annonce d'ores et déjà faisable de réaliser un tel système en limitant sa masse à 2,5 tonnes. Elle affiche par ailleurs l'ambition d'équiper ses chasseurs d'armes laser dans le courant de la décennie prochaine. L'*US Navy* a, quant à elle, annoncé en janvier 2017 qu'un laser cinq fois plus puissant que celui qu'elle déploie déjà serait testé à bord d'un bateau dans l'année et, qu'une année plus tard, cette arme serait opérationnelle sur un porte-avions ou un destroyer.

b) Les armes à micro-ondes

Les armes à micro-ondes fonctionnent en émettant un faisceau, ou de courtes impulsions, d'ondes à hautes fréquences (dans la gamme 30 – 300 GHz). Lorsque le flux d'énergie envoyé rencontre des circuits électriques ou électroniques non protégés, il provoque des dysfonctionnements qui peuvent aller jusqu'à une destruction complète. Ce type d'armes offre l'avantage d'une grande efficacité sur les infrastructures modernes qui sont de plus en plus dépendantes de l'électronique, tout en ne provoquant aucune victime, du moins par effet direct. Cependant, il a été constaté qu'à certaines fréquences (de l'ordre de 95 MHz), les ondes millimétriques pénétraient l'épiderme humain sur une très faible profondeur (de l'ordre de 15 mm) et provoquaient une sensation d'échauffement quasi-insoutenable. Des systèmes d'interdiction de zone utilisant ce principe ont été testés dans les années 2000 aux Etats-Unis à l'issue de recherches engagées dès les années quatre-vingt.

Plusieurs indices révèlent l'existence de programmes militaires chinois d'armes à micro-ondes, alors que des équipements américains sont déjà opérationnels et que d'autres sont en développement. L'*US Air Force* a testé en 2012 avec succès le concept d'un missile de croisière aéroporté emportant une charge utile générant des impulsions électromagnétiques[16]. Un de ses représentants a indiqué en 2016 que cette capacité était opérationnelle et que le missile de croisière *JASSM-ER* avait été choisi pour la déployer. En parallèle, a été développé par l'*Air Force* un système d'interdiction de zone non létal, l'*Active Denial System* (*ADS*)[17], qui est opérationnel depuis 2008 et a été déployé brièvement en Afghanistan en 2010. Une version plus compacte, susceptible d'être embarquée à bord d'un véhicule ou d'un aéronef est en développement. Un « fusil anti-drone » à micro-ondes serait par ailleurs actuellement déployé en zone syro-irakienne au sein des forces américaines.

15 - La masse visée est inférieure à 750 kg et l'encombrement de l'ordre de 2 m^3.

16 - Programme *CHAMP* (*Counter-electronics High Power Microwave Advanced Missile Project*).

17 - Selon l'*USAF*, l'*ADS* aurait été testé sur 13 000 individus et, dans deux cas seulement, des soins médicaux auraient été nécessaires. Des études médico-biologiques poussées auraient établi l'absence d'effets cancérogènes et d'impact sur la fertilité d'une « illumination » par l'*ADS*.

2 - Scénario de référence pour 2030

La technologie disponible en 2030 permettra au chef militaire de se placer à distance du danger mais suffisamment proche du champ de bataille pour percevoir la manœuvre et bénéficier d'une juste appréciation de situation. Les nombreux capteurs de renseignement mis à sa disposition généreront une abondance d'informations qui nécessitera un traitement algorithmique. L'organisation du commandement se sera adaptée pour tirer profit de ces capacités nouvelles.

2.1 – Des robots et systèmes autonomes omniprésents

En raison des avantages opérationnels avérés qu'ils offrent, **l'utilisation militaire de robots et de systèmes autonomes se sera développée de manière exponentielle, quoique différenciée, à l'échéance de 2030.** Les armées des grandes puissances utiliseront les matériels les plus sophistiqués ; les autres armées acquerront des matériels moins sophistiqués ou plus anciens. Les organisations non-étatiques, dont les organisations terroristes, procéderont par détournement d'usage de technologies civiles, aisément disponibles, à un coût faible. Cette utilisation généralisée de robots et de systèmes autonomes constitue un enjeu stratégique. Après la maîtrise des applications de l'énergie nucléaire dans les années 50 et l'informatique dans les années 70, ces objets pourraient devenir l'une des bases du 3ème « *offset* »[18], selon une expression américaine.

La miniaturisation des robots, leur intégration de capacités d'intelligence artificielle **et un rapport coût/efficacité favorable conduisent à envisager leur déploiement futur sous forme d'essaim de robots plutôt qu'en termes de plateformes coûteuses, peu nombreuses et exposées aux coups.** Le mode d'action en essaim permet de saturer les défenses ennemies et de créer un « effet de souffle » dont la nature psychologique ne doit pas être sous-estimée. Que ce soit pour des missions de renseignement ou de combat (avec des petites charges explosives embarquées), ces déploiements d'essaim de robots seront difficiles à contrer pour les unités combattantes qui auront à les affronter. Le mouvement des essaims reposant sur des algorithmes de calculs et sur l'intelligence artificielle sera très difficile à prévoir et donc à prévenir.

Le système de combat collaboratif, comprenant des composantes pilotées comme des composantes autonomes, **bénéficiera d'une capacité d'analyse et d'un délai de réaction sans commune mesure** avec un ensemble de systèmes pilotés par des humains. De ce fait, l**es armées qui disposeront de ces capacités**

18 - Avantage opérationnel perdurant sur plusieurs décennies.

bénéficieront des effets d'une rupture majeure dans l'équilibre des forces.

Dans les espaces aériens et maritimes, les robots et systèmes autonomes se seront fortement développés en 2030. Grâce aux drones aériens armés de longue endurance, dont l'emploi se sera généralisé dans les milieux permissifs, pourront être réunies en permanence au-dessus de ces théâtres une excellente connaissance de la situation tactique et une aptitude à délivrer sous très faible délai un armement de précision. **L'efficacité opérationnelle des armées qui seront dotées de ce type d'équipement sera grandement augmentée.**

Dans l'espace terrestre, les robots et systèmes autonomes se seront imposés comme éléments d'environnement du combattant pour l'appuyer, le soutenir et démultiplier son action. Ils seront indispensables pour la réalisation de missions en zone contaminée. Ils seront très présents en tant que capteurs de renseignement (drones tactiques notamment), pour réaliser les missions les plus exposées (déminage, reconnaissance en milieu hostile) et pour soutenir le combattant (robots agissant dans les différentes fonctions de ravitaillement, de maintenance et de santé pour l'évacuation). Ils seront aussi utilisés pour sécuriser les emprises (robots sentinelles), mission très consommatrice de soldats en opérations extérieures ou sur le territoire national. Les robots et systèmes autonomes armés évolueront dans des espaces attribués, éloignés des combattants humains pour éviter tout tir fratricide et pression psychologique sur ces derniers. A ce titre, **la préparation de la mission sur le champ de bataille terrestre s'inspirera de celle effectuée dans les espaces aériens et maritimes** avec l'attribution de zones d'évolution très précises.

Les robots et systèmes autonomes seront bien au cœur de la transformation des armées et de la conduite des opérations dans les décennies à venir. Cette transformation comportera des volets politique, stratégique et technologique et **devra être assortie d'un accompagnement normatif et doctrinal.** Compte tenu de la durée des cycles de renouvellement des équipements militaires, **tout retard capacitaire en systèmes autonomes, civils et militaires, induira potentiellement un déclassement opérationnel, puis industriel et enfin politique.** *A contrario*, leur emploi par une armée permettra une amélioration significative de son efficacité et de sa supériorité opérationnelle.

Les progrès technologiques à faire sont encore nombreux pour parvenir à la situation décrite plus haut. Il s'agira, en particulier :

- de maîtriser l'intelligence artificielle et les capacités de communications directes entre les composantes des systèmes ;
- d'augmenter le niveau d'autonomie des composantes ;
- de déterminer la place la plus adaptée pour l'être humain dans la chaîne de décision.

Des enjeux juridiques éthiques et sociaux devront aussi être pris en compte. Afin d'être accepté par la société et l'institution militaire, un système autonome devra démontrer sa supériorité sans conteste. Il devra donc commettre, dans son spectre de missions, moins d'erreurs, provoquer moins de dégâts collatéraux, atteindre des objectifs plus précisément qu'un système

habité, commandé ou supervisé à distance. A l'instar des systèmes télé-opérés, la mise en œuvre des systèmes autonomes ne devrait donc pas s'accompagner d'une augmentation du risque juridique individuel, tant que leur emploi restera conforme au droit international en vigueur et à une doctrine nationale politiquement assumée.

2.2 – Les nanotechnologies comme multiplicateur de forces

En 2030, **les nanotechnologies permettront notamment aux forces terrestres de se déplacer plus facilement** (pneumatiques aux renforts carbonés), d'être plus difficilement repérables (camouflage actif, furtivité), d'être soutenues par une logistique plus légère (robots d'allègement, autonomie accrue des piles, vêtements plus résistants) **et d'être mieux protégées** (équipements de protection, structures auto-adaptatives). Elles mettront à la disposition des forces une meilleure acquisition du renseignement (capteurs, drones, réseaux de surveillance), un traitement plus rapide des informations (calculateurs, écrans souples) et leur offriront des armes plus performantes (propulseurs, explosifs, lasers, armes non létales). Enfin elles permettront un meilleur soutien de l'homme par les progrès liés à la médecine (implants bio-compatibles, médecine d'urgence, antidotes, neuroprothèses). Les innovations issues du domaine des textiles (vêtement interactifs), de l'agriculture (traitement de l'eau, dépollution des sols) ou de l'alimentation achèveront cette métamorphose de la conduite des opérations. Sur le plan stratégique, les nanotechnologies pourront résoudre certaines difficultés politico-économiques actuelles (additifs nano pour les carburants, contournement des « terres rares »).

Les nouveaux matériaux nécessaires aux nanotechnologies devront cependant être accessibles. La diversité des sources d'approvisionnement nécessaires aux technologies clés (cas du graphène en particulier) ne pourra, comme pour la fonderie silicium actuellement, se réduire au couple Etats-Unis – Chine. **De nouveaux régimes de limitation et de contrôle des arsenaux devront probablement être envisagés.**

2.3 – Les armes à énergie dirigée, comme atout maître

Tout porte à croire qu'**en 2030, Etats-Unis et Chine, au moins, disposeront d'armes à énergie dirigée opérationnelles et efficaces.** A cette échéance, à laquelle près des deux tiers de la population mondiale résideront en milieu urbain, à laquelle par ailleurs se seront encore accrues les dépendances des sociétés aux moyens électroniques, il est vraisemblable que ces armes précises, non létales, et particulière-

ment efficaces contre des réseaux électriques et électroniques auront convaincu de leur intérêt les nations les plus avancées sur le plan militaire.

On peut aisément imaginer en 2030 des forces terrestres de ces pays progressant dans une ville qui aura au préalable été survolée par quelques missiles de croisière qui auront neutralisé toute l'électronique qui s'y trouvait par une impulsion électromagnétique. Un « bouclier » laser protégera leur progression de tous tirs de missiles ou d'artillerie. Des systèmes micro-ondes non létaux isoleront la ville et interdiront à tout élément ennemi de s'en approcher.

Selon toute vraisemblance, les technologies permettant aux Américains, et peut être aux Chinois, de disposer de systèmes d'autoprotection laser particulièrement performants à bord de leurs avions de combat auront été maîtrisées en 2030, alors que ces équipements se seront généralisés sur les navires de guerre des marines les plus modernes.

3 - Scenario de rupture : l'autonomisation complète de robots tueurs

La robotisation associée aux capacités d'intelligence artificielle s'imposera inéluctablement sur le champ de bataille en raison de ses nombreux atouts. La fonction létale de ces robots ne sera qu'une option additionnelle à des objets relevant de technologies duales[19]. Il est donc difficile d'imaginer que certains belligérants ne seront pas tentés de se doter de tels systèmes d'armes.

Le scénario de rupture qui pourrait être envisagé à l'échéance de 2030 serait donc le recours à des systèmes entièrement autonomes dotés de capacités létales (*SALA*).

Ce risque serait d'autant plus grand que les *SALA*, dotés d'une intelligence artificielle, utiliseraient leur capacité d'auto-apprentissage pour s'éloigner des règles initiales d'ouverture du feu.

Cette autonomisation serait aussi très dangereuse compte tenu du risque de déprogrammation et de reprogrammation des robots par des opérations cybernétiques adverses.

Cette autonomisation, qui aurait pour corollaire un désengagement de l'être humain du champ de bataille, transformerait assurément la physionomie de la guerre qui n'aurait plus comme limites que les capacités de robots, démultipliées par rapport à celles des êtres humains.

19 - De nature civile et militaire.

LISTE DES PRINCIPAUX ACRONYMES

A2/AD	*Anti-access/area denial* / Déni d'accès et interdiction de zone
ABM	*Anti Ballistic Missile* / Missile antibalistique
AHW	*Advanced Hypersonic Weapon* - Arme hypersonique avancée
AIEA	Agence internationale de l'énergie atomique
AM	*Additive Manufacturing* / Fabrication additive
AMU	*Aerial Maintenance Unit* / Unité de maintenance des avions
ANR	Agence Nationale de la Recherche
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASAT	Armes anti-satellitaires
ASMP	Air-Sol Moyenne Portée
ASMPA	Air-sol moyenne portée amélioré
AUSS	*Autonomous Underwater & Surface System* / Drone mixte de surface et sous-marin
BITD	Base industrielle et technologique de défense
BMD	*Ballistic missile defense* / Défense antimissile balistique de territoire
BRAIN	*Brain Research through Advancing Innovative Neurotechnologies*
C2	Système dit « C2 » : Système de commandement et de contrôle
C4ISR	*Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*
CCI	Chambre de commerce et d'industrie
CEA	Commissariat à l'énergie atomique et aux énergies alternatives
CEN	Centre d'études nucléaires (Belgique)
CERT-UE	*Computer Emergency Response Team*
CERTEC	Centre de ressources technologiques
CETIM	Centre technique des industries mécaniques
CGARM	Conseil Général de l'Armement
CIBDU	Commission interministérielle des biens à double-usage
CIEEMG	Commission interministérielle pour l'étude des exportations de matériels de guerre
CJUE	Cour de justice de l'Union européenne
CNCB	Conseil national consultatif pour la biosécurité
CNRS	Centre National de recherche scientifique
CoFIS	Comité de la filière industrielle de sécurité
COTS	*Commercial off the Shelf* / Accès réduit à la technologie
CPGS	*Conventional Prompt Global Strike* / Frappe intercontinentale sur court préavis

CUPEEA/ *COPUOS*	Comité des utilisations pacifiques de l'espace extra-atmosphérique / *Committee on the Peaceful Uses of Outer Space*
DAMB	Défense antimissile balistique
DARPA	*Defense Advanced research projects Agency* / Agence pour les projets de recherche avancée de Défense
DGA	Direction générale de l'armement
DGE	Direction générale des entreprises (Ministère de l'économie)
DoD	*Department of Defense* / Ministère de la défense américain
ENISA	E*uropean Network and Information security Agency* / Agence européenne chargée de la sécurité des réseaux et de l'information
EPAA	*European phased adaptative approach*
EPFL	Ecole Polytechnique Fédérale de Lausanne
ESCPI	Ecole supérieure de la physique et de la chimie industrielles de la ville de Paris
EUROPOL	Office européen de police
Fablab	*Fabrication laboratory* / Laboratoire de fabrication
FMAN	Futur Missile Anti-Navire
FMC	Futur Missile de Croisière
GAFA	Géants du Net : Google, Apple, Facebook, Amazon
GBI	*Ground Based Interceptor* / Intercepteurs longue portée basés sur le sol américain
GRAVES	Grand Réseau Adapté à la Veille Spatiale
HAWC	*Hypersonic Air Breathing Weapon Concept*
HCR	Haut-Commissariat aux Réfugiés
HSSW	*High-Speed Strike Weapon*
IADC	*Inter-agency Space Debris Coordination Committee* / Comité de coordination inter-agences sur les débris spatiaux
ICBM	*Inter-continental balistic missile* / missile balistique intercontinental
IDN	Identité numérique
IED	*Improvised explosive device* / Engin explosif improvisé
INRA	Institut National de la recherche Agronomique
INRIA	Institut National de la recherche en informatique et en automatique
INSERM	Institut National de la santé et de la recherche médicale
IRM	Imagerie par résonance magnétique
ISR	Intelligence, Surveillance, Reconnaissance
KET	*Key Enabling Technology* / Technologie capacitaire clé
LEO	*Low Earth Orbit* / Orbite basse terrestre
LRSO	*Long Range Standoff* / attaque de longue portée à distance de sécurité
MCO	Maintien en condition opérationnelle
MOOC	*Massive Open Online Course* / Cours en ligne ouvert et massif
MTCR	*Missile technology control regime* / Régime de contrôle de la technologie des missiles
NASA	*National Aeronautics and Space Administration* / Administration Aéronautique et Spatiale Nationale (Etats-Unis)
NBIC	Nanotechnologies, biotechnologies, informatique et sciences cognitives
NESD	*Neural Engineering System Design*

NIH	*National Institute for Health* / Institut National de la Santé (Etats-Unis)
NIST	*National Institute of Science and Technology* / Institut National de la science et de la technologie (Etats-Unis)
NNMI	*National Network for Manufacturing Innovation* / Réseau national d'innovation en matière de procédés de fabrication
NRBC	Nucléaire, radiologique, biologique et chimique
NSG	*Nuclear Suppliers Group* / Groupe des fournisseurs nucléaires
OCDE	Organisation de coopération et de développement économiques
OIG	Organisation inter-gouvernementale
ONERA	Office National d'Etudes et de Recherches Aérospatiales
ONG	Organisation non-gouvernementale
ONU	Organisation des Nations unies
OSCE	Organisation pour la sécurité et la coopération en Europe
OTAN	Organisation du Traité de l'Atlantique Nord
PARAFE	Passage Automatisé Rapide aux Frontières Extérieures
PAROS	*Prevention of an Arms Race in Outer Space* / Prévention d'une course d'armements dans l'espace extra-atmosphérique
PCRD	Programme cadre de recherche et de développement (UE)
PIA	Programme d'investissement d'avenir
PME	Petites et moyennes entreprises
PNR	*Passenger Name Record* / Données des dossiers passagers
R&D	Recherche et développement
RETEX	Retour d'expérience
RFID	*Radio Frequency Identification Device* / identification par radio fréquence
RTP	Registered Traveller Programme / Programme d'enregistrement des voyageurs
S&T	Science et technologie
SALA	Système d'arme létal autonome
SCAF	Système de combat aérien futur
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SIS	Système d'information Schengen
SNLE	Sous-marin nucléaire lanceur d'engins
SSA	*Space Situational Awareness* / Connaissance de la situation dans l'espace
TBG	*Tactical Boost Glide* / Programme de démonstrateur de planeur hypersonique
TBMD	*Theater ballistic missile defense* / défense de théâtre
TCP/IP	*Transmission control protocol/Internet protocol* / Protocole de contrôle des transmissions / Protocole Internet
THAAD	*Terminal High Altitude Area Defense* / Intercepteurs haut endo-atmosphériques mobiles
TNP	Traité de non-prolifération nucléaire
UCAV	*Unmanned Combat Air Vehicle* / Drone de combat
UE	Union européenne
UIT	Union internationale des télécommunications
USAF	*US Air Force* / Armée de l'air des Etats-Unis
WTEC	*World Technology Evaluation Center (Think Tank)*

Maquette : Pôle Conception graphique-Fabrication - DSAF/DPL
Impression : DILA - Mai 2017.

CHOCS FUTURS

Étude prospective à l'horizon 2030 :
impacts des transformations
et ruptures technologiques
sur notre environnement
stratégique et de sécurité

SGDSN

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 00
sgdsn.gouv.fr