N° 1664

—

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 9 juin 2004.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 146 du Règlement

PAR LA COMMISSION DES FINANCES, DE L'ÉCONOMIE GÉNÉRALE ET DU PLAN

sur la **stratégie de sécurité économique nationale**

ET PRÉSENTÉ

PAR M. BERNARD CARAYON,

Député.

—

SOMMAIRE

Pages

INTRODUCTION 5

I.– LES VULNERABILITES FRANÇAISES 7

A.– LES MENACES JURIDIQUES 7

1.– Le secret économique n'est pas suffisamment garanti 7

a) Une conception du secret des affaires extensive aux États-Unis 7

b) Une conception du secret des affaires restrictive en France 8

2.– Des entreprises sont parfois victimes de procédures judiciaires étrangères 9

B.– LES MENACES FINANCIERES 11

1.– Les fonds d'investissements appuient la stratégie de puissance des États-Unis 12

a) La stratégie de puissance des États-Unis 12

b) Le « modèle » In-Q-Tel 12

2.– Le contrôle des investissements étrangers 13

a) Le dispositif français a été récemment renforcé 13

b) Les dispositifs en vigueur aux États-Unis et en Allemagne 15

c) Un cadre européen et international qui permet de renforcer ce contrôle 16

C.– LES MENACES SUR LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION 18

1.– Les vulnérabilités de l'État et des entreprises 18

2.– Des moyens de lutte limités 20

II.– LA SECURITE NATIONALE : UNE MUTATION DE L'ETAT A ACCOMPLIR 23

A.– UNE STRATEGIE GLOBALE DE SECURITE NATIONALE EST NECESSAIRE 23

1.– Les États-Unis se sont donnés les moyens d'affermir leur puissance 23

a) Une législation et des structures fédérales adaptées aux enjeux 23

b) Un soutien public aux entreprises privées 24

2.– La sécurité nationale doit s'appuyer sur la définition d'un périmètre stratégique de l' économie française 25

3.– La sécurité nationale doit s'inscrire dans un cadre européen 26

B.– CETTE MUTATION DOIT S'APPUYER SUR UN RENOUVEAU DE L'ACTION PUBLIQUE 27

1.– Créer un conseil de sécurité économique 27

2.– Mutualiser les crédits en s'appuyant sur la création d'un « CEA » des technologies de l'information, de la communication et de la sécurité 28

a) Un contexte similaire à celui qui prévalait lors de la création du CEA 29

b) Les missions du Commissariat aux technologies de l'information, de la communication et de la sécurité 30

3.– Créer une plateforme industrielle des technologies de l'intelligence économique 30

4.– Européaniser l'Agence pour la diffusion de l'information technologique 31

III.– MIEUX PROTEGER LES ENTREPRISES FRANÇAISES 33

A.– PROTEGER LES INFORMATIONS ECONOMIQUES SENSIBLES 33

1.– La nécessité d'un nouveau droit du secret des affaires 33

2.– La proposition de loi de votre Rapporteur 33

B.– SOUTENIR LES ENTREPRISES STRATEGIQUES 35

1.– Le soutien à l'innovation aux États-Unis 35

a) Le soutien aux PME 35

b) Le financement public des hautes technologies 36

2.– Renforcer le tissu des petites entreprises innovantes 36

3.– S'assurer de la maîtrise des technologies critiques 37

C.– RENFORCER LA SECURITE DES SYSTEMES D'INFORMATION 38

1.– Renforcer la sécurité des systèmes de l'État 38

2.– Mettre en œuvre une stratégie industrielle 39

3.– Renforcer la coopération européenne 40

EXAMEN EN COMMISSION 41

INTRODUCTION

Les attentats de Madrid du 11 mars 2004 nous l'ont douloureusement rappelé : l'Europe est une cible privilégiée des terroristes. Si les bombes représentent dans notre subconscient collectif la menace essentielle, l'éventail des menaces qui pèsent sur nos sociétés est bien plus large.

Depuis une vingtaine d'années, notre pays est entré – sans en avoir nécessairement pris conscience – dans l'ère de la société de l'information. Outre la qualité des hommes, la production de la richesse nationale repose aujourd'hui sur une masse d'informations juridiques, financières, commerciales, scientifiques, techniques, économiques ou industrielles. Les menaces qui pèsent sur notre outil productif ont, elles aussi, évolué. Elles sont devenues plus diffuses.

L'exacerbation de la compétition internationale transforme les informations stratégiques des entreprises en enjeu d'une véritable « guerre économique[1] ». Le rachat annoncé le 18 mai dernier de Kroll (leader mondial de l'intelligence économique et de l'investigation) par Marsh&McLennan Companies, qui détient le leader mondial du courtage d'assurance, une société de consultants (Mercer) et l'un des plus gros fonds d'investissement américains (Putnam) illustre la maîtrise par les anglo-saxons de ce que votre Rapporteur appelait les « métiers stratégiques » dans son rapport [2] remis au Premier ministre : audit, conseil, investigation, assurance, etc [3]. **Ils sont au cœur de toute stratégie de puissance**.

Par ailleurs, des fonds d'investissement, pilotés par des États, tentent de s'emparer des joyaux technologiques étrangers. Les technologies de l'information et de la communication, devenues le cœur de l'économie du savoir, comportent des failles les rendant vulnérables aux intrusions concurrentielles, voire criminelles.

Face à ces vulnérabilités qui touchent les entreprises comme l'État, quelles actions ce dernier a-t-il conduit ? **Sans impulsion politique déterminante, seuls des efforts épars ont été entrepris**. En matière de sécurité des systèmes d'information, un centre de recensement et de traitement des attaques informatiques a été créé en 2000 au sein de la Direction centrale de la sécurité des systèmes d'information (DCSSI) du Secrétariat général de la défense nationale. S'agissant du contrôle des investissements étrangers dans des entreprises françaises sensibles, la loi n°2003-706 du 1er août 2003 de sécurité financière a renforcé les prérogatives du ministre chargé de l'économie.

---

(1) Selon l'expression utilisée dès 1971 par Bernard Esambert.

(2) « Intelligence économique, compétitivité et cohésion sociale », rapport remis au Premier ministre en juin 2003, La Documentation française, 176 pages.

(3) L'ensemble représenterait un chiffre d'affaires de 11 milliards de dollars (9,2 milliards d'euros) et plus de 60.000 emplois.

Un an après la publication de son rapport au Premier ministre, votre Rapporteur constate que l'intelligence économique est devenue un débat majeur, s'ouvrant sur une multitude d'initiatives. Mais l'état des menaces pesant sur la France reste alarmant : aussi est-il est urgent de **définir une stratégie de sécurité nationale, englobant à la fois les enjeux de défense nationale, la protection de notre économie et la lutte contre les nouvelles menaces**.

La nomination d'un haut responsable pour l'intelligence économique constitue une première étape. Mais il est aussi nécessaire de créer un **Conseil de sécurité économique, placé auprès du Président de la République** – à l'instar du conseil de sécurité intérieure – chargé de définir une stratégie nationale, assise sur la délimitation d'un **périmètre stratégique** de l'économie française. Cette politique sera ensuite appliquée par un Commissariat aux technologies de l'information, de la communication et de la sécurité. Cette stratégie doit, enfin, s'appuyer sur des fonds d'investissement à capitaux publics et privés, destinés à mutualiser l'effort public et privé et assurer l'indépendance technologique de la France.

Dominique de Villepin, Ministre de l'intérieur, de la Sécurité intérieure et des Libertés locales, déclarait récemment (1) qu'il souhaitait *« que, d'ici à trois ans, nos services de renseignements, dont les méthodes d'investigation classiques ont fait la réputation, soient également les meilleurs en matière technologique. Car il n'y aura pas de victoire contre le terrorisme sans un outil performant »*. L'effort pour se doter des meilleurs outils technologiques doit mobiliser l'État dans son ensemble. Il s'inscrit parfaitement dans la logique du passage de la conception de défense à celle de sécurité nationale. Un effort de mutualisation des crédits publics doit donc être réalisé.

La sécurité nationale est l'affaire de tous : citoyens, entreprises et pouvoirs publics. Comme le rappelait Nicolas Sarkozy, alors Ministre de l'intérieur, de la Sécurité intérieure et des Libertés locales, lors de l'ouverture de la 14ème session nationale de l'Institut des hautes études de la sécurité intérieure, le 8 octobre 2002 : *« Naturellement, il n'y a pas d'un coté l'État et de l'autre les entreprises, chacun assurant pour son propre compte sa sécurité. Bien au contraire, pour faire face à la cybercriminalité, pour assurer la sécurité des transactions financières et boursières, mais aussi prévenir les menaces sur les installations nucléaires, le transport des matières dangereuses ou la sécurité des télécommunications, nous devons travailler ensemble. Et l'État a sa place pour synthétiser, coordonner, définir les stratégies et utiliser les moyens qui sont les siens »*

C'est au prix d'un effort national et européen de sécurité que nous pourrons préserver la vigueur de notre tissu économique et donc, notre cohésion sociale.

---

(1) Le Figaro du 13 mai 2004

I.– LES VULNERABILITES FRANÇAISES

Dans une économie dont la richesse se fonde de plus en plus sur le savoir, les informations stratégiques des entreprises françaises ne semblent pas suffisamment protégées. En outre, les vulnérabilités des systèmes d'information mettent en danger la vitalité économique de notre pays.

A.– LES MENACES JURIDIQUES

1.– Le secret économique n'est pas suffisamment garanti

Si les États-Unis ont su se doter d'un droit des affaires protégeant efficacement et pragmatiquement les secrets économiques, ces derniers demeurent en France imparfaitement définis, et donc vulnérables.

a) Une conception du secret des affaires extensive aux États-Unis

La loi fédérale, dénommée *Economic Espionage Act* ou *Cohen Act*, assure la protection des entreprises et des particuliers contre le vol du secret d'affaires en réprimant lourdement les contrevenants.

Elle permet de sanctionner quiconque, avec l'intention de détourner un secret d'affaires en relation avec, ou inclus dans un produit fabriqué pour, ou mis sur le marché intérieur ou extérieur, dans l'intérêt économique de quelqu'un d'autre que son propriétaire, sachant que l'infraction nuira à tout propriétaire de ce secret, sciemment,

– vole, ou sans autorisation s'approprie, soustrait, emporte ou dissimule, ou par fraude, ruse ou tromperie, obtient de telles informations,

– sans autorisation copie, reproduit, établit des croquis ou dessins, photographie, transfère ou charge par voie informatique, modifie, détruit, photocopie, transmet, livre, envoie, expédie, communique ou transfère de telles informations,

– ou reçoit, achète, ou détient de telles informations en sachant qu'elles ont été volées, obtenues ou détournées sans autorisation.

En outre, toute personne morale commettant l'une de ces infractions encourra une amende d'un montant maximal de 5 millions de dollars (4,2 millions d'euros).

Ce dispositif pénal protége le secret des affaires, par ailleurs défini comme *« tout type d'information financière, commerciale, scientifique, technique, économique, industrielle, incluant modèles, plans, compilations, mécanismes, formules, dessins, prototypes, méthodes, techniques, procédés, procédures, programmes ou codes, qu'elle se présente sous forme matérielle ou immatérielle, qu'elle soit ou non stockée, compilée, ou mémorisée physiquement, électroniquement, graphiquement, ou par écrit »*.

b) Une conception du secret des affaires restrictive en France

En l'état actuel du droit, les informations sensibles de l'entreprise ne sont protégées que par un ensemble de textes dont la cohérence et l'efficacité restent imparfaites.

La loi n°88-19 du 5 janvier 1988 relative à la fraude informatique n'est efficace qu'en cas d'intrusion, ou tentative d'intrusion, avérée. L'article 323-1 du code pénal prévoit ainsi que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15.000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30.000 euros d'amende.

L'article 323-2 du même code prévoit que le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45.000 euros d'amende. L'article 323-3 du même code prévoit que le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45.000 euros d'amende. Enfin, l'article 323-7 du même code précise qu'une tentative de ces trois délits est punie des mêmes peines.

Cependant, **ce dispositif pénal vise l'intrusion dans le système informatique et non la détention des informations qu'il contient**.

Par ailleurs, **la législation sur le droit d'auteur et le droit des producteurs ne permet pas de protéger efficacement l'accès et l'utilisation des bases de données. La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ne protège que les informations nominatives. La législation sur les brevets ne protège pas les méthodes, les savoir-faire, ou les idées. Le secret de fabrique n'est opposable qu'aux personnes appartenant à l'entreprise. La protection des logiciels ne couvre pas le champ des informations traitées par le logiciel lui-même. La législation relative à la concurrence déloyale et aux clauses de non-concurrence sont peu contraignantes pour le contrevenant**.

Enfin, l'article 410-1 du code pénal est aujourd'hui l'un des rares fondements pertinents de la notion de sécurité économique. Celui-ci précise que les intérêts fondamentaux de la nation *« s'entendent (...) de son indépendance, de l'intégrité de son territoire, de sa sécurité, (...) et* ***des éléments essentiels de son potentiel scientifique et économique*** *et de son patrimoine culturel »*. Cette conception n'est malheureusement pas opérante contre les menaces actuelles contre les savoirs français.

2.– Des entreprises sont parfois victimes de procédures judiciaires étrangères

Les commissions rogatoires internationales (CRI) conduites sur notre territoire par une autorité judiciaire étrangère peuvent conduire, de manière détournée, à un recueil illicite de renseignement. En effet, il arrive parfois que des documents, sans lien avec la procédure judiciaire en cours mais comportant des informations sensibles susceptibles de compromettre des procédés industriels, soient saisis à l'occasion de l'exécution d'une CRI diligentée contre des sociétés françaises.

Dans le cadre d'une enquête criminelle pour entente illicite, une CRI a été diligentée par un tribunal américain à l'encontre de plusieurs sociétés japonaises et d'une société française.

Pour la firme française, la CRI prescrivait de rechercher tous les documents détenus depuis 10 ans et relatifs à une éventuelle entente frauduleuse ayant pour objectif de faire monter les prix ou de se répartir les territoires et les clientèles à travers le monde. Or, le PDG de cette entreprise française a fait état de la saisie de documents contenant des informations stratégiques portant, d'une part, sur des produits vendus à des entreprises appartenant au secteur militaire français et, d'autre part, sur des documents purement techniques contenant des détails de procédés de fabrication confidentiels sans aucun lien avec les infractions alléguées par les autorités américaines.

Estimant probable le risque de divulgation de secrets techniques, le juge français saisi du dossier a demandé à la Délégation générale pour l'armement d'évaluer la sensibilité des documents saisis avant de procéder à leur transmission à la justice américaine. Cet exemple, dans lequel aucune tentative d'appropriation de documents secrets n'est avérée, illustre le risque de transmission, à une autorité étrangère d'éléments sensibles.

Dans une autre affaire, à la suite d'un accident aéronautique, un motoriste français a fait l'objet d'une enquête diligentée par la justice italienne. L'enquête visait à obtenir des informations sur la fiabilité du moteur. Les responsables de la société française ont refusé, par trois fois, de répondre aux questions posées par l'expert judicaire italien, estimant que celui-ci, particulièrement virulent, tentait, *a priori*, de leur imputer l'entière responsabilité de l'accident.

Face aux méthodes de cet expert, les dirigeants du groupe français ont alors sollicité la délivrance d'une commission rogatoire internationale afin de bénéficier des règles du système judiciaire français. Exécutée en novembre 2003 par des magistrats français et italiens, accompagnés de deux experts italiens et assistés d'enquêteurs de la Gendarmerie nationale, cette commission rogatoire a permis de procéder à la saisie des documents réclamés par la justice italienne ainsi qu'à des interrogatoires d'ingénieurs.

Le magistrat français en charge du dossier a porté une attention particulière à la protection des données classifiées du motoriste français. Il a pu observer le comportement suspect de l'expert italien qui, profitant de son statut, avait tenté de se faire remettre des documents confidentiels portant sur l'ensemble des moteurs du groupe, alors que seul un moteur particulier était en cause dans l'accident. Informé par son homologue français, le juge italien a décidé de révoquer l'expert. **Cet expert judiciaire était par ailleurs un employé d'un groupe italien concurrent direct de la société française…**

Si le développement de ce type d'agissements demeure limité, il convient de rester vigilant sur les tentatives de recueil illicite d'informations sensibles. La **sensibilisation des magistrats à la protection des données techniques** doit permettre de déjouer les tentatives de captation d'information utilisant un cadre légal.

LE VOL OU LA CONFISCATION D'ORDINATEURS :
UN RISQUE CROISSANT DE COMPROMISSION D'INFORMATIONS SENSIBLES

– Les confiscations d'ordinateurs portables pour « raisons de sécurité »

Des cadres de l'industrie aéronautique, en voyage professionnel au Proche-Orient, se sont vus confisquer leurs ordinateurs portables par les autorités chargées de la sécurité de l'aéroport du pays visité. Cette pratique, justifiée officiellement par la lutte anti-terroriste, semble être devenue courante dans cet aéroport et dissimule assez mal des opérations d'espionnage économique et scientifique.

– Les vols d'ordinateurs survenus dans un groupe pharmaceutique.

Les ordinateurs dérobés contenaient des données confidentielles relatives à un médicament révolutionnaire, pour un chiffre d'affaire évalué à plusieurs milliards de dollars. Des soupçons se portent sur un groupe pharmaceutique américain concurrent.

– Le cambriolage commis, semble-t-il par des professionnels, dans les locaux d'une filiale d'un grand groupe industriel français.

Seules quelques pièces ont été visitées lors de ce cambriolage. Or ces locaux, non contigus et dispersés sur deux étages d'un même bâtiment, étaient tous attribués à des dirigeants de l'établissement. Si la valeur des ordinateurs portables est négligeable, celle des données stockées est importante dans la mesure où leur mise en commun offre une bonne vision de l'activité du groupe.

La quasi-totalité du savoir-faire de l'entreprise pourrait donc se trouver entre les mains d'une tierce personne, laissant penser que ce vol a été commandité par un concurrent. Cette hypothèse est d'autant plus privilégiée que le siège du groupe envisageait de céder sa filiale au moment des faits.

– Le vol d'ordinateurs portables des équipes chargées du développement d'un programme aéronautique.

Aucun de ces ordinateurs ne contenait d'informations classifiées. Néanmoins, ces données portaient sur le programme de développement ainsi que sur la stratégie commerciale du groupe.

– Le vol de données relatives à un projet de création d'une fondation scientifique à Séoul

En septembre 2003, un professeur d'un organisme scientifique français s'est rendu en Corée pour finaliser sur place un projet de création d'une fondation de droit privé à vocation scientifique. Son ordinateur portable a été volé à l'aéroport de Séoul, alors même que moins de trois vols de ce type y sont enregistrés chaque année. Manifestement, il s'agissait d'un vol ciblé. Or, ce projet de fondation gêne prioritairement certaines ambitions américaines…

– Le vol de données informatisées afférentes à un projet de construction d'une usine d'enrichissement de l'uranium par centrifugation gazeuse.

Le matériel informatique volé contenait le dossier des options de sûreté nucléaire choisies pour l'usine ainsi que les avis d'un institut de sûreté nucléaire sur ces choix. Sans être classifiées, ces données sensibles devaient permettre d'élaborer le dossier d'enquête d'utilité publique de la future usine.

Ces différents exemples montrent à quel point le facteur humain reste essentiel pour la protection des données informatiques. Dans chacun de ces cas, les vols ou confiscations sont le fait d'imprudences ou de négligences ou bien sont liées à une protection insuffisante contre les vols.

B.– LES MENACES FINANCIERES

Les cas de Saft, Eutelsat ou Gemplus, qui ont fait l'objet de tentatives ou de prises de contrôle par des fonds d'investissement américains, illustrent la vulnérabilité du capital des entreprises stratégiques françaises et européennes.

Des fonds d'investissement affichent souvent leur préférence pour des sociétés non cotées, comme le sont généralement les entreprises de technologie en phase de maturation. Détenant une part du capital de l'entreprise, le fond propose la signature d'un pacte d'actionnaires qui prévoit parfois la révocation de la direction en cas de résultats insuffisants. Dans ce cas, le pouvoir est transféré au fonds. La subtilité de l'opération repose sur le fait que l'indicateur retenu est généralement l'Ebitda, qui n'est pas défini en droit français. Ensuite, en cas de conflit dans l'appréciation de la situation, le pacte d'actionnaires prévoit qu'il fera l'objet d'un règlement arbitral sans appel… échappant à la justice nationale !

L'actualité montre que les fonds d'investissement peuvent, lorsqu'ils s'intéressent à des entreprises françaises stratégiques, mettre en cause notre indépendance. Cette prise de conscience n'est pas purement française : le parlement allemand vient d'adopter, en première lecture, un projet de loi permettant à l'État fédéral de contrôler certains investissements internationaux.

1.– Les fonds d'investissements appuient la stratégie de puissance des États-Unis

a) La stratégie de puissance des États-Unis

A l'appui de leur stratégie de puissance, les États-Unis réalisent des investissements directs dans des entreprises américaines ou étrangères via des sociétés écrans.

En pratique, il s'agit de prises de participations, par des sociétés sous contrôle des services de renseignement américains, dans le capital de sociétés innovantes dans des technologies ayant des applications jugées stratégiques en terme de sécurité. L'intérêt de cette action est multiple car elle permet :

– de promouvoir la recherche et le développement de sociétés américaines ayant une compétence sur des niches technologiques, afin de les utiliser au profit de la sécurité nationale ;

– d'assurer la pérennité des PME ayant développé un savoir-faire stratégique, afin de prévenir le risque de prise de contrôle par une puissance étrangère ;

– et de soutenir les PME innovantes américaines afin d'asseoir la suprématie technologique des États-Unis, en liaison avec l'administration chargée d'appuyer le développement des PME (*Small business administration*).

b) Le « modèle » In-Q-Tel

In-Q-Tel [(1)] est une société de capital-risque… créée par la CIA en 1999 ! Son objectif premier consiste à détecter des technologies innovantes susceptibles d'être utilisées par les services de renseignement. Une fois ce travail de ciblage effectué, In-Q-Tel a pour vocation d'investir dans les sociétés les plus avancées ou les plus prometteuses dans les secteurs sélectionnés.

La société de capital-risque travaille en liaison avec des grands organismes américains des hautes technologies, tels que la *Science Application International Corporation* (SAIC).

Les outils permettant le recueil et l'analyse de données (respectivement *data mining* et *knowledge management*) ont été jugés essentiels par la CIA. Il s'agit, en outre, d'un marché en plein développement. N'étant pas structuré, il est particulièrement perméable aux investissements ciblés. Les entreprises dans lesquelles In-Q-Tel investit sont particulièrement innovantes et essentiellement spécialisées dans la conception de logiciels et de moteurs dédiés à l'analyse linguistique, la récupération de données sur les réseaux informatiques, la sécurité et, depuis peu, les biotechnologies. La société investit environ 30 millions de dollars (25 millions d'euros) chaque année dans des sociétés innovantes.

(1) « Q » est le sobriquet du « Monsieur Gadget » dans… James Bond !

Les attentats de New-York du 11 septembre 2001 ont renforcé l'attrait d'In-Q-Tel pour les autorités américaines : cet événement, en effet, a mis en lumière les défaillances du système informatique américain dédié à la recherche du renseignement.

Un rapport du Congrès soulignait que *« l'activité de la société In-Q-Tel est justifiée et ce qu'elle a accompli, en si peu de temps, est remarquable »*.

2.– Le contrôle des investissements étrangers

La loi française permet au ministre de l'économie de s'opposer à un investissement étranger pouvant porter atteinte à la sécurité publique. Ce dispositif a récemment été étendu aux investissements pouvant mettre en cause la défense nationale.

a) Le dispositif français a été récemment renforcé

L'article L. 151-3 du code monétaire et financier permet au ministre chargé de l'économie, s'il constate qu'un investissement étranger est, ou a été réalisé dans des activités participant en France, même à titre occasionnel, à l'exercice de l'autorité publique, *« ou qu'un investissement étranger est de nature à mettre en cause l'ordre public, la santé publique, la sécurité publique, ou la défense nationale ou que cet investissement est ou a été réalisé dans des activités de recherche, de production ou de commerce d'armes de munitions, de poudres et substances explosives destinées à des fins militaires ou de matériels de guerre »* de soumettre cet investissement envisagé à une **autorisation préalable** et, en cas de refus soit d'autorisation soit de se conformer aux conditions dont l'autorisation est assortie, **d'enjoindre à l'investisseur** *« de ne pas donner suite à l'opération, de la modifier ou de faire rétablir à ses frais la situation antérieure »*.

Ce dispositif législatif est conforme aux articles 58 et 296 du Traité instituant la Communauté européenne. Il est complété par un décret n° 2003-196 du 7 mars 2003 réglementant les relations financières avec l'étranger.

L'article L. 151-3 a été modifié récemment, comme le souhaitait votre Rapporteur, par l'article 78 de la loi n° 2003-706 du 1er août 2003 sur la sécurité financière qui a ajouté le motif de la *« défense nationale »* à la liste des critères autorisant le ministre chargé de l'économie à soumettre un investissement étranger à autorisation préalable. En effet, la notion de sécurité publique ou de *« recherche, production ou commerce d'armes »*, dans le texte initial, était trop restrictive pour couvrir des activités industrielles concernant des biens à double usage – au sens du règlement CE 1334/2000 du 22 juin 2000 – ou encore le domaine des composants, qui sont des éléments sensibles pour la chaîne de fabrication d'équipements stratégiques.

La direction du Trésor instruit cette procédure qui repose sur l'initiative des opérateurs. **Seuls deux ajournements ont été prononcés depuis l'entrée en vigueur de l'article L. 151-3**. Il s'agissait, dans un cas, du rachat d'une activité de

fabrication de composants aéronautiques par un groupe américain, et dans l'autre cas, de l'acquisition par une société américaine de la totalité du capital d'une société française spécialisée dans la fabrication d'appareils pour la vision nocturne. Le Ministère de la défense ayant considéré que ces deux opérations auraient entraîné une situation de dépendance vis-à-vis des fournisseurs américains en a demandé l'ajournement. Dans le premier cas, l'ajournement a été prononcé en 1998, et en 2000 dans le second cas.

Le dispositif actuel doit être précisé et complété pour deux raisons : il convient de circonscrire, réglementairement, le champ de la « défense nationale » posé par la loi du 1er août 2003 et il faut assurer, en pratique, son effectivité.

Premièrement, le décret du 7 mars 2003 précité reprend, dans son article 7, la notion d' *« investissements mettant en cause la défense nationale »* sans en poser les critères précis et objectifs. **Cette situation ne répond pas parfaitement à l'état de la jurisprudence communautaire qui repose sur le principe de proportionnalité et tranche, avec une étonnante naïveté, avec les dispositions retenues aux États-Unis**. A la demande du ministère de l'économie, le SGDN a donc engagé un travail interministériel d'explicitation du champ des investissements mettant en cause la défense nationale. Une modification du décret du 7 mars 2003 est enfin envisagée.

Deuxièmement, **le SGDN a été chargé par le Premier ministre**, le 16 juillet 2003, **de conduire, conformément au vœu exprimé par votre Rapporteur dans son rapport sur l'intelligence économiqu**e, une réflexion interministérielle sur les prises de contrôles par des capitaux étrangers d'entreprises françaises liées à la défense ou la sécurité nationales, susceptibles de menacer notre autonomie technologique dans certains secteurs particulièrement sensibles et stratégiques.

Cette réflexion comporte quatre volets principaux :

– renforcer la concertation interministérielle « amont » et formaliser sa mise en œuvre pour veiller à rendre la loi plus opérationnelle ;

– envisager d'assortir l'autorisation ministérielle de **conditions**, selon une approche à la fois contractuelle et pragmatique que ne permet pas pleinement le décret du 7 mars 2003 ;

– assurer l'effectivité du dispositif de sanctions ;

– et explorer les autres moyens dont dispose l'État en cas de prises de contrôles par des capitaux étrangers d'entreprises françaises sensibles pour la défense.

Cette réflexion interministérielle est animée par le SGDN.

b) Les dispositifs en vigueur aux États-Unis et en Allemagne

La France n'est pas le seul État à disposer d'une législation visant à contrôler les investissements étrangers pour des motifs de défense ou de sécurité nationales dans des entreprises sensibles. À l'exception de la Grande-Bretagne, du Canada et des Pays-Bas, l'ensemble des autres grands pays industrialisés (notamment les États-Unis, l'Espagne, l'Italie, le Japon et bientôt l'Allemagne) dispose d'une législation qui autorise un contrôle gouvernemental pour des motifs de sécurité sur les investissements étrangers dans le domaine de la défense.

Aux États-Unis, la section 5021 de l'*Omnibus Trade and Competitiveness Act* de 1988 donne au Président la possibilité de bloquer ou de suspendre un projet d'acquisition ou de fusion qui menacerait les intérêts de la sécurité nationale. Chaque année, 8.000 dossiers sont examinés. Les projets d'investissements étrangers sont soumis au Comité pour les investissements internationaux aux États-Unis (*Committee on Foreign Investments in the United States*, CFIUS).

Un délai d'examen de 30 jours, pouvant être augmenté de 45 jours, sans excéder 90 jours, permet de rendre un avis – tenu secret – au Président. Il est envisagé que cette procédure soit étendue aux prises d'actifs dans une entreprise américaine ayant conclu des contrats classifiés ou ayant obtenu en trois ans des contrats du département de la Défense d'une valeur cumulée supérieure ou égale à un million de dollars, ou possédant des produits ou logiciels relevant des règles sur le commerce international des armes.

En Allemagne, le concept d'entreprise stratégique n'existait pas et les entreprises concernées ne faisaient l'objet d'aucun suivi. Cependant des opérations de prises de participations étrangères dans des entreprises de défense sont à l'origine d'une prise de conscience des lacunes de la législation allemande.

Le gouvernement fédéral a donc présenté un amendement à son projet de loi sur les relations économiques extérieures, qui lui permet de contrôler les opérations avec l'étranger pour en vérifier la compatibilité avec les *« intérêts majeurs de sécurité »*. Cette procédure concernerait les prises de participation étrangères de plus de 25 % dans le capital d'une société allemande. La gestion de cette procédure serait assurée par le ministère fédéral de l'économie et du travail. Seraient concernées les entreprises produisant des *« biens d'armement »*, ainsi que celles du secteur de la cryptologie. Ce projet de loi, adopté le 6 mai 2004 par le Bundestag, n'est pas encore définitivement adopté et a fait l'objet de critiques dans certains milieux économiques.

c) Un cadre européen et international qui permet de renforcer ce contrôle

– Le cadre international

L'Organisation mondiale du commerce (OMC), dont l'objectif consiste à favoriser le libre-échange, prévoit la possibilité pour les États de se doter de dispositifs spécifiques afin de préserver les intérêts essentiels de leur souveraineté. Ces possibilités de dérogations aux principes du libre-échange peuvent êtes observées dans les statuts du Fonds monétaire international ou bien encore dans l'accord sur les mesures concernant les investissements et liées au commerce (MIC) annexé à l'accord instituant l'OMC.

Cet accord contient une clause d'exception, dite de sécurité, qui s'appuie sur les articles XXI b) III de l'accord du GATT de 1994, et qui peut être utilisée lorsque les intérêts vitaux d'un État – qui ne sont pas précisément définis – sont en jeu.

De même, l'article 3 du code de libération des mouvements de capitaux élaboré sous l'égide de l'OCDE autorise les mesures nécessaires au maintien de l'ordre et la sécurité publique et à la protection des intérêts essentiels de la sécurité.

– Le cadre européen

Toute restriction aux mouvements de capitaux entre les États membres et les pays tiers est interdite, par principe, par le Traité instituant la Communauté européenne.

La libre circulation des capitaux est même l'un des fondements du droit communautaire. Pour autant, **l'article 58 de ce même traité stipule que le principe de libre circulation des capitaux n'empêche pas les États membres de prendre des mesures *« justifiées par des motifs liés à l'ordre public ou à la sécurité publique »***.

La jurisprudence communautaire a pris soin d'encadrer la portée de cette notion de *« motifs de sécurité publique »*. Les motifs de dérogation doivent être entendus strictement, de sorte que leur portée ne saurait être déterminée unilatéralement par chacun des États membres sans contrôle des institutions communautaires. Ils ne peuvent être invoqués qu'en cas de menace réelle et suffisamment grave affectant un intérêt fondamental de la société (arrêt *Calfa*, 1999).

La CJCE admet cependant que la *« sécurité publique »* s'entend aussi bien de la sécurité intérieure que de la sécurité extérieure, cette dernière entrant en ligne de compte dans le cas de marchandises susceptibles d'être utilisées à des fins stratégiques. Par un arrêt *Richardt*, rendu en 1991, la Cour a admis la validité d'une autorisation préalable de transit de matériel qualifié de **« *stratégique* »** par le Luxembourg.

Les considérations économiques ne peuvent justifier des mesures restrictives que si un objectif de sécurité publique les dépasse largement. C'est notamment le cas de la nécessité d'assurer un approvisionnement minimal en produits pétroliers.

Par ailleurs, la CJCE s'attache à vérifier le respect du principe de sécurité juridique. Dans un arrêt *Association Église de scientologie*, rendu en 2000 sur l'application du dispositif français de contrôle des investissements étrangers, la Cour a estimé qu'un régime d'autorisation préalable qui se limite à *« définir de façon générale »* les investissements concernés et qui ne permet pas aux intéressés d'être *« en mesure de connaître les circonstances spécifiques dans lesquelles une autorisation préalable est nécessaire »* n'est pas compatible avec l'article 58 précité.

TRAITE INSTITUANT LA COMMUNAUTE EUROPEENNE (EXTRAITS)

Article 56

1. Dans le cadre des dispositions du présent chapitre, toutes les restrictions aux mouvements de capitaux entre les États membres et entre les États membres et les pays tiers sont interdites.

2. Dans le cadre des dispositions du présent chapitre, toutes les restrictions aux paiements entre les États membres et entre les États membres et les pays tiers sont interdites.

Article 58

1. L'article 56 ne porte pas atteinte au droit qu'ont les États membres (…) de prendre toutes les mesures indispensables pour faire échec aux infractions à leurs lois et règlements, notamment en matière fiscale ou en matière de contrôle prudentiel des établissements financiers, de prévoir des procédures de déclaration des mouvements de capitaux à des fins d'information administrative ou statistique ou de prendre des mesures justifiées par des **motifs liés à l'ordre public ou à la sécurité publique**. (…)

En outre, l'article 296 du Traité instituant la Communauté européenne stipule que les dispositions de l'ensemble du Traité ne font pas obstacle à ce qu'un État membre puisse prendre *« les mesures qu'il estime nécessaires à la protection des intérêts essentiels de sa sécurité et qui se rapportent à la production ou au commerce d'armes, de munitions et de matériel de guerre »*.

La Cour a estimé que l'obligation, pour le demandeur d'une autorisation d'exportation d'un bien susceptible d'entrer dans le champ de la directive sur les biens à double usage, d'apporter la preuve que les biens seront exclusivement utilisés à des fins civiles, tout comme le refus de l'autorisation si les biens peuvent être utilisés à des fins militaires, peuvent être des exigences proportionnées.

Pour autant, **l'article 296 précité mentionnant explicitement le commerce d'armes, de munitions et de matériel de guerre, il est délicat d'y adosser une législation nationale sur le contrôle des investissements étrangers**. Cette opération est d'autant plus difficile que cet article rappelle qu'il n'est opérant que pour la préservation des *« intérêts essentiels »* de la sécurité d'un État, ce qui en réduit drastiquement le champ d'application.

Globalement, une **législation nationale encadrant les investissements internationaux n'est compatible avec le droit communautaire** qu'à deux conditions :

– les États doivent pouvoir **justifier la nécessité et la proportionnalité** de la restriction à la libre circulation des capitaux qu'ils imposent ;

– et les investisseurs doivent **connaître avec précision les conditions** qui leur sont imposées.

En outre, pour que ces restrictions soient fondées sur la *« défense nationale »*, notion absente, aussi étrange soit-il, en tant que telle du droit communautaire, **il faut que le dispositif national puisse correspondre à la nation communautaire de *« sécurité publique »***.

C.– LES MENACES SUR LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Les sociétés modernes sont de plus en plus dépendantes des technologies de l'information, y compris dans leur fonctionnement quotidien. Les transactions financières et commerciales se multiplient tandis que la production industrielle et la gestion de l'énergie (y compris nucléaire) reposent sur ces mêmes technologies. **Nos sociétés sont donc particulièrement vulnérables face aux actes de malveillance visant les systèmes d'information qui en constituent désormais le cœur.**

De même, les systèmes de défense incorporent de plus en plus d'informatique. Les engagements armés modernes impliquent, en effet, des systèmes fortement interconnectés entre eux. Ce rôle grandissant des technologies de l'information et de la communication dans les outils militaires occasionne donc également l'accroissement des vulnérabilités potentielles.

1.– Les vulnérabilités de l'État et des entreprises

Utilisant les mêmes outils de communication et d'information, l'État et les entreprises sont confrontés aux mêmes menaces.

Les *microprocesseurs* sont au cœur des systèmes d'information et en constituent le facteur déterminant de puissance. Ils conditionnent par conséquent directement la capacité et la rapidité de calcul, particulièrement déterminante pour les simulations à grande échelle, observables notamment dans les applications nucléaires ou de défense. L'enjeu stratégique des processeurs est clair : le processeur « PowerPC » de Motorola et d'IBM a été considéré initialement comme un matériel de guerre…

Mais les microprocesseurs peuvent être également à la source de vulnérabilités importantes pour les systèmes qui les embarquent. L'intégration toujours plus grande de fonctions « dans le silicium » conduit à la mise en place de microcodes non maîtrisés (et difficilement détectables) avec des risques latents de *backdoors* (failles du système) ou d'autres dispositifs de surveillance et de prise de contrôle à distance. Récemment, la polémique au sujet de la *Trusted Computing Platform Alliance* (TCPA) visant à intégrer au processeur, une partie cryptée directement utilisée par le système d'exploitation a mis en lumière ces enjeux. Les sociétés Microsoft et Intel comptaient ainsi pouvoir maîtriser le piratage des logiciels. Cependant, **ces fonctionnalités pourraient également permettre à des personnes malintentionnées ou des services de renseignement étrangers, de disposer d'un moyen de contrôler à distance l'activation de tout ou partie des systèmes à l'insu de leurs utilisateurs**.

Il faut souligner que **le secteur industriel des processeurs** ainsi que celui des mémoires ou des périphériques de stockage de données, **est aujourd'hui totalement sous la maîtrise de sociétés américaines**. Ni la France, ni l'Europe ne disposent plus des compétences et des industries nécessaires pour mettre au point un processeur compétitif sans coopération avec les États-Unis. Il s'agit là d'une vulnérabilité majeure pour l'avenir, même si l'Asie pourrait offrir, à terme, une alternative potentielle : la Chine s'est engagée dans le développement de ses propres microprocesseurs.

Les *systèmes d'exploitation* constituent **le cœur des systèmes d'information**. Même si la concurrence entre les sociétés Apple et Microsoft est aujourd'hui largement dépassée, ils sont au centre des enjeux du secteur informatique. Microsoft étant en situation quasi-monopolistique avec son système Windows, il n'existe plus de réel concurrent pour lui faire face. Le système d'exploitation de Apple ne touche plus qu'un public réduit et le système Unix, même s'il représente 40 % de parts de marché pour les serveurs, n'a jamais réussi à véritablement conquérir le marché des postes de travail.

La montée en puissance des logiciels libres – notamment Linux – pourrait constituer un nouvel espoir pour ceux qui souhaiteraient amoindrir l'hégémonie de Microsoft.

Les systèmes d'exploitation, constituent une des sources de vulnérabilité majeure des systèmes d'information : **c'est par leur intermédiaire qu'il est possible de pénétrer les systèmes, en utilisant les *backdoors* et des « vers » (chevaux de troie)**. La France, comme la plupart des autres pays européens, présente une forte vulnérabilité technologique dans ce domaine et **seule l'utilisation des logiciels libres de droit peut aujourd'hui encore constituer une parade possible**.

Le *contrôle d'accès* est **la partie la plus visible de la sécurité** mais sans doute, paradoxalement, **la moins sensible au plan de la vulnérabilité technologique nationale**. Les acteurs français sont nombreux et performants dans ce domaine : Sagem, Bull et… Gemplus. Cette dernière société, dont le capital est désormais contrôlé par un fonds d'investissement américain (1), illustre bien le risque inhérent aux entreprises performantes mais dont le capital est mal protégé face à des aux investisseurs étrangers.

La *transmission d'informations*, dans un monde de plus en plus interconnecté, constitue une cible privilégiée pour accéder de façon illégale aux données. Les principales vulnérabilités des réseaux filaires se situent au niveau des routeurs. Ces équipements – intégrant un système d'exploitation généralement spécifique au fournisseur – comportent également des *backdoors* de service. Seules deux entreprises – Alcatel et Cisco– se partagent le marché mondial.

Les réseaux sans fil de type « WiFi », dont le développement est actuellement très rapide, présenteront vraisemblablement de nouvelles vulnérabilités dont la pleine mesure n'a pas encore pu être prise. Au-delà des vulnérabilités liées à la transmission radio (brouillage de fréquence …), le protocole de cryptage des données prévu par la norme retenue n'apparaît pas véritablement performant. Ce défaut devrait être corrigé dans sa prochaine version. Peu d'entreprises françaises sont actives dans ce secteur. Or, pour la France, il peut s'agir pourtant à terme d'une vulnérabilité technologique importante : la transmission sans fil à longue distance offre de réelles potentialités tant pour des applications civiles que militaires.

Les *applications bureautiques* constituent **une cible privilégiée pour accéder à l'information**. La productivité des entreprises dépend, pour une large part, de ces logiciels. Microsoft a réussi à imposer un standard – Microsoft Office – et les grands acteurs, comme Adobe, sont américains. Comme pour les systèmes d'exploitation, l'alternative à l'hégémonie américaine pourrait venir des logiciels libres.

La France, pourtant fortement présente dans ce secteur avec Dassault Systèmes, reste technologiquement très vulnérable. Il conviendrait peut-être d'avancer l'idée d'une industrie nationale ou européenne du logiciel. En tout cas, il serait intéressant de mener une réflexion spécifique sur le mode de description des documents élaborés par ces logiciels pour faire émerger un format « neutre » de stockage, c'est-à-dire indépendant de l'applicatif ayant servi à le concevoir.

2.– Des moyens de lutte limités

Le développement de la société de l'information s'accompagne d'un accroissement tangible des menaces contre lesquelles les États sont le plus souvent désarmés et les parades entre les mains d'acteurs privés. La France s'est dotée de

(1) Texas Pacific Group ; le président de Gemplus, Alex Mandl, est… ancien administrateur d'In-Q-Tel !

plusieurs outils pour répondre à cet enjeu, en particulier par la **constitution de plans de prévention** et de réaction à une attaque cyberterroriste et par la mise en place d'un organe opérationnel de veille, d'alerte et de réponse : le Centre de recensement et de traitement des attaques informatiques (CERTA). Ce dernier agit en réseau avec les centres d'expertises des ministères régaliens et des organismes spécialisés homologues (Renater pour la Recherche).

Comme il l'a déjà fait dans son rapport spécial sur les crédits du Secrétariat général pour la défense nationale (SGDN), votre Rapporteur **souligne l'utilité de la fonction d'audit de la Direction centrale de la sécurité des systèmes d'information** (DCSSI). La cellule qui en est chargée est composée de 6 personnes, recrutées parmi les meilleurs spécialistes informatiques. **Cet effectif est dérisoire au regard de la tâche qui incombe à cette cellule, compétente pour l'ensemble des systèmes d'information de l'État.** L'ensemble des ministères doit prendre conscience des risques liées aux attaques informatiques et de leur devoir de protéger les informations personnelles des citoyens contenues sur les différents serveurs.

Par une lettre du 4 avril 2003, le directeur de cabinet du Premier ministre attirait l'attention des directeurs de cabinet de l'ensemble des ministres sur cet enjeu. Cette démarche s'inscrivait dans la logique qui sous-tendait la proposition de votre Rapporteur, dans son rapport [(1)] au Premier ministre sur l'intelligence économique, référence tendant à mettre en place une **mission interministérielle d'expertise technique et industrielle des systèmes d'information** des administrations publiques dont le SGDN assurerait l'exécution. Votre Rapporteur insiste sur le fait que **la sécurité des systèmes d'information est un devoir pour l'État, et donc une priorité**.

(1) Ibidem, page 43.

II.– LA SECURITE NATIONALE : UNE MUTATION DE L'ETAT A ACCOMPLIR

L'ordonnance n°59-147 du 7 janvier 1959 portant organisation générale de la défense prévoit, dans son article 18, que le ministre de l'économie *« oriente aux fins de la défense l'action des ministres responsables de la production, de la réunion et de l'utilisation des diverses catégories de ressources ainsi que de l'aménagement industriel du territoire »*. En outre, il assure la *« liaison permanente avec le ministre de l'intérieur et le ministre des armées afin de tenir compte dans son plan d'équipement économique des nécessités essentielles de la défense »*.

Comme votre Rapporteur a déjà eu l'occasion de l'indiquer dans son rapport sur l'intelligence économique, ces dispositions ne sont plus adaptées aux réalités économiques actuelles. Le rôle de l'État dans l'économie a évolué et les technologies de l'information et de la communication sont devenues des pièces maîtresses dans le jeu économiques.

Il convient aujourd'hui de **substituer à la notion de défense nationale, telle qu'elle a été imaginée il y a 45 ans, celle de sécurité nationale**, plus globale, qui inclut la protection économique et la lutte contre les nouvelles menaces.

A.– UNE STRATEGIE GLOBALE DE SECURITE NATIONALE EST NECESSAIRE

1.– Les États-Unis se sont donnés les moyens d'affermir leur puissance

Pour consolider leur suprématie économique et leur maîtrise des technologies d'information et de communication, les États-Unis s'appuient sur une législation adaptée et des organismes fédéraux protégeant leurs intérêts stratégiques, tout en appuyant la conquête des marchés internationaux par les acteurs économiques américains

a) Une législation et des structures fédérales adaptées aux enjeux

Les États-Unis se sont progressivement dotés d'outils législatifs leur permettant :

– d'éviter qu'une puissance étrangère ne porte atteinte à la sécurité nationale par les réseaux de communication,

– et de pouvoir intercepter le plus grand nombre possible de sources d'information.

Les attentats du 11 septembre 2001 ont été l'occasion de renforcer les dispositifs existants, notamment en matière de surveillance des communications.

Afin de lutter contre les réseaux terroristes, le *Patriot Act*, renommé par le Sénat *USA Patriot Act* permet d'augmenter fortement les pouvoirs des autorités américaines concernées par le recueil du renseignement.

S'agissant de la surveillance des communications, la législation antérieure prévoyait que la menace devait être clairement identifiée pour que le ministre de la Justice donne l'agrément permettant de procéder aux interceptions. **Le nouveau texte supprime cette contrainte**. **Mécaniquement, le nombre des interceptions peut croître. En outre, le champ de contrôle a été étendu aux courriers électroniques.**

Les structures fédérales, elles-mêmes, ont évolué, puisqu'un nouveau département ministériel a été créé : le *Department of Homeland Security* (Département de la sécurité du territoire national).

Cet organisme gouvernemental s'est vu confier la tâche d'éviter toute attaque ou catastrophe susceptible de menacer la sécurité nationale sur le sol américain. Il est chargé de :

– prévenir les catastrophes (risque nucléaire, bactériologique, radiologique ou chimique) et de prévoir d'éventuelles mesures d'urgence ;

– d'assurer la sécurité des frontières maritimes, terrestres et aériennes. C'est notamment dans ce cadre qu'a été renforcé le traitement des données relatives aux entrées et aux sorties du territoire des biens et des personnes. Le Département a mis en œuvre des contrôles biométriques, requiert la présentation de passeports à lecture optique et exige, sans réciprocité d'ailleurs [(1)], des compagnies aériennes des renseignements précis sur les passagers ;

– de surveiller et de contrôler les communications et les réseaux d'information afin de détecter tout renseignement susceptible de mettre au jour une menace contre le territoire américain ;

– de contribuer à la recherche et au développement de laboratoires universitaires ou d'entreprises, en pointe dans la prévention des risques terroristes.

Le Département s'appuie sur 22 organismes fédéraux pour la collecte et le traitement de l'information.

b) Un soutien public aux entreprises privées

Outre la possibilité de soutenir l'innovation américaine par des fonds d'investissements dédiés (parfois étroitement contrôlés par l'administration fédérale), les États-Unis se sont engagés dans une démarche volontariste de soutien à la conquête des marchés internationaux par les sociétés américaines. C'est la mission, depuis 1994, de l'*Advocacy Center* du Département du Commerce.

Il s'agit d'un bureau unique et central de coordination rassemblant les ressources de 19 organismes gouvernementaux des États-Unis pour s'assurer que les ventes des produits et des services américains puissent avoir les meilleures perspectives à l'étranger.

---

(1) Question écrite de votre Rapporteur n°38701, JO du 4 mai 2004, page 3226.

Il permet en outre de mettre au service des sociétés américaines la totalité des dispositifs publics – y compris les agences de renseignement – pour les aider face à leurs concurrents étrangers. Il n'est pas un seul déplacement commercial majeur des dirigeants de Boeing à l'étranger qui ne soit précédé d'une visite du directeur de la CIA !

Cette action, coordonnée à Washington s'appuie également sur les ambassades des États-Unis et d'autres organismes gouvernementaux, à l'instar des *American Presence Posts* (1).

Votre Rapporteur rappelle qu'il avait proposé (2), dans son rapport sur l'intelligence économique précité, qu'**une cellule de contact et de soutien aux entreprises soit mise en place** (proposition n°6). A la disposition des entreprises relevant du « périmètre stratégique », cette cellule serait chargée de recueillir les demandes et les besoins des entreprises et de favoriser le traitement transversal de dossiers liés à la compétitivité (soutien aux contrats stratégiques, normalisation, négociations internationales, etc.) et à la sécurité économique. Un de ses principes de fonctionnement reposerait sur une approche thématique et géographique qui rassemble entreprises, responsables des administrations centrales concernées et ambassadeurs.

Il apparaît anormal qu'une telle structure, qui permettrait à nos industries de lutter à armes égales avec leurs concurrents, n'ait pas encore été mise en place. Le rattachement du haut responsable pour l'intelligence économique au SGDN, structure administrative par ailleurs inadaptée à une telle mission, explique sans doute ce retard. En tout état de cause, une politique publique d'intelligence économique ne saurait être engagée efficacement que dans un cadre politique et administratif adapté et autonome.

2.– La sécurité nationale doit s'appuyer sur la définition d'un périmètre stratégique de l' économie française

La définition d'un « périmètre stratégique » de la performance globale de la France est le préalable à la mise en œuvre d'une stratégie de sécurité nationale.

Sur la base d'une impulsion politique forte, qui n'a pas encore été clairement affichée (3), une grille méthodologique doit être adressée aux ministères, qui seront chargés, chacun dans leur secteur, de formuler des propositions d'identification de ce périmètre stratégique. **Pour ce faire, les ministères doivent impérativement établir un cahier des charges avec leurs partenaires industriels et scientifiques.**

---

(1) Ibidem, page 60.

(2) Ibidem, page 31.

(3) Même si l'on notera avec satisfaction le rattachement par le Premier ministre de l'industrie pharmaceutique aux « intérêts stratégiques français ».

Dans un premier temps, il est souhaitable qu'un petit nombre de technologies de souveraineté (aérospatial, défense, informatique, télécommunications, nanotechnologies, pharmacie...) soient identifiées. En effet, ce processus porte en lui deux risques majeurs :

– une définition trop large de ces secteurs de souveraineté, qui conduirait nécessairement à l'**éparpillement de l'action publique**, et donc à son inefficacité ;

– une définition trop précise de ces secteurs, qui pourrait conduire à une **vision sclérosée, voire « gosplaniste »,** de l'État, dès lors vouée à l'échec.

Cette réflexion, issue de la proposition n°1 du rapport [(1)] sur l'intelligence économique précité, menée autour du haut responsable pour l'intelligence économique, est cruciale pour la construction d'une stratégie française de sécurité nationale.

3.– La sécurité nationale doit s'inscrire dans un cadre européen

Aujourd'hui, l'Union européenne est un espace en voie d'intégration, fondé sur le libre-échange économique. Pour autant, les États membres et l'Union elle-même doivent s'engager dans une **stratégie de puissance**. Ils doivent, collectivement, prendre en main leur sécurité globale, indépendamment des Américains, et s'affranchir des dépendances technologiques et normatives qui entravent leur destin partagé. Cette stratégie ne doit pas être conçue *contre* les États-Unis, mais *pour* affermir la **puissance de l'Europe**, dans un monde multipolaire, où de nouvelles puissances, notamment asiatiques, seront amenées à jouer un rôle politique et économique croissant.

Quel cadre européen pour une stratégie de sécurité nationale ? L'évolution de la défense nationale vers la sécurité nationale s'effectue d'un double mouvement.

Premièrement, la sécurité nationale recouvre un champ public plus vaste que la seule défense, entendue au sens strict. Elle inclut notamment la **sécurité sanitaire** ou bien encore la **sécurité environnementale**. Le droit communautaire, comme le droit international, permet cet élargissement de la notion. Il le favorise même : la production normative communautaire sur la protection de l'environnement et la sécurité nucléaire en témoigne, de même que la définition des missions de Petersberg a élargi les activités de défense aux actions humanitaires, puis aux actions civilo-militaires.

Deuxièmement, le cadre des interconnexions entre le secteur public et le secteur privé doit être consolidé.

---

(1) Ibidem, page 27.

D'une part, **les États membres disposent des dispositions dérogatoires des Traités**. Ces clauses de sauvegarde, déjà présentées, peuvent être utilement invoquées pour justifier des dispositions nationales destinées à la défense de l'ordre public. Globalement, le droit communautaire n'empêche pas l'expression juridique des pouvoirs régaliens de l'État mais il renverse la charge de la preuve. Le libre jeu du marché est la règle, toute distorsion provoquée par un État membre doit être justifiée.

D'autre part, il convient d'**élever ces dispositifs au niveau communautaire**. Le droit communautaire repose sur une philosophie contraire aux actes juridiques

– heurtant trop directement le fonctionnement libéral du marché ;

– ou trop protecteur des intérêts strictement nationaux.

Or de nombreuses mesures tendant à préserver la sécurité économique peuvent heurter le principe de liberté du commerce et de l'industrie. C'est notamment le cas d'un État qui interviendrait dans une transaction privée pour préserver ses intérêts stratégiques, par exemple dans des secteurs clés, à l'instar de la pharmacie.

Donc, pour qu'un dispositif européen soit le plus possible compatible avec le droit communautaire, il serait souhaitable qu'il ne limite que l'un des deux principes en cause : le fonctionnement libéral du marché. Les Européens doivent donc se mettre d'accord sur une législation communautaire cadre en la matière. Compte tenu du processus de décision communautaire, il faut que la Commission valide ces aspirations. L'enjeu est pourtant de taille, puisqu'il s'agit de défendre **la sécurité économique européenne, et partant, des stratégies industrielles qui portent en elles à la fois la puissance et la cohésion sociale.**

B.– CETTE MUTATION DOIT S'APPUYER SUR UN RENOUVEAU DE L'ACTION PUBLIQUE

Pour être pleinement réalisée, cette mutation doit reposer sur une architecture simple : une **impulsion politique forte**, donnée par un conseil de sécurité économique placé auprès du chef de l'État, s'appuyant sur une structure permettant la déclinaison des orientations en **mutualisant les ressources publiques**, un **fonds d'investissement à capitaux mixtes public-privé** en étant l'outil opérationnel.

1.– Créer un conseil de sécurité économique

Pour répondre aux nouveaux défis et aux nouvelles menaces pesant sur la sécurité intérieure, le Président de la République a décidé à juste titre la création d'un conseil de sécurité intérieure. Créé par le décret n°2002-890 du 15 mai 2002, ce conseil a pour mission de définir les orientations de la politique menée dans le domaine de la sécurité intérieure et d'en fixer les priorités. Il s'assure de la

cohérence des actions menées par les différents ministères, procède à leur évaluation et veille à l'adéquation des moyens mis en œuvre.

Présidé par le Président de la République, le conseil de sécurité intérieure comprend le Premier ministre, les ministres de l'Intérieur, de la Justice, de la Défense, de l'Économie et des Finances, du Budget et de l'Outre-mer. Son secrétaire général, en liaison avec les ministères concernés et le secrétariat général de la défense nationale, prépare les réunions du conseil et les relevés de décisions, et suit l'exécution des décisions prises.

Il est urgent aujourd'hui de donner à la sécurité économique le même type d'impulsion que celle qui a été donnée il y a deux ans à la sécurité intérieure. **Créer un nouveau conseil ou prévoir une formation du conseil de sécurité intérieure siégeant sur les questions économiques est une interrogation secondaire**. L'essentiel réside dans le fait qu'une **stratégie politique nationale de sécurité économique soit définie**. Une telle structure aurait un champ d'action beaucoup plus large que le conseil interministériel du renseignement consacré à la défense économique. **Il aurait surtout l'autorité politique nécessaire pour vaincre les réticences, les résistances, les cloisonnements et les lenteurs de l'administration**.

L'exemple américain est éloquent : il constitue même un modèle à suivre ! En 1993 a été créé un conseil économique national (*National Economic Council,* NEC), placé auprès du Président. Il conseille le Président sur les politiques économiques nationale et internationale. Depuis la mise en place, au lendemain des attentats du 11 septembre, d'une nouvelle politique de sécurité nationale, il a été intégré au *National Security Council*.

Il suffit de visiter le site internet de la présidence des États-Unis pour se convaincre de l'intérêt porté par ce pays à la sécurité économique : elle y est traitée au même niveau que la sécurité nationale et la sécurité intérieure, illustrant ainsi l'institutionnalisation de ces préoccupations.

Si votre Rapporteur est favorable à la création d'un tel conseil en France, il souligne aussi que cette structure doit n'être qu'une structure d'impulsion définissant les grandes orientations nationales. Il faut en effet **éviter toute tentation « gosplaniste »** qui consisterait à planifier l'ensemble des actions au niveau le plus élevé.

2.– Mutualiser les crédits en s'appuyant sur la création d'un « CEA » des technologies de l'information, de la communication et de la sécurité

Une véritable politique industrielle en faveur de la sécurité économique doit s'appuyer sur un service de programmes de sécurité jouant pleinement son rôle, capable de spécifier des besoins en intégrant dès l'origine la volonté d'exporter la solution ainsi développée, et par l'organisation de la commande publique.

Il faut donc créer un **Commissariat aux technologies de l'information, de la communication et de la sécurité** dont la mission consisterait à stimuler le développement d'une filière industrielle et technologique.

a) Un contexte similaire à celui qui prévalait lors de la création du CEA

Cet intitulé n'est pas sans rappeler celui du Commissariat à l'énergie atomique (CEA). Cette référence n'est, bien évidemment, pas fortuite. Créé par une ordonnance du 18 octobre 1945, le CEA est l'exemple type de la **réussite industrielle éclatante, suite à une impulsion politique forte**. Aujourd'hui, le CEA est en pointe non seulement sur l'énergie, mais aussi sur les sciences du vivant et les technologies de l'information et de la communication.

Rappelons qu'après l'explosion de deux bombes atomiques sur le Japon, les États-Unis avaient démontré leur maîtrise de l'atome comme arme de destruction massive. Deux attitudes s'offraient alors aux Alliés : la dépendance ou la souveraineté. Le Général de Gaulle, chef du Gouvernement provisoire de la République française, choisit alors la souveraineté en créant, le 18 octobre 1945, le Commissariat à l'énergie atomique.

L'exposé des motifs de l'ordonnance n°45-2563 du 18 octobre 1945 créant le CEA est d'une étonnante actualité. Son contenu peut être intégralement transposé à la situation actuelle des technologies de l'information :

« De pressantes nécessités d'ordre national et international obligent à prendre les mesures nécessaires pour que la France puisse tenir sa place dans le domaine concernant l'énergie atomique. La création d'un organisme susceptible d'assurer au pays le bénéfice de telles recherches a été mise à l'étude. Il est apparu que ***cet organisme devait être à la fois très près du Gouvernement****, et pour ainsi dire mêlé à lui, et cependant* ***doté d'une grande liberté d'action****.*

Il doit être très près du Gouvernement parce que le sort ou le rôle du pays peuvent se trouver affectés par les développements de la branche de la science à laquelle il se consacre, et qu'il est par conséquent indispensable que le Gouvernement l'ait sous son autorité.

Il doit, d'autre part, être doté d'une grande liberté d'action parce que c'est la condition sine qua non de son efficacité. »

Au-delà des blocages administratifs de l'époque, c'est l'implication personnelle du Chef du Gouvernement qui a permis la mise en place de cet acteur majeur de la recherche et de l'industrie françaises. **Après avoir été un acteur majeur de la société industrielle, la France doit être actrice de la société de l'information**. Dans ce cas, elle bénéficiera des retombées économiques induites, notamment en matière de souveraineté, par son effort. Dans le cas contraire, elle ne sera que cliente, et donc dépendante, de la société de l'information.

b) Les missions du Commissariat aux technologies de l'information, de la communication et de la sécurité

Le Commissariat aux technologies de l'information, de la communication et de la sécurité permettrait :

– de **mettre en œuvre les orientations** définies par le conseil de sécurité économique ;

– et d'assurer la **mutualisation des financements publics** en provenance des différents ministères et des organismes associés.

Dès sa création, cet organisme devra, en liaison avec les entreprises, **établir un panorama des vulnérabilités** françaises.

3.– Créer une plateforme industrielle des technologies de l'intelligence économique

Le maintien de la compétitivité de nos entreprises est intimement lié à la sauvegarde de la compétitivité technologique de la France et de l'Europe. La création d'une plateforme industrielle des technologies de l'intelligence économique est évidemment une nécessité, hélas encore mal perçue par les pouvoirs publics.

Les acteurs industriels innovants sont, en ce domaine, peu nombreux (quelques dizaines de jeunes pousses ou de PME particulièrement performantes), dispersés et de petite taille. De plus, même si des contacts informels existent entre eux, il n'existe pas de diffusion et d'enrichissement croisés des innovations. Enfin, ces entreprises sont fragiles à la fois au plan stratégique, dans la définition de leurs objectifs et de leur évolution, mais aussi au plan financier dans la mesure où ce marché est encore insuffisamment développé pour concourir à des réussites plus flagrantes.

Il faut désormais conforter leur démarche et les adosser, au cas par cas et collectivement, à des prescripteurs industriels, des grandes entreprises, qui pourront leur offrir une meilleure visibilité, des capacités nouvelles d'anticipation et accompagner de façon optimale leur développement.

Pour répondre à ce besoin, il convient de créer une **plateforme industrielle des technologies de l'intelligence économique**, fondée sur un partenariat entre l'État et de grandes entreprises. Quatre ou cinq grands groupes pourraient s'associer au sein d'un comité de parrainage et assurer une partie des capacités de financement mises à disposition des entreprises en charge de l'intelligence économique.

Leur action peut être relayée par deux instances :

– un **fonds d'investissement**, collectant une participation de l'État, des fonds des entreprises partenaires en lien avec la Caisse des dépôts et consignations et un ou plusieurs établissements financiers. Ce fonds devrait être doté d'un capital de référence de 120 à 150 millions d'euros. **Sa création est urgente et impérative et son absence d'autant plus inexplicable que les acteurs sont prêts**.

– un **comité d'experts**, composé de chercheurs et d'ingénieurs des différents grands groupes, chargé d'assurer le suivi stratégique – orientation et action – pour cet ensemble de jeunes pousses.

Ce projet de plateforme accompagne, de manière naturelle, la nomination du haut responsable à l'intelligence économique. Il faut, en effet, donner une **dimension opérationnelle et industrielle à cette nomination**, et non la réduire à un traitement administratif de ces dossiers.

Si la nomination d'un haut responsable pour l'intelligence économique, par un décret du Président de la République en date du 31 décembre 2003, s'inscrit dans l'esprit des recommandations de votre Rapporteur dans son rapport sur l'intelligence économique précité, il faut aujourd'hui fournir une illustration concrète et immédiate de ses conclusions, qui n'ont pas été contredites.

En outre cette plateforme montrerait qu'un **partenariat public-privé** est l'outil fondamental pour nous affranchir de nos dépendances. Ce projet peut avoir, dès l'origine, une dimension franco-allemande, ou à géométrie européenne variable, selon les « objets industriels ».

4.– Européaniser l'Agence pour la diffusion de l'information technologique

L'Agence pour la diffusion de l'information technologique (ADIT) occupe aujourd'hui une position de leader incontesté sur le marché français de l'intelligence économique. Devenue en 2003 une société nationale détenue à 100 % par l'État, elle intervient dans trois domaines :

– l'intelligence concurrentielle et stratégique pour les grands groupes nationaux ;

– l'intelligence territoriale pour développer une culture de projet et de réseau au profit des PME et PMI ;

– et la valorisation de l'information technologique mondiale au profit des acteurs économiques français.

Au sein du dispositif français d'intelligence économique, l'ADIT est devenue un élément clé, tant pour les pouvoirs publics – en particulier pour les ministères chargés des Affaires étrangères et de la Recherche, à l'origine de sa création – que pour les grands groupes industriels nationaux, pour lesquels elle traite certaines de leurs affaires les plus sensibles.

Les perspectives de développement de l'ADIT sont désormais conditionnées par sa capacité à intervenir demain sur une base non plus strictement nationale mais européenne. Dans sa taille actuelle, elle ne dispose pas des capacités suffisantes pour fournir l'ensemble des services et prestations qui lui sont demandées par les grandes entreprises françaises engagées sur les marchés mondiaux.

Il est donc urgent d'engager l'ADIT dans une stratégie internationale. Un développement européen pourrait être envisagé sur le fondement d'objets industriels précis.

Construire une **alternative crédible à l'offre anglo-saxonne**, sur une base européenne dominante, est aujourd'hui une priorité stratégique.

III.– MIEUX PROTEGER LES ENTREPRISES FRANÇAISES

Hier encore, l'entreprise était riche des biens qu'elle produisait et des sites immobiliers d'où sa production était issue. La dématérialisation de l'économie rend plus diffus aujourd'hui ce qui constitue le patrimoine d'une entreprise : ses hommes bien sûr, mais aussi leurs idées, leurs savoir-faire, leurs réseaux relationnels et commerciaux, leurs méthodes de gestion. Autant d'**informations** juridiques, financières, commerciales, scientifiques, techniques, économiques ou industrielles que les acteurs de l'entreprise partagent et mutualisent selon un mode de gestion devenu souvent bien plus horizontal que vertical.

A.– PROTEGER LES INFORMATIONS ECONOMIQUES SENSIBLES

L'utilisation croissante et les rapides progrès des technologies de l'information et de la communication fragilisent ce patrimoine malgré l'amélioration des moyens de défense technique, notamment sur les systèmes informatiques (pare-feu, anti-virus, etc.). Une protection juridique adaptée à ce patrimoine s'avère indispensable.

1.– La nécessité d'un nouveau droit du secret des affaires

En l'état actuel du droit, les informations sensibles de l'entreprise ne sont protégées que par un ensemble de textes dont la cohérence et l'efficacité restent imparfaites.

La législation permettant aux entreprises de protéger leurs informations stratégiques demeure largement lacunaire. Il faut donc créer un nouveau droit du secret des affaires permettant à une entreprise, si elle a respecté un référentiel de protection de l'information, de poursuivre les personnes cherchant à utiliser frauduleusement, piller ou divulguer ses informations sensibles.

Au moment où notre pays s'engage avec détermination et volontarisme dans une politique qui porte au premier rang de ses priorités l'emploi et la cohésion sociale, ces dispositions contribueront à réduire sensiblement le nombre des défaillances d'entreprise qui résultent souvent d'une captation frauduleuse de leur patrimoine dématérialisé.

2.– La proposition de loi de votre Rapporteur

Votre Rapporteur déposera donc une **proposition de loi** relative à la protection des informations économiques.

PROPOSITION DE LOI
RELATIVE A LA PROTECTION DES INFORMATIONS ECONOMIQUES

Article 1er

Après l'article 226-14 du Code Pénal, il est inséré un paragraphe 1er bis intitulé : « De l'atteinte au secret d'une information à caractère économique protégé. » et comprenant deux articles 226-14-1 et 226-14-2 ainsi rédigés :

Article 226-14-1.– Est puni d'une peine d'un an d'emprisonnement et de 15.000 euros d'amende le fait par toute personne non autorisée par le détenteur, d'appréhender, de conserver, de reproduire ou de porter à la connaissance d'un tiers non autorisé une information à caractère économique protégée.

Est puni du double de ces peines le fait, pour une personne autorisée, de faire d'une information à caractère économique protégée un usage non conforme à sa finalité.

Lorsqu'il en est résulté un profit personnel, direct ou indirect, pour l'auteur de l'infraction, les peines définies aux deux précédents alinéas sont doublées.

Les personnes physiques coupables des infractions prévues par le présent article encourent également une peine d'interdiction des droits prévus aux 2° et 3° de l'article 131-26 pour une durée de cinq ans au plus.

Les personnes morales peuvent être déclarées pénalement responsables dans les conditions prévues à l'article 121-2 des infractions définies par le présent article.

Les peines encourues par les personnes morales sont :

1° L'amende suivant les modalités prévues par l'article 131-38 du code pénal ;

2° Les peines mentionnées à l'article 131-39 du même code. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Article 226-14-2.– Présente le caractère d'une information à caractère économique protégée, les informations pouvant apporter directement ou indirectement une valeur économique à l'entreprise, et pour laquelle le détenteur légitime a pris pour en assurer la protection, des mesures substantielles conformes aux usages et aux pratiques en vigueur dans les entreprises et qui ne constituent pas en des connaissances générales, pouvant être facilement et directement constatées par le public.

Présente le caractère de détenteur de l'information la personne morale ou physique qui dispose de manière légitime du droit de détenir ou d'avoir accès à cette information. »

Article 2

Après l'article L. 152-7 du Code du Travail, il est inséré une section 8 intitulée : « Violation de la protection d'une information à caractère économique protégée. » et comprenant deux articles L. 152-8 et L. 152.9 ainsi rédigés :

Art. L. 152-8.– Le fait, par tout dirigeant ou salarié d'une entreprise où il est employé de révéler ou de tenter de révéler une information à caractère économique protégée au sens de l'article 226-14-2 du Code Pénal, est puni d'un an d'emprisonnement et de 15.000 euros d'amende.

Art. L. 152-9.– Nonobstant l'engagement de toute action pénale, le fait par tout dirigeant ou salarié de ne pas avoir respecté les mesures décidées par l'employeur pour assurer la confidentialité d'une information à caractère économique protégée au sens de l'article 226-14-2 du code pénal, et dont il était dûment informé, est passible d'une sanction disciplinaire tel que définie par l'article L. 122-40 du présent code. »

B.– SOUTENIR LES ENTREPRISES STRATEGIQUES

Les entreprises font appel à un nombre croissant de sous-traitants pour leur fournir des biens et des services nécessaires à leur production. De plus en plus fréquemment, les grands groupes deviennent des assembleurs de pièces détachées produites par des petites et moyennes industries. Or, il arrive fréquemment que ces entreprises détiennent des compétences spécifiques particulièrement cruciales. La maîtrise de leur savoir-faire revêt donc un caractère stratégique.

Acteurs majeurs de l'innovation et éléments indispensables d'une stratégie d'autonomie industrielle, les PME et PMI françaises et européennes doivent être soutenues tant par les pouvoirs publics que par les grands groupes industriels.

1.– Le soutien à l'innovation aux États-Unis

a) Le soutien aux PME

Les États-Unis se sont dotés d'un ambitieux programme de soutien à la recherche et à l'innovation des petites et moyennes entreprises américaines (*Small Business Innovation Research Program*). Son objectif est d'encourager les PME à accroître leurs activités de recherche et développement. Ce programme est fondé sur l'idée que progression globale des compétences nationales est bénéfique pour le pays. Il ne concerne que les petites industries privées.

Il s'articule en trois phases :

– une analyse de faisabilité de l'idée ou de la technologie via une première subvention d'un montant maximum de 100.000 dollars (80.000 euros) sur six mois ;

– une subvention d'un maximum de 750.000 dollars (625.000 euros) pour valider sur deux ans les options techniques et le marketing envisagé ;

– et une troisième phase où le programme ne finance rien mais cautionne le dossier auprès de partenaires financiers privés ou des agences fédérales.

Le budget accordé pour les opérations de première phase a atteint, en 2002, plus de 400 millions de dollars (340 millions d'euros), correspondant à un nombre dossiers analysés d'environ 5.000. Cette même année, le budget permettant de délivrer des subventions (deuxième phase) s'est élevé à plus d'un milliard de dollars (800 millions d'euros) correspondant à un nombre de *business plans* validés de 2.000.

Ce sont ces recherches qui permettent ensuite à l'agence fédérale pour les projets de recherche avancée (*Defense Advanced Research Projects Agency*, DARPA) ou aux autres agences fédérales d'accompagner la croissance des entreprises technologiques de pointe américaines.

b) Le financement public des hautes technologies

Le gouvernement américain a mis au point depuis plus de quarante ans une procédure de subvention systématique des sociétés de croissance **dans les domaines de haute technologie jugés importants pour le maintien de la « suprématie militaire et technique des États-Unis d'Amérique ». Expression qui, au passage, ne choque pas les Européens…**

Le processus de financement débute par l'identification de projets industriels innovants. Ces projets peuvent avoir été accompagnés par le programme de soutien à l'innovation et à la recherche des PME.

Un premier financement, toujours supérieur à un million de dollars (800.000 euros) est fourni en quelques semaines (au maximum six mois) par la DARPA ou une agence fédérale. Dans un domaine donné, l'agence peut financer simultanément plusieurs dizaines d'entreprises, en sachant pertinemment que seules une ou deux atteindront leurs objectifs. L'échec du plan d'entreprise est généralement considéré comme prévisible dès le départ et aucun reproche ne sera fait aux dirigeants malchanceux, s'il est prouvé qu'ils ont consacré tous leurs efforts à la réussite du projet, en toute loyauté vis-à-vis de leurs financiers.

Parallèlement, le Département de la défense prend à sa charge le financement de grands programmes de défense, en recommandant aux grands groupes américains, maîtres d'œuvre, d'y associer les sociétés de haute technologie financées par ailleurs. Ces mêmes sociétés peuvent ainsi facilement prendre le contrôle du marché européen naissant, interdisant de ce fait toute création rentable de concurrents locaux, tout en pouvant refuser à tout moment de vendre au nom de la sécurité nationale, si les autorités américaines le décident. **Une telle situation fragilise l'ensemble des industriels européens face à leurs concurrents d'outre atlantique**. Sans réaction significative, pour l'instant, des institutions communautaires !

2.– Renforcer le tissu des petites entreprises innovantes

L'innovation technologique est largement favorisée par la vigueur du tissu des PME innovantes. Si l'État, qui agit par la commande publique, et les grands groupes industriels – qui agissent par leur recherche et développement – sont bien conscients de cet enjeu, il n'en demeure pas moins que cet effort n'est pas optimal. **Le saupoudrage des crédits, aussi bien publics que privés, constitue la règle.**

L'État et les acteurs économiques doivent donc concentrer leur attention sur quelques PME, en pointe sur des technologies dont la maîtrise relève de la protection de la souveraineté. Sans volontarisme politique et industriel, le tissu de PME ne pourra être renforcé. Et pourtant, c'est de la qualité de ce dernier que dépend la compétitivité des grands groupes français, et, au-delà, européens.

La France a certes pris conscience de l'importance de l'enjeu en nommant un haut responsable chargé de l'intelligence économique et en confirmant, comme votre Rapporteur l'avait proposé, le rôle important des services spécialisés, notamment la direction de la surveillance du territoire, dans ce domaine. Cette stratégie doit être poursuivie et amplifiée.

Pour préserver l'avenir de l'industrie européenne de technologie, des fonds d'investissement doivent être capables d'intervenir pour consolider le développement les « champions » nationaux ou européens choisis jusqu'au stade de maturité.

3.– S'assurer de la maîtrise des technologies critiques

Les grands industriels français le savent parfaitement : un petit nombre de hautes technologies sont au cœur de nombreux procédés industriels. Il faut s'assurer que ces technologies, très souvent développées par des PME, demeurent en France et en Europe en toute indépendance de l'étranger.

Différentes procédures permettent aux pouvoirs publics d'identifier et de contribuer à développer et maintenir en France la maîtrise de technologies clés.

L'Agence nationale de valorisation de la recherche (ANVAR) – l'agence française de l'innovation – assure, pour le compte de la délégation générale pour l'armement (DGA), avec laquelle elle a signé une convention, le financement de projets portés par des entreprises d'intérêt stratégique.

La convention entre l'Anvar et la DGA prévoit d'une part, la mise en place d'un financement susceptible de soutenir l'innovation d'entreprises duales ou relevant d'intérêts de la défense et d'autre part, une collaboration en matière de veille technico-économique des PME et PMI considérées comme stratégiques.

Les cosignataires ont ainsi convenu de **favoriser les échanges d'informations technologiques**, d'organiser des rencontres entre experts sectoriels et de rechercher aussi en commun les opportunités au niveau européen et international.

En 2002 et 2003, 14 contrats ont été signés avec des entreprises innovantes, pour un montant total de 3,6 millions d'euros. Ces programmes concernaient notamment des circuits intégrés, un banc test pour un appareil de communication militaire, un micro serveur embarqué, un système de navigation pour charges aéroportées ou encore des dispositifs de sécurisation d'Internet.

Par ailleurs, il faut rester vigilant quant à la pérennité de la maîtrise des technologies critiques. Il suffit pour s'en convaincre de rappeler l'exemple de la société britannique de microprocesseurs Acorn qui, après avoir bénéficié d'un financement communautaire pour sa recherche et développement, a été rachetée par Intel…

C.– RENFORCER LA SECURITE DES SYSTEMES D'INFORMATION

La montée en puissance du traitement électronique de l'information, à un rythme sans précédent, a rendu nécessaire la sécurisation des infrastructures informatiques, pour assurer la protection de notre économie.

Nos sociétés doivent faire face à la menace des pirates informatiques et des services de renseignement d'États étrangers, chargés de pénétrer dans les systèmes d'information et de communication des autres pays dans un contexte de concurrence économique exacerbée.

Les États-Unis disposent d'une stratégie de contrôle du secteur de la sécurité de l'information. Grâce au soutien financier de l'État fédéral, cette stratégie permet aux entreprises américaines d'être en position dominante.

Face à cette hégémonie, les marchés européens semblent bien trop étroits pour permettre l'épanouissement d'industries nationales atteignant la taille critique.

Malgré sa tradition cryptographique la France risque de voir ses capacités autonomes s'appauvrir et disparaître progressivement si une véritable politique industrielle n'est pas lancée. S'appuyant sur la commande publique – puis, dans un deuxième temps, privée – des programmes de sécurisation des systèmes d'information doivent être amorcés.

L'État doit stimuler l'offre de solutions de confiance dont une partie importante sera achetée par les acteurs privés qui souhaitent se protéger. Ainsi, cette politique permettra-t-elle à l'**État de se protéger et à l'économie française de disposer de technologies de l'information, de la communication et de la sécurité de haut niveau.**

1.– Renforcer la sécurité des systèmes de l'État

La sécurité des systèmes d'information est l'art de combiner un ensemble de mesures préventives et curatives sur les plans technique et organisationnel pour faire face aux menaces que l'on aura au préalable identifiées et hiérarchisées. Elle repose sur trois techniques : la cryptographie, les procédés visant à lutter contre la compromission des données et la sécurité informatique, aujourd'hui étroitement imbriqués.

A partir de la demande du directeur du cabinet du Premier ministre – par une lettre du 4 avril 2003 précitée – **une politique de sécurité des systèmes d'information globale doit être programmée par l'État**.

En outre, l'identification des domaines présentant des vulnérabilités inadmissibles doit être réalisée dans tous les ministères. Des structures de protection doivent être mises en place. Il faut aussi poursuivre le développement des moyens interministériels de surveillance, d'alerte et de réponse. Les ministères

doivent aussi compter dans leurs rangs des spécialistes de la sécurisation des systèmes d'information et de communication : il faut donc les former et les fidéliser.

En la matière, **une prise de conscience de tous les ministères des enjeux cruciaux de la sécurité des systèmes d'information est primordiale**. Des exercices de grande ampleur, dans le cadre du plan « Piranet » (plan de lutte contre les attaques informatique) par exemple, pourraient sensibiliser les responsables ministériels.

Votre Rapporteur rappelle qu'il proposait, dans son rapport (1) au Premier ministre sur l'intelligence économique, la création d'une **mission interministérielle d'expertise technique et industrielle des systèmes d'information** des administrations publiques.

2.– Mettre en œuvre une stratégie industrielle

Il apparaît indispensable de valoriser le tissu d'entreprises qui maîtrisent ces technologies et qui disposent de la compétence nécessaire à la protection des réseaux.

Il faut **définir une stratégie de soutien à une offre industrielle de confiance française ou européenne** pour préserver l'indépendance à l'égard des sociétés étrangères.

La capacité d'améliorer en toute autonomie la sécurité des réseaux d'information d'une nation est liée à sa maîtrise des technologies, des produits et des savoir-faire nécessaires. Or, leur nombre est aujourd'hui très élevé. Il faut donc procéder à une étude minutieuse de leur intérêt pour l'État (architecture des serveurs et des postes de travail, logiciels de sécurité, ingénierie des systèmes, administration et exploitation, etc.)

Pour préserver l'autonomie de notre pays, il est souhaitable de voir se développer l'usage des **logiciels libres de droits**, à l'instar de nombreux pays (Allemagne, Brésil, Inde, Chine, Japon, Afrique du Sud, etc.), dont la sécurité est plus facilement vérifiable, puisque les codes sources sont connus.

Au sein des entreprises, les employés doivent être sensibilisés aux enjeux de la sécurité des systèmes d'information. Il faut donc que le cryptage des transmissions sensibles, la mise à jour des logiciels anti-virus, la protection des messages électroniques, la sécurisation des accès aux réseaux des entreprises deviennent autant de préoccupations partagées par l'ensemble des collaborateurs. Trop souvent, les salariés mettent involontairement les informations stratégiques de leur société en danger (vols d'ordinateurs portables, mots de passe trop simples). **La sensibilisation de tous les acteurs économiques doit encore être approfondie**.

(1) Ibidem, page 43.

3.– Renforcer la coopération européenne

La sécurité des systèmes d'information et de communication est un champ de coopération prometteur pour les pays membres de l'Union.

Les institutions communautaires ont constaté que les actions des États membres se sont avérées disparates et insuffisamment coordonnées pour pouvoir apporter une réponse efficace aux problèmes de sécurité. Ces questions de sécurité ne pouvant pas être considérées comme ne concernant qu'un seul pays, les instances européennes ont décidé de se doter d'une agence spécifiquement chargée de ce dossier.

Suite à un accord interinstitutionnel du 20 novembre 2003 entre le Conseil et le Parlement européen, le règlement européen n°460/2004 du 10 mars 2004 a créé l'Agence européenne pour la sécurité des réseaux et de l'information (*European Network and Information Security Agency*, ENISA).

Sa mission consiste à *« soutenir le marché intérieur en facilitant et en favorisant un renforcement de la coopération et de l'échange d'informations sur les questions de sécurité des réseaux et de l'information »*. En pratique, elle doit conseiller les États membres et la Commission, promouvoir la coordination des activités de sécurité des systèmes d'information au sein de l'Union et sensibiliser les citoyens, les entreprises et les administrations sur cet enjeu.

Les différents efforts menés à l'échelle européenne pour sécuriser les systèmes d'information doivent être évidemment encouragés. En outre, la démarche communautaire associe les entreprises puisqu'elle repose « sur une étroite collaboration avec les milieux d'affaires », selon les termes même du communiqué de presse de la Commission…

EXAMEN EN COMMISSION

Au cours de sa réunion du 9 juin 2004, votre Commission a examiné le présent rapport d'information.

Votre Rapporteur spécial a indiqué que le présent rapport s'inscrivait dans le prolongement du rapport qu'il a remis en 2003 au Premier ministre, intitulé « *Intelligence économique, compétitivité et cohésion sociale* ». En effet, ce dernier abordait quatre thèmes : la sécurité économique, la compétitivité de l'économie française, les stratégies d'influence et la formation. L'intelligence économique est une politique publique qui doit s'appliquer aux marchés stratégiques, qui ne peuvent être régulés par le seul marché. Les marchés de l'énergie, de l'aéronautique civile et de la défense appartiennent à ces secteurs. Si les attentats terroristes retiennent notre attention, l'évolution des menaces est bien plus large. Celles-ci pèsent notamment sur l'information qui est désormais au cœur de nos processus productifs. Nous sommes entrés dans une véritable guerre économique. L'actualité illustre cette situation, puisque le leader mondial de l'intelligence économique et de l'investigation, Kroll, est en train d'être racheté par Marsh&McLennan, qui est le plus grand groupe mondial de courtage d'assurance, lequel comprend en outre une société de consultants (Mercer) et l'un des plus gros fonds d'investissements américains (Putnam). Ce rapprochement montre la maîtrise des anglo-saxons sur les métiers stratégiques que sont l'audit, l'investigation ou le courtage d'assurance. Les États-Unis se sont donc dotés d'une plateforme d'intelligence économique privée intervenant dans tous ces métiers. En outre, des fonds d'investissement, comme le fonds In-Q-Tel contrôlé par la CIA, leur permettent de s'assurer de la maîtrise des hautes technologies.

Dans ce contexte, quelles actions ont été entreprises par l'État ? Sans impulsion politique déterminante, seuls des efforts épars ont été conduits. En matière de sécurité des systèmes d'information, un centre de recensement et de traitement des attaques informatiques a été créé en 2000 au sein de la Direction centrale de la sécurité des systèmes d'information du Secrétariat général de la Défense nationale (SGDN). S'agissant du contrôle des investissements étrangers dans des entreprises françaises sensibles, la loi de sécurité financière du 1er août 2003 a renforcé les prérogatives du Ministre de l'économie. Il est aujourd'hui urgent de définir une stratégie de sécurité nationale englobant la Défense nationale, la protection de notre économie et un système d'alerte contre les nouvelles menaces.

La France souffre de vulnérabilités juridiques. Elle ne dispose pas d'une réelle protection du secret des affaires telle que le Cohen Act l'assure aux États-Unis. La loi du 5 janvier 1988 relative à la fraude informatique, n'est efficace qu'en cas d'intrusion ou de tentative d'intrusion avérée. Par ailleurs, la législation sur le droit d'auteur et le droit des producteurs ne permettent pas de protéger efficacement l'accès et l'utilisation des bases de données. La loi du 6 janvier 1978

relative à l'informatique, aux fichiers et aux libertés ne vise que les informations nominatives. Globalement, ces dispositifs ne protègent qu'imparfaitement les savoir-faire français. De plus, des entreprises sont parfois victimes de procédures judiciaires étrangères. En effet, lors de commissions rogatoires internationales, des prises illicites de renseignements peuvent se produire.

Des menaces financières pèsent également sur notre économie. Les cas de Saft, Eutelsat ou Gemplus qui ont fait l'objet de tentatives ou de prises de contrôle par des fonds d'investissement, illustrent la vulnérabilité du capital des entreprises stratégiques françaises et européennes. Gemplus, qui est le leader mondial de la carte à puce, a fait l'objet d'une prise de participation de 550 millions de dollars par le fonds américain Texas Pacific Group. Le nouveau président de Gemplus a été administrateur du fonds In-Q-Tel. Ce fonds est un outil de veille ainsi qu'un incubateur de jeunes pousses. En ce qui concerne le contrôle des investissements étrangers en France, la loi de sécurité financière a étendu les pouvoirs du ministre de l'économie qui peut désormais s'opposer à un investissement dans une entreprise mettant en cause la Défense nationale. Pour autant, cette notion n'est pas précisément définie, alors même que les Américains ont une vision dynamique de la sécurité nationale. Le SGDN est chargé de conduire une réflexion interministérielle sur les prises de contrôle par les capitaux étrangers d'entreprises françaises.

Aux États-Unis, le Comité pour les investissements internationaux permet de les évaluer au regard des intérêts stratégiques des États-Unis. En Allemagne, le Parlement vient d'adopter un projet de loi permettant de contrôler la compatibilité des opérations financières avec les intérêts majeurs de sécurité. Au plan international, l'Organisation mondiale du commerce (OMC) permet aux États de déroger aux principes du libre échange quand leurs intérêts vitaux sont en jeu. Cependant, ceux-ci ne sont pas précisément définis. De même, une législation nationale encadrant les investissements internationaux n'est compatible avec le droit communautaire qu'à deux conditions : les États doivent pouvoir justifier de la proportionnalité de la mesure et les investisseurs doivent connaître avec précision les conditions qui leur sont imposées. Les mêmes menaces portant sur les technologies de l'information et de la communication pèsent sur l'État et les entreprises. Les microprocesseurs, les systèmes d'exploitation, le contrôle d'accès, la transmission d'information et les applications bureautiques constituent autant de cibles pour les personnes mal intentionnées souhaitant accéder à l'information. Les moyens de lutte contre ces menaces sont limités. La fonction d'audit de la Direction centrale de la sécurité des systèmes d'information du SGDN est particulièrement utile, mais elle n'est composée que de six personnes. Il convient donc de mettre en place une mission interministérielle d'expertise technique et industrielle des systèmes d'information des administrations publiques.

Pour faire face à ces menaces, l'État doit se réformer pour mettre en place une politique de sécurité nationale. Les États-Unis se sont dotés des outils législatifs (USA Patriot Act) leur permettant, notamment, d'intercepter les courriers électroniques. Un Département de la Sécurité du territoire national a été

créé. Ce dispositif pourrait être utilisé à des fins de renseignement économique. De plus, l'Advocacy Center du Département du commerce, en liaison avec les postes de présence américaine à l'étranger, assure la gestion de l'information ouverte. L'État soutient donc les grandes firmes américaines dans leurs contrats stratégiques. Dans ce contexte, une cellule de contact et de soutien aux entreprises françaises relevant du périmètre stratégique devrait être mise en place. Ce périmètre stratégique doit englober un petit nombre de technologies de souveraineté. Cette définition ne doit pas être trop large pour éviter l'éparpillement de l'action publique. Elle ne doit pas non plus être trop précise afin d'éviter une vision « gosplaniste » de l'État. La stratégie de sécurité nationale doit s'inscrire dans un cadre européen. La puissance de l'Europe repose en effet sur sa capacité à réduire ses dépendances technologiques et commerciales à l'égard du reste du monde. La mise en place d'une politique de sécurité nationale doit s'appuyer sur un renouveau de l'action publique. À l'instar du Conseil de sécurité intérieure, placé depuis 2002 auprès du Président de la République, il faut créer un Conseil de sécurité économique. Seule une impulsion politique donnée au plus haut niveau de l'État pourra vaincre les cloisonnements administratifs.

Afin d'appuyer une véritable politique industrielle en faveur de la sécurité économique, il faut créer un « CEA » des technologies de l'information, de la communication et de la sécurité. En effet, le CEA créé par le Général de Gaulle, en 1945, est l'exemple même d'une réussite industrielle éclatante issue d'une impulsion politique forte. Il faut aujourd'hui mutualiser les dépenses publiques en faveur de ces technologies dont les crédits servent trop souvent de variable d'ajustement des budgets des différents ministères. Ce Commissariat devra mettre en œuvre les orientations définies par le Conseil de sécurité économique et assurer la mutualisation des financements publics. Il établira, en liaison avec les entreprises, un panorama des vulnérabilités françaises. Une plateforme industrielle des technologies de l'intelligence industrielle économique devrait compléter ce dispositif. Celle-ci, s'appuyant sur un fonds d'investissement, pourra soutenir les jeunes pousses dans le domaine des technologies de l'information. La création de ce fonds est urgente et son absence est d'autant plus inexplicable que les acteurs sont prêts à le mettre en place. Enfin, il faut permettre à l'Agence pour la diffusion de l'information technologique d'étendre ses activités en Europe.

Pour mieux protéger les entreprises françaises, des actions concrètes doivent être entreprises. Il faut tout d'abord renforcer la définition du secret des affaires en droit français. Une proposition de loi relative à la protection des informations économiques sera prochainement déposée. Par ailleurs, il faut soutenir les entreprises stratégiques. Les États-Unis ont instauré depuis plus de 40 ans une procédure de subvention systématique des sociétés de croissance dans les domaines de haute technologie jugés importants pour le maintien de la « suprématie militaire et technique des États-Unis d'Amérique ». Cette expression ne choque d'ailleurs pas les Européens. Nous devons donc renforcer le tissu des petites entreprises innovantes. Aujourd'hui, le saupoudrage des crédits, aussi bien publics que privés est la règle. La France a, certes, pris conscience de l'importance de l'enjeu en nommant un haut responsable de l'intelligence économique, mais

cette stratégie doit être amplifiée. Il faut enfin s'assurer de la maîtrise des technologies critiques. À ce titre, une convention entre l'Agence nationale de valorisation de la recherche et la délégation générale pour l'armement prévoit de financer des petites entreprises innovantes du secteur de la Défense.

Le renforcement de la sécurité des systèmes d'information doit être une priorité pour l'État. Une stratégie industrielle est nécessaire. L'utilisation de logiciels libres de droits doit se développer et il convient de sensibiliser les salariés des entreprises à ces enjeux. De plus, cette politique doit s'appuyer sur la coopération européenne que permet la création, par un règlement européen du 10 mars 2004, de l'Agence européenne pour la sécurité des réseaux et de l'information. Il faut rappeler que les États-Unis se sont dotés d'un outil équivalent il y a plus de douze ans.

M. Michel Bouvard, Président, a estimé que cet excellent rapport contribue au débat actuel sur la désindustrialisation et les délocalisations. Il reste une place très importante pour l'action publique en la matière. Dans ce cadre, il est nécessaire de construire des objectifs par ministère en s'inspirant des résultats des expériences territoriales. Les indicateurs prévus par la loi organique doivent y contribuer. On peut cependant s'interroger sur la nécessité de créer un nouvel organisme sous la forme d'un Conseil de sécurité économique alors qu'il doit exister d'autres structures pour l'héberger.

M. Daniel Garrigue a souhaité placer le problème posé par le rapport au cœur du débat européen. Il existe un certain nombre de structures en matière de sécurité nationale qui ont mal vieilli et ont du mal à s'adapter aux évolutions technologiques, notamment pour les technologies de pointe, très évolutives. On peut ainsi regretter que des entreprises nationales, qui ont été pionnières dans des secteurs stratégiques, n'aient plus aujourd'hui la dimension suffisante dans un cadre strictement national. C'est pourquoi il faut s'interroger sur la détermination politique réelle de la France et de l'Europe en la matière par rapport aux États-Unis. L'exemple du système de positionnement par satellite Galileo permet de prouver qu'il est possible de soutenir des projets européens ambitieux.

M. Thierry Carcenac a considéré que le sujet abordé par le Rapporteur correspond à une question véritablement politique. Il est possible de prévoir d'autres utilisations pour les dispositifs déjà existants, comme cela s'est passé avec le satellite Spot par exemple. L'analyse du Rapporteur est pertinente sur le fond mais on peut cependant avoir des divergences d'appréciation sur les préconisations du rapport. Il semble en effet indispensable de mettre en œuvre un effort certain des ministères au niveau informatique, en utilisant des logiciels libres de droits. Il est également souhaitable de ne pas se faire piller le travail des chercheurs français dans les secteurs industriels stratégiques, ainsi que d'éviter leur départ à l'étranger.

M. Pierre Hériaud a estimé souhaitable que ce rapport soit porté à la connaissance du plus grand nombre de personnes concernées. Nous vivons, en effet, dans une société de risques où l'essentiel de la production normative,

législative ou réglementaire, vise à contrer ces risques. Or, la France et ses partenaires européens ont pris un retard important en la matière par rapport aux États-Unis. Il ne sert à rien de vouloir protéger de petits secrets avec de petits moyens ; il faut au contraire concentrer l'ensemble de l'effort budgétaire de l'État pour la sécurité civile ou informatique, soit plus de 1,6 milliard d'euros, sur les secteurs les plus stratégiquement importants.

La mise en œuvre de la loi organique relative aux lois de finances doit permettre un regroupement des moyens disponibles pour une plus grande efficacité de l'argent employé. Les cloisonnements entre ministères aboutissent à des investissements saupoudrés alors que l'État se doit de mener une stratégie globale à destination des entreprises en matière d'intelligence économique. Dans ce cadre, il est indispensable d'avoir des dispositifs très sécurisés.

M. Jean-Louis Dumont a estimé possible de dépasser les clivages politiques sur les questions de sécurité nationale. Le Parlement, dans son ensemble, doit faire pression sur le Gouvernement pour qu'il donne suite à ce rapport et définisse une véritable stratégie en matière de sécurité nationale.

Votre Rapporteur a apporté les réponses suivantes :

– Il est tout à fait possible d'intégrer le nouveau Conseil de sécurité économique, qu'il est souhaitable de créer au niveau ministériel, au sein du Conseil de sécurité intérieure, ce qui ne crée pas de structure supplémentaire.

– Le Comité pour la compétitivité et la sécurité économique (CCSE) mis en place par le gouvernement Balladur en 1995 ou le rapport Martre du Commissariat général du Plan n'ont pas abouti à des résultats tangibles car ils ne s'inscrivaient pas dans la perspective d'une véritable politique publique pour l'intelligence économique. Un simple effort de veille pour les entreprises n'est pas suffisant, même dans le cadre de nations libérales. Il faudrait réconcilier le Gouvernement et les affaires, car le marché ne peut pas disposer de la capacité de synthèse que seul l'État maîtrise en la matière.

– La question de la nationalité des entreprises à protéger est une préoccupation essentiellement franco-française. Elle ne repose guère dans les pays anglo-saxons. Au-delà des critères objectifs, il existe en effet un fort sentiment subjectif qui est le ciment d'un véritable patriotisme économique. Dans ces conditions, l'État, le Congrès aux États-Unis n'hésitent pas à intervenir publiquement lorsque des intérêts industriels et économiques nationaux concernant des entreprises privées sont en jeu. On a pu découvrir ce même type d'intervention en France, par exemple avec le rôle joué par le Premier ministre sur le dossier Sanofi-Aventis.

– Il faut résister à une tentation « gosplaniste » pour apprécier tout ce qui est stratégique. La mise en place de fonds d'investissement pour sauvegarder certains secteurs stratégiques rentables pour la France et l'Europe doit être ciblée au vu d'un accord entre le public et le privé sur ce qui est stratégique. La protection des réseaux publics et privés est un service rendu non seulement aux entreprises, mais aussi à tous les citoyens dans leur vie quotidienne.

– Un accord politique est tout à fait possible sur ce sujet. Pour preuve, la mise en place de la fondation « Prométhée », qui vise à cibler des actions de sécurité économique, s'est faite en collaboration avec M. Jean-Michel Boucheron, ancien président socialiste de la commission de la Défense nationale, comme vice-président. Dans ce cadre, tout le monde doit pouvoir participer à une réflexion déterminante pour le destin de la France et l'Union européenne.

En application de l'article 146 du Règlement de l'Assemblée nationale, la commission des Finances a *autorisé* la publication du présent rapport d'information.

N° 1664 – Rapport d'information sur la stratégie de sécurité économique nationale (M. Bernard Carayon)