N° 1796

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale

le 21 mars 2019

N° 402

SÉNAT

SESSION ORDINAIRE 2018 - 2019

Enregistré à la présidence du Sénat

le 21 mars 2019

RAPPORT

au nom de

L'OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

sur

LES ZONES À RÉGIME RESTRICTIF (ZRR) DANS LE CADRE DE LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION

Compte rendu des auditions, sous forme de table ronde, du 24 janvier 2019 et de la présentation des conclusions du 21 mars 2019

PAR

M. Cédric VILLANI, député et M. Gérard LONGUET, sénateur

Déposé sur le Bureau de l'Assemblée nationale

par M. Cédric VILLANI,

Premier vice-président de l'Office

Déposé sur le Bureau du Sénat

par M. Gérard LONGUET

Président de l'Office

Composition de l'Office parlementaire d'évaluation des choix scientifiques et technologiques

Président

M. Gérard LONGUET, sénateur

Premier vice-président

M. Cédric VILLANI, député

Vice-présidents

M. Didier BAICHÈRE, député
M. Patrick HETZEL, député
Mme Huguette TIEGNA, députée
M. Roland COURTEAU, sénateur
M. Pierre MÉDEVIELLE, sénateur
Mme Catherine PROCACCIA, sénateur

DÉPUTÉS	SÉNATEURS
M. Julien AUBERT	M. Michel AMIEL
M. Didier BAICHÈRE	M. Jérôme BIGNON
M. Philippe BOLO	M. Roland COURTEAU
M. Christophe BOUILLON	Mme Laure DARCOS
Mme Émilie CARIOU	Mme Annie DELMONT-KOROPOULIS
M. Claude de GANAY	Mme Véronique GUILLOTIN
M. Jean-François ELIAOU	M. Jean-Marie JANSSENS
Mme Valéria FAURE-MUNTIAN	M. Bernard JOMIER
M. Jean-Luc FUGIT	Mme Florence LASSARADE
M. Thomas GASSILLOUD	M. Ronan Le GLEUT
Mme Anne GENETET	M. Gérard LONGUET
M. Pierre HENRIET	M. Rachel MAZUIR
M. Antoine HERTH	M. Pierre MÉDEVIELLE
M. Patrick HETZEL	M. Pierre OUZOULIAS
M. Jean-Paul LECOQ	M. Stéphane PIEDNOIR
M. Loïc PRUD'HOMME	Mme Angèle PRÉVILLE
Mme Huguette TIEGNA	Mme Catherine PROCACCIA
M. Cédric VILLANI	M. Bruno SIDO

SOMMAIRE

Pages

CONCLUSIONS DES AUDITIONS ORGANISÉES PAR L'OFFICE LE 24 JANVIER 2019 SUR « LES ZONES À RÉGIME RESTRICTIF (ZRR) DANS LE CADRE DE LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION »

Les auditions organisées par l'Office le 24 janvier 2019 sur les zones à régime restrictif (ZRR) ont pris la forme de deux tables rondes : l'une sur les menaces de captation de savoirs et technologies sensibles, qui était confidentielle (à huis clos), en application de la loi de 1983 qui régit l'Office ; l'autre sur les procédures relatives aux zones à régime restrictif (ZRR), qui était ouverte à la presse et retransmise en vidéo.

En France, le dispositif des zones à régime restrictif (ZRR) constitue le cœur du régime de protection du potentiel scientifique et technique (PPST), régi par le secrétariat général de la défense et de la sécurité nationale (SGDSN), avec les hauts fonctionnaires de défense et de sécurité (HFDS) des six ministères de rattachement. Les ZRR actuellement créées ont pour but de protéger, au sein des établissements de recherche publics et privés, l'accès à leurs savoirs et savoir-faire stratégiques ainsi qu'à leurs technologies sensibles. Les ZRR offrent une protection juridique par des sanctions prévues dans le code pénal. Elles sont fondées sur le contrôle des accès, physiques comme virtuels, aux informations sensibles détenues. Les services de renseignement de l'État procèdent au criblage des candidats à l'embauche dans une ZRR, qui aboutit, au bout d'un délai ne devant pas excéder deux mois, à une décision – favorable ou non – du HFDS. Or les ZRR font l'objet de critiques significatives de la part d'une partie de la communauté scientifique française, au motif qu'elles ne seraient pas adaptées et occasionneraient des lourdeurs incompatibles avec le bon fonctionnement des laboratoires.

La **première table ronde**, sur les menaces et les risques, a réuni les principaux responsables du dispositif de PPST, Mme Claire Landais, secrétaire générale de la défense et de la sécurité nationale, M. Thierry Matta, directeur général adjoint de la sécurité intérieure (DGSI), et M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Les intervenants ont rappelé que les dispositifs de la PPST concourent au respect par la France de ses engagements internationaux en matière de lutte contre la prolifération des armes de destruction massive – nucléaires, radiologiques, biologiques et chimiques (NRBC) – et de leurs vecteurs. Ils protègent également les technologies duales, civiles et militaires.

La **DGSI** a rappelé les enjeux de la protection des savoirs et technologies en termes économiques et sociaux : innovation, propriété intellectuelle, croissance, emploi. Nous avons entendu que certains secteurs industriels sont particulièrement visés par les menaces de captation, nous ne pouvons les citer publiquement pour des raisons de confidentialité. Certains pays sont plus particulièrement à l'origine

de ces atteintes, notamment la Chine pour ne parler que d'elle. Certaines organisations terroristes ont également de telles pratiques. La captation peut prendre des formes variées : vol physique de prototype, d'ordinateur portable, de disque dur... ; intrusion « consentie » (chercheur invité) ; atteinte au système d'information…

L'ANSSI estime que les menaces informatiques pèsent lourdement sur la recherche. Les laboratoires ne sont pas à l'abri de la malveillance générale informatique, qui touche tout le monde. Leur puissance de calcul est particulièrement exposée au « minage » *(mining)*. La cybercriminalité passe également par le rançonnage ou les « rançongiciels » *(ransomware)*, qui sont très proliférants : il ne faut jamais payer, par principe, et, même si on paie, on ne récupère en général pas ses données. Si par définition l'espionnage informatique n'est en général pas visible, on sait qu'il a tendance à prendre des proportions considérables, notamment à des fins économiques (brevets). En outre, les attaques informatiques visant à détruire peuvent être très dangereuses : elles passent notamment par la gestion technique des bâtiments (GTB) en raison de la généralisation des dispositifs intelligents connectés. La difficulté provient de ce que l'utilité des systèmes informatiques résulte justement de leur connectivité et de leur ouverture sur l'extérieur. Sans imposer le « retour au Moyen-Âge », qui ne serait sans doute pas respecté, le directeur général de l'ANSSI a estimé qu'utilisateurs et responsables de la sécurité doivent définir ensemble des solutions raisonnées pour ne pas aller trop loin dans cette ouverture et dans ce partage d'informations.

Même en l'absence de preuves juridiques, on sait en général d'où proviennent ces attaques informatiques. Les instruments de coopération judiciaire sont efficaces entre pays alliés. La riposte passe par une « hygiène informatique » de base. Si l'ANSSI a élaboré et publié un « Guide méthodologique de la protection numérique du potentiel scientifique et technologique de la nation » [(1)], elle n'a cependant pas les moyens d'auditer toutes les ZRR de France ; la protection passe donc par un réseau local d'experts en cybersécurité. Le directeur général de l'ANSSI a beaucoup insisté sur le fait que la sécurité informatique repose sur une analyse de risque pour chaque situation, puis la définition de solutions spécifiques adaptées. L'ANSSI constate qu'en matière de malveillance informatique, l'humain est en général le maillon faible. Sensibilisation et explication sont des nécessités, imposer des règles qui seraient mal comprises serait probablement voué à l'échec. Il faut rendre les gens véritablement acteurs de leur propre sécurité, plutôt que simplement victimes des règles de sécurité.

La secrétaire générale de la défense et de la sécurité nationale (**SGDSN**) a indiqué être consciente de la nécessaire conciliation, d'une part, entre la protection de savoir-faire et de technologies sensibles, les impératifs sécuritaires, et, d'autre part, la liberté de la recherche, le besoin de communication entre chercheurs, le

(1) *https://www.ssi.gouv.fr/uploads/2018/05/guide_protection_scientifique_technique_nation_anssi-pa-049_v1.pdf*

besoin d'échange d'informations, le fait que l'accroissement de la connaissance est facilité par son partage.

La secrétaire générale a reconnu que la PPST avait être été mise en œuvre de façon trop lourde depuis la réforme de 2012 : il a pu y avoir des erreurs, ou un excès de précaution où chacun « ouvre le parapluie ». Pour elle, les textes règlementaires offrent une souplesse qui devrait permettre des marges de manœuvre pour une application mieux adaptée aux différents domaines scientifiques. Ainsi, l'autorisation préalable des publications, souvent contenue dans le règlement intérieur des ZRR, n'est en aucun cas une obligation contenue dans la circulaire interministérielle du 7 novembre 2012 relative à la mise en œuvre du dispositif de PPST de la nation.

La secrétaire générale a rappelé les procédures de concertation mises en place pour les ZRR, avec un collège des experts et des sous-commissions thématiques : désignation des secteurs à protéger, désignation des technologies ou des savoir-faire sensibles, constitution des ZRR. Par contre, pour des raisons de confidentialité, les décisions de refus d'accès ne peuvent effectivement pas être motivées.

La **deuxième table ronde** a réuni le haut fonctionnaire de défense et de sécurité (HFDS) adjoint des ministères de l'enseignement supérieur, de la recherche et de l'innovation et de l'éducation nationale et de la jeunesse (MESRI/MENJ) et des chercheurs de plusieurs disciplines ; mathématiques, informatique, sciences de la vie, agronomie et sciences de l'environnement, physique et sciences pour l'ingénieur. Elle a traité des procédures de mise en œuvre de la PPST, centrées autour du dispositif des zones à régime restrictif (ZRR). Les laboratoires classés ZRR ont dû protéger leurs accès physiques (badges magnétiques, autorisations d'accès) et logiques (sécurité informatique), quelquefois contrôler leurs publications.

Pour le **HDFS adjoint des MESRI/MENJ**, 9 400 demandes d'accès (français et étrangers) ont été déposées en 2018, pour lesquelles : 95 % des avis ont donné lieu à une absence totale d'objection ; 1,7 % des avis, soit 157, ont été négatifs ; et 3,5 % des avis ont été positifs sous réserve. Sur l'ensemble des domaines scientifiques, le flux des demandes annuelles est d'environ 20 000, et dans aucun des secteurs, le taux d'avis défavorable ne dépasse 2 %.

Un débat est intervenu sur les délais d'instruction des demandes d'accès : 24 jours selon le HDFS adjoint des MESRI/MENJ, mais 10 semaines, et même 2 mois ou plus pour les demandes refusées, selon des sources en provenance du CNRS. Dans les laboratoires de physique, il a été indiqué que le délai est de plus de 2 mois pour les recrutements, à quoi s'ajoute le délai d'établissement du visa pour les non-Européens, soit un délai total pouvant atteindre 4 mois... La différence s'explique par le fait que le HFDS adjoint établit des statistiques sur l'ensemble des demandes, qu'elles concernent les chercheurs français ou étrangers, alors que les laboratoires les établissent sur les seuls chercheurs

étrangers. Or ce sont justement les délais pour les chercheurs étrangers qui posent problème.

À la suite de l'audition publique, le HFDS adjoint a précisé les statistiques qu'il collecte. Le délai moyen de traitement des demandes d'accès des étrangers aux ZRR est de 34 jours, soit donc plus d'un mois, alors qu'il est de 16 jours (et même seulement 9 jours dans le cadre de la procédure simplifiée) pour les français. Le taux de refus des candidats étrangers est de 3,8 % (149 cas sur près de 4 000 demandes), alors qu'il est proche de 0 % (7 cas sur plus de 5 000 demandes) pour les français. Le taux d'avis favorables avec réserve est de 7,7 % (301 cas) pour les étrangers, alors qu'il est également proche de 0 % (19 cas) pour les français.

Le HDFS adjoint des MESRI/MENJ a présenté des propositions qui se déclinent en trois axes.

Le premier axe consiste en un « contrat PPST » avec les directeurs d'unité (DU) et les établissements qui donnerait quatre grandes garanties : 1° qu'il y ait un échange systématique avec chaque DU sur l'évaluation réalisée par le collège des experts ; 2° que les tracés physiques ou intellectuels des ZRR, c'est-à-dire des efforts de recherche sur lesquels on affecte des doctorants, prennent en compte les préoccupations des DU (les avis réservés en sont une illustration, mais le système est évolutif) ; 3° que le règlement intérieur de la ZRR soit un document à l'initiative de l'établissement et du DU ; 4° pour ce qui concerne les chercheurs étrangers, que l'on puisse définir, avec les DU et les établissements porteurs, les périmètres de recherche et les précautions raisonnables à apporter selon les nationalités – c'est la question de l'analyse sous réserve.

Le deuxième axe concerne les avis sur demande d'accès, pour lesquels le HFDS adjoint du MESRI propose, aux établissements qui peuvent certifier leur démarche, une expérimentation de procédure simplifiée, qui diviserait par deux les délais, hormis pour les cas plus délicats.

Le troisième axe propose de mener un travail d'aménagement du dispositif réglementaire par discipline.

Lors de l'audition, les **responsables de laboratoires en sciences de la vie, agronomie et sciences de l'environnement et sciences pour l'ingénieur – mécanique**, ont montré qu'ils avaient bien intégré le dispositif des ZRR. Ils ont détaillé leur participation aux dispositifs de concertation que sont le comité d'experts et les sous-comités thématiques. L'instauration des ZRR a été bien accueillie depuis 2012, même s'il faut surveiller leur bonne acceptabilité dans le temps.

Le cadre juridique et organisationnel permis par le classement en ZRR est considéré comme protecteur pour les laboratoires et leurs établissements de rattachement. L'assistance des services de l'État, par le criblage *(screening)* des candidats constitue une aide appréciable, s'agissant d'une compétence spécifique

dont ne disposent pas les scientifiques. L'accès à un audit informatique de l'ANSSI peut être facilité par l'existence d'une ZRR, même si l'ANSSI a reconnu ne pas être en capacité de contrôler toutes les ZRR de France. La classification en ZRR d'un laboratoire rassure des partenaires industriels, par exemple dans l'aéronautique ou l'énergie, elle peut même parfois s'avérer nécessaire pour contracter.

Si la mise en œuvre des ZRR a pu être perçue dans un premier temps comme autoritaire et technocratique, un effort de pédagogie a été fait depuis. Les réunions de sensibilisation des équipes sont absolument nécessaires pour prendre conscience des vulnérabilités. Après une période initiale de méfiance, les contraintes liées aux ZRR sont mieux acceptées et seuls de rares « couacs » sont à déplorer. Ces contraintes ne sont pas acceptées de gaieté de cœur et une souplesse, une pédagogie et un accompagnement sont indispensables. La coexistence dans des locaux classés ZRR d'activités de recherche et de formation pose cependant problème. Le coût de la protection des systèmes d'information des petites unités de recherche a été mentionné.

Lors de l'audition, les **responsables de laboratoires de mathématiques, d'informatique et de physique** ont exprimé les critiques qu'ils portaient à l'encontre du dispositif des ZRR.

Ils se plaignent du délai d'autorisation des candidats pour travailler dans une ZRR. Cela constitue un handicap considérable par rapport aux laboratoires étrangers, dans un contexte de concurrence forte pour le recrutement des meilleurs chercheurs. Le surcoût administratif de gestion des ZRR, ainsi que les frais induits de protection physique et logicielle, ont été mentionnés, quand bien même ils pèseraient sur les établissements d'accueil et non sur les unités de laboratoire. Pour tout ce qui a trait à l'international dans une ZRR, une cascade de responsables ont tendance à « ouvrir le parapluie », que ce soit pour une coopération avec une entreprise étrangère, un déplacement à l'étranger ou un accès dans des locaux. On ne peut « lever le petit doigt » sans que cela remonte au minimum au fonctionnaire de sécurité et de défense (FSD) de l'établissement, voire au HFSD du ministère.

Les DU de mathématiques se plaignent du fait que les identifications de laboratoire devant être classés en ZRR semblent réalisées selon un certain nombre de mots-clés, lesquels leur sont d'ailleurs inconnus, puisque le SGDSN n'en fait pas état.

Pour les laboratoires de physique, la mise en place des ZRR à partir de 2012 a entraîné un durcissement des dispositifs de PPST.

En informatique, la recherche publique en France a vocation à être partagée et les découvertes ne sont pas brevetables ni dangereuses en soi ; en particulier, les travaux en *open source* doivent intégralement être publiés. Les laboratoires d'informatique sont donc tout sauf des tours d'ivoire et les

interactions avec le monde extérieur sont multiples : recrutements, missions, publications, financements… Il est difficile de détecter quel périmètre il faut protéger et avec quelle intensité ; cela demande un gros travail, à la fois des laboratoires et des personnes amenées à porter des diagnostics ou des avis. La protection permise par les ZRR n'est d'aucune efficacité contre les mouvements de personnel et les comités d'experts internationaux. Les services de renseignement sont considérés comme trop éloignés de la recherche pour comprendre les enjeux, ainsi de la cryptologie, qui n'est plus un sujet sensible alors que beaucoup de personnes continuent à le croire. La gradation des risques sur une échelle de 0 à 3, telle que pratiquée dans les ZRR, n'est pas applicable car le risque strictement nul n'existe pas. Dans un contexte de concurrence internationale, l'agilité pour faire venir les chercheurs, pour se déplacer, pour publier, pour pouvoir recruter est primordiale.

Toutes disciplines scientifiques confondues, la taille optimale des ZRR a fait l'objet de débat : grande pour certains, afin de décloisonner les équipes, ou petite pour d'autres, afin de limiter les contraintes pesant sur les chercheurs.

Conclusions de l'Office

Les activités de recherche sensibles nécessitent certes une protection, mais la liberté académique et l'ouverture internationale des scientifiques, qui sont des principes fondamentaux du développement des connaissances, doivent être préservées autant que possible. Le maintien de l'excellence de la recherche française nécessite l'échange des idées et l'attraction des meilleurs chercheurs et étudiants dans ses laboratoires. Le souci de l'efficacité de la recherche est essentiel pour garder les laboratoires français au meilleur niveau international. Il en va de la place de la recherche française dans un contexte international de plus en plus concurrentiel.

Or depuis 2012, le dispositif des ZRR a été mis en place de façon trop rigide et trop contraignante, avec une concertation insuffisante. Il en est résulté une gêne considérable pour les laboratoires, qui a été plus ressentie dans certaines disciplines scientifiques (mathématiques, informatique) que dans d'autres (sciences de la vie). D'un laboratoire de physique à l'autre, le ressenti est très différent et l'acceptabilité des ZRR très variable. On peut comprendre que pour un laboratoire de biologie sensible, la lourdeur de la menace et le degré de sécurité nécessaire rendent naturelles les procédures ZRR, mais lorsque la menace est moins claire et perceptible, ainsi dans les domaines des mathématiques et de l'informatique, ces procédures sont moins légitimes.

Avec l'impression d'un certain arbitraire dans la mise en œuvre des ZRR, la confiance a été rompue du côté d'une partie des laboratoires. Les HFDS adjoints des six ministères n'ont pas suffisamment joué le rôle de médiateur qui aurait recueilli la confiance des scientifiques et qui, de par leur habilitation, auraient eu la possibilité d'entendre les éléments confidentiels qui ne peuvent pas être dits aux DU. Les chercheurs français vivent très mal l'absence de motivation

des décisions de rejet de demandes d'accès, perçues comme arbitraires, lointaines et souvent injustifiées. La concertation *a posteriori* prévue pour contester les décisions du HFDS consiste en un « parcours du combattant » difficile, long et très incertain (très peu de revirements). Tout en respectant la confidentialité des travaux des services de renseignement, le besoin d'explication ne peut cependant pas être éludé pour les refus d'autorisation d'accès aux ZRR.

Le rythme d'augmentation du nombre de ZRR, d'environ 20 % par an, ne laisse pas d'interroger, alors que nous sommes déjà quatre années après la création du dispositif des ZRR. En comparaison, les suppressions ne représentent que 2 à 3 % des ZRR chaque année (10 suppressions dans le champ du MESRI). Si ce rythme d'augmentation est vu comme un « succès » du dispositif par le SGDSN, nous ne savons pas s'il résulte d'une augmentation de la menace, d'une demande accrue de protection des laboratoires ou d'un durcissement du dispositif.

L'OPECST a pris acte des déclarations du HFDS adjoint des MESRI/MENJ selon lesquelles les enquêtes précédant une demande d'accès à une ZRR ne se limitaient pas à la présence de mots clés ou à la nationalité du candidat (excepté pour les États proliférants), comme cela a été critiqué par certains scientifiques lors de l'audition, mais reposaient sur une étude approfondie au cas par cas. Il prend acte du rappel selon lequel les publications des chercheurs des ZRR ne sont pas obligatoirement soumises à un régime d'autorisation préalable ; tout dépend de ce qui est prévu dans le règlement intérieur de la ZRR.

La circulaire interministérielle du 7 novembre 2012 relative à la mise en œuvre du dispositif de PPST de la nation prévoit une adhésion volontaire des laboratoires privés au régime des ZRR, les entreprises privées concernées pouvant aussi choisir de se protéger par leurs propres moyens. Pourquoi, dès lors, imposer ce dispositif aux seuls laboratoires publics ?

L'OPECST regrette que la PPST repose sur une logique binaire dans laquelle un laboratoire est soit ZRR, avec une application uniforme de toutes les contraintes sans tenir compte de la particularité des disciplines et des laboratoires, soit non-ZRR, auquel cas il est exonéré de toute discipline. Le caractère contraignant du dispositif ZRR entraîne de fait, *a contrario*, une déresponsabilisation des chercheurs travaillant dans un laboratoire non classé ZRR. La protection de type ZRR est soit trop lourde dans certains domaines (mathématiques, informatique), où trop de demandes remontent au ministère, soit pas assez forte dans d'autres (technologies de défense et de sécurité), où il faut renforcer les dispositifs de sécurité. Des règles trop lourdes conduisent systématiquement les personnes qu'elles régissent à essayer de les contourner, pour ne pas être bloquées dans leurs travaux. À l'opposé, le ministère de la défense applique des procédures plus strictes que celles des ZRR pour ses laboratoires internes ou partenaires. Une réflexion doit être menée sur l'organisation et le niveau de décision, acteurs locaux dûment informés ou centralisation au ministère. Au regard du niveau relativement bas du taux de refus

d'accès – moins de 2 % –, il serait plus efficace de se concentrer sur les cas réellement à risque que d'alourdir toutes les procédures de recrutement.

Or il existe un continuum entre les fuites « courantes » et les captations sanctionnées pénalement par la PPST : débauchage de personnel (chercheur français qui s'expatrie) ; pillage de propriété intellectuelle (inventions non protégées par des brevets, puis exploitées commercialement par des entreprises étrangères) ; vol d'ordinateur portable ; piratage informatique ; espionnage… Le cas d'un jeune chercheur français sur un sujet sensible qui trouve un poste dans une université américaine ou chinoise constitue très certainement un sujet de préoccupation en termes de protection de savoir ou de propriété intellectuelle. On peut également citer les programmes de coopération internationale des établissements supérieurs dont les contrats seraient léonins en termes de propriété intellectuelle ou qui iraient à l'encontre des engagements internationaux de la France en termes de prolifération ou d'exportation de biens à double usage. Le seul cadre des ZRR, conçu comme un territoire fermé à protéger, ne couvre donc qu'une partie des risques de captation.

Un effort en matière d'éducation sur la sécurité informatique doit être réalisé dès le collège, peut-être dès l'école primaire, pour la diffusion d'une meilleure « hygiène informatique ». La matière est déjà dans les programmes, il reste encore à la construire et à former des enseignants.

D'une analyse comparative de la pratique de PPST dans deux pays d'excellence en matière de recherche comme de protection contre l'espionnage – les États-Unis et le Royaume-Uni –, il ressort les éléments suivants : très large déconcentration au niveau des universités et des centres de recherche, permettant une souplesse de mise en œuvre adaptée à chaque cas ; information, formation et responsabilisation des acteurs plutôt que mesures contraignantes ; aux États-Unis, protection des projets pris individuellement, et non des secteurs ou des spécialités scientifiques ou technologiques déclarés « sensibles » ; absence de véritable équivalent du dispositif des ZRR (laboratoires fermés) dans les deux pays.

Propositions de l'Office

Au vu de tous ces éléments, l'Office estime que les problèmes rencontrés par les laboratoires de recherche français ne relèvent pas des seules modalités d'application du dispositif des ZRR. Il recommande en conséquence un véritable changement de doctrine, un changement d'état d'esprit, dans la mise en œuvre de la PPST.

L'Office recommande également la mise en place d'une procédure de recours interne des décisions prises dans le cadre de la création et de la gestion des ZRR. Cette procédure serait confiée à trois personnes : l'une représentant les sciences et devant être une personne à la légitimité incontestable et reconnue, habilitée confidentiel défense ; la deuxième représentant les services de l'État en

charge de la sécurité ; et la troisième avec un profil plus juridique et dont l'indépendante serait assurée.

L'Office accepte les propositions du préfet Inglebert de plus grande souplesse et plus grande concertation dans la mise en œuvre du dispositif des ZRR. La même évolution est attendue dans les autres ministères de tutelle. L'Office souhaite suivre ces évolutions en restant en contact avec la communauté scientifique et par une nouvelle audition sous forme de table ronde, dans un délai à déterminer en fonction des avancées qui auront pu être constatées mais qui ne pourrait excéder deux ans. Il s'agira alors de se prononcer sur l'opportunité ou non de demander la modification de la réglementation de mise en œuvre de la PPST au moyen des ZRR.

Pour éviter les distorsions de concurrence entre pays, une certaine harmonisation des procédures de sécurité pourrait être recherchée dans les pays de l'OCDE. L'OPECST souhaite que l'on s'inspire des pratiques aux États-Unis et au Royaume-Uni pour faire évoluer les procédures françaises de mise en œuvre de la PPST afin :

– d'adapter le dispositif des ZRR aux spécificités des différentes disciplines scientifiques avec une gradation des dispositifs en fonction des risques (ZRR+ +, ZRR– – et non ZRR) ;

– de protéger des projets sensibles, au cas par cas, plutôt que des secteurs ou spécialités au sens large ;

– de reposer sur une plus grande responsabilisation des chercheurs, avec des actions de formation et d'information, plutôt que sur des mesures contraignantes ;

– de développer une culture de sécurité de tous les acteurs pour permettre, au-delà des seuls laboratoires sensibles, une prise de conscience des enjeux de la recherche en termes de compétition internationale, de propriété intellectuelle, de valorisation de l'innovation et de défense nationale.

Seul un travail approfondi sur ces pistes de réflexion, associant chercheurs et services de sécurité, permettra l'émergence d'un consensus sur les modalités de protection, et donc sur leur mise en œuvre effective.

TRAVAUX DE L'OFFICE

I. COMPTE RENDU DES AUDITIONS SUR « LES ZONES À RÉGIME RESTRICTIF (ZRR) DANS LE CADRE DE LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION » DU 24 JANVIER 2019

M. Gérard Longuet, sénateur, président de l'Office.– Bienvenue à toutes les personnes présentes dans cette salle. C'est à l'initiative de notre premier vice-président Cédric Villani que se tient aujourd'hui cette audition publique sur les zones à régime restrictif (ZRR) dans le cadre de la protection du potentiel scientifique et technique (PPST) de la nation.

Je vais maintenant lui passer la parole pour introduire cette matinée. Je la reprendrai ensuite pour présider la première table ronde. La seconde table ronde sera présidée par Cédric Villani, qui aura également la charge de conclure nos débats.

M. Cédric Villani, député, premier vice-président de l'Office.– Je souhaite également la bienvenue à tous les intervenants des deux auditions de ce matin. Ces auditions ont pour objet un problème d'organisation de la recherche dans notre pays, qui fait partie du périmètre de compétence de l'Office.

En France, le dispositif des zones à régime restrictif (ZRR) constitue le cœur ou l'un des cœurs du régime de protection du potentiel scientifique et technique (PPST), régi par le secrétariat général de la défense et de la sécurité nationale (SGDSN), avec les hauts fonctionnaires de défense et de sécurité (HFDS) des six ministères de rattachement (recherche, défense, agriculture, écologie, finances et santé). Une organisation complexe, dont l'importance et le principe sont plus que jamais nécessaires, à une époque où les questions d'espionnage scientifique et industriel, les questions de renseignement, sont clés.

Le dispositif de PPST a pour but de protéger, au sein des établissements de recherche publics et privés, l'accès à leurs savoirs et savoir-faire stratégiques ainsi qu'à leurs technologies sensibles. Le dispositif de PPST offre une protection juridique et administrative fondée sur le contrôle des accès, physiques comme virtuels, aux informations sensibles détenues au sein de zones protégées, appelées ZRR. Celles-ci constituent des espaces définis à l'intérieur desquels se déroulent des activités de recherche ou de production stratégiques, donc à protéger en raison de l'intérêt qu'elles présentent pour la compétitivité de l'établissement ou de la nation.

Or les ZRR font l'objet de critiques significatives de la part d'une partie de la communauté scientifique française, au motif qu'elles occasionneraient des lourdeurs incompatibles avec le bon fonctionnement des laboratoires. Certaines disciplines comme l'informatique ou les mathématiques se sont exprimées collectivement et publiquement en ce sens. C'est un dossier et un mouvement que j'ai pu suivre alors que j'étais chercheur, puis directeur d'institut, avant de devenir député. C'est l'occasion de le « mettre sur la table », avec les regards croisés des uns et des autres.

Les auditions organisées par l'Office ce jour prennent la forme de deux tables rondes : l'une sur les menaces de captation de savoirs et technologies sensibles, qui est confidentielle, à huis clos, ainsi qu'il est d'ailleurs prévu par la loi de 1983 qui régit l'Office depuis sa création ; l'autre sur les procédures relatives aux zones à régime restrictif (ZRR),

qui est ouverte à la presse et retransmise sur le portail vidéo de l'Assemblée nationale. J'invite tous les intervenants à participer aux deux tables rondes, afin de favoriser les échanges et la compréhension mutuelle. Le respect des temps de parole de chacun (10 minutes pour les institutionnels, 5 minutes pour les chercheurs) permettra de consacrer un temps suffisant à la partie débat de chacune des deux tables rondes.

A. PREMIÈRE TABLE RONDE : LES MENACES DE CAPTATION DE SAVOIRS ET TECHNOLOGIES SENSIBLES

COMPTE RENDU RESTREINT

Application du VII de l'article 6 ter de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires qui prévoit que : « Les travaux de la délégation sont confidentiels, sauf décision contraire de sa part. »

M. Gérard Longuet, sénateur, président de l'Office.– Pour cette première table ronde, organisée à huis clos, ne sont donc présents dans cette salle que les intervenants, les députés, les sénateurs et les membres du secrétariat de l'Office. Le compte rendu sera soumis à chaque intervenant, qui pourra le relire et supprimer tout propos qu'il estime, pour des raisons de sécurité, ne pas devoir être porté sur la place publique.

Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) vise à protéger les savoirs, savoir-faire et technologies les plus sensibles des établissements publics et privés localisés sur le territoire national, dont le détournement ou la captation pourraient : porter atteinte aux intérêts économiques de la nation ; renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense de la nation ; contribuer à la prolifération des armes de destruction massive et de leurs vecteurs ; ou encore être utilisés à des fins terroristes sur le territoire national ou à l'étranger.

Pour répondre à ces questions, je souhaite la bienvenue à Mme Claire Landais, secrétaire générale de la défense et de la sécurité nationale, M. Thierry Matta, directeur général adjoint de la sécurité intérieure (DGSI), et M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Madame Claire Landais, vous êtes secrétaire générale de la défense et de la sécurité nationale (SGDSN), c'est une responsabilité éminente que j'ai déjà croisée dans ma vie professionnelle, notamment comme ministre de la défense. Pouvez-vous nous préciser le dispositif mis en place pour protéger le potentiel scientifique et technique (PPST) de la nation ?

Mme Claire Landais, secrétaire générale de la défense et de la sécurité nationale (SGDSN).– Merci beaucoup monsieur le président, monsieur le premier vice-président, mesdames et messieurs les parlementaires. Je ne suis pas forcément la mieux placée pour vous parler dans le détail des risques de captation, c'est pourquoi je suis accompagnée de représentants d'institutions qui sauront le faire mieux que moi, notamment MM. Thierry Matta et Guillaume Poupard, qui vous donneront des éléments précis sur les risques et les vulnérabilités.

Si vous me permettez, je voudrais d'abord vous remercier pour l'organisation de cette matinée, qui est précieuse à la fois pour le dialogue qui va pouvoir se nouer et de façon générale, pour la bonne collaboration qui existe traditionnellement entre nos deux institutions. Je suis à la tête du SGDSN depuis moins d'un an mais je comprends qu'il existe une tradition de discussion et de dialogue entre nous : drones, sécurité nucléaire, ZRR… Nous serons évidemment à votre disposition pour continuer cette coopération. Si vous en êtes d'accord et si vous êtes demandeur, je pourrai venir vous rendre compte de ce qui s'est

passé sur la sécurité nucléaire depuis quelques mois ; c'est une offre de services que je fais volontiers à l'Office. Je voudrais indiquer dans quel état d'esprit nous arrivons ce matin en disant que, probablement, le SGDSN est parfois caricaturé, comme le sont les services de renseignement avec lesquels il travaille. Nous pouvons être vus comme parties prenantes d'un appareil « sécuritaire » avec tout ce que cela emporte, et suspects d'une certaine rigidité dans le rappel à l'ordre sur les menaces et les dangers. Or notre intention est de protéger, vous l'avez dit, contre ce qui se développe aujourd'hui, ce qui se renforce : le terrorisme, mais aussi le retour de la puissance des États, les risques de la prolifération, la guerre économique et toutes les tentations de captation de données stratégiques, de savoir-faire et de technologies.

Nous sommes bien sûr là pour le rappeler, pour le détecter, pour sensibiliser à cette menace. Nous sommes là aussi pour réfléchir à des modes de protection, et parfois les imposer. Mais je voudrais dire aussi que, et c'est mon sentiment depuis que je suis arrivée au SGDSN, nous sommes évidemment aussi conscients du besoin de conciliation des impératifs sécuritaires avec d'autres, qu'il s'agisse d'impératifs de modernité, de fluidité de l'information, d'ouverture, de transparence ou de dialogue. Donc nous sommes bien conscients que l'efficacité même des dispositifs de protection contre des menaces croissantes passe par une capacité à assurer cette conciliation entre certains impératifs de défense de nos intérêts fondamentaux – les intérêts fondamentaux de la nation, comme vous le savez, sont protégés par la Constitution et doivent donc faire l'objet de mesures et de certaines politiques de protection – mais aussi d'autres impératifs, qui eux aussi peuvent avoir un fondement constitutionnel et qui méritent évidemment d'être mis en balance avec les impératifs sécuritaires.

Je prends un peu de champ par rapport à la PPST, nous le vivons dans d'autres domaines, par exemple avec le secret de la défense nationale, qui est essentiel mais qui suscite curiosité et parfois fantasme. Nous devons être capables d'expliquer pourquoi le secret sert bien au « cœur du cœur » et n'est pas dévoyé. Nous devons faire attention à ne pas utiliser la classification de façon excessive, à savoir déclassifier et à pousser un peu les choses pour être capables de donner de l'information. Nous devons donc veiller à bien cantonner le secret dans le strict champ où il est légitime. C'est aussi le cas avec la politique de sécurité des activités d'importance vitale (SAIV) et la désignation d'opérateurs d'importance vitale (OIV), auxquels on impose des sujétions en termes de protection de leur activité parce que son interruption poserait de réelles difficultés. Les textes disent qu'il s'agit d'organismes dont la continuité de l'activité est essentielle à la vie de la nation. La désignation des OIV, et aujourd'hui aussi des opérateurs de services essentiels (OSE) dans le champ cybernétique, fait partie d'une politique pour laquelle nous savons être prudents quant à la façon dont nous imposons les choses. Je trouve que nous avons bien progressé ces dernières années dans le maniement d'outils réglementaires autoritaires, et parfois alternativement d'outils de sensibilisation, de conviction et de concertation, pour faire en sorte de concilier des impératifs qui parfois peuvent être contradictoires.

Vous me voyez venir, je pense que la PPST est évidemment un des champs dans lesquels une conciliation est nécessaire entre ce besoin de protection de savoir-faire et de technologies sensibles, et la liberté de la recherche, le besoin de communication entre chercheurs, le besoin d'échange, le fait que la connaissance grandit grâce au fait que, précisément, elle est partagée. Nous en sommes d'autant plus conscients que nous pouvons avoir un dialogue avec les chercheurs eux-mêmes, ceux qui sont à la tête des laboratoires et qui savent nous aider à concilier ces impératifs.

La première fois que j'ai lu les textes réglementaires relatifs à la PPST, je les ai trouvés assez peu classiques, presqu'imprécis. Je pense aujourd'hui que cette imprécision est précisément liée à l'objectif de souplesse, avec une certaine capacité d'adaptation du

dispositif aux situations particulières. Ce dispositif a été rénové en 2012 dans un sens justement d'adaptabilité et de capacité à être aménagé en fonction des concertations qui peuvent être menées. C'est pour cela d'ailleurs qu'on trouve de la souplesse dans la désignation des secteurs à protéger en priorité, dans la désignation des technologies ou des savoir-faire particulièrement sensibles, ou dans la constitution des ZRR elles-mêmes. La concertation est présente dans cette caractérisation, dans cette identification des secteurs et des laboratoires. Ce dispositif s'applique notamment, et on y reviendra largement, aux laboratoires de recherche, mais pas seulement – aujourd'hui on compte moins de mille ZRR dans les six secteurs ministériels que le premier vice-président a indiqués –, puisque de nombreuses entreprises hébergent également des ZRR. Donc je crois que la souplesse est présente dans la conception même du dispositif.

Je remercie le préfet Inglebert, qui sera plus disert que moi sur la façon dont ce dispositif s'applique dans le champ du ministère de l'enseignement supérieur, de la recherche et de l'innovation (MESRI), avec une souplesse de mise en œuvre pour laquelle on peut encore mieux faire en simplification, en adaptation et en dialogue. Voilà le message que je voulais vous faire passer, et encore une fois je vous remercie pour cette audition. Il est certain que l'État n'a pas en propre toutes les capacités à intégrer par lui-même, par ses personnels – même si nous avons des ingénieurs, des scientifiques ou des personnes qui ont une culture économique – toute l'expertise permettant d'assurer cette conciliation. D'où le besoin d'échange, d'où l'existence dans le cas de la PPST d'un comité des experts avec des sous-commissions thématiques qui doivent être les lieux d'échanges et d'adaptabilité potentielle de ce régime.

M. Gérard Longuet, sénateur, président de l'Office.– Madame la secrétaire générale, je vous remercie, nous enchaînons avec l'intervention de M. Thierry Matta, directeur général adjoint de la sécurité intérieure (DGSI). Pouvez-vous nous présenter l'analyse des menaces et des risques : provenance, prévalence, formes ?

M. Thierry Matta, directeur général adjoint de la sécurité intérieure (DGSI).– Merci monsieur le président, permettez-moi d'abord de présenter les excuses du directeur général, qui a été requis hier par un ministre pour un déplacement à l'étranger, d'où ma présence ici pour le représenter.

Je vous remercie également de me donner l'occasion de vous présenter les grandes missions de la DGSI, surtout celles qui concourent à la protection des savoir-faire nationaux stratégiques et sensibles, qui est l'objet de notre réunion. La DGSI est le service de sécurité intérieure qui, selon les termes du décret d'avril 2014 [(1)], est chargé, sur l'ensemble du territoire de la République, de rechercher, de centraliser et d'exploiter les renseignements intéressant la sécurité nationale et des intérêts fondamentaux de la nation. Cela se décline en grandes missions. La première, qui est pour des raisons d'évidence, malheureusement, la grande priorité du service depuis quelques années, est évidemment la lutte contre le terrorisme. Elle peut partiellement recouper nos préoccupations, je saisis l'occasion de le préciser. Le contre-espionnage est notre mission essentielle, en tout cas la mission historique du service. Je mentionne ensuite notre mission de protection du patrimoine de la nation au sens large, qui est l'objet de nos échanges, avec une sous-catégorie qui a une importance toute particulière dans notre réflexion, la lutte contre la prolifération des armes de destruction massive. Et enfin nous assumons une mission de police judiciaire spécialisée, puisque nous sommes compétents avec d'autres services en matière de contre-terrorisme et que nous le sommes exclusivement en matière de contre-espionnage, de compromission du

(1) Décret du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure (DGSI).

secret, d'atteintes aux systèmes d'information des réseaux institutionnels, gouvernementaux ou OIV, de ZRR et de tout ce qui concerne la lutte contre la prolifération.

Plus précisément, notre mission de protection en matière économique est évidemment devenue ces dernières années une mission très importante sous deux angles. C'est d'abord la protection des savoir-faire et des potentiels d'innovation des entreprises et des laboratoires français, avec bien évidemment une traduction très concrète en matière économique, de préservation des emplois et de croissance du pays. L'autre dimension est, comme je le disais, la lutte contre la prolifération des armes de destruction massive – nucléaires, biologiques et chimiques – et de leurs vecteurs.

Cette mission de protection suppose, de la part du service, un suivi attentif des structures françaises, publiques ou privées, qui opèrent dans les secteurs concernés par nos préoccupations et qui pourraient être ciblées par des intérêts étrangers. C'est aussi une nécessité pour la France de respecter ses engagements vis-à-vis de la communauté internationale en matière de coopération et de lutte contre la prolifération des armes de destruction massive. Cela suppose d'assurer une veille sur les dossiers sensibles et de pouvoir être en capacité d'alerter nos autorités. En France, sont particulièrement visés par les manifestations étrangères : l'aéronautique, la filière énergétique – le nucléaire notamment –, les biotechnologies, le secteur médical, les télécommunications et les petites entreprises, parfois très petites entreprises ou jeunes pousses (*start-up*), qui sont en capacité de développer des technologies de rupture, qui sont très concurrentielles et qui intéressent nos « adversaires », selon une terminologie propre à notre service. Cela permet de bien cibler nos préoccupations.

Ces actions d'ingérence peuvent se manifester de plusieurs façons, sous plusieurs formes. D'abord une atteinte physique au patrimoine matériel ou immatériel d'établissements, par exemple tout simplement des vols. De nombreuses entreprises ou laboratoires déplorent régulièrement la disparition de documents ou de prototypes, à l'occasion de visites de délégations étrangères, mais pas seulement, puisque cela peut aussi être la conséquence de ce que nous appelons des « intrusions consenties », notamment lorsqu'un laboratoire ou une entreprise héberge un coopérant ou un chercheur étranger. Un deuxième vecteur est constitué par les intrusions dans les systèmes d'information – M. Guillaume Poupard en parlera beaucoup plus savamment que moi, ou le vol de supports informatiques. Cela peut également prendre la forme d'atteintes capitalistiques, lorsqu'une petite société est en difficulté financière et qu'elle est obligée d'accepter une prise de participation étrangère, qui peut se solder à terme par un transfert de savoir-faire et des capacités de production à l'étranger. Nous en avons connu plusieurs exemples. Pour l'enseignement supérieur et la recherche, dont nous comprenons bien la particularité, une coopération internationale dans le domaine scientifique s'avère nécessaire. Mais c'est un facteur potentiel de vulnérabilité pour nos laboratoires et nos entreprises.

Je vais rapidement vous donner quelques exemples qui me permettront de bien poser les enjeux concernant des vulnérabilités qui ont pu être exploitées par des intérêts divergents des intérêts de laboratoires et d'entreprises françaises. Nous avons eu l'exemple d'un laboratoire de recherche qui a été victime de vol de matériel hautement stratégique au sein d'une ZRR, vol de matériel qui était le produit de deux années de recherche. Les accès étaient réglementés et protégés, mais l'examen a permis de constater qu'un chercheur étranger, invité par le laboratoire pour une durée de quelques mois, avait accédé au local de stockage du matériel le jour présumé du vol, jour où le laboratoire est normalement fermé au personnel. C'est donc objectivement une faille de contrôle. Cette situation a conduit à l'ouverture d'une enquête pour livraison d'informations à puissance étrangère, dont nous avons été saisis. L'existence de la ZRR a permis de caractériser le déroulement du vol et l'exploitation de la vulnérabilité par la personne qui était hébergée par l'établissement.

Un autre exemple parlant concerne un laboratoire de recherche spécialisé en génie électrique, qui travaillait depuis plusieurs années sur un projet de brevet sur les technologies permettant d'améliorer la sûreté de systèmes industriels utilisés dans plusieurs secteurs d'activité, notamment les applications sensibles pour l'automobile, l'avionique et le nucléaire. Un doctorant étranger, qui avait été recruté pour plusieurs années au sein du laboratoire, a copié et déposé le brevet dans son pays d'origine. Faute d'action en contestation du brevet, ce pays étranger pourrait interdire de manière pérenne l'utilisation de la technologie française sur son territoire. Le laboratoire, qui était initialement classé en ERR (établissement à régime restrictif), ne disposait d'aucun dispositif de protection renforcée au moment des faits. C'est après les faits, malheureusement, que le ministère compétent a pu le convertir en ZRR.

Autre exemple, un laboratoire spécialisé dans les matériaux innovants a déploré l'accès illégal d'un étranger à plusieurs ZRR de laboratoires, qui lui étaient interdites en raison de la sensibilité des activités de recherche. Boursier de son gouvernement, cet étudiant a en fait profité des accès qui avaient été concédés à un de ses compatriotes, qui l'a fait pénétrer dans cette zone protégée ; il a utilisé plusieurs équipements scientifiques de haute technologie qui n'avaient aucun lien avec l'objet de son étude. Le dispositif de protection était en vigueur, mais l'incident relevait, je dirais, d'un problème comportemental ; si les réglementations ou les dispositifs ne sont pas mis en œuvre, ne sont pas respectés, la vulnérabilité reste entière.

Deux ou trois autres exemples rapidement. De 2006 à 2018, la DGSI a détecté à trois reprises la candidature d'un chercheur à des postes dans des laboratoires français sensibles. Ce chercheur avait été formé au sein d'une entité clé de son pays d'origine, liée à un programme balistique. Il est intéressant de constater qu'à trois reprises, ce chercheur avait fait acte de candidature dans trois laboratoires différents, en modifiant systématiquement son CV. Le nom était toujours le même, avec une volonté manifeste de dissimuler son parcours et son profil avec des études et une adresse différentes. Autre exemple, en 2018, la DGSI a détecté la présence dans un laboratoire de recherche d'un groupe de quatre stagiaires originaires d'un pays développant plusieurs programmes d'armes de destruction massive. Ces derniers se sont relayés pendant plusieurs mois au sein du laboratoire afin de capter des données technologiques sensibles, utiles pour le développement de missiles. Depuis, le laboratoire a décidé de créer une ZRR afin de bénéficier de la protection juridique et administrative adaptée.

En conclusion, je rappelle les deux axes principaux de nos préoccupations, d'une façon purement clinique, issue de l'observation objective du service. La première, évidemment, c'est la protection du savoir-faire français et du potentiel d'innovation, dans un but de protection économique pour la croissance du pays, pour servir ses capacités scientifiques, industrielles, et pour ses emplois, tout simplement. La deuxième dimension, à laquelle on ne pense pas assez, mais qui est très importante, est la dimension de contre-prolifération, puisque la réglementation PPST, notamment, est un outil permettant à la France de garantir le respect de ses engagements à l'égard des résolutions du conseil de sécurité des Nations unies, qui nous imposent de disposer d'outils juridiques nationaux permettant d'entraver la prolifération et le développement des armes de destruction massive.

M. Cédric Villani, député, premier vice-président de l'Office.– Merci beaucoup monsieur Matta. Juste une petite question qui vient directement dans la foulée de votre exposé. Est-ce que vous pouvez nous en dire un peu plus globalement, au-delà de ces exemples, sur la structure des menaces telles que vous les analysez, à travers soit des incidents avérés avec des vols, des effractions, des dépôts de brevets malhonnêtes…, soit des tentatives qui auraient pu être détectées, en fonction des secteurs et en fonction des pays, pour essayer une première classification ?

M. Thierry Matta.– Je vais passer la parole à M. Jean-Philippe Couture, sous-directeur chargé de la protection du patrimoine national et de la lutte contre les proliférations. Il y a effectivement, non pas une modélisation, ce serait présomptueux, mais des axes de recherche qui sont très clairement identifiés.

M. Jean-Philippe Couture, sous-directeur chargé de la protection économique, DGSI.– Oui monsieur le député, Thierry Matta a dit l'essentiel de ce que nous considérons comme étant des problématiques liées à nos adversaires ou concurrents dans le domaine économique et scientifique. Je pourrais dire que nous avons une responsabilité dans le suivi de la mise en œuvre des réglementations relatives à la protection du secret de la défense nationale, qui va au-delà du simple relevé d'incidents. Cela consiste aussi à sensibiliser les laboratoires : un certain nombre d'actions de sensibilisation sont menées très régulièrement par la DGSI sur la protection de l'information stratégique. Nous assumons les missions de conseil et de détection des vulnérabilités, au-delà des incidents. Lorsque nous observons des vulnérabilités dans le fonctionnement des laboratoires, qui sont liées aux coopérations internationales, nous avertissons les autorités, nous en parlons avec les laboratoires, et nous pouvons, le cas échéant, suggérer la mise en place d'une ZRR qui, pour nous, reste un dispositif extrêmement utile, dans la mesure où il nous permet de mieux caractériser les incidents que j'évoquais tout à l'heure et puis, éventuellement, de mettre en œuvre les actions judiciaires qui relèvent de notre compétence.

M. Gérard Longuet, sénateur, président de l'Office.– Pardonnez-moi car je devrais le savoir, qu'est-ce que concrètement une ZRR ? Quelles sont les contraintes pour un laboratoire public ou pour une entreprise privée ?

M. Cédric Villani, député, premier vice-président de l'Office.– Nous aurons l'occasion dans la table ronde suivante de revenir plus en détail là-dessus, mais je suis d'accord que, pour la suite de la discussion, il est bon de commencer à parler concrètement du dispositif.

Mme Claire Landais.– J'aurais dû le faire en introduction. Beaucoup dépend de la mise en œuvre pratique, mais concrètement, la ZRR est une zone à accès physique réglementé. Le dispositif des ZRR recouvre en réalité deux grands aspects. Dans cette zone, physique ou logique – quand il s'agit de protéger des systèmes d'information et des données -, l'intrusion est pénalement répréhensible, c'est une protection juridique. Le code pénal permet que des poursuites judiciaires soient engagées sur le fait même d'accéder alors qu'on n'en a pas l'autorisation. Le deuxième grand volet de la ZRR est précisément le fait que, avant un accès des personnes amenées à travailler dans la zone, l'État effectue des contrôles. C'est un mécanisme d'avis préalable qui offre une protection administrative. Cet avis n'est pas un avis conforme au sens où il est asymétrique : si le haut fonctionnaire de défense donne un avis favorable, le directeur de l'établissement peut encore dire qu'il ne souhaite pas l'accès ; mais à l'inverse un avis défavorable bloquera effectivement l'accès, dans des cas qui restent très marginaux. Mais encore faut-il que la ZRR existe pour empêcher ces cas-là, l'aspect d'auto-dissuasion fait qu'en réalité, il y a probablement des personnes qui ne demandent pas d'accès, en raison du régime d'autorisation après vérification.

M. Gérard Longuet, sénateur, président de l'Office.– L'autorisation est-elle par site ? Quels sont les effectifs concernés ?

M. Cédric Villani, député, premier vice-président de l'Office.– Combien y a-t-il de dossiers par an ?

Mme Claire Landais.– L'autorisation est par zone effectivement.

M. Xavier Inglebert, préfet, haut fonctionnaire de défense et de sécurité (HFDS) adjoint des ministères de l'enseignement supérieur, de la recherche et de l'innovation (MESRI) et de l'éducation nationale et de la jeunesse (MENJ).– Pour le périmètre du ministère de l'enseignement supérieur, de la recherche et de l'innovation (MESRI), nous représentons 60 % des ZRR des six ministères concernés. Nous avons reçu 9 400 demandes d'accès en 2018, pour lesquelles : 95 % des avis ont donné lieu à une absence totale d'objection ; 1,7 % des avis, soit 157, ont été négatifs ; et 3,5 % des avis ont été positifs sous réserve. Cette dernière éventualité est une nouveauté depuis un an, j'y reviendrai dans la deuxième table ronde, l'idée étant de négocier avec les unités en leur disant que nous sommes favorables à ce que vous acceptiez cette personne dans la ZRR, mais à condition de respecter quelques précautions d'usage que nous préconisons. Généralement, c'est accepté.

M. Gérard Longuet, sénateur, président de l'Office.– Mais le stock de ceux qui sont dans les ZRR ?

M. Xavier Inglebert.– Leur nombre total s'élève à peu près à 20 000 personnes.

Mme Claire Landais.– En dehors du MESRI, on constate à peu près les mêmes proportions. Le flux des demandes annuelles sur l'ensemble des ministères est d'environ 20 000, avec un taux moyen d'avis défavorable qui ne dépasse pas 2 %.

M. Jean-Marc Jézéquel, professeur en informatique à l'université Rennes 1, directeur de l'Institut de recherche en informatique et systèmes aléatoires (IRISA).– Si je peux me permettre de compléter ce point de vue par le ressenti du terrain, c'est qu'évidemment, même si je ne mets pas en doute tout ce qui vient d'être dit dans l'intention et dans la manière avec laquelle c'est réalisé, y compris sur les chiffres, la cascade des gens en place pour la mise en œuvre de ces règles fait que chacun essaye de se protéger, d'en « rajouter une couche ». Ce qui fait qu'à la fin, au niveau du laboratoire, dès qu'il y a une coopération internationale, dès qu'il y a le moindre aspect international, on a l'impression de ne pas pouvoir « lever le petit doigt » sans que cela remonte, au minimum au fonctionnaire de sécurité et de défense (FSD) de l'établissement, voir au HFSD du ministère, pour une coopération avec une entreprise étrangère, un déplacement à l'étranger, l'accès de stagiaires dans des locaux, etc. Ce qui génère au total, en pratique, un énorme surcoût de bureaucratie pour le laboratoire, j'y reviendrai tout à l'heure dans mon intervention.

M. Xavier Inglebert.– Je voudrais juste apporter une précision aux propos de M. Jézéquel. Un volet distinct du dispositif PPST porte sur les avis sur les programmes de coopération internationale, mais cela concerne l'ensemble des laboratoires français, ce n'est pas propre au dispositif ZRR.

M. Cédric Villani, député, premier vice-président de l'Office.– Je répète avec ténacité ma question sur les secteurs qui sont concernés : quelles applications, quelles industries, quelles disciplines scientifiques ?

M. Jean-Philippe Couture.– Je ne vais pas nécessairement entrer dans le détail, mais je vais essayer de répondre à votre question, monsieur le député. Le constat que nous faisons depuis plusieurs années, à partir d'un certain nombre d'éléments qui remontent à la DGSI, montre une constante dans les secteurs d'activité économique et industrielle qui sont visés par nos concurrents et adversaires. En premier, lieu la filière nucléaire est un sujet d'intérêt constant pour un certain nombre de pays qui cherchent à profiter du constat qu'ils peuvent faire d'une relative perte de compétitivité française dans ce domaine et qui cherchent eux-mêmes à monter en compétences. C'est vrai avec deux pays avec lesquels nous coopérons, mais qui ont recueilli depuis plusieurs années, au travers des coopérations justement, un certain nombre de données techniques et technologiques qui leur ont permis de

monter en puissance et de venir concurrencer directement la filière française. Ces acteurs peuvent être asiatiques ou occidentaux, bien entendu.

Le deuxième secteur que nous considérons comme particulièrement exposé aux agressions extérieures est celui de la filière de l'industrie aéronautique, spatiale, de défense et de sécurité, prise dans sa globalité. Un certain nombre de dossiers très actuels montrent à quel point des industriels de premier plan au niveau européen, notamment, peuvent être déstabilisés par un certain nombre d'actions venant de l'étranger. Dans le domaine de l'espace, dont je ne suis pas un spécialiste, je vois bien aujourd'hui que son « arsenalisation », la montée en puissance de capacités militaires dans ce domaine, l'excellence de l'industrie française, suscitent un certain nombre de convoitises et qu'elle expose nos entreprises aux intérêts étrangers.

Pour la filière des technologies de l'information et de la communication (TIC), là aussi M. Guillaume Poupard connaît le sujet mieux que nous, un certain nombre de petites entreprises, de jeunes pousses, sont particulièrement compétentes ; elles sont, là aussi, très exposées aux agressions étrangères. D'une manière générale, les technologies liées à la 5G, qui n'est pas encore mise en place, mais qui le sera demain ou très prochainement, donnent lieu à des enjeux extrêmement forts pour des acteurs étrangers.

Et puis, bien entendu, pour revenir au cœur du sujet, la recherche française est particulièrement exposée parce qu'elle est excellente dans la plupart des domaines. Je fais à nouveau référence à ce que disait M. Thierry Matta en matière de lutte contre les prolifération d'armes de destruction massive, une action internationale très déterminée est mise en œuvre par un certain nombre de pays, elle vise à contrarier et à entraver des filières d'acquisition de biens à usage dual. Aujourd'hui, on observe qu'un certain nombre de chercheurs étrangers qui servent des programmes de pays proliférants, viennent pour essayer de rééquilibrer les choses ou d'acquérir des connaissances, essayent d'intégrer des laboratoires français sur un certain nombre de sujets qui peuvent servir à alimenter ces programmes.

M. Gérard Longuet, sénateur, président de l'Office.– Nous avons évoqué les systèmes d'information, nous avons la chance d'avoir M. Guillaume Poupard. Pouvez-vous nous indiquer quels sont les risques pour les systèmes d'information ?

M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).– Merci beaucoup. Certains d'entre vous m'ont déjà entendu raconter la litanie de menaces numériques qui pèsent sur nous, mais je vais le refaire encore une fois, j'en suis désolé. Je vais le faire de manière croissante, en allant du plus faible au plus fort, comme je le fais habituellement. Je commence par la malveillance générale à laquelle tout le monde est exposé dans le monde numérique, que ce soit professionnellement ou personnellement, avec juste une anecdote. La semaine dernière, est apparu un fichier contenant 772 millions d'adresses de messagerie électronique piratées, avec de nombreux mots de passe associés. J'ai eu moi-même une mauvaise surprise concernant mon adresse personnelle… Cela, simplement parce que nous passons notre vie sur internet. Ceux qui achètent sur internet doivent constamment ouvrir des comptes et créer un mot de passe, donner leur nom, leur adresse de messagerie électronique, leur adresse, pour être livrés un jour. Tout cela évidemment fuite car c'est ciblé par des attaquants, cela circule sur internet et je ne parle même pas de *Darknet*, mais simplement d'internet. Il faut faire avec, j'en parlerai un tout petit peu dans une deuxième partie.

La deuxième chose qui peut affecter des laboratoires de recherche, on a eu des cas, c'est le fait que la puissance de calcul aujourd'hui a une valeur, c'est même une valeur qui se monétise, notamment dans le cadre de ce qu'on appelle le minage de Bitcoin (*Bitcoin*

mining). Ces monnaies informatiques nécessitent une puissance de calcul massive ; d'ailleurs, un jour il faudra faire le bilan écologique de tout cela, c'est catastrophique.

M. Cédric Villani, député, premier vice-président de l'Office.– Nous l'avons fait, le sénateur Ronan Le Gleut ici présent était corapporteur d'une étude qui portait sur ce thème, et ses conclusions ne sont pas joyeuses.

M. Guillaume Poupard.– Nous sommes bien d'accord. Beaucoup de laboratoires disposent d'une capacité de calcul, par définition, et on voit des attaquants qui prennent pied dans ces réseaux, pour faire du minage. Pour la victime, l'impact est normalement limité, puisqu'en fait les attaquants utilisent la puissance de calcul que vous n'utilisez pas, ils essayent d'être discrets pour pouvoir y rester. Enfin si je peux prendre une comparaison un peu osée, c'est un peu comme si des gens entraient chez vous la journée pendant que vous n'êtes pas là pour aller prendre une douche et se faire à manger. C'est assez désagréable, mais ce qui peut se passer ensuite est inquiétant.

Le troisième effet, toujours lié à la malveillance générale, qui n'est pas spécifique aux laboratoires de recherche, est le développement de cybercriminalité, tout à fait organisée, qui vise à rançonner les victimes. Nous avons un nombre de cas absolument incroyable. On peut être rançonné de différentes manières. Vous pouvez l'être par de l'escroquerie astucieuse, avec par exemple des mails de chantage. Le nombre de personnes qui sont ciblées est incroyable. C'est très facile à faire et si une personne sur mille accepte de payer la rançon, qui aujourd'hui tourne en général autour de quelques centaines voire quelques milliers d'euros, au final, à l'échelle mondiale, en utilisant cette base de données de 700 millions d'adresses de messagerie, cela fait beaucoup d'argent. Il y a toute une mécanique d'escroquerie qui se développe autour de ça.

L'autre exemple, qui peut avoir beaucoup plus de conséquences, est ce qu'on appelle les *ransomwares*, ou « rançongiciels ». C'est la version moderne des virus que l'on connaît depuis toujours ; ce sont des virus qui se propagent, qui chiffrent les données, qui les bloquent, qui les rendent inaccessibles aux utilisateurs, et qui proposent de donner les clés de déchiffrement en échange d'une rançon, là encore, de quelques centaines, quelques milliers d'euros. Dans le meilleur des cas, ça fonctionne bien, c'est-à-dire que, quand on paye, on récupère ses données. Mais dans le pire des cas, qui est fréquent, ça ne fonctionne pas, donc vous payez, mais ensuite vous ne récupérez rien. Nous avons eu des cas très graves. C'est très proliférant, on trouve parmi les victimes des entreprises, probablement des laboratoires aussi, mais je n'ai pas de statistiques. Et même en cherchant à payer la rançon – on dit qu'il ne faut pas le faire, mais enfin, on peut comprendre la tentation – elles n'arrivent pas à récupérer leurs données. Des PME ont mis la clé sous la porte suite à des attaques comme celles-là, notamment au printemps 2017. Le secteur de la recherche n'est pas plus à l'abri que les autres de cette malveillance générale.

M. Cédric Villani, député, premier vice-président de l'Office.– Pardon, désolé d'interjeter, pourquoi au printemps 2017 ?

M. Guillaume Poupard.– Parce qu'on y a eu deux vagues d'attaques qui ont été particulièrement virulentes. Tout cela est très compliqué, c'est volé puis réutilisé, c'est extrêmement proliférant. La première attaque, qu'on a appelé *WannaCry*, a touché des cibles de manière très aléatoire. En France, des chaînes de montage chez Renault, par exemple, ont été bloquées pendant plusieurs jours. Économiquement, cela peut vite peser très lourd. En Allemagne, ce sont les chemins de fer qui ont été touchés, avec des messages de demande de rançon qui s'affichaient sur les quais des gares à la place des horaires… C'est très anxiogène. Mais de façon encore plus grave, le système de santé britannique, le *National Health Service* (NHS), a été complètement paralysé. Mon homologue savait que le système

était faible, mais là, pour le coup, il a été complètement bloqué : les ambulances ne fonctionnaient plus, la planification des hôpitaux ne fonctionnait plus… Il y aura jamais de bilan complet : un bilan financier a été dressé, autour de 90 millions de livres, mais on ne fera jamais de bilan humain, évidemment, au moins publiquement, il y a probablement eu des décès prématurés. Quand les systèmes d'hôpitaux fonctionnent mal, c'est plus compliqué de soigner les gens, surtout aux urgences.

L'autre exemple est arrivé un mois après avec ce qu'on a appelé *NotPetya*, là c'est l'Ukraine qui a été ciblée, avec quelque chose qui ressemblait à du rançonnage, mais qui en fait était simplement destructif. L'Ukraine était ciblée, mais certains de ceux qui avaient un pied en Ukraine, ou seulement un orteil, ont aussi été contaminés. Saint-Gobain en effet a perdu 80 millions d'euros de résultat net en l'espace de quelques jours. D'autres acteurs à travers le monde également, qui n'étaient pas ciblés par l'attaquant, l'ont été car ces réseaux ne s'arrêtent pas aux frontières : des pharmaciens, des transporteurs maritimes, qui ont perdu énormément d'argent, et ça aurait pu être bien plus grave. Ce genre de choses est très proliférant, très contaminant, quand c'est mal géré par l'attaquant lui-même.

La deuxième menace est l'espionnage. L'espionnage est extrêmement complexe parce que personne ne veut en parler. Les attaquants, évidemment, font tout pour être très discrets, parce que l'intérêt d'entrer dans un système est également d'y rester, pour récupérer l'information au fil de l'eau. Si on ne les cherche pas, on ne les voit pas en général, c'est en apparence indolore. Les victimes ne veulent pas non plus en parler, parce que ce n'est pas glorieux, cela remet en question les relations de confiance avec des partenaires, avec des clients, dans un contexte de concurrence. Je suis allé voir des comités de direction (*comex*) très vite après la détection de telles attaques. Leur réaction en général est qu'il ne faut surtout pas en parler parce que, si ça se savait, cela ferait perdre 10 % en bourse et rendrait opéable, cela ferait échouer telle opération de fusion acquisition… Ces préoccupations sont des effets collatéraux, indépendamment de l'effet direct de l'espionnage, qui est la perte de savoir-faire ou de compétitivité.

Nous-même n'en parlons pas non plus, en tout cas pas autrement qu'en termes très génériques, comme je le fais ici, parce que notre rôle est d'aider les victimes, il n'est pas de les enfoncer. Donc c'est un sujet qui est totalement sous-estimé dans la conscience collective parce qu'on en parle peu, on a peu d'exemples, peu de cas qui sont mis en exergue, ce n'est pas visible. Et pourtant les effets sont probablement à long terme très importants. Pour donner une idée, 95 % des opérations que nous menons sont causées par l'espionnage, et quand nous menons une opération, c'est que c'est vraiment grave en termes de sécurité nationale, typiquement dans les secteurs que mentionnait la DGSI.

La dernière menace que je voulais mentionner, qui est de loin la plus inquiétante pour nous, est l'usage d'attaques informatiques contre des systèmes, non pas pour voler de l'information ou pour chercher à extorquer de l'argent, mais bien pour porter atteinte au fonctionnement de ces systèmes. Et là, on ne parle plus de la bureautique, on ne parle plus de capacités de calcul, on parle de tout ce qui gère aujourd'hui, ce qu'on appelle la gestion technique de bâtiments (GTB), informatique bâtimentaire, informatique de gestion, informatique industrielle. Là évidemment, des laboratoires sont directement concernés, des laboratoires qui ont des activités potentiellement dangereuses, certains ont des représentants ici, dans les domaines liés à tout ce qui est virologie, tout ce qui est chimie dangereuse, bref tout ce qui peut exploser, contaminer… Dans ces systèmes, aujourd'hui, il y a des automates, c'est-à-dire des équipements qui avant étaient électromécaniques mais qui sont désormais informatisés. On trouve des petits ordinateurs un peu partout, tout cela s'interconnecte, c'est pour ça que ça marche bien et que c'est particulièrement pratique. Souvent ça s'interconnecte à l'extérieur des labos eux-mêmes, vers les fournisseurs, vers ceux qui administrent, vers l'internet. C'est très pratique, mais objectivement ça crée des risques très

nouveaux qu'il faut vraiment prendre en compte. Je ne veux pas citer d'exemple trop précis pour ne pas être stigmatisant, mais on voit très bien tout ce que peut faire un attaquant qui prend le contrôle de ces automates, il peut faire fonctionner ces systèmes de manière totalement non conforme et provoquer des catastrophes. S'il y avait finalement un seul point où je voudrais vraiment attirer votre attention, c'est celui-là, parce qu'il peut avoir des conséquences absolument dramatiques pour les gens qui travaillent dans le laboratoire, et pour l'extérieur. On ne parle plus du tout d'espionnage, mais vraiment de sécurité des personnes et des biens, comme on dit pudiquement.

Je voudrais mentionner trois éléments, sur les solutions et la manière avec laquelle l'ANSSI envisage les choses. Premièrement on parle de socle de base de règles d'hygiène informatique. La plupart des gens se comportent sans le savoir, sans penser à mal, de manière totalement inconsciente, inconséquente. Donc devraient être vraiment acquis par la grande majorité d'entre nous une hygiène de base, une prudence de base, des réflexes.

Deuxièmement, la sécurité numérique ne doit pas être un dogme, elle ne doit pas être rigide, elle doit avant tout s'appuyer sur l'analyse des risques. Une fois que l'analyse de risque est effectuée, on sait se protéger avec des règles que l'on va retrouver dans les mesures liées à la PPST ou pour les ZRR. Il faut bien toujours se demander : de quelles règles ai-je besoin ? De quelle démarche ai-je besoin ? De quels efforts ai-je besoin pour me protéger et contre quoi ? Toute approche trop automatique et dogmatique est vouée à l'échec.

Troisièmement, la sécurité ne peut fonctionner que si on associe les gens qui doivent devenir des acteurs de cette sécurité, qui ne sont pas les experts de la sécurité justement. Tant qu'on opposera les utilisateurs à ceux qui veulent faire de la sécurité, ce sera pénible pour tout le monde et ce ne sera pas efficace. Quand, au contraire, tout le monde avance dans la même direction, cela a vocation à être efficace et beaucoup plus compréhensible par tous. Je vous remercie.

M. Cédric Villani, député, premier vice-président de l'Office.– Merci beaucoup, on revient ici sur le sujet, qui avait déjà été évoqué il y a quelques instants, de la sensibilisation et sur cette idée majeure qui est l'une des motivations de cette table ronde : tant que les acteurs, ceux qu'il faut protéger et ceux qui sont responsables de la protection ne seront pas alignés, il y aura conflit, et qui dit conflit dit fragilisation, en raison de procédures qui ne sont pas respectées et de contournements. C'est bien de cela qu'il faut parler, si le processus est bon sur le papier, mais pas appliqué sur le terrain, c'est qu'il est mauvais en fait.

M. Gérard Longuet, sénateur, président de l'Office.– Je vous propose de donner la parole à ceux de nos collègues qui souhaitent la prendre, et puis on lancera le débat. Ronan Le Gleut est sénateur représentant des Français de l'étranger, il a beaucoup travaillé notamment sur les chaînes de blocs *(blockchains)* et sur les cryptomonnaies (Bitcoin…).

M. Ronan Le Gleut, sénateur.– Merci monsieur le président, ma question n'est pas relative aux chaînes de blocs, mais plutôt à la définition des acteurs qui mènent la cyberguerre, d'une certaine manière. J'imagine qu'il est particulièrement difficile de les identifier, mais ma question n'est pas tellement de savoir qui sont les *hackers* (pirates informatiques), individuels ou groupusculaires, mais est-ce que des organisations plus importantes, voire paraétatiques ou proches d'un gouvernement, mèneraient une véritable guerre contre d'autres intérêts nationaux ?

M. Guillaume Poupard.– Je n'aime pas le terme de *hacker*, parce que pour moi ce n'est pas péjoratif dans le sens anglo-saxon du terme, je prendrai le terme de « pirate » ou d'« attaquant » ; l'image de l'étudiant surdoué qui fait ça dans sa chambre et qui attaque le

Pentagone a pu exister, c'est vrai, il y a longtemps, mais aujourd'hui c'est beaucoup moins romantique. On a en effet affaire à des organisations qui se structurent. Les mafias, typiquement, ont tout à fait compris que le sujet numérique était intéressant pour elles, parce que les risques sont faibles et que ça rapporte gros. L'équation économique est très intéressante pour eux. On sait très bien que, quand bien même on arriverait à les identifier – je vais y revenir, c'est extrêmement difficile –, les processus de coopération internationale, d'extradition pour des faits d'attaque informatique ne sont pas encore en place.

Donc, pour les mafias, c'est vraiment optimal, elles développent ce type de pratiques. Celles qui viennent du trafic de drogue, la DGSI connaît ça bien mieux que moi, s'orientent notamment vers les rançongiciels, qui sont des extorsions de fonds par voie numérique. Les États développent également des capacités offensives très fortes, ce n'est pas forcément péjoratif puisque la France elle-même développe une capacité militaire dans le domaine numérique. Les conflits de demain auront lieu, au moins en partie, dans le cyberespace, c'est l'évolution, il n'y a pas forcément à porter de jugement là-dessus. Ce qui peut varier d'un État à l'autre, c'est clairement l'éthique, les valeurs et l'usage qui peuvent être faits de ces capacités offensives. On sait que certains États n'hésitent pas à utiliser l'arme informatique pour faire de l'espionnage, notamment à des fins économiques.

Les missions des services de renseignement sont variables d'un pays à l'autre. Certains États n'hésitent pas à utiliser l'arme informatique pour contribuer à la guerre de l'information qu'ils mènent. Cela fait écho à des sujets plus compliqués de type infox *(fake news)*, manipulations de l'opinion publique, notamment lors d'élections. Et puis, avec ce que l'on observe dans la « vraie vie », la frontière est très marquée dans des pays démocratiques, mais elle l'est beaucoup moins dans certains autres. Certains États utilisent des groupes criminels, un peu comme une sorte de réserve opérationnelle. La frontière entre les services étatiques et les groupes criminels est floue. Je ne cite personne parce que ce n'est pas mon métier, mais on peut imaginer à qui je pense.

Donc c'est assez variable, et cela pose de façon récurrente la question de l'attribution, pour savoir qui est derrière l'attaque. En général on sait qui est derrière les grandes attaques dans ce que l'on traite à l'ANSSI, avec nos partenaires de la DGSI et de la DGSE, avec les armées, avec les différents services, avec de plus en plus la justice. Il est plus compliqué de mettre sur la table des preuves recevables pour le juge, devant une juridiction, parce que nous n'avons en général que des faisceaux d'indices. Chaque indice pris individuellement peut être manipulé. Dans le domaine informatique, il est assez facile de faire porter le chapeau à d'autres, nous connaissons beaucoup d'exemples. Le fait par exemple d'introduire dans les codes ou logiciels malveillants des commentaires en cyrillique – c'est un grand classique –, n'est pas très compliqué à faire. Évidemment tous les attaquants y ont pensé. Les attaquants eux-mêmes laissent de faux indices pour essayer de brouiller les pistes. L'attribution n'est pas immédiate du tout, il faut faire très attention. Malgré cela, on y arrive en général, quand on voit ce qui est ciblé, l'intérêt que ça peut représenter, tout un faisceau d'indices jusqu'à des choses très bêtes que j'illustre dans l'exemple suivant : avec certains pays, on sait qu'à Noël, on est tranquille pendant 15 jours. Mais face à un juge ce n'est pas une preuve matérielle. Donc en général on sait qui est derrière, mais apporter la preuve irréfutable est extrêmement difficile.

Dernière chose, je pense qu'il faut se poser la question de le dire publiquement ou pas. Si le but est de faire cesser les attaques, de faire baisser la conflictualité, parfois il est plus efficace d'en parler, de manière très ferme, mais dans un contexte fermé. Si on le fait dans un contexte public, cela force à la mauvaise foi.

M. Bruno Sido, sénateur.– J'ai une question double. D'une part, n'est-il pas possible de cloisonner cette informatique ? Tout arrive sur la toile et devient fragile. Pourquoi alors y met-on tout ? Je suppose qu'en matière de défense, par exemple, – mais vous ne pourrez pas me le confirmer – le bouton rouge pour lancer la bombe atomique n'est pas sur la toile, j'espère que non. Deuxièmement, n'est-il pas possible de tuer, informatiquement bien entendu, les attaquants ? Y a-t-il un programme au sein du ministère de la défense, de la DGSE, de la DGSI, qui « tuerait » informatiquement ces attaquants ?

M. Guillaume Poupard.– S'agissant du cloisonnement, dans les cas extrêmes, on impose bien sûr des réseaux qui ne sont pas connectés à l'internet, qui sont cloisonnés, qui sont fermés, dont l'accès est strictement contrôlé. Mais ce qu'il faut bien voir, c'est que ça ne peut être réservé qu'à des cas extrêmement limités. Tout l'intérêt d'un système d'information moderne, et ça fait un certain temps que ça dure, c'est justement d'être capable de fonctionner en interconnexion et en échange avec l'extérieur. Aujourd'hui, je ne connais plus beaucoup de systèmes d'information qui fonctionnent sans avoir une interface assez forte avec l'extérieur. Deuxièmement, parfois, on a l'impression de faire des réseaux cloisonnés, des réseaux fermés, mais en fait ce n'est pas cloisonné si vous passez votre temps à entrer et sortir avec des clés USB. On peut donc avoir un faux sentiment de sécurité. Nous avons observé de manière courante que les attaquants savent passer par des canaux qui ne sont pas des canaux de connexion directe. Cela prend un peu plus de temps, cela induit de la latence, mais en pratique, cela marche tout aussi bien. Je cite un exemple qui est public, c'est celui d'un logiciel malveillant *(malware)*, d'un virus qu'on a appelé Stuxnet, qui a manifestement ciblé des sites nucléaires iraniens. Ce virus a mis à mal le programme des centrifugeuses iraniennes, qui était pourtant complètement déconnecté. Il a fait cela pendant trois ans, en passant par des clés USB. L'isolement *(air gap)*, la coupure, avaient été franchis par le fait qu'il y avait des échanges. Je m'en méfie beaucoup, parce que, pour la plupart des partenaires avec qui nous travaillons, il est extrêmement compliqué d'expliquer qu'il faut fermer leur réseau, car cela va complètement à l'encontre de leurs besoins. Il faut tenir compte de cet aspect fonctionnel. Et puis, d'un point de vue technologique, on peut parfois résister, mais l'informatique en nuage *(cloud computing)* consiste précisément à supprimer les frontières.

Toute la difficulté de notre métier aujourd'hui est de savoir comment faire pour accompagner cette évolution technologique. Quand on explique aux gens que l'informatique est dangereuse, et qu'ils pensent qu'on veut les ramener au Moyen-Âge, évidemment ils ne nous entendent pas, c'est tout à fait naturel. L'idée est de voir comment on peut aller ensemble vers un usage raisonné de ces nouvelles technologies, comment, parfois, il faut accepter de ne pas aller trop loin dans cette ouverture et dans ce partage. C'est un équilibre. Comme je le disais un peu tout à l'heure, si on l'impose aux gens sans leur expliquer, ça ne marche pas, il faut vraiment que nous soyons capables de définir des solutions ensemble.

M. Gérard Longuet, sénateur, président de l'Office.– Monsieur Poupard, je souhaiterais vous interrompre, non pas à cause de l'horaire, bien qu'il faille en tenir compte, mais pour une question précise sur les ZRR. En tant que patron de l'ANSSI, est ce que vous êtes associé à la mise en place de ces zones ? Avez-vous un contrôle particulier sur l'informatique de ces zones ?

M. Guillaume Poupard.– L'ANSSI est associée à la définition générale des règles. Ensuite, par zone, on avise s'il faut faire cette analyse. Je pense que certains systèmes parmi les plus critiques, notamment les systèmes industriels, les systèmes de GTB (gestion technique de bâtiments), méritent un cloisonnement physique réel, sans lien avec l'extérieur. Par exemple, dans un laboratoire biologique sensible, le contrôle de la pression intérieure est probablement assuré par un automate. C'est tellement critique que ça ne devrait pas être

connecté à l'internet. Cet exemple est un peu trivial, mais on en trouverait plein d'autres. L'ANSSI n'a cependant pas les moyens d'aller visiter chacune des ZRR.

M. Gérard Longuet, sénateur, président de l'Office.– Disons les choses plus précisément, en tant que patron de cette agence, est-ce que vous êtes amené à donner des préconisations ou à examiner une situation ?

M. Guillaume Poupard.– L'ANSSI donne des préconisations génériques et publiques, mais cela mérite probablement une adaptation au cas par cas. Dans certains cas, l'agence est amenée à faire des audits, à aller sur site pour accompagner des gens qui veulent se sécuriser, ou des gens qui veulent comprendre quel est leur niveau réel de sécurité.

M. Gérard Longuet, sénateur, président de l'Office.– Pouvez-vous préciser dans quels cas ? Je veux dire qui déclenche ?

M. Guillaume Poupard.– C'est variable, cela peut être par le SGDSN, par le ministère, par un laboratoire directement, cela peut aussi être suite à un problème observé. L'ANSSI a une capacité d'inspection des administrations, mais pour les ZRR elle est plutôt dans une logique d'accompagnement et d'aide offerte.

M. Gérard Longuet, sénateur, président de l'Office.– Par exemple, est-ce qu'il y a une coordination ? Imaginons que la DGSI identifie un scientifique membre d'une organisation terroriste ou extrémiste étrangère dans tel ou tel laboratoire : est-ce qu'on va vous demander de faire un approfondissement de la situation du système informatique dudit laboratoire où voulait accéder le scientifique ?

M. Guillaume Poupard.– Le scénario pourrait se présenter, mais je pense qu'il ne faut pas attendre d'avoir un scientifique avec un tel profil pour se préoccuper de tester la sécurité d'un laboratoire, ce n'est pas vraiment comme cela que ça se passe en pratique. Nous avons quelques cas où en effet nous pouvons être requis pour accompagner des services d'enquête ou des services plus professionnels.

M. Thierry Matta.– Monsieur le président, si nous identifions un tel profil, il n'entrera pas dans le laboratoire. La question est censée ne pas se poser.

M. Gérard Longuet, sénateur, président de l'Office.– Une fois que vous avez identifié qu'une personne avait pénétré dans un laboratoire alors qu'il aurait été préférable qu'elle n'y soit pas, demandez-vous à l'ANSSI de vérifier si, par ailleurs, elle n'aurait pas branché toutes sortes de choses, pour que le travail humain soit doublé par un travail informatique ?

M. Thierry Matta.– Si la direction du laboratoire en est d'accord, il n'y a pas d'objection de principe.

M. Xavier Inglebert.– Le cas a pu arriver, on a exclu la personne de la ZRR. On a pu aussi découvrir après coup qu'une personne…

M. Gérard Longuet, sénateur, président de l'Office.– On ne regarde pas l'informatique de la ZRR ?

M. Xavier Inglebert.– Comme on l'a dit ce matin, ça dépend du directeur de l'unité, du responsable de l'établissement, j'aurai l'occasion d'en reparler. Les ZRR sont portées par les établissements, universités ou organismes de recherche.

M. Cédric Villani, député, premier vice-président de l'Office.– De ce que je comprends, il y a un sujet qui est la qualité du réseau humain local d'experts en cybersécurité dans l'ensemble de ces laboratoires. C'est un enjeu fondamental, au-delà de

savoir quelle est la qualité de l'agence qui chapeaute, coordonne l'ensemble et édicte des règles.

M. Guillaume Poupard.– C'est exactement cela, d'où ma gêne. Il est hors de question que l'ANSSI fasse le tour de l'ensemble des ZRR, ce n'est pas une question de bonne volonté, c'est une question de moyens. Cela ne peut fonctionner, comme le dit Cédric Villani, que par une prise de conscience et une implication locale. Ce n'est certainement pas l'ANSSI – ou un autre service de l'État – qui pourrait faire cela tout seul, ce ne serait d'ailleurs pas justifié.

Pour répondre à la question de « tuer les attaquants », nous disposons de toute une palette de réactions possibles, la loi a été adaptée en ce sens. Ce qu'il faut savoir, c'est qu'en général, quand vous êtes attaqué, les machines qui se connectent et vous attaquent sont elles-mêmes des victimes. L'attaquant agit rarement directement sur sa victime, ou alors c'est un très mauvais attaquant. Donc il commence par attaquer un premier, puis un deuxième, puis un troisième, comme dans les films, et à la fin sa victime finale. Il faut faire très attention dans la réaction. Légalement, on peut se connecter à l'attaquant pour comprendre ce qu'il fait et le caractériser. Dans les cas les plus graves, on peut même neutraliser l'attaque, ce qui ne veut pas dire le tuer, mais au moins, peut-être, arrêter certains serveurs, avoir un effet actif. Quand c'est relativement simple à faire, l'ANSSI le fait, quand ça devient beaucoup plus compliqué, et qu'il peut y avoir des conséquences, on fait plutôt appel aux capacités offensives, Il y a un lien, une continuité, mais nous avons des missions totalement séparées. Dans l'avenir, globalement en France, on ne s'interdit pas d'utiliser l'arme informatique – ou d'autres – pour contre-attaquer, je n'aime pas trop le terme, pour opposer une résistance, une réaction, face aux attaques les plus critiques.

M. Cédric Villani, député, premier vice-président de l'Office.– Notre collègue Mme Valéria Faure-Muntian souhaite la parole, je précise qu'elle est une députée très active, en particulier sur les questions du numérique. Elle était également aux côtés de Ronan Le Gleut sur le rapport sur les chaînes de blocs que j'évoquais tout à l'heure.

Mme Valéria Faure-Muntian, députée.– Merci Monsieur le vice-président. J'ai plusieurs questions. Tout d'abord, je voulais compléter celle du président, on a d'un côté les OIV et de l'autre les ZRR. Est-ce que, par moments, cela se recoupe ? Est-ce que, même si vous n'allez pas faire le tour de l'ensemble des ZRR, cela a un sens de les regrouper ? Dans votre discours à tous, il ressort que l'humain est le maillon faible de la sécurité, informatique ou physique. Donc est-ce qu'il n'y a pas un souci de formation et d'explication ? Est-ce qu'on ne devrait pas l'approfondir, sachant qu'aujourd'hui, le ministre de l'éducation nationale, en coopération avec le secrétaire d'État au numérique, met en place un certain nombre de formations technologiques et numériques dès le collège, puis le lycée ? Est-ce que la sécurité, et la sécurité numérique en particulier, ne seraient pas des sujets à inclure ? On en a déjà parlé à plusieurs reprises, M. Poupard estime qu'on est encore au XVII^{e} siècle en termes d'hygiène numérique, est-ce qu'on ne devrait pas en faire plus ? Juridiquement, au niveau national et international, est-on à la hauteur pour poursuivre les intrusions physiques et numériques ? Ou alors y aurait-il un arsenal à développer, aux niveaux national et international, pour améliorer nos capacités à poursuivre en justice ces criminels, qui essaient de détruire ou voler un certain nombre de données ?

S'agissant de la présence des étudiants étrangers, nous ouvrons de plus en plus de droits aux scientifiques étrangers pour les attirer, pour travailler en France. En amont de l'acceptation de leur visa ou de leur contrat, ne devrait-on pas s'interroger sur qui ils sont et d'où ils viennent ?

Une dernière question sur l'accès aux ZRR : pour combien de temps est-il autorisé ? Est-ce qu'on contrôle régulièrement, comment surveille-t-on dans la durée, sachant que la personne peut soit rester endormie pendant longtemps et s'activer plus tard, soit être un ressortissant français qui est embrigadé ou payé pour faire une action ? On a évoqué la question du terrorisme, un rapport a été récemment réalisé sur la présence de personnes radicalisées dans les services sensibles de l'État. Le même problème n'existerait-il pas dans les ZRR ? Est-ce qu'on « rebrasse le stock » pour apprécier l'évolution de la personnalité de ceux qui y ont accès ?

Mme Claire Landais.– Si vous le permettez, je vais réagir sur l'aspect des éventuels recoupements des législations OIV et PPST. C'est possible, les champs de la défense et de l'économie, par exemple, comportent des opérateurs, parfois privés, qui peuvent être soumis à un régime OIV et aussi avoir mis en place des ZRR. Pourquoi cela peut-il coexister avec des finalités différentes ? La législation sur les OIV protège la continuité d'activité de certains opérateurs critiques, alors que, comme on l'a vu, la PPST protège l'intégrité de savoirs et de technologies. Le recoupement peut parfois induire le besoin de se caler sur la protection la plus importante, d'autres fois au contraire permettre une certaine souplesse. Par exemple, dans le champ OIV, c'est seulement une faculté que de pouvoir bénéficier des capacités de criblage des services de l'État pour l'accès à certains points d'intérêts vitaux (PIV), qui sont la déclinaison en leur sein de la matérialisation de certains aspects particulièrement critiques. Au contraire, l'accès aux ZRR, comme on l'a vu, implique nécessairement qu'il y ait cette vérification du passé, des antécédents et de l'honorabilité des accédants.

Sur la capacité à revisiter ces profils, l'autorisation est délivrée pour cinq ans en principe, dans la limite de la durée du contrat de travail. Il n'y a pas d'automaticité pour revisiter l'autorisation. En revanche, bien sûr, les services de renseignement font preuve d'une vigilance particulière, qui les conduira éventuellement à surveiller davantage et donc à accroître la fréquence des contrôles, comme d'ailleurs pour la radicalisation des agents publics. Dans certains domaines, ils pratiquent ce qu'on appelle le rétro-criblage, c'est-à-dire une automaticité de réexamen de certains « stocks » de personnel. À l'inverse, pour d'autres domaines où le besoin de systématisation des contrôles à échéance régulière n'est pas avéré, cela dépend davantage de signaux déclencheurs de vérification.

M. Guillaume Poupard.– Sur la question de l'humain, je suis entièrement d'accord, on en a souvent parlé. La question de la sensibilisation est une nécessité, parce que l'hygiène informatique n'est pas intuitive, elle doit être expliquée. Surtout, il faut faire appel à l'intelligence : imposer des règles qui seraient mal comprises serait vraiment voué à l'échec. Il faut vraiment expliquer aux gens ce qui est dangereux, ce qu'on peut ou ne peut pas faire. Il faut les rendre véritablement acteurs, plutôt que simplement victimes de ces règles de sécurité.

La question de la formation est suivie par les instances de gouvernance au plus haut niveau. Elle est déjà incluse dans les programmes scolaires, mais elle n'est pas réellement enseignée en raison d'un problème de matière et d'enseignants. Nous avons fait la moitié du chemin, nous travaillons en ce moment, notamment avec le laboratoire d'innovation du ministère de l'éducation nationale, pour construire cette matière d'enseignement, pour être capable de véritablement l'enseigner. Cela commence clairement dès le collège, certains disent même dès le primaire, et cela continue au lycée beaucoup plus encore. L'idée étant de toucher les gens, et pas uniquement les experts en cybersécurité, qui forment une population très à part. Globalement, chacun devrait avoir les bons fondamentaux de sécurité numérique, au bon moment, tout ça est encore une affaire de dosage.

Concernant l'aspect judiciaire, pour simplifier, et je laisserai la DGSI éventuellement me contredire : aujourd'hui, quelqu'un qui mènerait des attaques informatiques en France, depuis la France, sur des victimes françaises, prendrait de sérieux risques. Même chose en Europe, la coopération se développe et on a fait de vrais progrès. Mais il est évident que la coopération judiciaire n'est pas facile pour quelqu'un qui serait à l'autre bout du monde, dans des pays hostiles à la France, on sait que l'échange de données permettant de mener l'enquête ne fonctionne pas, les attaquants eux-mêmes le savent très bien. Dans les rebonds que je mentionnais tout à l'heure avant de toucher la cible finale, grand classique, il suffit à un moment de rebondir entre les frontières de deux pays qui ne peuvent pas se parler – il y en a beaucoup – pour être à peu près certain que la coopération judiciaire n'ira pas au bout, faute de pouvoir remonter le fil. Ainsi l'avantage reste aux attaquants. Mais l'époque où les attaquants ont été intouchables ou avaient des ponts d'or dans l'industrie est totalement révolue. Ceux qui ont trop joué, notamment du côté américain, sont aujourd'hui condamnés, pour certains à perpétuité. Il s'agit vraiment de crimes qui sont totalement répréhensibles et punis.

M. Thierry Matta.– Sur deux ou trois points dans votre intervention, Madame, je peux m'exprimer. Nous sommes très attentifs au contrôle en amont, comme vous disiez, de tous ceux qui veulent venir en France pour exercer leur talent, ou plutôt pour en acquérir…

Le criblage de toutes les personnes, comme Claire Landais le disait, c'est quelque chose qui n'est pas envisageable, puisque, comme le disait Xavier Inglebert, nous avons un stock d'environ 20 000 personnes. Nous pouvons mettre un coup de projecteur avec une enquête plus approfondie lorsqu'il existe de forts soupçons d'ingérence étrangère. Cela justifie que le service se saisisse du cas et soit un peu plus intrusif pour l'examiner.

Je termine sur l'aspect judiciaire. Guillaume Poupard a très bien résumé la situation : les outils juridiques dont nous disposons sont satisfaisants, de mon point de vue, il n'y a pas vraiment matière à intervention législative. Dans l'effectivité de la réponse, disait Guillaume Poupard, aujourd'hui, un attaquant français qui attaque une cible française à partir de la France, je ne dis pas qu'on le retrouve toujours, mais effectivement il prend beaucoup de risques. On arrive très fréquemment, pas toujours, mais dans la plus grande majorité des cas, à remonter jusqu'à la source de l'attaque. Quand ça vient de l'étranger, encore une fois, et là aussi Guillaume Poupard résume bien la situation, et sans même parler d'aspect judiciaire, il le disait tout à l'heure, on a systématiquement un problème d'attribution des attaques informatiques, parce qu'on ne sait jamais si effectivement l'attaquant d'origine ne se serait pas caché derrière des rebonds, s'il n'aurait pas semé lui-même de faux indices pour orienter vers une fausse direction. Dès que l'attaque provient de l'étranger, elle devient plus compliquée.

Mais on a des contre-exemples. Nous avons eu une affaire récente où nous avons pu remonter à la source de l'attaque, parce que nous étions covictimes avec un grand et très puissant allié, qui avait le même intérêt que nous, et en collaboration avec lui. Mais c'est un cas d'espèce.

Mme Angèle Préville, sénatrice.– Merci monsieur le président, merci à toutes et tous pour vos présentations sur un sujet très sensible. Ma question sur les ZRR sera très courte. Quel est le risque le plus important finalement ? On a beaucoup parlé du risque d'intrusion d'un chercheur qui, en cours de route, évolue, est contacté, à l'intention de, etc. Sachant que les accès physiques sont réglementés, est-ce que le risque le plus important pour l'avenir ne résiderait pas dans le risque informatique ? Je suppose que, sur ces zones-là, des dispositifs bloquent aussi l'accès aux matériels informatiques. Globalement, le risque le plus important concerne-t-il le personnel ou porte-t-il plus loin, avec par exemple une attaque numérique sur les ordinateurs qui sont dans ces laboratoires ? Comment le chiffrez-vous en

proportion ? On a beaucoup parlé de ces chercheurs qui se transformeraient au cours du temps, il y a des exemples. Mais vous n'avez pas parlé de la prise de contrôle par l'extérieur des laboratoires, sauf un peu M. Poupard. Est-ce un risque important ? Est-ce qu'il est déjà apparu dans les laboratoires de recherche ? Est-ce que ce risque sur le personnel est important en proportion ?

M. Bruno Sido, sénateur.– J'ai entendu à la radio, comme tout le monde je suppose, que les Américains sont en train de s'inquiéter du fait que le matériel informatique, les nœuds de connexion, etc. sont chinois. Ils ont peur maintenant que les Chinois coupent l'électricité dans tous les États-Unis ou à peu près. Ils sont donc maintenant en train d'interdire ces matériels chinois. Que pensez-vous de ce risque de prendre la main sur des systèmes, par exemple de signalisation de la SNCF ou autre ?

M. Cédric Villani, député, premier vice-président de l'Office.– Ma question sera quadruple. Premièrement, nous avons eu des statistiques sur le nombre de dossiers examinés, le nombre des ZRR, est-ce qu'on pourrait connaître la proportion d'incidents sérieux et graves chaque année ? Comment évolue cette proportion d'une année à l'autre ?

Dans les réponses que vous nous avez fournies, on constate une augmentation considérable, de l'ordre de 20 % par an, du nombre de ZRR. Qu'est-ce qui explique cette augmentation considérable ? Est-ce une augmentation de la menace, une augmentation de la précaution, un secteur en particulier ? Ce pourcentage de progression interroge forcément.

Il y a quelques instants, M. Matta parlait de cas dans lesquels un allié puissant avait permis d'aller jusqu'au bout de l'identification qu'apparemment nous n'étions pas en mesure de mener par nous-mêmes. Est-ce qu'on peut clairement dire que nous ne sommes pas suffisamment pointus, que nous n'avons pas suffisamment de puissance, je ne sais comment le caractériser, pour assurer au niveau français, au niveau européen, notre défense en la matière ? Est-ce que les alliés très puissants évoqués restent une composante indispensable de notre système actuel en la matière ?

Je développe ce que disait Bruno Sido à l'instant. Très précisément, au cours des dernières années, puis des derniers mois, puis des dernières semaines, avec de plus en plus d'intensité, de plus en plus régulièrement, l'opérateur chinois Huawei a été montré du doigt. Il y a quelque temps, c'était une mesure annoncée par les États-Unis, encore plus récemment par le Royaume-Uni, où l'université d'Oxford annonçait qu'elle refuserait toute contribution provenant de Huawei. Que peut-on dire sur un acteur particulier, ou sur d'autres ? Que peut-on savoir en la matière ?

Mme Claire Landais.– Ce que je trouve intéressant dans la PPST est précisément qu'elle prend en compte les deux types de risques d'intrusion et de captation, qu'elle permet à la fois de faire de la protection physique et de la protection logique, qu'elle est assortie de régimes répressifs qui portent sur les deux aspects.

Sur le succès, parce que je le vois comme ça, de l'augmentation du nombre de ZRR, je pense que c'est aussi l'effet de la rénovation du dispositif en 2012, dont la mise en place a pris un certain temps. Comme je l'ai dit en introduction, ce régime est mis en place dans la concertation, c'est-à-dire qu'en réalité, il faut que les entités qui mettent en place des ZRR soient effectivement convaincues de l'intérêt qu'elles peuvent y trouver, qui évidemment rejoint l'intérêt des pouvoirs publics à protéger certains éléments de notre potentiel scientifique. Je pense que l'effet de mise en route fait que ça monte progressivement en puissance, probablement aussi l'effet de sensibilisation sur la réalité de la menace. Je pense que ce succès tient aussi au fait, et nous y reviendrons dans la deuxième table ronde, qu'il y a un besoin d'adaptation, ça ne fonctionne pas dans toutes les disciplines et thématiques et auprès de tous les opérateurs de la même façon. Un certain nombre d'entités, en réalité, sont

aujourd'hui demandeuses de mécanismes d'accès à certaines capacités de l'État, et notamment de ce que savent faire les services de renseignement en criblage. Cela crée un environnement de confiance qui favorise en réalité les coopérations, cela rassure les interlocuteurs des entités qui demandent à constituer des ZRR, parce que leurs cocontractants ou leurs partenaires savent que cela favorise un environnement sécurisé, et donc la protection de leurs propres informations et échanges.

M. Thierry Matta.– En 2017 et 2018, nous avons enregistré 35 incidents sérieux, mais je ne doute pas un seul instant qu'il nous en échappe beaucoup. Ce sont seulement ceux dont nous avons connaissance. S'ajoutent à ces incidents que nous qualifions de sérieux des détections de situation de vulnérabilité, auxquelles nous avons pu mettre fin en faisant des propositions, soit à la direction de l'établissement, soit au ministère de tutelle. Nous pensons que nous avons pu les résoudre avant qu'elles ne dégénèrent en incident sérieux. Sur deux ans, nous avons eu entre 130 et 140 situations qui ont ou qui auraient pu entraîner des préjudices.

Pour répondre à Mme Préville, à la DGSI, nous constatons quasi systématiquement une intervention humaine dans l'incident ou dans la situation de vulnérabilité de la ZRR. Cette situation peut prendre un biais informatique, bien évidemment, puisqu'à partir du moment où il y a une pénétration indue à l'intérieur du laboratoire, et un accès aux systèmes d'information, la faiblesse humaine se transforme en risque informatique. Mais l'origine des incidents que nous avons détectés, je crois, est toujours humaine, je n'ai pas en tête d'exemple que nous ayons pu caractériser avec une attaque informatique directe venant de l'extérieur sur une ZRR. Cela a toujours résulté soit de l'absence de PPST par la mise en œuvre d'une ZRR, soit, malgré sa mise en œuvre, une faille qui a permis à l'attaquant de se livrer aux manœuvres dont il avait envie, qui peuvent avoir une composante informatique, mais à partir de l'intérieur de la ZRR.

M. Cédric Villani, député, premier vice-président de l'Office.– Et donc, typiquement, si je comprends bien, vous parlez de quelqu'un qui arrive avec une clé USB pour copier ou qui va lire un document, en tout cas une intrusion physique le plus souvent ?

M. Thierry Matta.– Tout à fait. Sur l'aide que nous avons reçue d'un allié puissant, dont parlait M. Villani dans le cas que je mentionnais, c'est la puissance de l'enquête judiciaire menée par cet allié qui nous a permis, dans la mesure où nous étions embarqués dans la même affaire d'attaques informatiques avec la même origine, par un échange croisé d'information, de progresser probablement bien plus que nous n'aurions pu le faire tout seuls.

M. Jean-Marc Jézéquel.– Je souhaite apporter un petit complément et illustrer cela avec un exemple concret, celui de mon laboratoire de recherche en informatique. Nous sommes un cas particulier, puisque les experts en cybersécurité sont chez nous. Nous travaillons évidemment de près avec l'ANSSI. Mais historiquement, la première apparition du premier ver informatique qui est arrivé chez nous date de 1988 ; on l'a arrêté parce que l'ingénieur avait été prévenu par téléphone par son collègue américain, et donc il a juste débranché le routeur qui nous connectait avec les États-Unis. Donc nous avons arrêté la première attaque de cette manière-là, très physique, et depuis 1988, jamais aucune attaque n'a réussi à pénétrer dans notre laboratoire au niveau informatique, ce qui illustre ce qui vient d'être dit par la DGSI. Sur les dix dernières années, par contre, nous avons subi un cas de tentative interne de la part de quelqu'un qui n'était probablement pas très professionnel, parce qu'il était assez maladroit de vouloir copier l'intégralité des données du laboratoire sur un disque. Évidemment, comme cela a généré un trafic réseau un peu violent, ça s'est vu, il a été pris sur le fait et une suite judiciaire a été donnée. Pour vous donner l'ordre de grandeur, en 30 ans depuis que les vers informatiques existent, nous n'avons constaté aucun cas, mais

sur les 10 dernières années, nous avons constaté un cas de tentative interne de pénétration dans un laboratoire.

M. Guillaume Poupard.– Je reviens sur les risques, la réponse est dans votre question. Il ne faut pas opposer les risques, malheureusement ils s'additionnent, voire se combinent dans certains cas. Dans les scénarios possibles, celui que nous dénommons « femme de ménage », c'est une expression, consiste à aller voir quelqu'un, lui dire de prendre une clé USB, de la brancher sur un ordinateur, de la laisser 10 minutes, de la retirer et qu'il n'entendra plus jamais parler de vous C'est quelque chose de très facile à faire, probablement dès qu'on a un moyen de pression sur la personne. L'impression de trahir est très limitée, et pourtant les conséquences peuvent être dramatiques. C'est beaucoup plus facile de sortir d'un réseau que d'y rentrer, pour le dire de manière très simple. On peut avoir une combinaison d'intrusion physique et d'attaque informatique, c'est assez classique. Sur la réalité des cyberattaques observée dans les laboratoires, je suis très gêné parce que je n'ai pas de statistiques, pour être franc. Je pense au cas particulier des labos qui sont eux-mêmes compétents en informatique, mais il y a aussi tous les autres labos : avec nos collègues du ministère de l'intérieur, nous constatons un véritable « chiffre noir » de la sécurité informatique. Il y a un grand nombre d'attaques que nous ne connaissons pas, tout simplement, et c'est gênant de pas pouvoir s'appuyer sur des données solides.

Enfin, la coopération est réelle avec nos alliés, même si elle est compliquée, si elle n'est pas naïve, si elle est subtile. Notamment nos alliés anglo-saxons ont fait un choix d'organisation très différent du nôtre, nos homologues sont en général les agences de renseignement techniques. Mais malgré cela, cette coopération est réelle parce que nous avons des intérêts communs. Tout est très pesé, tout est très mesuré, mais en même temps c'est une priorité pour nous, c'est un axe fort de coopération. Les Anglo-Saxons ont fait le choix, dès le départ, de confier l'attaque et la défense aux mêmes, pour mutualiser les compétences. Nous avons vu le risque et les conséquences en cascade qu'il y avait à faire de même en France et de risquer des conflits d'intérêts. Notre métier est plus la confiance numérique que la sécurité numérique. Je ne dis pas que les services de renseignement ne sont pas constitués de gens de confiance, – surtout en présence de la DGSI ! –, mais avec certains acteurs c'est beaucoup plus complexe. Cette séparation, qui n'empêche pas du tout la coopération au niveau national, bien au contraire, nous semble beaucoup plus saine. C'est à prendre en compte dans les coopérations.

Sur la Chine, l'axe que nous privilégions en France est de revenir systématiquement à de véritables analyses de risques. On peut faire des systèmes très mauvais avec des produits de confiance qui sont faits chez nous. Donc il faut maîtriser l'architecture, il faut comprendre ce que l'on fait et il faut maîtriser l'administration de ce système, avec tous ceux qui les font fonctionner, je pense évidemment aux réseaux télécoms. Et puis, pour chaque brique qui constitue l'architecture du système, il faut se poser la question du risque, en fonction des hypothèses raisonnables. Ensuite, tout ça se combine avec la possibilité de voir les produits en détail, de les observer, de les évaluer, de les certifier dans certains cas, tout cela est très subtil et en même temps relativement efficace.

M. Cédric Villani, député, premier vice-président de l'Office.– Mes chers collègues, nous arrivons à la fin de cette première table ronde. La deuxième table ronde, ouverte à la presse et retransmise en vidéo, sera orientée vers le fonctionnement des ZRR : procédures, dialectique, façon de coopérer entre protégés et protecteurs, pour le dire de façon résumée. Je vous remercie.

B. DEUXIÈME TABLE RONDE, *OUVERTE À LA PRESSE* : LES PROCÉDURES RELATIVES AUX ZONES À RÉGIME RESTRICTIF (ZRR)

M. Cédric Villani, député, premier vice-président de l'Office.- Cette deuxième table ronde sur le sujet du potentiel scientifique et technique de la nation concerne les procédures relatives aux zones à régime restrictif (ZRR). Elle est retransmise sur le site internet de l'Assemblée nationale.

Le constat qui s'inscrit en droite ligne de notre première table ronde est celui de la nécessité d'une protection du potentiel scientifique et technique de la nation (PPST). La PPST est claire et nécessaire de manière avérée. Les menaces bien identifiées sont liées à la malveillance, l'espionnage, à des possibilités de dommages collatéraux. Le monde de la science, basé sur le partage sincère d'informations, ne doit pas naïvement oublier que le monde actuel a besoin d'une sécurité considérable.

En revanche, les modalités de mise en œuvre peuvent faire l'objet de discussions, de dialectique, et s'il n'y a pas accord entre les experts qui sont protégés et les agences, les institutions, qui énoncent les règles de protection, on peut craindre des refus, des comportements contre-productifs, et à la fin des failles de sécurité.

C'est ce genre de problématiques que nous allons aborder et discuter avec tous les participants. Lorsqu'une personne souhaite accéder à une ZRR pour y travailler, que ce soit un travail contractuel ou relevant de conventions de coopération, il faut formuler une demande d'accès auprès du ministère de rattachement de l'établissement. Vient ensuite une instruction par le ministère du dossier de demande d'accès et un avis fondé sur une analyse technique et de sécurité dans un délai maximum de deux mois.

Les publications, qui sont également soumises à autorisations préalables, posent une question : le délai induit par une éventuelle demande d'autorisation peut-il avoir des conséquences sur la compétitivité de l'entreprise scientifique ?

La politique de sécurité des systèmes d'information s'inscrit dans l'ensemble du dispositif de sécurité.

Cela nous fait trois volets : qui a le droit de pénétrer ? Que peut-on publier ? Quels sont les processus de sécurité informatique ?

Il y a actuellement en France moins de 1 000 ZRR, avec une augmentation importante de l'ordre de 20 % par an. Le dispositif de ZRR permet de protéger le potentiel scientifique. Un certain nombre de cas qui ont été, soit empêchés, soit détectés du fait du dispositif ZRR, montrent que le dispositif a son utilité. Pour autant, il a fait l'objet d'un certain nombre de critiques que nous devons aborder et examiner.

Certains ont dénoncé le faible niveau de protection qu'il procure, en raison de l'inadaptation des dispositifs aux risques. Je me fais ici l'écho des critiques sans prendre parti moi-même. D'autre part, a été critiquée la gêne que ce dispositif peut occasionner, soit pour la vie quotidienne, soit pour le développement scientifique en s'appuyant sur des chercheurs invités ou de nouveaux doctorants, tant il est vrai que la science est ouverte à l'international.

Certains ont critiqué le fait qu'entre le régime ZRR et non-ZRR, il y a comme une activation binaire de processus, sans tenir compte de la particularité des disciplines et des laboratoires, alors que les risques, les comportements, les chaînes hiérarchiques, peuvent être très différents d'une discipline à l'autre : mathématiques, biologie, physique… De même, dans un milieu de recherche industrielle, on n'est pas organisé de la même façon, au niveau

de la gouvernance de la recherche comme des habitudes, que dans la recherche fondamentale.

Certains acteurs ont également critiqué une concertation insuffisante entre services de sécurité et directeurs de laboratoire. Lors du classement en ZRR, la question du bien-fondé des critères a pu être parfois mise en cause, ainsi que les questions de mise en œuvre. Une fois un laboratoire déclaré ZRR, sur quels critères et quand évaluer la pertinence d'un refus d'accès, d'un refus d'embauche, ou d'un refus de publication ? Les procédures sont-elles justes et efficaces ?

Au centre des critiques, il y a l'obligation de déclarer plus de 2 mois à l'avance toute visite d'une collaboration de plus de 5 jours au sein d'un laboratoire, et puis d'attendre l'autorisation du fonctionnaire de défense et de sécurité du ministère de tutelle. Les critiques pointent du doigt le handicap significatif des centres de recherche français qui en découlerait, dans un contexte international très concurrentiel, où il convient, pour avoir la meilleure science possible, d'attirer les chercheurs post-doctorants, les stagiaires, les talents du monde entier.

Est également parfois pointée du doigt la lourdeur administrative, avec des délais qui peuvent être incompatibles avec le fonctionnement d'un laboratoire, ou simplement le temps que prennent les décharges administratives, ou encore les frais induits. Le dispositif ZRR est-il bien équilibré entre la protection qu'il apporte et la lourdeur qu'il induit ?

Dans notre contexte de développement scientifique et technologique hautement concurrentiel à l'échelle internationale, la question se pose aussi de la comparaison de nos règles de sécurité avec celles des pays étrangers.

Enfin, la lutte contre la fuite des cerveaux *(brain drain)* est une question majeure. Dans un contexte où l'attractivité française dans certaines disciplines est érodée et où notre système a du mal à attirer certaines catégories de chercheurs dans certaines disciplines, l'application des ZRR ne vient-elle pas constituer un handicap supplémentaire ? Si oui, comment améliorer les procédures ?

Pour discuter de tout cela, nous accueillons dans notre table ronde des représentants de l'administration, de différents laboratoires dans des disciplines différentes : mathématiques, informatique, sciences de la vie et de l'environnement, sciences physiques, sciences de l'ingénieur… Je vous propose de commencer par une présentation du dispositif ZRR par le préfet Inglebert**.**

M. Xavier Inglebert, préfet, haut fonctionnaire de défense et de sécurité (HFDS) adjoint des ministères de l'enseignement supérieur, de la recherche et de l'innovation (MESRI) et de l'éducation nationale et de la jeunesse (MENJ).- J'assure la fonction de HFDS adjoint depuis janvier 2018, je suis en charge de la conception et de la mise en œuvre de la politique de défense et de sécurité des deux ministères MESRI et MENJ, notamment des dispositifs réglementaires qui concernent la protection du potentiel scientifique et technique dans les 2 200 laboratoires concernés par le MESRI, hors sciences humaines et sociales qui ne sont pas dans le dispositif, ce qui représente 60 % du dispositif national de PPST.

Dans ce champ précis, mes fonctions consistent : en premier lieu, sur la base des textes réglementaires disponibles, à élaborer la stratégie globale du ministre en ce domaine, et j'aurai à la fin de cette audition des propositions à faire aux directrices et directeurs d'institut et de laboratoire ; en second lieu, à mettre en œuvre opérationnellement cette stratégie.

Cela recouvre quatre volets : identifier les laboratoires qui ont un besoin de protection en ZRR. Pour cela, nous avons créé, avec le Secrétariat général de la défense et de la sécurité nationale (SGDSN), un collège d'experts. Il est constitué, d'une part, des directeurs d'unité proposés par les établissements, que ce soit la Conférence des présidents d'université (CPU) ou les grands organismes de recherche, d'autre part, d'experts scientifiques de la défense et de la sécurité du SGDSN ou du MESRI**.**

Ce comité d'experts va coter, sur une échelle de 1 à 3 pour chacun des risques, chaque laboratoire au regard des quatre risques définis par la PPST : risque économique, risque en matière de défense conventionnelle, risque de prolifération d'armes de destruction massive et risque terroriste. Environ 10 à 15 % des laboratoires couverts par le MESRI ont été identifiés comme pouvant relever du dispositif ZRR, soit entre 250 et 300 laboratoires. Le comité y travaille sur la base d'un questionnaire qui est renseigné par les directeurs d'unité, à partir des rapports du Haut Conseil de l'évaluation de la recherche et de l'enseignement supérieur (HCERES) et de sources fermées. Il travaille en méthode d'analyse des risques – et absolument pas à partir de mots-clés.

Le deuxième aspect de mes compétences porte sur les unités les plus sensibles, à condition que l'établissement et les tutelles le demandent : l'instruction des dossiers de passage en ZRR, avec la signature *in fine* d'un arrêté de création ou de suppression. J'insiste sur le fait que je n'ai pas l'initiative de la création des ZRR. Ma mission est d'encourager cette création quand elle est nécessaire. Dans la précédente table ronde, on a cité le cas d'un problème dans un laboratoire. Je l'ai contacté suite à ce problème, et effectivement, avec le directeur d'unité et le président de l'établissement, nous avons décidé ensemble de créer une ZRR. Depuis 2015, 394 ZRR ont été créées, sur les moins de 1 000 du dispositif global avec les autres ministères, ce qui représente 108 unités de recherche. Parfois il y a plusieurs ZRR par unité de recherche. En 2018, j'ai également signé 10 arrêtés de suppression. Ce dispositif vit, avec des entrées et des sorties.

Troisième aspect de mes compétences : pour toutes les unités en ZRR, je signe les avis sur les demandes d'accès. Cela a représenté 9 400 demandes d'accès en 2018. Le délai moyen de réponse sur les 60 jours imposés par les textes est en moyenne de 24 jours. La décomposition est la suivante : 95 % des avis sont sans objection, 1,7 % des avis sont négatifs (157) en 2018, et, c'est une nouveauté en 2018, environ 3,5 % des réponses sont des avis favorables sous réserve. Globalement, le but dans ce dernier cas, est d'impliquer les acteurs, d'assortir l'avis de réserves qu'il faut lever : limitation d'accès physique dans certains cas, compte rendu périodique du directeur de thèse quand il s'agit d'un doctorant, etc. L'ensemble des avis sur demande d'accès s'appuient sur le travail d'un groupe d'experts scientifiques qui est à mes côtés. Ces experts travaillent sur le dossier complet, les CV des chercheurs, essaient d'analyser ces dossiers par rapport à la réalité du risque, à l'activité du laboratoire, au profil du candidat et au projet de recherche. Là non plus, nous ne travaillons pas à partir de mots-clés.

Dernier volet de mon activité : les avis sur les programmes de coopération internationale des établissements supérieurs. Cela n'a rien à voir avec les ZRR, cela s'applique à l'ensemble des laboratoires. Le but est d'accompagner les établissements pour que les contrats qu'ils signent ne soient pas léonins en termes de propriété intellectuelle, ce qui peut être parfois le cas, et qu'ils n'aillent pas à l'encontre des engagements internationaux de la France en termes de prolifération ou d'exportation de biens à double usage.

De mon point de vue, une problématique se pose : nous avons ensemble à gérer une tension. D'une part, il y a le fait que la recherche ne se conçoit aujourd'hui qu'au niveau international. Le rayonnement français sur l'échiquier de la recherche mondiale et des

scientifiques nécessite absolument l'échange, la confrontation des idées, ainsi que l'attractivité des meilleurs chercheurs et étudiants dans nos laboratoires. C'est indispensable à la recherche française, la cinquième du monde. D'autre part, simultanément, on l'a vu, des menaces croissantes et réelles convoitent notre production scientifique, et ce dans le monde entier.

Cette tension porte deux enjeux : un premier enjeu est lié aux intérêts fondamentaux de la nation, c'est-à-dire que des puissances étrangères cherchent à s'emparer du produit de notre recherche et de nos brevets, et parfois, ces produits impliquent la défense nationale. Le deuxième enjeu est plus considérable : c'est celui de la survie même de notre modèle de recherche, démocratique, républicain, porteur d'universalité. Certains pays ne s'embarrassent pas de ces principes et ne développent pas une recherche démocratique. Si nous les laissons s'emparer de notre recherche, c'est leur modèle qui l'emportera.

Quelle utilité pour la PPST ? D'abord, l'utilité est générale. Le fait qu'elle existe permet de développer l'attention, l'interrogation, le signalement, pour le milieu scientifique de la recherche. Le fait même que la PPST existe permet de tracer une frontière.

Le deuxième aspect est plus concret. En 2018, j'ai connu quatre cas de figure, avec de vraies difficultés, équivalentes à celles évoquées tout à l'heure. Ces difficultés auraient été évitées si ces laboratoires avaient été en ZRR, car les candidats étrangers qui venaient auraient été refusés selon nos critères. Les trois premiers cas concernaient des volumes de brevets potentiels. L'un de ces trois cas comportait un vol de brevet au détriment d'un industriel français qui finançait la recherche. Le quatrième cas concernait une unité de recherche qui, sur 30 doctorants, accueillait 10 étudiants de la même nationalité et de la même université militaire. Le laboratoire en question est un laboratoire d'excellence, dont certains des sujets peuvent mettre en jeu les intérêts fondamentaux de la nation.

On dit beaucoup de choses sur la PPST. D'emblée, ce dispositif est contraignant, parce que c'est un dispositif de sécurité et que c'est une contrainte collective. Ce dispositif mobilise des ressources. À ses débuts, il a pu connaître des difficultés de mise en œuvre. Oui, nous devons faire plus de pédagogie, nous devons mieux prendre en compte les préoccupations des chercheurs et essayer d'éviter toutes les contradictions dans son déploiement. Moi-même, entre 2010 et 2015, j'étais directeur général délégué aux ressources humaines du CNRS, et j'ai pu voir l'arrivée de la PPST et comprendre les difficultés que cela posait.

On dit beaucoup de choses qui ne correspondent pas forcément à la réalité. Monsieur Villani, vous avez parlé des publications soumises à autorisation du directeur de laboratoire. Je suis désolé, mais aucun texte ne préconise une telle contrainte de portée générale. La circulaire interministérielle de 2012 du SGDSN précise à la page 30 que : « Le règlement intérieur de la ZRR précise les règles encadrant les publications relatives aux travaux menés dans la ZRR. [Ces règles doivent concilier le besoin légitime de publication des chercheurs et le respect des impératifs de sécurité.] En cas de besoin, le chef de la ZRR peut demander un avis technique au haut fonctionnaire de défense et de sécurité (HFDS) […]. » Ce n'est donc vraiment pas systématique. Dans certains cas, il est possible qu'on ait pu mobiliser ce dispositif. Mais il serait d'ailleurs tout à fait impensable et impossible qu'un directeur d'unité doive lire l'ensemble des articles émanant de son unité, surtout dans les très grosses unités. Donc ce n'est pas une préconisation ministérielle, les textes ne le disent pas ainsi. J'insiste sur ce point : dans l'arsenal juridique aujourd'hui, il y a de la souplesse, des marges de manœuvre, des champs sur lesquels nous pouvons travailler ensemble.

Par la suite, je ferai des propositions, si vous m'y autorisez, en direction des chercheurs et des scientifiques de notre pays.

M. Cédric Villani, député, premier vice-président de l'Office.- Merci monsieur le préfet. J'ai juste une remarque technique. Vous évoquez un délai moyen de 24 jours pour le traitement des demandes d'accès, là où le chiffre que nous avons reçu pour le délai de traitement et de demande du côté du CNRS est plus proche de 10 semaines. Ces statistiques nous sont indiquées depuis 2014. Avez-vous une idée de ce qui explique la disparité de ces deux valeurs ?

M. Xavier Inglebert.- Je tiens à votre disposition les statistiques de mon service. Il s'agit d'une moyenne. Le problème de l'intermédiation peut également se poser, entre l'établissement et le service. Avec le CNRS, comme avec le CNES, nous avons une procédure simplifiée, qui va dépendre ensuite des cas. Dans certains cas plus complexes, l'analyse du dossier peut prendre du temps, parce que nous sommes confrontés à des situations compliquées. Je ne peux pas vous les citer précisément. Dans le cadre d'une procédure simplifiée, le délai en tout cas est de 9 jours.

L'une des propositions que je ferai aux établissements et laboratoires est de généraliser cette simplification administrative aux établissements qui peuvent certifier une démarche, et de mettre en œuvre ce délai simplifié.

M. Marc Drillon, docteur ès sciences physiques, ancien directeur de l'Institut de physique et de chimie des matériaux de Strasbourg (IPCMS), directeur de recherche émérite au CNRS.- Par rapport à ces 24 jours, les statistiques indiquent-elles d'où viennent ces personnes pour lesquelles l'autorisation est demandée ? On imagine bien qu'entre les candidats français, européens et chinois, le délai n'est pas le même.

M. Xavier Inglebert.- Les statistiques sont couvertes par l'aspect confidentiel défense, mais je peux les mettre à disposition des services qui peuvent en avoir connaissance.

M. Cédric Villani, député, premier vice-président de l'Office.- Nous touchons ici un point récurrent sur les sujets sensibles. On regrette de ne pas avoir au sein du Parlement des représentants habilités secret défense pour avoir connaissance de ce type d'informations.

M. Marc Drillon.- Vous avez parlé d'avis sur les programmes de coopération. Qu'est-ce que cela signifie exactement ? Nous avons eu ce cas de figure. Lorsqu'on a fait une demande d'autorisation pour un candidat étranger, on nous a demandé si nous avions une convention de coopération avec son université. Est-ce systématique ou pas ?

M. Xavier Inglebert.- Nous sommes plutôt dans le champ des demandes d'accès aux ZRR.

M. Marc Drillon.- Non, je parle d'une personne qui venait visiter le laboratoire.

M. Xavier Inglebert.- Le cas de la personne qui vient visiter le laboratoire fait partie de la problématique d'accès aux laboratoires.

M. Marc Drillon.- Mais si l'on nous demande si nous avons une convention de coopération, cela peut rallonger considérablement les délais. Le cas dont je vous parle concernait un professeur chinois en visite dans un laboratoire pour trois semaines. On nous a demandé une convention de coopération avec l'université concernée. Nous n'en avions pas. Nous avons été obligés de passer cette convention, ce qui a pris 6 mois, alors que c'était pour une visite de 3 semaines.

M. Xavier Inglebert.- Ce cas particulier a-t-il donné lieu à un avis réservé ?

M. Marc Drillon.- Non, il n'y avait pas d'avis réservé. Au cours de l'instruction, on nous a demandé une convention de coopération. On ne s'y attendait pas.

M. Xavier Inglebert.- La question des visites et des cas particuliers mérite que nous travaillions ensemble. Dans le cas que vous citez, la convention de coopération a été demandée parce qu'il s'agissait visiblement d'une personne sensible et que nous avons eu besoin d'un complément d'information. Les gens ne sont pas sensibles en fonction de leur nationalité. Nous regardons les CV, les champs de recherche, etc. L'étude qui est menée est assez complète. Nous ne travaillons ni par mots-clés, ni par nationalité, excepté pour les pays considérés comme proliférants, ce que vous pouvez comprendre.

M. Cédric Villani, député, premier vice-président de l'Office.- Merci monsieur le préfet. Cet échange aura eu le mérite d'illustrer qu'il y a des marges de progression dans le dialogue entre l'édiction des règles et d'analyse et les laboratoires eux-mêmes. Continuons le fil de nos présentations avec M. Drillon pour la physique.

M. Marc Drillon.- Je vais vous faire part de mon expérience de terrain. Pendant dix ans j'ai dirigé une unité de 250 personnes dans les domaines des nanosciences et des nanotechnologies, dans un institut regroupant des physiciens et des chimistes des matériaux. Mon laboratoire est classé ZRR, parce que l'un des départements utilise des lasers femtoseconde. J'ai ensuite assuré durant six ans la fonction de délégué scientifique à l'AERES, puis au HCERES, et c'est en visitant un grand nombre de laboratoires en physique, entre 8 et 10 par an, que j'ai pu constater l'effet des ZRR en physique.

Je distingue deux périodes dans le domaine de la sécurité qui a été renforcée dans les laboratoires. Avant 2012, avant la mise en place de la ZRR, quand j'étais directeur de laboratoire, je rencontrais régulièrement, deux à trois fois par an, un officier de la direction de la surveillance du territoire (DST), pour qu'il me sensibilise à l'action de surveillance qui était menée sur les ressortissants étrangers dans mon laboratoire, en particulier quand il s'agissait de pays dits sensibles. Cette interaction a eu un impact important sur mon laboratoire, très positif, dans le sens où l'accès au laboratoire a été complètement modifié, avec un accès unique, un code électronique d'entrée, et une procédure d'enregistrement des visiteurs du laboratoire qui a été mise en place à l'accueil pour le suivi des entrées et sorties dans le laboratoire. Auparavant, comme dans beaucoup de laboratoires universitaires, c'était quasiment en *open access*, la libre circulation des personnes prévalait. La modification des accès au laboratoire a un coût.

Depuis 2012, avec la mise en place de la ZRR, on a observé un durcissement du dispositif de PPST qui s'applique à toute personne, quelle que soit sa nationalité, souhaitant effectuer un séjour au laboratoire ou être recrutée au laboratoire en CDD ou sur un poste permanent.

Les conséquences de la ZRR me paraissent importantes à divers titres. D'abord, lorsque votre ZRR ne concerne que certaines zones du laboratoire, il y a un morcellement du laboratoire, avec accès à certaines zones par carte électronique. Il n'y a pas de libre circulation du personnel dans tout le laboratoire. Lorsqu'on a modifié la ZRR dans notre laboratoire, j'ai considéré qu'il valait beaucoup mieux que tout le laboratoire soit ZRR, cela posait moins de problèmes. Un laboratoire de nanosciences et de nanotechnologies est pluridisciplinaire, avec des physiciens et des chimistes. Les gens utilisent beaucoup d'équipements pour étudier leurs matériaux, les caractériser, donc ils sont obligés d'aller dans différentes zones du laboratoire.

Ensuite, pour le recrutement des chercheurs, tous les laboratoires sont en compétition aux plans national et international pour recruter les meilleurs chercheurs à des postes de permanents. C'est un peu comme dans les équipes de football : on essaie de recruter les meilleurs, la compétition est sévère. Les demandes d'autorisation prennent deux mois au minimum. Moi, je suis à plus de deux mois pour des étrangers, auxquels s'ajoute le système de visa dès qu'il s'agit de non-Européens. Au final, plusieurs mois sont nécessaires pour un recrutement. On observe que les meilleurs, qui candidatent dans d'autres laboratoires au plan international, vont ailleurs, chez nos concurrents en Europe ou aux États-Unis, où cette procédure ne s'applique pas. Les non-Européens doivent faire une demande d'autorisation, suivie d'une demande de visa, et au total vous êtes à quatre ou cinq mois. Évidemment, recruter des post-doctorants ou de bons doctorants est un problème également de durée de la procédure, puisque les meilleurs vont ailleurs. Le constat est le même pour les permanents, les post-doctorants ou les doctorants.

La ZRR a une conséquence sur l'image de la recherche en France. Pour les non-Européens, les délais sont très importants. Au bout de quatre à cinq mois, on peut annoncer à quelqu'un que, finalement, il n'est pas accepté, et en plus, sans lui donner la raison. J'ai des cas de figure. L'un des plus savoureux concerne un étudiant souhaitant préparer un doctorat au laboratoire. Il obtient une bourse de l'ambassade de France pour venir au laboratoire. On demande au fonctionnaire de défense et de sécurité la demande d'autorisation, celui-ci l'accepte, ensuite je contacte le candidat pour qu'il demande un visa. Au bout de deux mois, le candidat s'est vu refuser le visa, alors que c'était une bourse de l'ambassade de France ! Ce type de dysfonctionnement ne donne pas une bonne image de la France.

C'est aussi une entrave forte au démarrage des contrats. Lorsque vous recrutez un CDD pour un post-doctorant ou une thèse sur un contrat de l'Agence nationale de la recherche (ANR) ou européen, l'autorisation est rarement négative, on l'a vu, c'est moins de 2 % d'avis négatifs. Mais la procédure handicape fortement le management du contrat, c'est-à-dire qu'il faut parfois attendre trois à quatre mois avant de démarrer le contrat, parce que vous ne pouvez pas avoir le candidat immédiatement. C'est une difficulté pour manager un certain nombre de contrats. Des contrats sur un an peuvent être impactés par cela.

Nous avons évoqué la convention de coopération. Je ne sais pas si elle est systématique ou pas. Soit le dossier était incomplet, soit il avait des aspects négatifs, et donc une convention de coopération nous a été demandée.

En physique et en chimie, les personnels ne contestent pas le besoin de sécurité. Mais la procédure ZRR telle qu'elle est appliquée nuit à la compétitivité, à l'attractivité de nos laboratoires, en particulier lorsque ces laboratoires réalisent des recherches amont, sans finalité à court terme et sans apporter toute la protection recherchée. La priorité pour ces laboratoires de recherche fondamentale est la publication dans les meilleures revues. Les recherches qui y sont effectuées sont mises sur la place publique une fois que les résultats sont publiés. Les chercheurs sont extrêmement vigilants, ils ne dévoilent pas leurs travaux avant publication.

M. Cédric Villani, député, premier vice-président de l'Office.- Vous avez évoqué les comparaisons internationales. Avant cette audition, l'Office a fait un travail de comparaison, en particulier avec les pays emblématiques que sont les États-Unis et le Royaume-Uni. On pourra en rediscuter, mais il nous semble que le dispositif ZRR est unique en son genre dans ses modalités. Même si les modalités de protection existent ailleurs bien entendu, les organisations sont beaucoup moins centralisées aux États-Unis et au Royaume-Uni. Des documents de synthèse vous ont été distribués sur ce sujet pour votre information.

M. Pascal Auscher, professeur des universités en mathématiques, directeur de l'Institut national des sciences mathématiques et de leurs interactions (INSMI), CNRS.- Au plan administratif, l'INSMI est placé sous l'autorité du PDG du CNRS, il dispose de tous les outils de l'organisme de recherche CNRS en termes de personnel, de subvention de l'État, etc. qui vont ensuite dans les laboratoires. Au plan scientifique, cet institut a une particularité : une mission nationale d'animation et de coordination dans le domaine des mathématiques. Là est ma responsabilité. Parmi ses missions, il doit favoriser l'excellence dans toutes les branches de la discipline mathématique, développer l'action internationale et favoriser la mobilité des chercheurs.

L'INSMI ne fait pas de recherche en lui-même, mais il l'organise au travers d'un réseau de 41 laboratoires, des unités mixtes de recherche (UMR) avec le plus souvent des universités, 11 fédérations de recherche, des réseaux sans mur qui sont des regroupements thématiques. Sur une population de 4 000 professionnels en mathématiques en France, 90 % de cette communauté est concernée par ce dispositif CNRS, et donc peut utiliser les outils développés à la fois par l'institut et aussi par le CNRS. Je n'ai pas la responsabilité d'hébergeur. La plupart du temps, les laboratoires sont hébergés par nos partenaires universitaires.

Je ne suis pas directeur d'unité, mais avec les autres tutelles, je propose les directeurs et directrices d'unités, qui sont choisis parmi les enseignants-chercheurs pour leurs compétences scientifiques et humaines. Ces personnalités sont responsables. On ne va pas nommer des gens qui mettraient le désordre dans les unités. Ils prennent leurs responsabilités au sérieux, et le rôle de l'institut est de les aider à gérer leurs unités en y affectant des personnels, des moyens, en fonction des possibilités budgétaires qui me sont ouvertes.

M. Cédric Villani, député, premier vice-président de l'Office.- J'ajoute que dans l'organisation mathématique nationale, pour des raisons historiques et culturelles, le CNRS, bien au-delà des moyens qu'il peut mettre, est considéré comme une autorité morale extrêmement forte. C'est certainement l'autorité de référence qui compte le plus pour les mathématiciens.

M. Pascal Auscher.- C'est pourquoi j'ai rappelé la mission nationale. Ma mission est vraiment que les laboratoires produisent la meilleure recherche possible. Je dois dire qu'ils le font. Ils maintiennent la France dans le peloton de tête des nations en matière de recherche en mathématiques. On dit parfois que la France est au deuxième rang après les États-Unis. La semaine dernière encore, un prix prestigieux a été décerné à un mathématicien français, le prix Wolf.

Les raisons de ce succès sont multiples. D'abord, en mathématiques, il y a une forte tradition de formation, on pense aux Écoles normales supérieures, mais les universités ont également de très bons masters et doctorats. La mobilité entrante et sortante est exceptionnelle, à tous les niveaux : étudiants, doctorants, post-doctorants, recrutements. L'an dernier, le CNRS a recruté 6 chargés de recherche de nationalité étrangère sur les 18 qui sont entrés en mathématiques. C'est une moyenne annuelle. Le but est de collaborer avec les meilleurs à l'international. La politique scientifique est exigeante, dynamique, et il est fait confiance aux chercheurs et enseignants-chercheurs pour faire émerger les sujets internes et externes de la discipline.

En mathématiques, on démontre des théorèmes, c'est-à-dire des énoncés déduits de façon logique, des axiomes ou d'autres énoncés. Et puis on les diffuse, en les publiant. Il faut les publier les premiers, dans les revues où ils seront lus par les collègues de la discipline. Le CNRS nous encourage à les prépublier, sur des archives ouvertes, avant qu'ils soient vérifiés par les pairs. En fait, la diffusion de l'information va très vite. Lire et comprendre un article

de mathématiques demande du temps, des efforts, qui ne sont pas à la portée du premier venu. On est souvent très loin d'une application industrielle et technologique. Le transfert vers un produit prend des années, requiert autant d'innovations technologiques que le résultat avait demandé d'ingéniosité pour le démontrer.

Dans la procédure ZRR, il y avait eu toutes sortes de dialogues avec les directeurs d'unité (DU) organisés en collectifs pour discuter avec le SGDSN. Après un certain nombre de réunions et d'années d'échanges, les DU et le SGDSN ont finalement rompu le dialogue sur un constat d'échec au niveau des comités d'experts consultés sur les cotations des risques.

J'ai entendu qu'il y a absence de choix par mots-clés. Je dois dire que le sentiment de mes collègues DU à l'époque n'était pas celui-ci. Au contraire, à l'époque, il y avait ce sentiment que les identifications de laboratoire devant être classés en ZRR étaient réalisées selon un certain nombre de mots-clés, lesquels étaient d'ailleurs inconnus de nos collègues DU, puisque le SGDSN n'en faisait pas état.

La lourdeur évoquée par mon collègue physicien est la même pour nous. Pour les procédures de recrutement, c'est vraiment un frein. Le surcoût administratif est pratiquement intenable pour l'ensemble des unités. Pour rappel, ces unités sont hébergées par nos partenaires universitaires, et donc ce surcoût est essentiellement supporté par eux. Si j'y ajoute les frais induits et diverses autres raisons, au bout d'un moment, les collègues ont décidé de ne plus participer à ces discussions et de rompre le contact.

Actuellement, des discussions se sont rétablies à la demande du préfet Inglebert. Je m'y suis rendu et je vais proposer aux DU d'avoir une nouvelle discussion avec le HFDS. Pour l'instant, nous en sommes là.

M. Cédric Villani, député, premier vice-président de l'Office.- Sur les applications pratiques en tout cas, nous comprenons qu'il y a convergence de vues sur l'analyse, entre MM. Drillon et Auscher. Nous allons passer à un domaine complètement différent, celui de la virologie, avec M. Hervé Raoul, directeur du laboratoire P4 Jean Mérieux de Lyon, d'une très grande notoriété pour ses recherches de haute tenue sur des virus et bactéries parmi les plus tristement célèbres du monde. Ce centre dépend de l'INSERM, qui a été à de nombreuses reprises invité à nos tables rondes.

M. Hervé Raoul, directeur du laboratoire P4 Jean Mérieux de Lyon, centre européen de recherche en virologie et immunologie, Institut national de la santé et de la recherche médicale (INSERM).- Je représente un domaine un peu particulier qui, par la nature des matières que l'on va être amené à manipuler et des savoir-faire que l'on va accumuler, méritait d'être protégé depuis le début. Dans la mesure où le directeur d'unité est responsable et doit être responsable, finalement, sans qu'on ait le choix au départ, dès sa mise en service en 2000, le laboratoire a été classé établissement à régime restrictif (ERR), puis ZRR. Nous avons un retour d'expérience en la matière et nous avons été amenés à nous interroger sur les avantages et les inconvénients du classement en ZRR.

Parmi les avantages que nous avons vus immédiatement, cela permettait d'abord de conférer un cadre légal, qui était extrêmement important pour nous. Vous pouvez être responsable, mais sans le cadre qui vous associe à la loi, les choses peuvent devenir très vite compliquées. Ensuite, cela fixait un cadre organisationnel. Nous avons été aidés dans notre démarche de définition du risque, au travers de la définition de critères, de la nature et des niveaux de responsabilité, ce qui est très souvent difficile à appréhender quand on n'est pas du domaine. Par nature, nous venons du monde de la science, nous n'avons pas été formés spécifiquement pour ce genre de choses.

Cela permet également le contrôle d'accès, ce qui ne peut pas se mettre en place partout sans un certain niveau de classement. Évidemment, il était important pour nous d'être en capacité de mettre en place un tel contrôle d'accès. Cela donne accès à l'assistance des services de l'État, un thème déjà évoqué plusieurs fois. Pour nous, il était très important de savoir qui l'on reçoit au laboratoire. L'assistance des services de l'État est un vrai avantage dans notre cas. Il est arrivé plusieurs fois qu'il ne soit pas souhaitable de recevoir certains individus. Au niveau de l'unité, nous n'avons pas la compétence nécessaire pour opérer ce type de criblage *(screening).*

Ce matin, on a discuté de ce que pouvait apporter la vision de l'ANSSI. Parce que nous sommes classés ZRR, nous avons pu avoir accès, de façon très simple, à un audit consultatif de l'ANSSI, qui va être conduit très prochainement. La responsabilité restera au directeur d'unité, mais cet audit va peut-être nous permettre, ou pas, d'évoluer. Il y a également des contraintes qui peuvent être importantes, mais qu'il convient parfois aussi de relativiser. Concernant le contrôle d'accès, dans notre cas, le système de zonage présente un avantage, parce qu'il nous permet d'ouvrir certaines zones sur le site, sans être soumis à réglementation ou autorisation, à des personnels avec qui l'on peut échanger.

Vous imaginez bien que tout le personnel ne peut pas avoir accès à une zone de niveau 4 où l'on manipule des pathogènes. Le zonage permet donc de définir des zones de circulation pour les secrétaires, et d'interdire par exemple pour les personnels administratifs, certaines zones où l'on manipule des pathogènes extrêmement dangereux. Un coût est associé à toutes ces contraintes, notamment au contrôle d'accès. Il y a un avantage à être classé : cela oblige l'institution ou la tutelle dont vous dépendez à couvrir ces frais. Ce n'est pas systématique, mais en tout cas, pour l'INSERM, cela s'est fait de façon automatique. Je ne dis pas qu'ils étaient heureux au départ, mais cela a été fait. Les coûts associés sont extrêmement importants chaque année.

Les demandes d'autorisation restent une contrainte. Vous ne pouvez pas faire ce que vous voulez. En revanche, je constate que nous avons toujours obtenu une réponse sous trois semaines à nos demandes d'autorisation d'accès. Sur tous les aspects qui portent sur la nature des collaborations, ou la façon dont on va communiquer, il n'y a pas d'obligation d'obtenir des autorisations. Cela reste de notre domaine de responsabilité. Cela peut être vécu comme une contrainte, parce que l'on est parfois tout seul à choisir, mais en revanche, c'est très limité dans la vie de tous les jours.

Pour finir, je voudrais dire que, bien que le laboratoire soit classé sous ce type de régime depuis maintenant plus de vingt ans, c'est aujourd'hui l'un des laboratoires qui a une grande visibilité dans le monde, des collaborations nationales, européennes, internationales, malgré ces contraintes que l'on préférerait ne pas avoir. Mais le monde étant ce qu'il est, on est bien obligé de faire avec.

M. Cédric Villani, député, premier vice-président de l'Office.- La parole est à M. Aumont, au nom de l'agronomie et des sciences de l'environnement.

M. Gilles Aumont, directeur de recherche à l'Institut national de la recherche agronomique (INRA).- Je ne vais pas apporter un témoignage de directeur d'unité, parce que je ne le suis plus depuis bien longtemps. Je suis ici parce que j'ai en charge le sous-comité agronomie, environnement, biotechnologie du comité d'experts des ZRR. J'ai aussi en charge l'ensemble des infrastructures scientifiques de l'INRA, et donc je « touche » directement aux questions du potentiel scientifique du pays dans le domaine considéré. Par ailleurs, en raison d'activités passées, je coordonne des programmes de mobilité européens de post-doctorants, mobilité entrante ou sortante de grande ampleur, ce qui me permet d'avoir une idée des pratiques d'échanges de scientifiques entre différents pays, qu'il

s'agisse des collègues qui vont à l'étranger ou des post-doctorants que nous recevons dans différents laboratoires d'agronomie.

Je vais donner quelques éléments précis permettant d'apprécier la charge que représentent les nouvelles modalités de la PPST. Depuis 2015-2016, le sous-comité a analysé 44 entités, dont 36 ont été proposées par les services du HFDS, les autres étant proposées par des établissements qui avaient souhaité qu'un certain nombre d'unités soient analysées. Ces unités concernent des établissements publics scientifiques et techniques (EPST), des universités, des établissements d'enseignement supérieur, des unités propres de certains établissements, des unités mixtes de recherche (UMR), mais aussi des unités de service et des plates-formes technologiques. Sur ces 44 unités, 26 analyses ont été achevées, et seulement 7 ont conduit à proposer des ZRR. Vous voyez la parcimonie du comité dans son activité pratique en termes de nombre de ZRR. L'ensemble des ZRR qui ont été proposées sont le plus souvent partielles, zonées, comme l'a évoqué M. Raoul. Cela tient beaucoup à notre domaine spécifique, géographique, bâtimentaire, scientifique et technologique. Tout le monde n'est pas dans le même laboratoire. Le zonage présente un certain intérêt.

Les premières années de mise en œuvre de la PPST ont été un peu compliquées dans le dialogue, puisqu'il fallait épurer des listes d'unités à traiter, auxquelles s'ajoutaient des ERR qu'il a fallu transformer en ZRR. Cela a conduit à un travail assez important du sous-comité. Mais ensuite, le sous-comité a eu un travail de présélection des entités soumises par le HFDS, de façon à éviter d'avoir trop de travail à mener et d'être prudents en termes de nombre de ZRR à traiter. On évolue vers un dialogue de plus en plus développé entre la proposition d'analyse et ce que peut en faire le sous-comité et les propositions qu'il fait ensuite au HFDS en matière de classement. En effet, certains laboratoires peuvent refuser l'autoanalyse par le questionnaire, ou même refuser d'avoir une ZRR. Dans ces cas-là, une discussion bilatérale est mise en œuvre, qui consiste à dialoguer en présentiel entre le sous-comité et le directeur d'unité qui conteste la décision. Dans notre cas, nous n'avons eu que deux réunions bilatérales, et à chaque fois la solution a été trouvée après le dialogue.

En matière de mise en œuvre, globalement les directeurs d'unité font une analyse du coût de transaction, plutôt administrative, *versus* la protection apportée, protection juridique, ou la mise en œuvre de solutions par l'établissement qui ensuite adapte la ZRR aux conditions réelles. Par ailleurs, se développe une sensibilité aux questions de sécurité et de protection. C'est l'un des avantages déjà soulignés.

Au niveau de l'INRA, 2 ZRR existent, et 6 autres sont en cours de création. Dans la mise en œuvre de ces ZRR, 104 demandes d'accès ont été faites sur les 2 ZRR existantes, avec un délai d'attente de 23 jours (délai de départ du FSD) et aucun refus. Nos ZRR étant très orientées sur des risques 3 et 4 en matière de sécurité et de microbiologie, ces entités n'ont pas généralement vocation à être complètement ouvertes. Cela s'explique par la nature de la technologie qui est mise en œuvre. Sur l'ensemble des coopérations internationales demandées en 2018, le temps de réponse moyen enregistré à l'INRA était de 16 jours, avec un seul refus.

À ce stade, globalement, pour le domaine assez large dont je m'occupe, agronomie, environnement, étude des écosystèmes, nutrition humaine et biotechnologie, qui est probablement l'endroit où il y a le plus de risques économiques de type R1, il semble pour le sous-comité, et il me semble dans la mise en œuvre, que l'évolution des modalités de déclaration et d'identification des ZRR va plutôt vers un dialogue qui conduit, au bout d'un certain temps, à une acceptation par les directeurs d'unité. Pour autant, ces ZRR ont été mises en place il y a très peu de temps, entre 2015 et 2017, et donc il faudra éprouver cette impression de bonne acceptabilité sur la durée. La lourdeur s'accumule au fur et à mesure des années. La question de la récurrence de ces lourdeurs se posera inévitablement.

Dernier point : l'INRA est dans une période de vive tension, du fait qu'il traite de questions sociétales compliquées, faisant l'objet de vives controverses : pesticides, OGM, expérimentation animale… Cela entraîne de forts risques d'atteinte du potentiel scientifique et technologique. Des atteintes et des destructions ont déjà eu lieu. Bien sûr, nous sommes très éloignés des grandes questions d'aéronautique, de cybernétique, qui ont précédemment été évoquées. Mais concrètement, dans le passé, il y a déjà eu des alertes. Il nous semble que la protection juridique apportée par le dispositif ZRR est un élément très important pour l'établissement INRA.

Cette protection juridique est une valeur ajoutée plutôt pour le directeur d'établissement que directement pour le scientifique en charge des coopérations internationales ; on peut voir cet écart dans le bénéfice comme une source des débats, qui sont légitimes, entre l'intérêt d'une ZRR et les lourdeurs administratives de leur mise en œuvre, au moins telles qu'elles sont vues dans le domaine dont je m'occupe au niveau du sous-comité des experts.

M. Cédric Villani, député, premier vice-président de l'Office.- Continuons avec les sciences de l'ingénieur en mécanique.

M. Éric Arquis, professeur à l'École nationale supérieure de chimie, biologie et physique (ENSCBP) de Bordeaux INP, chercheur à l'Institut de mécanique et d'ingénierie de Bordeaux (I2M), président de l'association française de mécanique (AFM).- J'étais encore directeur d'une unité assez importante de 350 personnes dans le secteur des sciences pour l'ingénieur (SPI) il y a deux ans, avec de multiples tutelles. C'est assez important à prendre en considération dans l'examen des dossiers PPST-ZRR, puisqu'il y avait à la fois une université, deux écoles d'ingénieur, une école nationale et Bordeaux INP au niveau local, ainsi que le CNRS et l'INRA avec un statut d'unité sous contrat (USC). J'évoquerai également mon expérience de pilote de deux sous-comités SPI.

En tant que directeur d'unité, il y avait une certaine inquiétude au moment de la mise en place de la ZRR. Des bruits circulaient, inquiétants. Un changement d'attitude a eu lieu depuis. À une époque, j'ai senti que la mise en place de la ZRR était relativement autoritaire, ou technocratique. N'étaient fournis ni explications ni accompagnements. Même les tutelles étaient un peu hésitantes, et parfois, pardonnez ma trivialité, elles « refilaient la patate chaude » à une autre tutelle. Ceci a beaucoup évolué. Depuis quelques années, on a fait preuve de davantage de pédagogie.

Personnellement, au niveau de mon unité, nous avions mis en place une démarche qualité en termes de management. Cette très importante unité avait des composantes assez différentes. J'ai expliqué à mes collègues que la ZRR s'apparentait à une démarche qualité, c'est-à-dire un chemin, parfois parsemé d'embûches, mais qu'il fallait prendre pour tendre vers une amélioration de la prise en considération des risques encourus.

La mise en place de ZRR correspond à des contraintes, que l'on a rappelées : tenir un registre des entrées, mettre en place des systèmes de contrôle électronique, ce qui n'était pas forcément le plus compliqué, ainsi qu'un certain nombre de procédures… Ce n'était pas très nouveau dans le cadre d'une UMR du CNRS, car ces procédures de demande d'accès existaient déjà. En tant qu'ERR, c'est quelque chose qui était parfaitement compris et accepté.

Pour revenir au sujet des publications, il n'y n'a pas du tout de demande d'autorisation. De toute façon, compte tenu des travaux que nous menons très fréquemment avec des industriels, nos publications sont soumises à l'acceptation de ces derniers, au titre du risque de divulgation d'informations de type technologique et industriel. Ceci ne nous est pas apparu comme un facteur limitant dans nos collaborations. J'ajoute que c'est plutôt un

aspect positif, dans la mesure où cela constitue une « carte de visite » importante, susceptible de rassurer les partenaires industriels, notamment ceux des secteurs de l'aéronautique et de l'énergie, où la compétition est très grande. C'est même en fait presque un tampon qui devient une nécessité pour contracter avec ces unités.

En ce qui concerne les collaborations internationales, pour l'instant je n'ai pas eu de retour négatif. Dans un cas, j'ai voulu inviter un collègue, d'une nationalité que je ne citerai pas ici, qui était déjà venu sans aucun problème travailler avec moi pendant de nombreuses années, une collaboration très productive, et de manière assez incompréhensible, c'est vrai qu'il a été récusé très temporairement. Je n'ai pas bien compris, je pense qu'il y avait peut-être une erreur sur l'identité de la personne, une certaine confusion. Un an après, il a été autorisé de nouveau à venir. De temps en temps, il y a peut-être des petits couacs, mais c'est tout à fait admissible.

En tant que pilote de sous-comités, dont mon collègue a rappelé les modes de fonctionnement, j'ajoute que la première étape me semble la plus importante : celle de la tenue des réunions de sensibilisation. Avant que les directeurs d'unité ne remplissent le fameux questionnaire, on leur explique les fondements généraux de la PPST et ce qu'ils doivent faire pour remplir au mieux ce questionnaire d'autoévaluation. Dans notre secteur, il y a une certaine méfiance au début, mais elle s'estompe assez rapidement. Certaines personnes découvrent même que leurs laboratoires sont vulnérables dans certains aspects.

Ensuite, dans le cadre de la mise en place des ZRR, il est vrai que lorsqu'on passe à certains détails beaucoup plus pratiques, un certain nombre de problèmes se posent, dont un qui n'a pas encore été évoqué : la coexistence dans les locaux de recherche avec des personnels de la formation. C'est notamment vrai dans les écoles d'ingénieur ou dans les laboratoires, qui servent aussi de lieu de formation. Cette perméabilité n'est pas toujours très facile à gérer ni compatible avec la mise en place d'un certain type de contrôle des accès.

En conclusion, pour le secteur SPI, les relations partenariales fortes amènent à une prise de conscience marquée des risques de captation des savoirs théoriques et technologiques. Les contraintes induites par la PPST et leur traduction sous forme de la mise en place de ZRR ne sont certes pas acceptées de gaieté de cœur. Pour ce faire, une souplesse, une pédagogie et un accompagnement sont indispensables. Le contrôle des accès est important, et à mon avis, c'est l'instruction *ab initio* des dossiers des candidats entrant au laboratoire qui doit être privilégiée, peut-être plus que l'accès journalier. C'est une opinion très personnelle.

À côté du contrôle personnel, il y a un aspect plus critique, beaucoup plus insidieux, qui n'a pas été mis en exergue ce matin : le contrôle de la sensibilité des systèmes informatiques. Celui-ci doit être suivi de manière très étroite. Cela ne se voit pas forcément, et quand cela se voit, il est trop tard. Par contre, ce contrôle a un coût humain. Il faut faire appel à des spécialistes. Des unités de petite taille ne peuvent peut-être pas se le permettre. Il y a également un coût financier pour protéger les serveurs, etc.

M. Cédric Villani, député, premier vice-président de l'Office.- Nous allons terminer par l'informatique.

M. Jean-Marc Jézéquel, professeur en informatique à l'université Rennes 1, directeur de l'Institut de recherche en informatique et systèmes aléatoires (IRISA).- Beaucoup de choses ont déjà été dites. Pour rappel, les missions d'un laboratoire de recherche publique, telles que définies par la loi, consistent à produire des connaissances et à les transférer, au sens très large du terme, vers la société, les étudiants, les entreprises, etc. Les connaissances qui sont produites ne sont généralement ni protégeables, en particulier en informatique car on ne protège pas, au sens des brevets, ni des algorithmes, ni des

théorèmes, et elles ne sont pas dangereuses en elles-mêmes. Bien sûr, l'utilisation de ces connaissances peut parfois poser problème, par destination, ce qui ouvre la porte à beaucoup de fantasmes, d'autant plus grands que la communauté du renseignement est éloignée du monde de la recherche, comme cela est bien mis en évidence dans les notes d'analyse sur la mise en œuvre de la PPST aux États-Unis et au Royaume-Uni. On peut penser par exemple au fantasme autour de la cryptographie qui aujourd'hui n'est plus du tout un sujet sensible, alors que beaucoup de gens continuent à le croire.

Force est de reconnaître une tension naturelle entre les missions de diffusion d'un laboratoire public et la PPST qui essaie de restreindre cette diffusion. En informatique, il y a un cas particulier lié au monde des codes sources ou logiciels libres *(open source)*, qui est aujourd'hui constitutif de la recherche en informatique, et au-delà de l'industrie mondiale de l'informatique, laquelle est basée essentiellement sur de l'*open source*. Je ne vais pas avoir le temps de détailler mais c'est un sujet particulier.

J'insiste sur le fait qu'un laboratoire de recherche publique est un seau percé avec de très gros trous : il y a les mouvements de personnel, qui sont constitutifs de la recherche, mais aussi les comités d'experts internationaux. Aujourd'hui, les grands laboratoires vivent de projets, et pour monter un projet, on va donner nos meilleures idées à des comités d'experts internationaux, non français, qui se les approprient plus ou moins, sans vraiment de contrôle. Il y a d'énormes trous à ce niveau-là, aux côtés des trous plus petits déjà mentionnés : vols de données, vols d'ordinateur, etc. Ces derniers sont des réalités, mais en termes de quantité d'informations qui fuitent, c'est infiniment plus faible que les deux « trous » que j'ai mentionnés. L'IRISA est un laboratoire de recherche de 850 personnes, partagé entre 8 tutelles, l'essentiel des gens qui font de la recherche informatique en Bretagne font partie de ce laboratoire. La ZRR y est seulement partielle, sur quelques équipes.

Quelques chiffres très précis vont vous donner une idée des flux dans ce laboratoire en 2016. Nous avons recruté 20 nouveaux fonctionnaires, signé 239 contrats de travail en CDD, dont 86 doctorants (pour 86 thèses), 857 conventions de stages, dont 81 au niveau du master 2 (le reste étant au niveau master 1 et licence 3), plus de 2 000 missions avec frais, dont la moitié à l'étranger. Environ 1 000 articles ont été publiés, environ 200 projets ont été déposés. Je reviens sur cette fuite massive des meilleures idées au moment où elles ne sont pas encore développées. Sur ces 200 projets, 35 ont été acceptés, avec des financements collaboratifs, et au total une centaine de partenaires différents. Il faut imaginer le flux d'interactions avec le reste du monde. Un laboratoire n'est pas une tour d'ivoire, contrairement à ce que s'imaginent beaucoup de gens. Le total des financements s'élève à 12 millions d'euros sur ces 35 contrats. Cet argent est vital pour travailler dans le laboratoire et payer les CDD.

Aujourd'hui, la tendance du CNRS est d'insister pour que des laboratoires entiers passent en ZRR. Pour nous, ce serait absolument catastrophique. Faire gérer ces flux-là et les remonter systématiquement au niveau du haut fonctionnaire de défense, ce n'est pas envisageable. En tout cas c'est mon point de vue.

En conclusion, une ZRR à l'échelle d'un laboratoire, c'est à la fois trop et trop peu. C'est trop pour les raisons déjà mentionnées de coûts de la gestion technique et administrative, qui est proportionnelle à l'activité du laboratoire. Plus forte est l'activité du laboratoire, plus ça coûte cher. Le gain marginal de PPST est faible, parce qu'elle se concentre sur les petits trous et laisse les grands béants.

Une ZRR, c'est aussi trop peu. Dans un laboratoire comme le mien, des choses sont réellement sensibles : une base de virus informatiques particulièrement virulents, quelques matériels qui ne sont pas à mettre entre toutes les mains, quelques données très sensibles (données personnelles, médicales, etc.), qu'il faut protéger de manière très forte. Dans quelques-uns de nos contrats avec des industriels, ceux-ci demandent que leurs données soient protégées. Nous le faisons avec toute la rigueur nécessaire. Nous travaillons également beaucoup avec la direction générale de l'armement (DGA) du ministère de la défense sur un certain nombre de dossiers, et nous appliquons leurs procédures.

Force est de constater que ce que propose la ZRR est surtout de coller des étiquettes sur les portes. Face à ces problèmes-là, nous devons aller au-delà. Notre proposition est de concentrer la protection sur ces artefacts. Cette protection serait organisée en plusieurs niveaux concentriques, avec un premier cercle très fortement sécurisé, une sorte de ZRR ++, à l'entrée de laquelle il y aurait un vrai contrôle d'accès, une vraie séparation des réseaux, etc. Je ne vais pas rentrer dans les détails techniques. Ce premier cercle se concentrerait sur les artefacts et non pas sur les personnes, de sorte que ce ne soit pas les personnes qui soient en ZRR, mais leur outil de travail, sur sa partie sensible.

Le deuxième cercle, sorte de ZRR - -, offrirait un certain nombre de protections de type juridique, tout à fait bienvenues dans certains cas, avec contrôle d'accès quand c'est nécessaire pour les laboratoires qui s'y prêtent, sous la responsabilité du DU. Mais pour y entrer, le DU ne demanderait pas forcément, compte tenu de nos flux, de remonter jusqu'au HFDS.

Dans le troisième cercle, pour la perméabilité avec l'enseignement, les contrôles pourraient se faire de manière beaucoup plus périphérique, comme c'est déjà le cas au travers des procédures de visas ou de filtres sur les visas.

M. Pierre Paradinas, professeur titulaire de la chaire systèmes embarqués au Conservatoire national des arts et métiers (CNAM), président de la Société informatique de France (SIF).- Je précise que ce qui a été mentionné par M. Jézéquel ne concerne pas seulement son laboratoire, mais l'ensemble des laboratoires informatiques. Effectivement, il y a cette difficulté particulière en informatique, d'être capable de bien travailler sur certains objets ou artefacts informatiques, lesquels sont duaux. Pour pouvoir se protéger, il faut connaître les techniques des gens qui attaquent. Quand on connaît bien le sujet et qu'on travaille scientifiquement sur ces domaines-là, il suffit de faire fonctionner les objets de manière un peu différente pour changer de côté. Il est difficile de détecter sur quel périmètre il est nécessaire de positionner une ZRR, ou comme le disait M. Jézéquel, une ZRR ++. Cela demande un gros travail, à la fois des laboratoires et des personnes amenées à porter des diagnostics ou des avis.

Pour compléter les propos de M. Jézéquel, les spécificités de notre discipline comme l'*open source* sont extrêmement contraignantes. J'évoquerai aussi les données ouvertes *(open data)*, le pendant de l'*open source*, qui conduit à la nécessité, pour que le travail des chercheurs soit reconnu, rendu public et utilisé, de publier l'ensemble de leurs travaux. Cela permet d'avoir des expériences reproductibles. Dans le monde scientifique, c'est de plus en plus important, beaucoup de résultats scientifiques étant parfois contestés parce que ce sont de faux résultats. Si nous publions l'ensemble de nos outils – dans notre secteur, cela signifie des logiciels et des données –, cela permet que d'autres soient en mesure de reproduire nos expériences. C'est intrinsèquement nécessaire à notre discipline et à notre travail.

Pour conclure par quelques recommandations, je suis favorable à des sous-zones ou des sous-équipes. Il n'est pas vivable de soumettre l'ensemble d'un laboratoire à de trop fortes contraintes. D'ailleurs, c'est le cas en entreprise. Avant d'être enseignant-chercheur, j'étais chez un opérateur d'importance vitale (OIV). On savait travailler à la fois pour Visa et Mastercard. Je vous prie de croire que les équipes travaillant pour Visa n'étaient pas les mêmes que pour Mastercard. C'est pareil quand on travaille pour l'industrie de la défense. Beaucoup d'équipes pensent que ce serait important de vraiment spécialiser leur organisation, à travers des sous-équipes ou des sous-laboratoires.

Un autre point extrêmement important : les coûts administratifs induits ne doivent pas empêcher de conserver une grande agilité pour la recherche. Agilité pour faire venir les gens, agilité pour se déplacer, agilité pour publier, agilité pour pouvoir recruter, ce qui est vraiment primordial. Si vous mettez trois mois à répondre, les personnes iront à Zürich ou aux États-Unis sans aucun problème, les conditions y sont au moins aussi bonnes qu'en France.

M. Cédric Villani, député, premier vice-président de l'Office.- Je remarque que ce que vous dites sur la difficulté d'avoir tout un laboratoire sous régime restrictif est un peu à l'opposé de ce que nous décrivait M. Drillon, qui estimait plus contraignant d'avoir des sous-équipes en ZRR. Cela traduit peut-être des manières de fonctionner différentes, selon que l'on est en informatique ou en physique.

En tout cas, dans le panel des réactions des scientifiques, on a bien vu la diversité des points de vue et des attitudes d'une discipline à l'autre face au dispositif ZRR. Monsieur le préfet Inglebert, je vous propose de réagir à ces différents commentaires, certains étant plutôt positifs, d'autres critiques.

M. Xavier Inglebert.- Sans répondre à tous les points précis, je veux simplement vous dire de ne pas prendre des vieux chiffres datant de quatre ou cinq ans. Mes chiffres datent de 2018 et ils sont nets et précis.

Un troisième acteur dans notre débat n'est pas présent ici, ce sont les établissements. Le dispositif PPST concerne les directeurs d'unité, nous en administration centrale et les établissements. J'ai utilisé tout à l'heure l'expression « délai hors FSD ». Vous parlez de deux mois. J'ai ici tous les cas de votre laboratoire qui ont transité au niveau central : le délai moyen est de 26 jours.

M. Cédric Villani, député, premier vice-président de l'Office.- Français et étrangers en moyenne, n'est-ce pas ? Ce sont les délais pour les étrangers qui sont le plus l'objet de critiques.

M. Xavier Inglebert.- Tout à fait, en moyenne globale. Il n'en reste pas moins qu'il y a aussi des problématiques avec les établissements. Les établissements sont porteurs, surtout les universités. C'est un travail que nous devons mener ensemble. Il faut les intégrer dans le travail et les propositions que je vais vous faire.

Concernant l'attractivité, je note que le dernier prix Nobel de chimie, M. Karplus, était dans un laboratoire à Strasbourg il y a trois ans. Cela ne fait pas fuir non plus les grands scientifiques hors de France. Un tiers des recrutements de chercheurs au CNRS sont des étrangers. On l'a vu en mathématiques, c'est vrai dans les autres disciplines.

Je peux répondre de gré à gré ultérieurement sur chaque point, mais en public, je pense que ce n'est pas utile. Sachez aussi qu'il y a des cas de refus, et que, toujours tenu par le confidentiel défense, je ne peux alors pas vous expliquer pourquoi. Je n'en n'ai pas la capacité juridique. Sachez cependant que si un cas est refusé, c'est vraiment parce qu'il y a un point délicat, y compris en termes de prolifération.

Voici mes propositions. Elles se déclinent en trois axes.

Premier axe, j'aimerais proposer une sorte de contrat PPST, avec vous, directeurs d'unité (DU) et les établissements, qui vous donnerait quatre grandes garanties en tant que DU :

– 1. Une garantie d'échange systématique avec chaque directeur d'unité de l'évaluation réalisée par le collège des experts. En discutant avec M. Jézéquel, je me suis rendu compte qu'il n'avait pas eu connaissance du contenu de l'évaluation du collège des experts. Il faut en discuter avec chaque directeur d'unité. C'est notre devoir de pédagogie.

– 2. Garantir que les tracés des ZRR, tracés physiques ou intellectuels, c'est-à-dire des efforts de recherche sur lesquels on affecte des doctorants, prennent en compte les préoccupations des DU. On commence à progresser sur ces principes avec les avis réservés, ils peuvent être évolutifs en fonction de l'évolution des laboratoires. Le système n'est pas figé.

– 3. Garantir que le règlement intérieur de la ZRR soit un document à l'initiative de l'établissement et du DU. Nous devons avoir cette discussion avec chaque établissement.

– 4. Garantir, pour ce qui concerne les chercheurs étrangers, que nous puissions définir, avec les DU et les établissements porteurs, les périmètres de recherche et les précautions raisonnables à apporter selon les nationalités. On peut en parler ensemble. C'est la question de l'analyse sous réserve. Pour certains cas concrets, cela a déjà été mis en œuvre récemment.

Le deuxième axe concerne les avis sur demande d'accès. Je vous propose une expérimentation de simplification administrative pour deux ans : une procédure simplifiée, pour les établissements qui le souhaitent, et qui certifie leurs capacités à les mettre en œuvre. C'est la réciprocité dans l'effort. Cela diviserait par deux les délais, hormis les cas plus délicats où il faut comprendre que nous sommes parfois face à des impératifs plus complexes, qu'il est possible de régler au cas par cas. Il reste que même dans le cadre d'un dialogue dans un lieu plus confidentiel, je ne pourrais pas tout dire à un directeur d'unité.

Troisième axe : je propose de mener un travail d'aménagement du dispositif réglementaire par discipline. C'est effectivement ce que met en valeur ce débat. Je remercie le directeur de l'INSMI d'avoir accepté d'organiser, avec les directeurs d'UMR mathématiques, un dialogue. Nous verrons ce qu'il en ressort.

Sachez que nous avons fait une première évaluation, très empirique, du nombre de laboratoires de mathématiques susceptibles de pouvoir passer en ZRR. C'est moins d'un cinquième par rapport à tous ceux qui existent. Tout le monde ne passe pas en ZRR, loin de là. Cela demande à être travaillé, évalué au cas par cas. La meilleure façon de savoir, c'est d'être dans le collège des experts. Plus vous serez dans ce collège, plus vous serez partie prenante du dispositif, et mieux vous maîtriserez, mieux vous contrôlerez. La politique de la chaise vide n'aide pas à travailler. Je suis ravi de venir vous rencontrer le 11 mars prochain. Je répondrai à tous les arguments. Je vous remercie du dialogue que vous ouvrez.

Dernier point : je propose aux informaticiens, avec les établissements et l'INRIA, de travailler avec vous, de façon partagée, sur les spécificités informatiques, autour des pistes que vous avancez. Nous devons les creuser dans le détail. Est-ce qu'elles peuvent s'articuler avec les textes existants ? Je ne peux pas vous répondre du tac au tac. Nous devons creuser ces pistes.

Dans cette démarche, moi-même et mon service sommes à la disposition des laboratoires, établissements et organismes. Je vous propose ces trois axes, mais naturellement, si vous en avez d'autres, nous les ajouterons. C'est une suite que je veux donner à ces travaux. Je suis à votre disposition pour en rendre compte quand vous le souhaitez et à votre demande.

M. Cédric Villani, député, premier vice-président de l'Office.- Merci beaucoup monsieur le préfet. Nous sommes très reconnaissants. Soyez certains que nous répondrons avec plaisir à votre invitation de vous interroger et contrôler aussi souvent que nous en avons besoin sur ce sujet qui intéresse aussi bien la communauté scientifique que la représentation nationale.

Chers collègues, je vous propose de continuer nos échanges autour de ces thématiques. Je vous fais part de quelques éléments qui m'ont frappé. En premier lieu, nous avons vu qu'en fonction des disciplines et des sujets, le dialogue est perçu de façon fort différente. On comprend que du côté d'un laboratoire P4, la lourdeur de la menace et le degré de sécurité nécessaire rendent tout à fait naturels, légitimes, les procédures ZRR telles qu'elles sont.

Lorsque la menace est beaucoup moins claire et perceptible, en particulier dans les domaines des mathématiques et de l'informatique, on voit que le dialogue est bien plus « conflictuel » si l'on peut employer ce mot. Le préfet Inglebert indiquait à l'instant que moins de 20 % des laboratoires pouvaient passer en ZRR, mais je suis tout de même assez surpris d'un chiffre aussi élevé alors qu'il lui semble plutôt faible. Je me demande quel est le pourcentage des incidents détectés, incidents sérieux relevés, qui font intervenir les laboratoires de mathématiques. Si quelqu'un a des éléments diffusables dans cette audition publique, ce sera intéressant. Sinon nous pourrons revenir sur ces discussions dans un autre cadre.

Je retiens aussi des interventions sur la notion de gradation. Peut-être que le dispositif ZRR fonctionnant en « tout ou rien » peut évoluer vers des dispositifs de différentes amplitudes. On a bien noté, dès le début avec Mme Landais, que les textes réglementaires qui définissent le régime ZRR comportent une marge de manœuvre. C'est aussi de la doctrine et de la jurisprudence qui ont mis en place les procédures. Il faudrait certainement revoir cela.

Dernier point qui m'a frappé : cette notion de confiance dans les décisions, avec un arbitraire qui a été ressenti à plusieurs reprises.

Pour la résolution de ces questions, nous devrons mettre en place une institution, ou une personne, ayant à la fois la confiance des autorités de défense au plus haut niveau et la confiance du milieu scientifique. Cette sorte de médiateur peut être une personne, ou un très petit nombre de personnes, habilité(es) confidentiel défense qui, de par leur carrière et leur passé, ont la confiance du milieu scientifique, et qui, de par leur habilitation, ont la possibilité d'entendre les choses qui ne peuvent même pas se dire aux directeurs d'unité.

Mme Claire Landais, secrétaire générale de la défense et de la sécurité nationale (SGDSN).- Le message collectif du côté des institutions et des entités de l'État représentées ici est bien de prolonger le débat à la demande et dans les instances qui existent d'ores et déjà. Le préfet Inglebert l'a dit, nous n'avons pas intérêt à nous retourner vers le passé, mais en revanche, nous avons intérêt à dialoguer et à trouver le moyen d'adapter le dispositif. Vous parliez de gradation, et vous avez effectivement relevé ce que j'ai dit à propos des marges de manœuvre et de la souplesse potentielles. Il faut les utiliser, et pour cela, être dans le dialogue, avec des médiateurs le cas échéant, pourquoi pas.

Il n'a pas seulement été question de la PPST, nous avons également évoqué la politique consulaire, des dispositions qui sont dans le code de l'éducation. Si l'on veut juger et évaluer l'efficacité de la PPST, je pense qu'il ne faut pas lui reprocher des choses qui relèvent d'autres champs, par exemple du visa consulaire.

À l'inverse, je reconnais qu'il a pu y avoir des erreurs, ou un excès de précaution. J'entends ce qui est dit sur le fait que chacun peut parfois « ouvrir le parapluie », et que ce cumul de parapluies peut faire beaucoup à la fin. Il faut y travailler. Parfois, des comportements isolés ont pu gêner, mais il ne faut pas nécessairement en tirer des conséquences excessives sur la politique générale.

Enfin, je disais en introduction qu'on a besoin du secret de la défense nationale, mais qu'il doit être calibré au juste besoin. Au SGDSN, nous passons notre temps à le manier. Assez régulièrement, nous avons nous aussi besoin de justifier des décisions administratives devant les juges, pas seulement devant le Parlement. Pour cela, il faut être capable de restreindre le champ du secret à ce qui est absolument nécessaire de protéger. Parmi les pistes de réflexion qui ont été données, c'est une piste sur laquelle il faut avancer. Là aussi, ce n'est pas du tout ou rien dans la motivation et dans ce que l'on est capable de dire. Il peut y avoir un cœur indicible et des informations à côté qui peuvent être déclassifiées, ou non protégées, et qui peuvent être dites en étant compréhensibles par le destinataire sans entrer dans le cœur du cœur.

J'ai le sentiment qu'il y a des possibilités d'ajustement, d'adaptation à des particularités. Tout cela passera par le dialogue.

M. Cédric Villani, député, premier vice-président de l'Office.- Une remarque. Dans les exposés de plusieurs collègues scientifiques, la question de la comparaison internationale est revenue, avec cette idée en filigrane que la procédure ZRR est sensiblement plus dure, plus lourde, plus centralisée, que ce qui se pratique à l'étranger, y compris dans des pays comme le Royaume-Uni ou les États-Unis, qui ne passent pas pour naïfs en matière de sécurité.

En revanche, autant du côté des institutions, j'ai entendu parler de coopération internationale dans la détection de problèmes, autant je n'ai pas entendu évoquer de coopération dans la coordination des règles de sécurité. On imagine qu'elles devraient aussi être liées. Par exemple, si un individu suspect cherchant à s'introduire dans une ZRR est détecté dans un pays, il pourrait sembler normal que les autres pays en soient informés. Une certaine homogénéisation des procédures de sécurité entre pays apparaîtrait naturelle, afin de ne pas perdre en attractivité et en souplesse les uns par rapport aux autres dans la compétition économique et scientifique.

Mme Claire Landais.- Je ne connais pas l'origine des deux fiches sur le Royaume-Uni et les États-Unis qui vous ont été adressées. J'ai pour ma part plutôt le sentiment qu'au contraire, on n'est pas dans une situation isolée, il y a des dispositifs très comparables à l'étranger. Parfois, cela a été dit par Guillaume Poupard, ils mélangent des considérations de sécurité et de concurrence économique qui font que nous ne sommes pas du tout les plus durs de ce point de vue. Je n'ai pas du tout le sentiment qu'on fait peser sur nos opérateurs des contraintes particulièrement fortes. Ce sentiment est partagé par les postes diplomatiques à l'étranger. Encore une fois, nous devons travailler sur cette contrainte, sur la façon de la calibrer.

M. Cédric Villani, député, premier vice-président de l'Office.- Parfois, un pays ou une institution annonce quelque chose, et en réalité, il fait autre chose sur le terrain. Il faut comparer à la fois ce qui est effectué et les réputations.

Mme Claire Landais.- Il existe des partenariats entre services de renseignement. Beaucoup d'échanges se pratiquent. Par ailleurs, au SGDSN, nous réfléchissons avec nos homologues à nos modalités de protection, nos politiques en la matière. Par exemple, le champ de la non-prolifération constitue le domaine dans lequel nous avons le plus d'interactions avec nos homologues, le plus d'exercices en commun, le plus de comparaisons de nos dispositifs, le plus d'actions coordonnées pour intercepter, entraver des mécanismes de prolifération qui dépassent les frontières.

M. Jean-Marc Jézéquel.- Je me permets de vous contredire sur la manière dont est gérée la PPST aux États-Unis ou en Angleterre ; ce qui est décrit dans ces notes correspond tout à fait aux retours de mes collègues en poste dans ces pays-là. Elle est très différente dans sa nature, même s'il existe des coopérations, par exemple entre les services américains ou l'armée et certaines universités. La différence majeure, c'est que les choses n'y sont pas gérées de manière aussi jacobine ou centralisée qu'en France, où systématiquement toutes les demandes remontent au ministère, ce qui induit toute cette lourdeur que n'ont pas nos collègues à l'étranger, sauf cas particulier, si l'université est dite militaire, aux États-Unis par exemple.

Mme Claire Landais.- L'une des pistes de simplification vise à répondre à cet empilement qui fait qu'il y a de la lourdeur administrative dans le système.

M. Hervé Raoul.- Sur la question internationale, il me semble important de se pencher sur les comparaisons avec ce qui est vécu ailleurs, en faisant bien attention à une chose : dans le domaine de la protection, on n'a pas forcément le miroir exact de la ZRR dans les pays étrangers. Il faut regarder l'ensemble des réglementations. Des établissements comme les nôtres sont régis par des réglementations très diverses, dont certaines, je peux vous le garantir, y compris en France, sont beaucoup plus contraignantes que la PPST elle-même. Il faut regarder domaine par domaine, et sur ce point, je suis d'accord avec l'ensemble de mes collègues. Les choses ne sont pas comparables pour tous les domaines. Dans le nôtre en tout cas, la réglementation sur l'accès aux micro-organismes et toxines est certainement beaucoup plus contraignante aux États-Unis. En revanche, au niveau européen, cette réglementation est plus contraignante en France qu'en Allemagne ou dans les autres pays limitrophes.

M. Pascal Auscher.- Dans le domaine des mathématiques, aux États-Unis, en Grande-Bretagne et dans d'autres pays que je connais bien, il n'y a pas du tout ce genre de contrôles. D'ailleurs, les collègues qui viennent nous rendre visite, américains ou autres, sont parfois un peu surpris de l'esprit un peu tatillon des procédures françaises pour les accueillir, parfois temporairement. Il faut faire attention à ce que la lourdeur, et parfois la lenteur des procédures, ne nuisent pas à l'attractivité des mathématiques en France. Nous sommes au plus haut niveau international. Il faut absolument maintenir l'attractivité et la place des mathématiques françaises dans le monde.

Pour rebondir sur ce qu'a dit M. Inglebert, ce n'est pas la politique de la chaise vide que veulent pratiquer les mathématiciens. Ils ont pratiqué la politique assis sur la chaise pendant un certain temps, jusqu'à ce que le désaccord soit acté entre les deux services. Il y a une volonté peut-être de reprendre un dialogue, il y a d'autres propositions, on veut les entendre, et l'on verra bien ce qui se passera.

M. Gilles Aumont.- Je voulais apporter quelques compléments sur la comparaison internationale. Je peux témoigner qu'il faut vraiment regarder dans le détail. Dans certains domaines, les États-Unis et la Chine sont bien plus restrictifs que la France en matière de coopération et de technologie, y compris s'agissant des plantes cultivées qui nous intéressent

directement, en génétique ou en génomique. Nous devons être attentifs aux cas d'espèce. Les effets peuvent être très différents selon les pays et les domaines.

Deuxième point : on a souvent évoqué l'attractivité de la France, avec la question des chercheurs qui viennent en France. Je voudrais évoquer en sens contraire la situation des chercheurs qui vont à l'étranger. Il y a là une fuite potentielle. On s'aperçoit que certains de nos jeunes chercheurs, post-doctorants en particulier, qui ont vocation à partir à l'étranger avant de trouver un poste en France, vont dans certaines universités américaines, chinoises, etc., où très naturellement, ils délivrent tous leurs droits de propriété intellectuelle à l'université qui accueille. Sous ses attraits accueillants, celle-ci récupère pas mal d'éléments. Dans cette vision de la protection, il faut à la fois nous protéger nous, mais aussi faire en sorte que les jeunes chercheurs qui partent à l'étranger aient un bagage, une sensibilité en matière de PPST.

M. Jean-Marc Jézéquel.- Je voulais donner un exemple où la communication entre les services et les scientifiques est par définition difficile. Si vous regardez la manière dont est faite la gradation des risques, les critères évalués vont de 0 à 3 : 0 pour le risque nul, 1 pour un risque possible, etc. Aucun scientifique qui se respecte ne dira jamais que le risque est nul. Par construction, la gradation est donc déformée ou alors interprétée de manière bizarre. Je conteste profondément cette échelle en tant que scientifique. On connaît d'autres échelles qui sont moins mauvaises en termes de formulation. Dès le début, vous avez un problème de dialogue entre les services ; pour eux, peut-être que cette échelle fait sens, mais pour les scientifiques, elle ne fait pas sens.

M. Frédéric Marie, responsable de la PPST auprès du service du HFDS.- Monsieur Jézéquel, je me permets de vous répondre au sujet de cette échelle. Je l'ai suivie à la direction générale de la recherche et de l'innovation (DGRI) du MESRI une première fois, et maintenant je la suis depuis deux ans, en tant que coordinateur de l'ensemble du collège d'experts et du suivi de tous les sous-comités thématiques, y compris celui du domaine des sciences et technologies de l'information et de la communication (STIC). Je peux vous assurer que très souvent, des risques sont évalués à 0 et que l'on sait aboutir, avec les experts, y compris avec l'aide des DU, à une cotation à 0 même si, effectivement, on n'est pas dans un risque absolument nul. Le risque existe toujours. En physique, le risque nul comme le risque absolu n'existe pas, mais on est bien obligé de définir une échelle de cotation. Cette échelle va de 0 à 3. On considère que 3 est un maximum. Parfois on serait tenté de monter à 5. On ne peut pas descendre en dessous de 0. Sur l'ensemble des 350 unités qui ont déjà été évaluées par le collège d'experts depuis 2014, très peu d'unités ont l'ensemble des 3 risques non nuls.

M. Jean-Marc Jézéquel.- Il n'en demeure pas moins que la négociation vise à quantifier le risque. Si vous, vous me dites que ce risque n'est pas possible, moi, en tant que scientifique, je ne pourrai pas vous dire le contraire. Je suis « piégé » en quelque sorte, et donc ce n'est pas bon pour la confiance.

M. Cédric Villani, député, premier vice-président de l'Office.- Chers collègues, on voit que le dialogue et la confiance sont à établir et que le choix des mots n'est pas anodin, dans la loi comme dans les négociations.

Il est temps de clore cette seconde table ronde. Comme on l'a compris, toutes ces interventions ne constituent que le début de la discussion. Il va falloir revenir plus précisément sur les questions de comparaison internationale, analyser ce qui a été pointé par les uns et les autres. Il y aura également des questions sur la méthodologie. On a bien compris que le cas des laboratoires de mathématiques est encore en suspens. Au vu de ce que

nous avons entendu, je pense qu'il va falloir encore un peu de temps avant que le dialogue soit conclusif.

De façon générale, j'ai le sentiment qu'il faut bien avoir en tête :

– en premier lieu, la question des spécificités discipline par discipline, qui visiblement induisent de fortes différences d'appréciations entre les comportements, les besoins et les acceptabilités ;

– en second lieu, la nécessité de combiner la question de la défense nationale avec celle de la coopération internationale forte qui règne dans les différentes sciences ;

– troisièmement, la prise en compte des intérêts de défense et des intérêts économiques. Parfois on a envie de les considérer ensemble, parfois séparément ;

– quatrièmement, les questions de délais, il y a eu des confrontations de statistiques et de chiffres ;

– cinquièmement, la question de l'organisation et du niveau de décision. À plusieurs reprises, ont été opposées les décisions locales, laissées à l'appréciation des acteurs locaux dûment informés, aux décisions centralisées, obtenues par l'avis d'un acteur central – le ministère. L'un et l'autre modèle ont leurs avantages et leurs inconvénients.

Nous avons encore du pain sur la planche avant d'aboutir à un vrai accord, et surtout une bonne confiance sur tous les domaines dans le sujet. Nous avons vu que la question de la protection du patrimoine scientifique et technique (PPST) n'est ni totalement conflictuelle, ni totalement consensuelle. Elle est quelque part entre les deux, et il convient de faire en sorte qu'elle puisse devenir autant consensuelle que possible, aussi bien pour le bien-être de nos chercheurs et ingénieurs, que pour l'efficacité de nos procédures de défense.

Nous continuerons à suivre cette problématique au niveau de l'Office parlementaire. Nous aurons certainement l'occasion d'autres échanges, avec les uns et les autres, au fur et à mesure que la discussion progressera. Il est probable que nous aurons un jour une nouvelle audition dans un format qui s'apparentera à celui-ci, mais pas trop tôt. Laissons le temps faire son œuvre pour la recherche de procédures optimisées. Dans cette attente, je vous remercie toutes et tous chaleureusement pour le temps que vous avez consacré à cette problématique capitale.

II. COMPTE RENDU DE LA RÉUNION DE L'OPECST DU JEUDI 21 MARS 2019 PRÉSENTANT LES CONCLUSIONS DES AUDITIONS SOUS FORME DE TABLE RONDE

Mme Catherine Procaccia, sénateur, vice-présidente de l'Office. – Ces auditions, qui ont eu lieu le 24 janvier dernier, avaient pour l'objet de faire un point sur les menaces de captation de savoirs et technologies sensibles et de faire le bilan des procédures relatives aux zones de recherche à régime restrictif, dites ZRR.

La première audition sous forme de table ronde, présidée par Gérard Longuet, s'est déroulée à huis clos, en raison du caractère sensible de certaines informations qui ont été évoquées à cette occasion. La seconde, présidée par Cédric Villani était ouverte à la presse. Je cède la parole à ce dernier pour la présentation des conclusions de cette audition.

M. Cédric Villani, député, premier vice-président de l'Office, rapporteur. – C'est un sujet dont j'ai eu à connaître en tant que directeur de laboratoire. Il se traitait de façon fermée et quelque peu traumatisant pour la communauté scientifique, en raison d'une divergence entre la volonté des autorités chargées de la sécurité nationale d'éviter tout risque d'espionnage et la volonté des scientifiques de travailler dans un contexte ouvert, accueillant et international. Les représentants de la sécurité nationale estimaient qu'il leur appartenait de décider de ce qui était bon pour les scientifiques, tandis que ces derniers revendiquaient leur liberté d'organisation.

La première table ronde sur les menaces et les risques, confidentielle, a réuni les principaux responsables de la protection du potentiel scientifique et technique (PPST) de la nation ; secrétariat général de la défense et de la sécurité nationale (SGDSN), direction générale de la sécurité intérieure (DGSI) du ministère de l'intérieur et Agence nationale de la sécurité des systèmes d'information (ANSSI).

Les intervenants ont exposé les menaces et risques de captation de savoirs, savoir-faire et technologies – thésards espions, récupération de documents par exemple. Le dispositif des ZRR, au cœur de la PPST de la France, a été rappelé : accès physiques sécurisés, autorisation des personnels travaillant dans la zone après enquête, protection informatique, procédures de concertation entre les directeurs d'unité et les services chargés de la sécurité avec un collège d'experts et des sous-commissions thématiques. C'est un régime très restrictif, alors que les laboratoires scientifiques préfèreraient disposer d'outils de réponse à la menace.

La deuxième table ronde, ouverte à la presse, a réuni le haut fonctionnaire de défense et de sécurité (HFDS) adjoint des ministères de l'enseignement supérieur, de la recherche et de l'innovation (MESRI) et de l'éducation nationale et de la jeunesse (MENJ), et des chercheurs de plusieurs disciplines. Les responsables de laboratoires en sciences de la vie, agronomie et sciences de l'environnement et sciences pour l'ingénieur (mécanique), ont montré qu'ils avaient bien intégré le dispositif des ZRR. En revanche, leurs homologues des laboratoires de mathématiques, d'informatique et de physique ont exprimé de vives critiques à son encontre : délais d'autorisation des candidats, frais de protection physique et logicielle, surcoût administratif de gestion, insuffisance du dialogue avec les services chargés de la sécurité, incompréhension des décisions prises. Pour les seuls candidats étrangers, le délai moyen d'autorisation d'accès est de 34 jours et le taux de refus est de 3,8 %, contre

respectivement 16 jours et 1 ‰[1] pour les Français. En aparté, on nous a indiqué que certains pays, l'un d'entre eux en particulier, posaient de vrais problèmes.

Le haut fonctionnaire de défense et de sécurité (HDFS) adjoint qui participait à la table ronde a formulé trois propositions : un « contrat PPST » avec les directeurs d'unité (DU) et les établissements, comportant des garanties en matière de concertation et d'échanges ; l'expérimentation d'une procédure simplifiée pour les avis sur demande d'accès, qui réduirait les délais de moitié ; un travail d'aménagement du dispositif réglementaire, par discipline.

C'est en mathématiques que la contestation des ZRR a été la plus violente, à tel point que les directeurs de laboratoire dans cette discipline ont envisagé une démission collective. L'un des objectifs de la table ronde était de mettre les parties en présence et de confronter leurs positions, pour parvenir ensuite à un éventuel accord.

En conséquence, je propose de conclure dans les termes qui suivent.

L'Office rappelle d'abord que, si les activités de recherche sensibles nécessitent une protection, la liberté académique et l'ouverture internationale des scientifiques, principes fondamentaux du développement des connaissances, doivent être préservées. Le maintien de l'excellence de la recherche française nécessite l'échange des idées et l'attraction des meilleurs chercheurs et étudiants dans ses laboratoires. Le souci de l'efficacité de la recherche est essentiel pour garder les laboratoires français au meilleur niveau international. Nous retrouvons ici la même tension entre sécurité et efficacité que dans le précédent sujet.

L'Office estime également que, depuis 2012, le dispositif des ZRR a été mis en place de façon trop rigide et contraignante, avec une concertation insuffisante. D'où une gêne considérable pour les laboratoires, qui a été plus ressentie dans certaines disciplines scientifiques comme les mathématiques, l'informatique ou la physique que dans les sciences de la vie, déjà soumises à des contraintes et procédures très importantes qui leur rendent plus acceptable ce type de restrictions.

L'Office regrette que la PPST repose sur une logique binaire : soit un classement en ZRR entraînant une application uniforme de toutes les contraintes sans tenir compte de la particularité des disciplines et des laboratoires, soit une absence de classement exonérant le laboratoire de toute discipline. Or un algorithme ne réclame pas nécessairement le même type de protection qu'un virus…

À cet égard, l'Office prend acte des déclarations du haut fonctionnaire de défense et de sécurité (HDFS) adjoint : selon ce dernier, les enquêtes précédant une demande d'accès à une ZRR ne se limitent pas à l'utilisation de mots-clés ou à la nationalité du candidat, comme avancé par certains scientifiques lors de l'audition, mais reposent sur une étude approfondie au cas par cas ; les publications des chercheurs des ZRR ne sont pas obligatoirement soumises à un régime d'autorisation préalable, tout dépend de ce qui est prévu dans le règlement intérieur de la ZRR.

L'Office souhaite rester en contact avec la communauté scientifique en organisant une nouvelle table ronde, dans un délai à déterminer en fonction des avancées constatées, mais en tout cas dans une limite de deux ans.

L'Office recommande la mise en place d'une procédure de recours interne des décisions prises dans le cadre de la création et de la gestion des ZRR. Cette procédure serait confiée à trois personnes : l'une représentant les sciences et devant être une personne à la légitimité incontestable et reconnue, habilitée confidentiel défense ; la deuxième représentant

(1) Un pour mille.

les services de l'État en charge de la sécurité ; et la troisième avec un profil plus juridique et dont l'indépendante serait assurée.

L'Office estime, au vu de tous ces éléments, que les problèmes rencontrés par les laboratoires de recherche français ne relèvent pas des seules modalités d'applications du dispositif des ZRR et recommande, en conséquence, un véritable changement de doctrine et d'état d'esprit dans la mise en œuvre de la PPST.

L'Office souhaite que l'on s'inspire des pratiques aux États-Unis et au Royaume-Uni, qui ne sont pas réputés naïfs en matière de sécurité, pour : adapter le dispositif des ZRR aux spécificités des différentes disciplines scientifiques ; protéger des projets sensibles au cas par cas, plutôt que des secteurs ; s'appuyer sur une plus grande responsabilisation des chercheurs, avec des actions de formation et d'information, plutôt que sur des mesures contraignantes ; et développer une culture de sécurité de tous les acteurs pour permettre, au-delà des seuls laboratoires sensibles, une prise de conscience des enjeux de la recherche en termes de compétition internationale, de propriété intellectuelle, de valorisation de l'innovation et de défense nationale.

Enfin, l'Office recommande un effort en matière d'éducation sur la sécurité informatique, qui doit être réalisé dès le collège, pour la diffusion d'une meilleure « hygiène informatique ».

Mme Huguette Tiegna, députée, vice-présidente de l'Office. – Avec le rapport que nous avons présenté la semaine passée, nous avons eu peu de temps pour regarder ce sujet mais ces conclusions nous paraissent tout à fait satisfaisantes en l'état.

Mme Catherine Procaccia, sénateur, vice-présidente de l'Office. – Les scientifiques devaient être satisfaits que l'Office s'intéresse à la question des ZRR ?

M. Cédric Villani, député, premier vice-président de l'Office, rapporteur. – Ils étaient heureux que le Parlement s'en empare. Pour les scientifiques, le face-à-face avec les représentants des ministères chargés de la sécurité, souvent convaincus de leur naïveté, peut être délicat.

M. Jérôme Bignon, sénateur. – Ces pesanteurs étaient palpables au cours de la table ronde.

Mme Catherine Procaccia, sénateur, vice-présidente de l'Office. – Je propose que nous autorisions la publication de ces conclusions.

L'Office autorise la publication du rapport présentant les conclusions et le compte rendu des deux auditions, sous forme de tables rondes, sur les zones à régime restrictif (ZRR) dans le cadre de la protection du potentiel scientifique et technique de la nation.

ANNEXES

ANNEXE 1 :
ÉLÉMENTS DE COMPARAISON AVEC LES ÉTATS-UNIS ET LE ROYAUME-UNI

(Sur la base des réponses des services pour la science la technologie (SST) des ambassades de France dans ces deux pays)

A– Les États-Unis et le Royaume-Uni sont deux pays réputés pour **l'excellence de leur recherche et l'efficacité de leur protection contre l'espionnage**. Ils concilient le principe de liberté de la recherche, indispensable au développement des savoirs, avec le besoin de protection des activités de recherche sensible. Les communautés scientifiques américaine et britannique s'accordent à dire que la liberté académique et l'ouverture à l'international sont au cœur de l'excellence de leur système.

C'est l'ouverture à l'international qui fait la force du système de recherche et d'innovation américain, attirant chaque année plus d'un million d'étudiants étrangers. La communauté scientifique estime que la liberté académique du monde scientifique doit être préservée autant que possible. Des mesures de sécurité trop restrictives pourraient atteindre les capacités d'innovation des universités et centres de recherche américains en menaçant la libre circulation des personnes et des idées. La réussite des États-Unis est en partie due à sa capacité à attirer des talents internationaux dans la recherche et les technologies de pointe. Les décisions visant à restreindre l'accès à la recherche scientifique doivent être prises en concertation avec les membres de la communauté scientifique et industrielle, la communauté du renseignement n'ayant pas d'expertise scientifique. Le Congrès américain s'est néanmoins inquiété, à plusieurs reprises, de l'accroissement des risques d'espionnage scientifique, notamment en provenance de Chine.

Au Royaume-Uni, l'ouverture et les échanges internationaux sont au cœur de l'excellence de leur recherche publique.

B– La gestion de **la PPST est fortement centralisée en France**. Ainsi, en France, le système unique des ZRR, « one size fits all », peut sembler en même temps adapté aux laboratoires du CEA, surdimensionné pour certains laboratoires de mathématiques ou d'informatique et sous-dimensionné pour certains projets sensibles impliquant la défense nationale. Et que dire d'un laboratoire pour lequel le classement ou non en ZRR se discute ? Déclaré ZRR, il sera soumis à toutes sa rigueur, non classé, il échappera à toute surveillance. À l'opposé de la France, la PPST est **très largement décentralisée et multiforme aux États-Unis comme au Royaume-Uni**. Elle est donc plus souple et mieux adaptée aux différentes situations.

Aux États-Unis, l'administration et les services fédéraux mettent en place des mesures globales de restriction (visas, contrôles à l'exportation présumée – deemed export controls). Le modèle américain se prête peu à des initiatives telles que les ZRR, qui requièrent une connaissance fine des thématiques des recherches des universités et la

possibilité d'impacter le fonctionnement d'un laboratoire de recherche. Les universités américaines, qui disposent d'une forte autonomie, sont libres de mettre en place des mesures de protection spécifiques. La décision et la responsabilité sont donc majoritairement déléguées au niveau de chaque université et centre de recherche. La nature des mesures de protection dépend essentiellement de l'institution qui finance la recherche. Il existe donc une très grande diversité des dispositifs de protection. Dans le cas des centres de recherche financés par le gouvernement fédéral et qui revêtent un enjeu stratégique pour la sécurité nationale (les 42 FFRDC de différents ministères – Federally Funded Research and Development Centers et les 10 UARC du département de la défense – University Affiliated Research Centers), les mesures de protection sont établies conjointement par l'université d'accueil et l'agence fédérale finançant le centre.

Au Royaume-Uni, la PPST n'est pas gérée centralement au niveau national, elle est traitée par chaque université. Les décisions sont partiellement déléguées, si un problème surgit avec l'un des employés, c'est l'université qui doit trouver une solution. Ceci résulte sans doute du très fort éclatement du cadre de développement de la recherche publique britannique au sein des universités et de leur forte autonomie, et donc de celle des laboratoires de recherche associés. Il est de la responsabilité de la faculté d'identifier le besoin d'accorder une habilitation de sécurité à un employé de l'université, le plus souvent dans le cadre d'un financement alloué pour des travaux de recherche portant sur des technologies ou du matériel sensibles. Cette habilitation ne concerne que le niveau basique de vérification (Basic Check) ; les trois niveaux de vérification suivants sont accordés par des organisations habilitées par le ministère de la défense, appelées sponsors (agence gouvernementale, gouvernement étranger, ou prestataires privés du ministère de la défense, répertoriés dans une liste dite « X »). En cas de besoin, l'université se tourne donc vers l'un des sponsors pour obtenir l'habilitation du chercheur. La décision du responsable des ressources humaines et du doyen de la faculté est finale. La stratégie de protection appliquée se veut adaptée à la situation et au niveau de risque.

C– En France, la PPST repose sur deux listes comportant les **secteurs protégés** (quasiment tous les champs de connaissance) (1) et des **spécialités sensibles** (liste classifiée). Aux États-Unis, elle repose sur des **projets**.

Aux États-Unis, en fonction de la nature des contrats et des financements de recherche, ce sont les projets de recherche qui sont classifiés et donc protégés – et non les thématiques de recherche ou les structures d'accueil. Ainsi, 95 % des projets de recherche dans le domaine « intelligence et renseignement » ne nécessiteraient pas de politique de confidentialité spécifique.

(1) 1.biologie-médecine-santé ; 2.chimie ; 3.mathématiques et applications ; 4.physique ; 5.agronomie et sciences de l'environnement ; 6.sciences de la terre et de l'univers ; 7.sciences et technologies de l'information et des communications ; 8.sciences pour l'ingénieur.

D– **Il n’existe pas de dispositif comparable aux ZRR ni au Royaume-Uni, ni aux États-Unis.**

Au Royaume-Uni, il n’existe pas de dispositif équivalent aux ZRR. En amont de l’acceptation dans un établissement d’enseignement supérieur, pour des études ou des travaux de recherche liés à des domaines sensibles, il est nécessaire d’obtenir un certificat dans le cadre de l’Academic Technology Approval Scheme (ATAS). Mis en place en 2007, révisé en 2013, l’ATAS est administré par le Foreign and Commonwealth Office. Cette procédure concerne les ressortissants de pays tiers (hors Espace économique européen et Suisse) désirant étudier des sujets sensibles — notamment en lien avec les armes de destruction massive. Ils se doivent d’obtenir un certificat ATAS spécifique à un établissement d'enseignement supérieur et à un programme d’études avant de demander l’entrée au Royaume-Uni ou une prolongation de leur séjour. Ces règles s'appliquent aux étudiants en recherche (Visiting researcher, post-doc, PhD) ou inscrits dans des programmes de maîtrise, dans certaines matières. Les programmes d’études nécessitant l’obtention d’un certificat ATAS ont été actualisés le 2 janvier 2019 ; sont concernées certaines matières liées à la médecine, la biologie, les sciences vétérinaires et l’agriculture, les sciences physiques , les mathématiques et l’informatique, l’ingénierie, et certaines technologies (polymères, matériaux, minéraux, marines, ..).

Aux États-Unis, les SCIF (Sensitive Compartmented Information Facilities) sont des espaces (une pièce, un étage ou un bâtiment entier) construits selon les normes définies par le National Counterintelligence and Security Center. Le personnel non autorisé ne peut y entrer sans être détecté. Ces installations sont conçues pour empêcher les sons, les émissions électroniques et les vibrations de s’échapper. La Maison blanche, les ambassades, les installations des services de renseignement et les bases militaires sont par exemple équipées de SCIF. Certaines universités américaines ont mis ou vont mettre en place des SCIF sur leur campus afin de pouvoir conduire des recherches classifiées dans le domaine de la sécurité nationale et de se positionner comme des universités phares dans ce domaine. Les installations SCIF sont donc étroitement liées à des contrats de défense et relèvent des choix stratégiques des universités. Les universités américaines disposant de SCIF sur leur campus sont peu nombreuses : le MIT (au sein du MIT Lincoln Laboratory), l’Université Auburn, l’Université du Wisconsin à Madison (construite en 2013), l’Université Georgia Tech (au sein du Centennial Research Building), l’Utica College (construit en 2008), l’Université de Caroline du Nord à Charlotte (au sein du PORTAL building inauguré en 2011). Plusieurs autres universités envisagent de mettre en place une installation SCIF sur leur campus : l’Université d’État du Dakota (au sein du futur Madison Cyber Labs building, dont la construction a été annoncée en 2017), l’Université du Texas à San Antonio (au sein du futur National Security Collaboration Center, dont la construction a été annoncée en 2018) et l’Université du Maryland. Il s’agit d’universités réputées en matière de sécurité et cybersécurité, qui espèrent ainsi renforcer leur position et leurs capacités de recherche et obtenir des financements fédéraux de la part du département de la défense (DoD) et des agences de sécurité nationale. Le programme fédéral de bourses Cyber Corps envisage par exemple d'accorder la préférence aux étudiants qui peuvent obtenir une habilitation de sécurité gouvernementale top-secret, ce qui favorise les universités ayant un SCIF.

E– Aux États-Unis comme au Royaume-Uni, la PPST repose essentiellement sur **l'information, la formation et la responsabilisation des chercheurs**.

Aux États-Unis, il revient aux chercheurs et responsables des centres de recherche de prendre les décisions appropriées, de s'assurer de la fiabilité de leurs collaborateurs et de notifier tout comportement suspect. Les contraintes de fonctionnement lourdes (restrictions des accès physiques aux laboratoires et des publications) ne s'appliquent que lorsqu'elles sont requises par un contrat de recherche particulier (par exemple, dans le cas d'un contrat de recherche classifiée avec la défense). Pour des activités non classifiées, il est par exemple de la responsabilité des directeurs de centres de recherche d'engager ou non des étudiants et chercheurs de pays « à risque ». Les chercheurs sont tenus de signaler lorsqu'ils observent des activités ou comportements suspects. Face aux risques croissants d'espionnage scientifique, la communauté scientifique américaine se prononce en faveur de mesures basées sur l'adhésion et la responsabilisation des chercheurs, plutôt que sur des restrictions sécuritaires lourdes. Les chercheurs demandent une meilleure sensibilisation et plus d'informations concernant la marche à suivre en cas de vols de propriété intellectuelle. L'opinion prévaut que la mise en place de mesures basées sur l'adhésion et la responsabilisation de la communauté scientifique, plutôt que des restrictions sécuritaires contraignantes, pourrait permettre de mieux préserver l'innovation américaine. Pour se protéger, les universités devraient mieux sensibiliser les chercheurs et leur indiquer la marche à suivre en cas de vol de propriété intellectuelle. La mise en place de garde-fous raisonnables est préférée à des mesures extrêmes qui nuiraient aux universités. À titre d'exemple, le Los Alamos National Laboratory, classé FFRDC, dispose de son propre bureau de contre-espionnage et compte sur la responsabilisation de ses employés. Tous doivent suivre une formation dans les dix jours suivant leur arrivée, et reçoivent un guide insistant sur les précautions à prendre en matière de sécurité et contre-espionnage. Ce guide identifie clairement les employés du laboratoire comme étant la première ligne de défense face à l'espionnage et les invite à signaler tout comportement suspect.

Au Royaume-Uni, la responsabilisation des chercheurs est très forte. L'information explicite, la formation et la responsabilisation des acteurs sont au cœur du processus de protection. Ainsi, et la presse britannique s'en est tout récemment fait l'écho, l'université d'Oxford a annoncé le 17 janvier dernier qu'elle n'acceptait plus, depuis le 8 janvier de financement de l'entreprise chinoise Huawei Technologies, le fournisseur leader mondial d'équipements de réseau de télécommunications, après avoir investigué sur les relations de l'entreprise avec le gouvernement chinois. Les étudiants et doctorants qui travaillent déjà sur des fonds de Huawei ont été informés qu'ils peuvent rester à Oxford mais qu'ils ne peuvent plus être en contact avec des informations confidentielles ou liées à la propriété intellectuelle. Huawei se voit opposer le même type de d'objections dans d'autre pays : États-Unis, Canada, Allemagne, Pologne, Inde, Nouvelle-Zélande, Australie….

ANNEXE 2 :
CONTRIBUTION DE M. JEAN-MARC JÉZÉQUEL, DIRECTEUR DE L'INSTITUT DE RECHERCHE EN INFORMATIQUE ET SYSTÈMES ALÉATOIRES (IRISA), ET DE M. PIERRE PARADINAS, PRÉSIDENT DE LA SOCIÉTÉ INFORMATIQUE DE FRANCE (SIF)

À propos des ZRR : position de Jean-Marc Jézéquel, directeur de l'IRISA, et Pierre Paradinas, président de la SIF

Le texte suivant est un support à l'audition de Jean-Marc Jézéquel, directeur de l'IRISA, et Pierre Paradinas, président de la SIF, par OPECST à l'Assemblée nationale le 24 janvier 2019 sur les ZRR.

Les problèmes et questions autour des ZRR (Jean-Marc Jézéquel)

Les missions d'un laboratoire de recherche public sont à la fois de produire des connaissances et de les transférer. Les connaissances en elles-mêmes ne sont généralement ni protégeables (en particulier, en informatique, un algorithme ou un théorème ne peuvent être brevetés) ni dangereuses en elles-mêmes. En revanche l'utilisation de ces connaissances peut parfois poser problème, en quelque sorte comme arme par destination, ce qui ouvre la porte à quelques situations problématiques, mais aussi des tas de fantasmes d'autant plus grands que la communauté du renseignement est éloignée du monde de la recherche (cf. notes d'analyses sur la PPST aux USA et au RU). Force est donc de reconnaître une tension naturelle entre les missions d'un laboratoire de recherche public et la PPST.

Cas particulier de l'informatique : autant il est facile d'écrire du logiciel simple, autant il est difficile d'écrire du logiciel complexe de manière fiable. Les logiciels les plus complexes qui nous entourent (Internet, cloud, smartphones, outils des GAFA) résultent aujourd'hui de l'effort collectif de l'ensemble de l'humanité au travers de l'open source. Même les adversaires historiques du mouvement (cf. Microsoft) s'y sont mis. Y compris un grand industriel français de la défense qui a mis en place en interne des processus de développement inspirés de l'open source. La gestion de la PI est donc tout à fait particulière dans notre domaine, et le risque économique est particulièrement difficile à mesurer.

Un laboratoire, en particulier un laboratoire de recherche public en informatique, est donc par construction un seau percé, avec de gros trous structurels (flux des chercheurs, ingénieurs et étudiants, reviewing de projets) et de plus petits trous conjoncturels (vols d'ordinateurs, attaques informatiques, vols de documents).

Pour être précis : IRISA 2016

– arrivées fonctionnaires: 20

– contrats de travail CDD: 239 dont 86 doctorants

– conventions de stage: 157 (dont 81 M2)

– missions avec frais: 2010

– articles publiés : environ 1 000

– dépôts de projets : environ 200

– 35 nouveaux projets de financements collaboratifs avec 100+ partenaires pour un total de 12 millions d'euros

Compte tenu de cela, placer un laboratoire sous le régime global de la ZRR est donc à la fois trop et trop peu.

Trop car le coût de la gestion technique et administrative d'une ZRR est proportionnelle à l'activité du labo (cf. ci-dessus) et donc très élevée tant pour le laboratoire que pour son hébergeur : le gain marginal de PPST apporté par une ZRR (qui se concentre sur les petits trous et laisse béants les grands) n'en vaut certainement pas la chandelle, en particulier dans un contexte d'une part de maîtrise des dépenses publiques et d'autre part de concurrence féroce à l'échelle internationale pour attirer les talents : c'est pour les laboratoires français comme de courir la finale du 100m avec un boulet aux pieds.

Mais c'est aussi trop peu, car la protection actuelle reste pour l'essentiel de l'affichage, alors qu'il reste, même si c'est minoritaire, des artefacts sensibles (matériels, logiciels, données) qu'il conviendrait de protéger bien mieux que ce qu'une ZRR (telle que proposée) impose.

Notre proposition serait donc de réfléchir à une protection adaptée, construite avec les laboratoires plutôt que contre eux, en concentrant l'effort sur les artefacts plutôt que les équipes ou les personnes. Pour cela, nous pouvons imaginer un système de cercles :

– Un premier cercle fortement sécurisé (sorte de ZRR++) pour les artefacts et projets très sensibles.

– Un second cercle (sorte de ZRR--) offrant contrôle d'accès et protection juridique sous la responsabilité du DU.

– Un éventuel troisième cercle pour la perméabilité avec l'enseignement.

ZRR et les laboratoires informatiques (Pierre Paradinas)

Les propos de mon collègue **Jean-Marc Jézéquel** sont ceux d'un directeur de laboratoire important dans le paysage français, je peux vous assurer que ces points mentionnés concernent **TOUS** les laboratoires d'informatique en France.

D'ailleurs la Société informatique de France avait déjà pris position en **2014** sur ce sujet et on se réjouit de l'entrée de l'informatique et du numérique au collège et au lycée, qui de fait l'explication des choses techniques et scientifiques iront dans le sens de l'augmenter de l'**hygiène informatique.**

Pour certains laboratoires ces problèmes de sécurité sont bien connus et maîtrisés car en effet, ils travaillent sur les questions scientifiques et techniques de la sécurité informatique et les laboratoires de Rennes, Toulouse, Nancy ou Paris comptent parmi les plus réputés dans ce domaine dans le monde.

La mise en place des ZRR dans nos labos comme expliqué par **Jean-Marc Jézéquel**, *est parfois* ***trop ou trop peu*** *!!! Ce qui est paradoxal.*

En effet, pour certains travaux ou contrats avec des entreprises et/ou ministères, les protections imposées par les ZRR sont insuffisantes.

L'informatique est un outil pour les autres sciences, si des calculs, simulations et/ou expérimentations sont effectués sur des serveurs, cela ne doit pas nécessairement impliquer la contamination complète des ressources informatiques et des laboratoires informatiques – ou autres – en ZRR.

Je tiens à souligner qu'en informatique – mais je pense aussi chez beaucoup d'autres sciences – la grande difficulté est de ***décider de ce qui est stratégique*** *au sens de la ZRR de ce qui ne l'est pas !*

Les ***mots clés*** *comme mode de* ***sélection*** *sont d'une pauvreté absolue… Ceci est peut être beaucoup plus simple lorsque qu'il s'agit de recherche finalisée (et rentre alors dans un cadre projet bien défini).*

Une autre analogie est celle « **d'arme par destination** ». Comme la notion physique « arme par destination », le même concept s'applique aux algorithmes. En soi l'algorithme n'est pas une « arme », mais son usage dans un cadre terroriste (hypothétique) le transforme en une menace. Exemple, si une voiture Renault (tunée éventuellement) est utilisée par un employé de Renault pour commettre un attentat, Renault est-il responsable ou fallait-il interdire à Renault d'employer la personne.

Spécificité **open source**

Les ZRR telles que définies actuellement peuvent introduire un risque juridique pour les personnels impliqués dans des projets open source avec la conséquence du **confidentiel par défaut**. Par ailleurs, comment prendre une décision, alors que ce sont les applications futures qui détermineraient de l'intérêt de protéger tel ou tel résultats ? Qui serait responsable dans ce cas, le chercheur ? Celui qui a autorisé la diffusion (FSD) ? Le responsable de la ZRR ?

Il faut aussi considérer l'**open data**, là encore les pratiques scientifiques et les textes législatifs sont incompatibles :

– On fait référence ici au guide d'analyse du cadre juridique en France réalisé par les organismes de recherche [(1)].

– La lecture de ce document et des contraintes imposées par les ZRR conduisent à des impossibilités.

– Par ailleurs, certains travaux étant mené avec des financements ANR et/ou H220, ce qui une fois de plus induit des contraintes.

De même, les politiques et besoin de **reproductibilité** des résultats et expériences scientifiques – ce qui veut dire les données + les programmes –, dont le mouvement actuellement est très important dans la communauté, ces contraintes s'opposent de fait avec celle de la protection !

Nos recommandations :

Il faut éviter la contamination de tout un laboratoire et avoir une approche permettant de distinguer plusieurs niveaux de sécurité dans le fonctionnement quotidien d'une entité/laboratoire – je me rappelle ainsi que dans une entreprise spécialisée dans la conception et la fabrication de cartes à puce, des bureaux étaient réservés à certaines

(1) *http://www.bibliotheque scientifiquenumerique.fr/wp-content/uploads/2017/01/Guide_analyse_Cadre_ Juridique_Ouverture_donness_Recherche_V1.pdf*

personnes travaillant sur des projets et/ou des entreprises spécifiques sur projets concurrents pour Visa et Mastercard.

Il faut éviter le « je protège tout (le labo) », pour protéger juste un projet ou une équipe de recherche travaillant sur un sujet sensible ou un contrat réellement délicat d'un point de vue de la sécurité.

Préserver la compétitivité de notre recherche, des équipes et des labos :

– Prévoir une articulation de la notion de ZRR avec la politique de financement de la recherche publique fondée sur les projets de recherche collaboratif (surcoût ZRR ? contraintes des financeurs ?)

– L'agilité des équipes de recherche est un atout essentiel pour une bonne compétitivité : rapidité de publication ; diffusion des résultats ; coopération fluide entre les scientifiques est nécessaire.

– La capacité à bien et vite recruter est centrale pour avancer et les méandres administratifs des ZRR font perdre des opportunités !

– Prendre en compte les **coûts induits** par les éléments placés ZRR (prise en compte des coûts de mise en œuvre de la protection sur les éléments essentiels ce qui permettra une protection de bonne qualité).

Liens complémentaires

– ZRR : (https://fr.wikipedia.org/wiki/Zone_à_régime_restrictif)

– Lettre ouverte de J-M Jézéquel (https://www.societe-informatique-de-france.fr/wp-content/uploads/2018/11/LettreOuverte-Jean-Marc-Jézéquel.pdf)

– Rappel de la position de la SIF en 2014 sur cette question (https://www.societe-informatique-de-france.fr/position-mise-en-place-zrr/)

Rappel du texte de 2014 de la SIF

2 avril 2014

Les « Zones à régime restrictif » (ZRR) sont actuellement en discussion. Il s'agit de mesures de sécurité s'appliquant aux laboratoires de recherche. Le régime de sécurité proposé est nettement plus contraignant que le précédent (ERR) ; de plus, le nombre de laboratoires concernés passe de 150 ERR à 500 ZRR. Les ZRR s'appliqueraient, non seulement aux recherches touchant la sécurité et la défense, mais aussi aux « intérêts économiques de la nation », ce qui consiste de fait à inclure quasiment toute recherche : l'ensemble des disciplines scientifiques, hors sciences humaines, semble concerné.

Une ZRR fait l'objet de restrictions diverses :

Tout accès est soumis à un avis favorable du FSD (Fonctionnaire Sécurité Défense), qu'il faut solliciter deux mois à l'avance. De même, l'embauche de tout personnel, quelle que soit sa nationalité et son rôle, doit être appouvée par le FSD.

Toute visite du laboratoire doit être approuvée par le directeur et ne peut dépasser cinq jours. La pièce d'identité du visiteur est vérifiée à l'entrée, et le visiteur est accompagné en permanence.

Toute publication est soumise à l'autorisation du directeur du labo et du responsable d'équipe. De même, un site web personnel ou un blog est soumis à autorisation.

Si ces restrictions se justifient peut-être dans des structures comme la DGA ou le CEA, spécialisées dans les recherches sensibles, elles nous semblent injustifiées, disproportionnées et contre-productives dans la plupart des laboratoires de recherche en informatique. Il est utile de rappeler que la mission de la recherche est de produire et de diffuser de la nouvelle connaissance. L'émulation mutuelle par la coopération internationale, la curiosité et l'ouverture scientifique, le brassage des idées et des informations, l'initiative personnelle du chercheur, sont des ingrédients essentiels au succès de la recherche. Enfin, tout délai dans la publication d'une nouvelle idée est un handicap dans la compétition internationale.

La ZRR paraît spécialement inadaptée, non seulement à la recherche fondamentale en informatique, mais tout autant à la coopération avec l'industrie. D'une part, nous publions prioritairement dans des conférences, dont les dates limites de soumission ne souffrent pas de délai. D'autre part, le partage des idées et des technologies elles-mêmes, dans le mouvement du logiciel libre, a fait la démonstration de son efficacité à accélérer l'innovation, et est adoptée y compris par les industriels les plus innovants, en France comme ailleurs.

Devant les réactions de la communauté, en particulier en mathématiques, la ministre de la recherche, Mme Fioraso, a demandé en décembre 2013 un moratoire sur la création des ZRR. Malgré cela, les ZRR continuent à se mettre en place, comme par exemple au CRAN (Nancy) récemment.

La Société informatique de France soutient les analyses de deux Comités scientifiques des instituts du CNRS, INS2I et INSIS, alertant les pouvoirs publics sur les dangers des mesures proposées et sur le frein pour la recherche que leur mise en œuvre représenterait.