Stratégie nationale de recherche et d'innovation 2009

Rapport du groupe de travail

Risques, aléas, sécurité des personnes, des biens et des communications

RESUME

Le monde doit faire face à de nombreux changements. Il devient de plus en plus complexe d'annoncer des perspectives d'évolutions crédibles car de nombreux facteurs induisent l'apparition d'évènements aléatoires, voire imprévisibles, dont la maîtrise demeure extrêmement difficile. Cette rapidité d'évolution couplée à une instabilité apparente ou réelle conduit à une perception exacerbée des risques et menaces auxquelles doit faire face notre société.

La problématique du changement climatique et le choix des ses possibles contre-mesures est un très bon exemple. Les solutions qui seront proposées pourraient être porteuses intrinsèquement de risques qu'il faudra anticiper et maîtriser. Par exemple, le développement de nanomatériaux pour produire de l'énergie solaire implique des recherches sur les risques liés aux nanotechnologies et sur le cycle de vie des matériaux en question.

Les avancées technologiques et la mondialisation de l'économie ont conduit au développement de vastes réseaux (énergie, communications, transport, finance). Leur complexité constitue une source de vulnérabilité. Ainsi, le développement des transports aériens facilite la propagation d'agents infectieux et des épidémies afférentes (par exemple, le SRAS). Le cyberespace peut constituer un support d'actes illégaux (par exemple, la pédopornographie) ou de malveillance portant directement préjudice aux individus dans leur vie quotidienne.

Toute société humaine reste assujettie à des risques de catastrophes naturelles : éruptions volcaniques, séismes, inondations, cyclones, tsunamis. Tous ces évènements peuvent porter atteinte à l'intégrité de tout ou partie de notre territoire.

L'Etat en particulier et la société dans son ensemble doivent également faire face à des menaces variées, qui peuvent être difficiles à appréhender, provenant d'organisations extrémistes fédérées par une communauté d'intérêts, idéologiques et/ou criminels.

De son côté, l'opinion publique revendique un droit à la sécurité et attend de l'Etat qu'il remplisse cette fonction régalienne dans des domaines aussi variés que la protection du patrimoine, la lutte contre le crime et la délinquance, ou encore la diminution des accidents de la route.

L'activité humaine reste sujette à tous ces risques et menaces qu'il convient en conséquence de réduire sensiblement et dont les effets doivent être maîtrisés au mieux. Il appartient à l'Etat de définir une stratégie globale, y compris dans le domaine de la recherche, permettant d'identifier, de prévenir et de protéger les citoyens contre toutes les formes de risques et menaces. Dans ce cadre, les principales orientations du défi « Risques, aléas, sécurité des biens, des personnes et des communications » sont les suivantes :

Objectif 1 : établir les conditions d'un dialogue indispensable avec la société

Les solutions de sécurité doivent être acceptées par les utilisateurs finaux et par les citoyens. Dans le cas contraire, elles n'auront qu'un impact relatif, voire seront contre-productives. La recherche en sécurité doit être accompagnée d'un dialogue social, dans un souci de préserver les libertés et non de les restreindre.

- *Définir avec l'ensemble des parties prenantes les mesures de prévention adaptées et l'acceptabilité des risques potentiels* des nouvelles technologies

Objectif 2 : jouer la carte de l'Europe pour développer nos potentiels

Les questions de sécurité ne s'arrêtent pas aux frontières nationales. L'efficacité des solutions de sécurité repose donc sur leur mise en œuvre à l'échelle européenne, voire mondiale, qui peut seule permettre d'accéder à une taille critique en capacité de recherche, en base industrielle ou en terme de marché.

- *inscrire la thématique « sécurité » dans l'ensemble des instruments* mis en œuvre dans le cadre de l'Espace européen de la recherche ;

- *influencer l'élaboration des législations et des normes de sécurité* communes.

Objectif 3 : Coordonner les instruments et développer, par de nouvelles initiatives, cette thématique scientifique en devenir

Les problématiques autour de la sécurité prennent une part de plus en plus importante dans le débat public. Néanmoins, le caractère relativement récent de cette préoccupation sécuritaire fait que l'environnement nécessaire à une bonne prise en compte scientifique de ces sujets n'est pas encore optimal. Plusieurs voies d'action sont donc envisagées :

- *appuyer l'innovation par les marchés publics* : par des commandes spécifiques de solutions technologiques de sécurité, l'Etat peut favoriser l'innovation en amorçant le nécessaire marché initial sur lequel viendront se greffer les industriels ;

- *mettre en réseau les différentes plateformes nationales d'expérimentation* et s'assurer qu'elles demeurent adaptées aux besoins de la recherche ;

- *coordonner les instruments de prospective des ministères impliqués dans la recherche en sécurité* ou en bénéficiant pour parvenir à une vision partagée des tendances futures et des évolutions technologiques possibles et pour mieux anticiper l'émergence de vulnérabilités nouvelles ;

- *réaliser une programmation pertinente de la recherche* en :

- favorisant l'interaction entre les sciences dures et les sciences humaines et sociales afin d'assurer la continuité de toute la chaîne de l'innovation (recherche – industrie – usagers). L'élaboration de cette programmation doit être l'occasion d'un dialogue avec les entreprises et les usagers ;
- coordonnant la demande des services de sécurité et d'urgence (police, pompiers, médical et paramédical, équipe de sécurité civile) et des opérateurs privés d'infrastructures critiques (énergie, transport, logistique, télécommunications) ;
- renforçant la dualisation des technologies : la recherche en sécurité civile doit bénéficier des résultats d'une dualité comparable à la dualité civile – militaire. Des produits à bas coût, appartenant au marché civil de masse, peuvent trouver des applications en matière de sécurité, comme par exemple la localisation géographique par GPS. Réciproquement, des systèmes développés pour des besoins de sécurité peuvent être utilisés par le grand public, pour la surveillance de personnes âgées, malades ou handicapées par exemple. Il faut également s'assurer que des technologies développées dans le cadre de programmes de défense trouvent des débouchées dans le domaine de la recherche en sécurité afin de limiter les coûts de développement.
- améliorant la résilience de la société face aux risques sous toutes leurs formes.
- développant et s'appuyant sur des indicateurs quantitatifs et qualitatifs de la recherche en sécurité

SOMMAIRE

1 DEFINITION, ENJEUX

1.1 Définition

Notre société est confrontée à de nombreux changements. Ceux-ci sont de plus en plus difficiles à anticiper car de nombreux facteurs induisent l'apparition d'évènements aléatoires. Ainsi, la maîtrise des risques et des menaces demeure extrêmement difficile.

Le présent chapitre mobilise différents concepts. Le risque doit tout d'abord être distingué du danger. Le danger est ce qui « menace ou compromet la sûreté, l'existence, d'une personne ou d'une chose ». Le risque est un « danger éventuel plus ou moins prévisible » (Robert). Il faut relever que le risque n'est pas un aléa. Un aléa est un événement imprévisible qui n'est pas connoté par un jugement de valeur.

Un risque peut être potentiel (hypothétique) ou avéré. Cette distinction est importante dans le cadre d'une démarche qui cherche à anticiper les risques. En situation d'incertitude, la première étape d'une analyse rationnelle consiste à formuler des hypothèses de risque. Cette exploration intellectuelle du champ des possibles peut conduire à un grand nombre de scenarii. Un travail d'analyse doit conduire ensuite à retenir ceux qui sont jugés plausibles et à négliger les autres. Cette démarche n'est pas complètement rationalisable. Elle mobilise des connaissances disponibles, mais aussi l'intuition. Elle met en jeu des réactions immédiates, des convictions qu'il est généralement utile d'affiner et de valider par des discussions et la confrontation des points de vue divers. Les scénarii retenus sont autant de risques potentiels qu'il convient d'analyser plus avant et contre lesquels il doit être décidé de se prémunir, ou non.

La notion de risque potentiel est elle-même d'un maniement délicat. Pour qui retient surtout l'idée de danger contenue dans le terme risque, le risque potentiel devient un « risque de risque ». L'interprétation la plus pessimiste, procédant de la conviction selon laquelle le pire finit toujours par arriver, voit le risque potentiel comme un risque immature, en attente de réalisation. Cette assertion est erronée. Certes, les risques potentiels ont une histoire, et beaucoup de risques avérés ont commencé par être potentiels, mais de nombreux risques potentiels n'ont jamais été avérés. Enfin, on ne peut atteindre le risque zéro.

Le périmètre de ce défi couvre donc la recherche visant à identifier, prévenir et protéger des risques et des aléas pouvant posséder un impact sur les personnes physiques et morales (c'est-à-dire aussi bien les citoyens que les entreprises ou les institutions étatiques), sur les biens matériels ou immatériels (infrastructures critiques, bases de données, biens immobiliers et patrimoniaux sous toutes les formes possibles) et sur les communications (infrastructures et données). Cela constitue le champ de la recherche pour la sécurité.

Il convient de noter que, ces dernières années, les citoyens ont exprimé plus fortement des exigences en matière de sécurité. Ils souhaitent que les solutions qui leurs sont proposées améliorent sensiblement leur protection tout en préservant leurs libertés individuelles et leur vie privée. Un des enjeux majeur est donc d'apporter des réponses de sécurité performantes, issues de la recherche, qui répondent à leurs exigences. Il s'agit de trouver un équilibre entre ce besoin de sécurité et le respect des libertés.

Dans ce contexte, la recherche en sécurité joue un rôle crucial dans le développement de stratégies et de technologies pour faire émerger des solutions adaptées aux enjeux. Les objectifs généraux de cette recherche sont alors :

- Anticiper les ruptures majeures potentielles par une démarche de prospective et identifier les éléments précurseurs ou annonciateurs (les « signaux faibles »).

- Identifier, évaluer et caractériser les risques, leurs probabilités d'occurrence, les vulnérabilités sur lesquelles ils peuvent agir et leur détectabilité.

- Définir les mesures et les moyens techniques nécessaires pour prévenir, anticiper et gérer les risques, y compris en situation de crise.

- Définir les modèles généraux de sécurité, y compris ceux afférant à une recherche responsable.

- Développer et entretenir un dialogue constant avec l'ensemble des parties prenantes afin d'assurer une cohérence et une mise en adéquation entre les solutions de sécurité issues de la recherche et les besoins exprimés par la société.

1.2 Identification des composantes

La recherche en sécurité couvre donc un champ très vaste. Elle est au service de nombreux usagers (Etat, entreprises, citoyens) et fait appel à une multitude de technologies :

- **Systèmes et complexité.**

L'analyse des systèmes sous toutes leurs formes (collectivités humaines, Etats, systèmes de télécommunication ou de transport d'énergie, etc.), de leurs interrelations et la compréhension des phénomènes complexes constituent le premier champ de recherche de ce défi. Des risques naturels et technologiques, aux risques environnementaux, épidémiques, alimentaires, etc. Il s'agit d'identifier, d'analyser, de prévenir et de protéger (voire de réparer) l'apparition de ruptures des grands systèmes pouvant mettre en cause des intérêts collectifs vitaux, de porter atteinte aux fondements sociopolitiques et/ou d'affecter gravement les capacités de connaître et d'interpréter la réalité. Parmi les problématiques situées au cœur de cette réflexion, on notera les questions liées à la gestion de crise ou à la résilience des systèmes.

- **Surveillance et maîtrise des espaces (extra atmosphérique, aérien, maritime, terrestre).**

Ce champ d'étude couvre aussi bien la sécurité des territoires nationaux qu'européens. Face à la multiplicité des risques et des menaces tant sur l'environnement que sur les ressources, il est indispensable de disposer des capacités scientifiques et techniques permettant d'assurer une surveillance globale (ou locale) en continu (si possible) de l'ensemble des territoires. On peut intégrer dans cette thématique la surveillance des routes d'approvisionnement, celle des sites sensibles (d'intérêt de l'Europe dans le monde ou les sites exposés aux risques naturels et industriels) et/ou la sécurité des zones d'activités scientifiques ou économiques (y compris les zones de pêches et les zones d'exploitation des ressources d'exploitations énergétiques).

- **Impact des technologies sur la société.**

L'introduction de nouvelles technologies (ex. : les nanotechnologies, les OGM, les instruments de télécommunications portatifs, etc.) conduisent la société à s'interroger sur l'impact sanitaire et sociétal du développement. De la toxicologie à l'étude sociologique des usages des technologies, ce domaine de recherche constitue un enjeu majeur de la recherche en sécurité.

- **L'Homme et la Société.**

Il s'agit d'un champ de recherche impliquant particulièrement les sciences humaines et sociales. Y sont abordées les questions de violence, de criminalité, de délinquance, de victimes, de fonctionnement des institutions de la police et de la justice, ou encore d'usage de drogues et d'autres comportements à risques. Toute une école française existe à ce niveau qui doit être impliquée dans la démarche globale de recherche sur les risques et la sécurité.

1.3 Repérage des croisements majeurs avec les autres défis

L'ensemble des interactions au cœur duquel est placé le défi « Risques, aléas, sécurité des personnes, des biens et des communications » peut être schématisé comme suit :

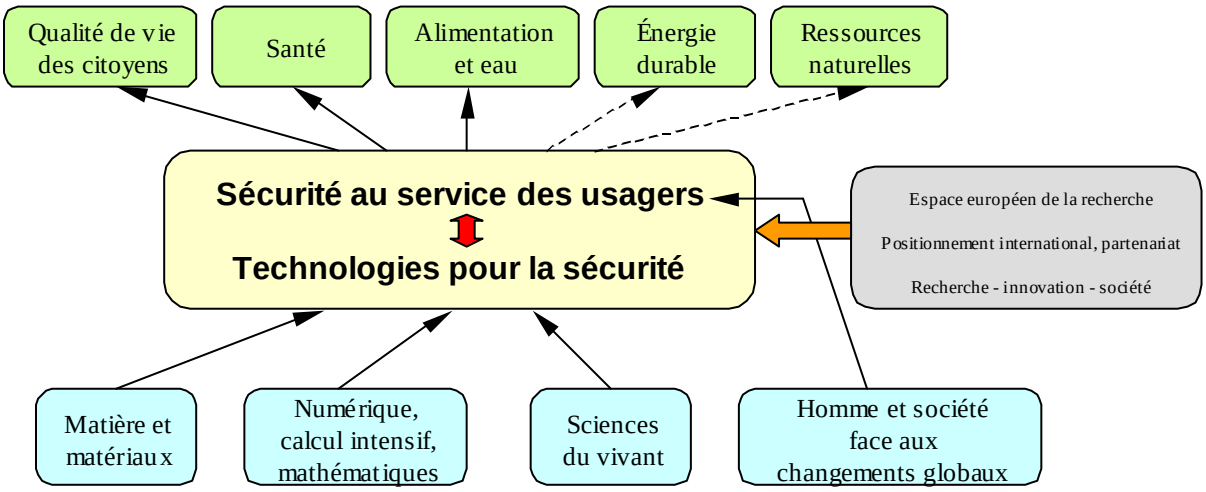

Figure 1. Les défis de la connaissance (en bleu) sont les sources de connaissances scientifiques et techniques ainsi que d'innovations qui constituent les éléments de base pour élaborer les technologies pour la sécurité. Pour être le plus efficace possible, lors d'une phase d'intégration, les solutions de sécurité au service des usagers sont adaptées aux demandes et enjeux définis par certains défis sociétaux et économiques (en vert). Les défis d'organisation du système de recherche et d'innovation (en gris) interviennent alors d'une manière transversale en favorisant le mieux possible cette phase d'intégration.

Le défi « Risques, aléas, sécurité des personnes, des biens et des communications » est porteur à la fois de questionnements et de solutions en relation avec d'autres défis : il est fait mention ci-après, sans viser à l'exhaustivité, des problèmes ou technologies d'interface entre ce défi et d'autres.

- La **qualité de vie des citoyens** : protection des personnes et des biens, protection des infrastructures ou gestion en cas d'attentats, d'accident ou de catastrophe naturelle.

- La **santé** : protection contre le bioterrorisme et les épidémies, amélioration des soins aux personnes âgés ou handicapées, impacts des nouvelles technologies sur la santé.

- L'**alimentation et l'eau** : épidémies animales (vache folle, grippe aviaire), sécurité alimentaire ou protection contre l'agroterrorisme.

- L'**énergie durable** : sécurisation des réseaux d'énergie électrique et développement de futurs réacteurs nucléaires (GEN IV) plus sûrs et moins proliférants.

- La préservation des **ressources naturelles** : protection de l'environnement et conservation de la biodiversité.

- Les **sciences et technologies innovantes autour de la matière et des matériaux** : systèmes de détection (infrarouge ou terahertz) ou d'authentification (RFID, *smart-dust*), sources d'énergie portables (pile à combustible ou batterie), systèmes biométiques (empreintes digitales, iris, vaisseaux sanguins), systèmes autonomes de surveillance (robots, drones).

- Le défi **numérique, calcul intensif,** mathématique : objets communicants, cryptographie, bases de données, systèmes de localisation géographique, reconnaissance de forme, intelligence artificielle.

- Les **sciences du vivant** : biocapteurs, laboratoires sur puce, puces à ADN, savoir-faire en virologie, immunologie ou épidémiologie.

- Le défi **homme et société face aux changements globaux** : relations interhumaines, compréhension du comportement de l'individu et du groupe dans des situations extrêmes, des causes qui mènent à l'extrémisme et à des actions terroristes, à la criminalité et à la délinquance ; élaboration d'une politique de communication en cas de crise ; évaluation du risque de restriction de liberté, des coûts et les bénéfices des mesures et stratégies de sécurité ; question éthiques et légales, nécessité et acceptabilité des solutions en sécurité ; effets sur les consommateurs.

- **Recherche, innovation et société** : application du principe de précaution, questions éthiques et participation des citoyens aux orientations et à l'évaluation de la recherche.

2 CARACTERISATION DE LA SITUATION DE LA FRANCE

2.1 Les indicateurs

Peu de données pertinentes sont disponibles à l'heure actuelle pour caractériser la recherche en sécurité, en particulier sur le nombre des chercheurs, des publications ou des brevets. L'analyse de la situation ne peut donc être fondée principalement que sur les dire d'experts ou encore sur l'analyse de la participation des équipes françaises aux appels à projets du PERS (Programme européen de recherche en sécurité) dans le cadre du 7e programme cadre de recherche et développement technologique (PCRDT). Ainsi, dans le premier appel à projets du programme spécifique « sécurité » lancé en 2007 (doté d'un budget de161 millions d'€), les résultats ont été les suivants :

- Cinq acteurs français, trois industriels (EADS, Thalès, Sagem) et deux organismes de recherche (CEA, ONERA), concentrent 60% du financement obtenu par des équipes françaises.

- Face à ces cinq grands, on note la faible part obtenue par les laboratoires universitaires français (4 %) ce qui est préoccupant et doit être souligné d'autant que la moyenne européenne pour les équipes universitaires se situe à 20,3 % et celles de nos deux principaux partenaires, le Royaume-Uni et l'Allemagne à 34,9 % et 20,9 %. Cela est en partie dû à la place centrale qu'occupent les universités dans les systèmes de recherche de ces deux pays.

- Le taux de participation des équipes françaises aux projets retenus est d'environ 52 %, soit une modeste 4ème place. En revanche, pour 16% des projets, c'est une équipe française qui est coordinateur, ce qui nous place au premier rang à égalité avec le Royaume-Uni. Cela témoigne de la qualité et de la capacité d'entraînement des acteurs français de la recherche en sécurité.

2.2 La politique nationale et communautaire

2.2.1 Le niveau national

La politique nationale de sécurité a été définie par plusieurs documents de référence :

- Le *Livre blanc sur la défense et la sécurité* paru en 2008.

- Les recommandations du groupe recherche COMOP 19 lors des travaux du *Grenelle de l'environnement*.

- La Stratégie nationale du développement durable 2009 – 2012 (en particulier le défi n°5 Santé publique, prévention et gestion des risques)

- Le Plan National Santé Environnement 2.

La recherche en sécurité est financée par une grande variété de programmes incitatifs. On peut ainsi illustrer la recherche pour la sécurité intérieure par les éléments suivants :

- *Concepts, systèmes et outils pour la sécurité globale* (CSOSG) de l'Agence nationale de la recherche (ANR), lancé en 2006, qui dispose d'un budget de 12 millions d'€ en 2008. Ce programme est abondé par la délégation générale de l'armement et la direction générale de la police nationale.

- Le Fonds unique interministériel (FUI) qui finance les projets des pôles de compétitivité. Plus de 10% des projets financés entrent dans la thématique « sécurité », pour environ un montant de 50 millions d'€. Plusieurs pôles de compétitivité affichent une thématique « sécurité », et notamment : *Aérospace Valley* (Midi-Pyrénées), *Images et Réseaux* (Bretagne), *Mer PACA et Bretagne*, *Solutions communicantes sécurisées* (PACA), *System@tic* (Ile-de-France), *Transactions électroniques sécurisées* (Normandie).

- Les programmes d'aide à l'innovation d'OSEO, qui s'adressent aux PME, avec environ 13 millions d'€ de subventions et d'aides remboursables dans cette thématique.

- Le programme interministériel de lutte contre le risque NRBC, dont le budget annuel s'élève à 15 millions d'€.

La somme des montants de ces programmes est d'environ 90 millions d'€ et représente ainsi le montant investi dans la recherche en sécurité, en France, au titre de financements incitatifs. Ces programmes ne bénéficient pas d'une structure de coordination, de concertation et d'impulsion unique. Cela rend difficile le lancement de projets nationaux ambitieux (équivalents aux programmes de démonstration du PERS). Le paysage de la recherche française en matière de sécurité apparaît donc fragmenté et manquant d'une stratégie globale.

Cela étant, des efforts ont été entrepris pour assurer une approche interministérielle dans certains volets de la recherche en sécurité. Ainsi, dans le cadre de la préparation des positions françaises au comité de programme du PERS, une coordination interministérielle pilotée par le Secrétariat général pour la défense nationale (SGDN) a été instituée. Celle-ci permet d'élaborer une position nationale portée vers les instances européennes. Cette position est d'ailleurs connue et appuyée par l'ensemble des acteurs publics ou privés de la recherche *via* leur participation au Groupe thématique national (GTN) correspondant au programme.

Enfin, il faut souligner la création d'agences nationales en charge de l'évaluation de la sécurité sanitaire (ex. : AFSET, AFSSAPS, AFSA, etc.). Leur mise en place confère à la France une capacité d'expertise pour anticiper et comprendre les risques émergents, tant au niveau européen que mondial.

2.2.2 Le niveau communautaire

Au niveau européen, plusieurs actions ont marqué le développement d'une politique communautaire de recherche en sécurité :

- Décembre 2003 : élaboration du document cadre *A Secure Europe in a Better World,* qui pose les principes d'une stratégie européenne de sécurité.

- Mars 2004 : rapport du *Group of Personalities* (GoP) qui détermine le rôle de la coordination européenne et du développement des technologies de pointe sur la sécurité.

- Septembre 2006 : rapport *European Security Research Agenda* rédigé par l'*European Security Reseach Advisory Board* (ESRAB) qui définit les orientations et le cadre d'un programme de R&D en sécurité.

- 2007 : suite aux recommandations contenues dans le rapport ESRAB, lancement du programme PERS dans le cadre du 7ème PCRD pour un montant global de 1 350 millions d'€ (sur un budget global du 7ème PCRD de 50,5 milliards d'€), pour la période 2007-2013. Ce niveau de financement (2,7 % du total du budget alloué tout au long de l'exercice) montre l'importance de la recherche en sécurité pour l'Union européenne.

Notons que les efforts communautaires en matière de politique de recherche ont joué un rôle structurant sur les Etats membres. En France, le programme CSOSG de l'ANR a choisi comme axes de son appel à projets les quatre grands thèmes (protection du citoyen, protection des infrastructures critiques, protection et surveillance des frontières, gestion de crise) établis par le rapport ESRAB et mis en pratique par le programme PERS. De même, par exemple, la politique allemande de recherche en sécurité a été définie en harmonie avec celle de l'Union européenne. Le programme européen de recherche en sécurité permet ainsi d'ouvrir les perspectives d'un futur espace européen de la sécurité dans lequel les acteurs français doivent jouer un rôle significatif.

2.3 *Analyse synthétique de la situation française*

	FORCE	**FAIBLESSE**
Gouvernance	Action interministérielle. Expression centralisée des besoins. Outils de suivi. Retour d'expérience.	Spécifications techniques des besoins encore assez floues. Carence dans la mutualisation de l'expression des besoins
Financement	Financement d'une R&D principalement partenariale. Diversité des sources de financement.	Parcellisation des crédits entre différents programmes.
Communauté de la recherche	Forte implication des grands industriels et de quelques grands organismes. Communauté portée sur les défis technologiques.	Faiblesse de l'implication du monde universitaire. Faible participation des sciences humaines et sociales liée à des problèmes structurels propres aux laboratoires.

	OPPORTUNITES	MENACES
International et Européen (collaboration dans la recherche et marché)	Accès à des ressources nouvelles (équipements, financement, RH) ou à des technologies nouvelles. Influence sur les normes techniques.	Laboratoires publics pas toujours efficaces dans la protection de la propriété intellectuelle. Fuite des cerveaux. Imposition de nouvelles normes techniques.
Européen (collaboration dans la recherche et marché)	Développement d'une dimension européenne dans la sécurité.	Risque de fractionnement de la recherche en sécurité au niveau européen.
National	Un potentiel sur lequel développer une R&D de qualité. Des besoins technologiques croissants. Développement de l'expertise dans le domaine de la sécurité.	Perte de souveraineté technologique. Insuffisante compétitivité des entreprises (y compris PME/PMI).
Régional	Apparition de nouveaux acteurs (Régions, PRES, etc.). Nouvelles sources de financement.	

3 L'ANALYSE STRATEGIQUE

3.1 Eléments de prospective

Nous vivons dans un monde où de nombreuses technologies se développent et convergent. Ces évolutions apporteront des bénéfices économiques et sociaux. Elles constituent également une source de nouveaux risques.

Ainsi, le développement des technologies du numérique dans les années à venir conduira à un monde fortement interconnecté où les objets qui nous entourent (appareillage électroménager, mobilier, emballages alimentaires, documents papier) deviendront communicants. La localisation, le contrôle et la surveillance à distance des objets les plus usuels seront possibles au risque cependant de créer des espaces nouveaux pour des actes malveillants.

L'informatisation des activités économiques devrait conduire à une optimisation accrue des chaînes logistiques, des systèmes de transport, des réseaux de distribution d'énergie, des réseaux de télécommunication, des systèmes bancaires et financiers ou de toute autre grande infrastructure. Ces activités devraient fonctionner avec une plus grande efficacité pour un moindre coût, mais deviendront également plus vulnérables et plus sensibles à un acte de malveillance.

Les avancées technologiques en robotique et systèmes autonomes pourront donner naissance à de nombreuses applications : remplacement du travail physique, exécution de tâches ménagères, assistance aux personnes handicapées, malades ou âgées. La disponibilité de

robots à coût abordable sur le marché pose la question de leur sûreté et de leur détournement possible à des fins terroristes ou d'autres actes criminels ou délictuels.

Notre planète sera également confrontée à des défis plus globaux. La croissance démographique et le développement économique induiront de vives tensions sur l'énergie et sur les ressources naturelles, dont celles en eau potable. Dans le même registre, nous devrons également faire face au problème du réchauffement climatique et de la préservation de la biodiversité.

Enfin, les progrès de la science et de la technologie vont conduire à une interrogation sans cesse plus pressante de la part des citoyens sur les risques induits.

Ces quelques éléments mettent en lumière l'importance de la problématique de la sécurité dans le paysage de demain.

3.2 Les orientations stratégiques

Le principal défi auquel doit répondre l'Etat dans la définition d'une stratégie nationale pour la recherche en sécurité est d'assurer au pays les capacités scientifiques et technologiques suffisantes pour répondre aux évolutions des risques et menaces en tout genre. Ces capacités s'entendent à la fois en terme de diversité (disponibilité multidisciplinaire) et de qualité (maîtrise de domaines scientifiques et technologiques de pointe, voire stratégiques) de la part de l'ensemble des acteurs (organismes de recherche, universités, industriels). Ceci implique également de disposer des ressources humaines suffisantes.

La stratégie nationale dans le domaine de la recherche pour la sécurité doit reposer sur une action visant les trois niveaux de fonction du système français de recherche et d'innovation.

Au niveau de la fonction orientation, il s'agit d'abord de permettre une coordination des instruments de prospective des ministères impliqués dans la recherche en sécurité ou en bénéficiant. L'objectif est de parvenir à une vision partagée des tendances futures et évolutions technologiques possibles et de mieux anticiper l'émergence de vulnérabilités nouvelles. Le ministère de l'enseignement supérieur et de la recherche devra également élaborer des indicateurs quantitatifs et qualitatifs de la recherche en sécurité afin de disposer d'un tableau de bord lui permettant de suivre la production de la recherche française en sécurité. Les ministères impliqués dans la recherche en sécurité devront travailler ensemble à l'élaboration de référentiels permettant de mieux formaliser l'expression des besoins, définir les axes de recherche prioritaires et dans certains domaines identifier les technologies critiques dont la maîtrise doit être assurée au niveau national ou européen.

La coordination interministérielle devra veiller davantage à la cohérence des différents programmes de recherche en sécurité, notamment en lien avec les agences de financement. Une complémentarité entre les différents agendas des appels à projets sera recherchée. Une évaluation des procédures mises en place permettra de diffuser l'expérience des bonnes pratiques identifiées.

Enfin, un dialogue sociétal approfondi devra être institué pour informer le public sur la recherche en sécurité et sur les opportunités associées à celle-ci, pour discuter et mettre en débat les risques potentiels des nouvelles technologies. L'objectif serait de définir avec l'ensemble des parties prenantes des mesures de prévention adaptées.

Au niveau de la fonction de programmation, outre la nécessaire coordination, il faut s'assurer que l'ensemble des organismes financeurs ainsi que les opérateurs publics de la recherche maintiennent une approche multidisciplinaire d'excellence des recherches en sécurité afin de tirer partie des processus de convergence technologiques. Il faut également favoriser une programmation permettant l'interaction entre les sciences dures et les sciences humaines et sociales afin d'assurer la continuité de toute la chaîne de l'innovation (recherche – industrie – usagers).

Au niveau de la fonction de réalisation de la recherche, il faut maintenir une capacité de recherche et d'expertise diversifiée (universités, organismes de recherche, industriels, etc.) afin de pouvoir disposer des ressources intellectuelles permettant de réagir aux évolutions et/ou risques non envisagés/émergents.

3.2.1 Un indispensable dialogue avec la société

Les solutions de sécurité doivent être acceptées par les utilisateurs finaux et par les citoyens. Dans le cas contraire, elles n'auront qu'un impact très relatif, voire seront contre-productives. La recherche en sécurité doit être accompagnée d'un dialogue social, dans un souci de préserver les libertés et non de les restreindre. Elle doit être aussi transparente que possible : le public doit être informé des sujets de recherche, des opportunités et des risques associés.

Le dialogue social envisagé implique que les ministères en charge de la recherche en sécurité créent des liens avec l'ensemble des parties prenantes issues aussi bien du monde académique, que des milieux économiques et de la société civile au sens large bien au-delà des instances techniques déjà existantes (ex : le groupe thématique national mis en place pour le suivi du PERS). L'office parlementaire des choix scientifiques et technologiques (OPECST), le Haut conseil de la science et de la technologie (HCST) et le conseil supérieur de la recherche et de la technologie (CSRT) devraient recevoir régulièrement des informations sur les programmes de recherche en sécurité et rendre des avis.

Des canaux d'informations modernes devraient être développés afin d'informer au mieux les citoyens sur les thèmes abordés par la recherche en sécurité. Par ailleurs, toute une palette d'outils (études, enquêtes d'opinion…) devrait être utilisés pour connaître l'avis des citoyens sur les orientations de la recherche en sécurité.

Enfin, un ensemble de mesures devraient être prise afin de favoriser le travail d'expertise qui est de plus en plus demandé à la communauté scientifique afin de répondre aux questions de la société face aux incertitudes et aux risques. Le pendant de cette action devrait être l'élaboration de politiques publiques favorisant l'émergence d'une culture du risque, y compris dans le milieu scientifique.

3.2.2 Inscrire la stratégie nationale dans le cadre de l'espace européen de la recherche

La principale action au niveau européen est de lancer, avec nos partenaires, un processus de programmation conjointe[1] dans le but de développer des agendas stratégiques communs pour la recherche en sécurité et de mieux coordonner les financements nationaux.

[1] Le processus de programmation conjointe est explicité dans le chapitre « Espace européen de la recherche ».

En effet, les questions de sécurité ne s'arrêtent pas aux frontières nationales. L'efficacité des solutions de sécurité repose donc sur leur mise en œuvre à l'échelle européenne voire mondiale qui, au-delà des questions de moyens humains et financiers disponibles :

- peut seule permettre d'accéder à une taille critique en capacité de recherche, en base industrielle ou en terme de marché ;
- sera fondée sur l'élaboration de normes de sécurité communes et de législations adéquates.

Il convient dès lors de s'assurer que la thématique « sécurité » sera prise en compte par l'ensemble des instruments mis en œuvre dans le cadre de l'Espace européen de la recherche. L'insertion des acteurs français dans ce paysage doit être volontariste. Ainsi, la participation des organismes de recherche dans des réseaux européens ayant un impact sur le thème de la sécurité doit être maintenu voire renforcée (ex : réseaux Eranet, plateformes technologiques, associations d'organismes…). La création d'une communauté de la connaissance sur la sécurité au sein de l'Institut Européen de la Technologie (IET) doit être initiée. La part des experts « sécurité » français au sein de l'espace européen de la recherche doit être renforcée.

3.2.3 Créer les instruments adaptés à cette thématique scientifique en devenir

Les problématiques autour de la sécurité prennent une part de plus en plus importante dans le débat public. Néanmoins, le caractère relativement récent de cette préoccupation sécuritaire fait que l'environnement nécessaire à une bonne prise en compte scientifique de ces sujets n'est pas encore optimal. Plusieurs voies d'action sont donc envisagées.

- **appuyer l'innovation par les marchés publics** : par des commandes spécifiques de solutions technologiques de sécurité, l'Etat peut favoriser l'innovation en amorçant le nécessaire marché initial sur lequel viendront se greffer les industriels ;
- **mettre en réseau les différentes plateformes nationales d'expérimentation** et s'assurer qu'elles demeurent adaptées aux besoins de la recherche ;
- **réaliser une programmation pertinente de la recherche** en :
  - coordonnant la demande des services de sécurité et d'urgence (police, pompiers, médical et paramédical, équipe de sécurité civile) et des opérateurs privés d'infrastructures critiques (énergie, transport, logistique, télécommunications).
  - renforçant la dualisation des technologies : la recherche en sécurité civile doit bénéficier des résultats d'une dualité comparable à la dualité civile – militaire. Des produits à bas coût, appartenant au marché civil de masse, peuvent trouver des applications en matière de sécurité, comme par exemple la localisation géographique par GPS. Réciproquement, des systèmes développés pour des besoins de sécurité peuvent être utilisés par le grand public, pour la surveillance de personnes âgées, malades ou handicapées par exemple. Il faut également s'assurer que des technologies développées dans le cadre de programmes de défense trouvent des débouchés dans le domaine de la recherche en sécurité afin de limiter les coûts de développement.
  - améliorant la résilience de la société face aux risques sous toutes leurs formes.
  - développant et s'appuyant sur des indicateurs quantitatifs et qualitatifs de la recherche en sécurité.