De la PPST des laboratoires publics de recherche en informatique et de l'inanité des ZRR comme solution à un vrai problème

Jean-Marc Jézéquel
Directeur de l'UMR 6074 - IRISA

13 novembre 2018

Résumé

La problématique de la protection du potentiel scientifique et technique (PPST) de la nation est une réalité qu'il n'est pas question de nier ici, y compris dans le contexte d'un laboratoire public de recherche en informatique comme l'IRISA. Cependant la solution proposée par l'État de mise en place de zones à régime restrictif (ZRR), probablement bien adaptée dans son fonctionnement actuel à des structures comme le CEA ou des laboratoires de recherche militaires, est totalement inadaptée pour des laboratoires publics de recherche en informatique. Ce document vise à en expliquer les raisons, en particulier pour un public peu familier avec le fonctionnement quotidien de la recherche publique en informatique, tant dans que hors de nos frontières. Ce document se focalise sur la recherche en informatique, que l'auteur a la prétention de bien connaître, mais il est fort probable que beaucoup des aspects mentionnés ici soient tout à fait pertinents pour d'autres disciplines.

Préambule

Je suis professeur à l'Université de Rennes 1 et directeur de l'IRISA, l'un des plus grands laboratoires publics de recherche en informatique de France. Auteur de plus de 300 publications et de 4 livres traitant de science et d'ingénierie du logiciel, je suis membre de plusieurs comités éditoriaux de revues scientifiques (IEEE Computer, JSS, SoSyM, etc.), ainsi que de nombreux comités de programme. J'ai reçu en 2016 la médaille d'argent du CNRS. Précédemment j'ai été responsable scientifique de l'équipe de recherche Triskell (Inria/IRISA), qui a eu en particulier une longue histoire de collaboration avec un grand industriel français de la défense.

Mon service militaire, effectué comme EOR Marine, m'a donné le plus grand respect pour la chose militaire. J'ai en particulier eu à manipuler des données techniques classées « secret défense », et j'ai pleinement conscience des dommages qu'auraient pu causer à la nation la fuite de ces données.

Au-delà de mon expérience personnelle, le laboratoire que je dirige, l'IRISA, a aussi, en particulier dans le cadre du PEC (pôle d'excellence Cyber), de très fortes collaborations avec DGA-MI, partenaire dont nous respectons scrupuleusement les

contraintes, et qui est parfaitement organisé pour travailler avec nous avec toute la sécurité voulue.

1 Introduction

Pourquoi remettre ici sur le tapis la problématique de la protection du potentiel scientifique et technique (PPST) et des zones à régime restrictif (ZRR) alors que celle-ci est ancienne, et que la position de la communauté est clairement connue (Cf. la position de la Société informatique de France (SIF) [1], ou la tribune d'André Seznec dans le blog Binaire du journal *Le Monde* [2], etc.) ?

Le fait est qu'on assiste à des dérives invraisemblables et à de véritables entraves au fonctionnement normal de nos laboratoires du fait de personnes certainement pleines de bonnes intentions mais qui semblent méconnaître totalement nos problématiques et modes de travail. Quelques exemples :

— Toute publication est soumise à l'autorisation du directeur du laboratoire, ce qui est impossible à mettre en œuvre en pratique, et contraire au code de l'éducation pour les enseignants-chercheurs.

— Suite à une interprétation extrémiste de la circulaire interministérielle 3415/SGDSN/AIST/PST du 7 novembre 2012, obligation faite à des chercheurs d'une demande d'autorisation au fonctionnaire sécurité défense (FSD) [3] pour participer au comité de programme de conférences internationales (pour mémoire, le travail qui y est effectué consiste à évaluer et sélectionner des articles, donc à acquérir de l'information et non en donner !).

— Début 2015, une équipe de l'IRISA a été sollicitée pour monter un partenariat par un équipementier chinois des télécoms. Cette collaboration, très intéressante pour nous, a été bloquée par le HFDS sans qu'on en connaisse les raisons, mais soit. Ce qui est choquant ici est que peu de mois après cela, d'autres laboratoires, avec des équipes concurrentes de la nôtre, étaient autorisés à collaborer avec la même entreprise, qui allait jusqu'à ouvrir un centre de R&D en France, y employant tout à fait légalement de nombreux collègues. Inutile de dire que nous vivons très mal cette incohérence de l'action de l'État.

— Un maître de conférences UBS de l'IRISA a été promu professeur. Il était à l'IRISA à Vannes, reste à l'IRISA à Vannes sans même changer de bureau, mais le HFDS[3], pour valider son arrêté de nomination, exige qu'il demande une autorisation d'accès à la ZRR de l'IRISA gérée à Rennes par Inria (pourquoi celle-ci et pas celle gérée par CentraleSupelec ?), ZRR située à 120 km de son lieu de travail et dans laquelle il n'a aucune vocation à mettre les pieds. Et le plus surréaliste est que, devant l'intransigeance du HFDS, la formulation du motif de demande d'accès à la ZRR finalement rempli a été : « sans objet » (sic).

1. `https://www.societe-informatique-de-france.fr/position-mise-en-place-zrr/`
2. `http://binaire.blog.lemonde.fr/2014/04/02/les-zrrrrr/`
3. Relais dans l'établissement de recherche ou d'enseignement supérieur du HFDS, haut fonctionnaire de défense et de sécurité, lui localisé au ministère (MESRI).

— Une de nos équipes fait de la recherche sur les drones. Sans même aller voir la nature de cette recherche, le mot « drone » fait classer cette recherche comme sensible. C'est aussi stupide que de classer sensible la recherche sur les engrais agricoles sous prétexte qu'on peut facilement fabriquer des explosifs avec ceux-ci.

Après avoir rappelé en Section 2 quelques éléments de contexte sur la PPST et les ZRR, nous essayerons en Section 3 de dissiper les fantasmes pour cerner la vraie nature du potentiel scientifique et technique (PST) en informatique. Ceci nous permettra d'établir en Section 4 une quantification des risques sur une base rationnelle. Nous montrerons en Section 5 pourquoi la notion de ZRR actuelle est une réponse inadaptée pour diminuer ces risques dans un laboratoire public de recherche en informatique. Parce que la PPST est une problématique réelle, nous ferons en Section 6 des propositions concrètes pour faire face aux risques réels identifiés précédemment.

2 Contexte

2.1 Rappel sur la PPST

Le potentiel scientifique et technique (PST) de la nation est constitué de l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée et au développement technologique de la nation française. Les éléments essentiels du potentiel constituent des intérêts fondamentaux de la nation définis à l'article 410-11 du code pénal.

La protection du potentiel scientifique et technique de la nation (PPST) est organisée par un dispositif réglementaire rénové en 2012. Dans un laboratoire de recherche public, cela se décline en la codification de sensibilité PPST des activités de chacune de ses équipes. Cette codification s'appuie sur l'évaluation des quatre risques :

— économique (risque de porter atteinte aux intérêts économiques de la nation),
— défense (risque de renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense de la nation),
— prolifération (risque de contribuer à la prolifération des armes de destruction massive et de leurs vecteurs),
— terrorisme (risque de favoriser des actes terroristes sur le territoire national ou à l'étranger).

Chacun de ces risques est évalué avec une cotation de 0 à 3 :

0 : risque nul,

1 : risque possible,

2 : risque probable,

3 : risque avéré et constaté,

la règle étant que si le total des cotations est supérieur à un « seuil établi par le HFDS après concertation avec le FSD[4] » (typiquement 5 pour ce qui concerne l'IRISA), l'équipe concernée doit être placée en ZRR.

4. cf. note de création des ZRR du MESRI du 03/04/2013 (chapitre 4.1.1).

2.2 Rappel sur les ZRR

Selon les informations publiquement disponibles, ici par exemple sur Wikipédia [5], *in extenso* :

Une zone à régime restrictif (ZRR), en France, est une zone à accès réglementé dans le cadre de la protection du potentiel scientifique et technique national, lequel comporte cinq niveaux de protection imbriqués :

- *une liste de secteurs scientifiques et techniques dits « protégés », objets d'un « annuaire national » recensant leurs laboratoires ;*
- *une liste de spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs, établie par un arrêté confidentiel Défense ;*
- *des « zones protégées », délimitées soit par des autorités militaires, soit par des autorités civiles ;*
- *dans les laboratoires relevant d'un secteur protégé, parmi les zones protégées, des ZRR, dont l'accès (physique ou électronique) est soumis à autorisation spéciale ;*
- *à l'intérieur des ZRR, éventuellement, des « locaux sensibles », à la protection renforcée.*

Tout accès à une ZRR pour y effectuer un stage, y préparer un doctorat, y participer à une activité de recherche, y suivre une formation, y effectuer une prestation de service ou y exercer une activité professionnelle est soumis à l'autorisation du chef de service, d'établissement ou d'entreprise, après avis favorable du ministre de tutelle ou, à défaut, du ministre qui a compétence sur les activités concernées.

Les hauts fonctionnaires de défense et de sécurité (HFDS) instruisent, pour le ministre, les demandes d'accès transmises pour avis. L'instruction repose sur une analyse scientifique et technique des candidatures destinée à prévenir la captation d'informations sensibles.

En pratique, la perception des acteurs de terrain est que l'avis donné par les HFDS est plus fondé sur l'identification de mots clés que sur une analyse réelle du fond des dossiers.

3 Nature du potentiel scientifique et technique (PST) en informatique

Les missions d'un laboratoire de recherche public en informatique sont à la fois de faire progresser les connaissances mais aussi d'en assurer le transfert vers la société (incluant par exemple le transfert vers des entreprises et la médiation scientifique). Concrètement, la « production » d'un tel laboratoire est constituée d'une part d'artefacts et d'autre part de *cerveaux*.

Coté artefacts, on trouve :

- des articles, rapports, monographies, thèses, livres, aujourd'hui tous sous forme numérique, qui ont pour but de diffuser les résultats de recherche ;

5. https://fr.wikipedia.org/wiki/Zone_%C3%A0_r%C3%A9gime_restrictif?

— des logiciels, à très forte majorité en *open source* ;
— très exceptionnellement des brevets.

Coté cerveaux, on trouve :

— les chercheurs et enseignants-chercheurs permanents, fonctionnaires pour la plupart, dont une des missions est d'enseigner, c'est-à-dire de transmettre leur savoir à leurs étudiants, qui deviendront les ingénieurs de demain ;
— les docteurs qui y ont passé leur thèse, et qui transfèrent ainsi [6] leurs compétences vers d'autres laboratoires ou des entreprises ;
— les autres scientifiques, post-doctorants, ingénieurs, stagiaires, qui ont passé entre quelques mois et quelques années dans le laboratoire avant d'aller irriguer la société.

Quand en octobre 2018 IBM achète Red Hat, le numéro un de l'*open source*, pour un montant de 34 milliards de dollars, qu'achète réellement IBM ? Pas les lignes de code bien sûr, car celles-ci sont en accès libre et gratuit, mais bien pour la même raison qu'il est bien connu qu'acheter une startup en laissant partir les responsables techniques revient à acheter une coquille vide : pour les *cerveaux*, c'est-à-dire le savoir-faire qui est dans la tête des gens.

Donc la réalité du potentiel scientifique et technique (PST) d'un laboratoire de recherche en informatique, ce sont d'abord et pour l'essentiel les *personnes*.

Ensuite, en second ordre, il reste quelques logiciels « non libres » et quelques brevets (qui coûtent plus cher qu'ils ne rapportent à une écrasante majorité). La plupart de ceux-ci sont élaborés conjointement avec des entreprises, et suivent donc des règles adaptées de protection.

Au-delà de ces productions, un laboratoire peut aussi être amené à stocker ou manipuler des données sensibles. À cet égard, il faut noter le travail très constructif effectué en commun par le CNRS, Inria et l'INRA sur la définition d'une échelle de sensibilité qui devra permettre aux laboratoires concernés de traiter ces données sensibles avec toute la rigueur et le niveau de protection nécessaires.

4 Quantification des risques

Après avoir identifié la réelle nature du potentiel scientifique et technique (PST) de la recherche publique en informatique, c'est-à-dire d'abord le contenu du cerveau des chercheurs et ingénieurs, listons les risques afférents par ordre décroissant d'importance et d'impact sur le PST du laboratoire, avec les occurrences sur les dix dernières années à l'IRISA.

1. Pillage des cerveaux : débauchage de personnel (tous les acteurs, y compris la DGA, doivent maintenant faire face à cette menace !). Occurrences du risque : 1 à 3 fonctionnaires par an, de l'ordre de 200 contractuels par an. Est inclus dans ce risque le cas difficile à quantifier d'agents étrangers introduits sciemment pour acquérir de l'expertise sur un sujet donné.

6. Le laboratoire d'informatique d'une célèbre université californienne considère même que c'est le seul critère à l'aune duquel elle devrait être évaluée.

2. Vol d'idées lors de phases de *reviewing* (projets européens, etc.). Occurrences du risque : de l'ordre de la centaine de cas par an.
3. Vol d'ordinateurs portables (ou de téléphones). Occurrences du risque : de l'ordre de la dizaine de cas par an.
4. Attaques informatiques venant de l'extérieur. Occurrences du risque : quelques cas mineurs par an (défigurations de sites web, chevaux de Troie), car nous disposons d'une équipe technique très compétente qui maintient une grande vigilance sur ce sujet.
5. Vol de données de l'intérieur. Occurrences du risque : 1 tentative avérée en 10 ans, essentiellement parce que nous n'avons que peu de données sensibles, et que celles-ci sont protégées de manière *ad hoc*.

5 La ZRR : une réponse inadaptée

Nous ne mettons pas en cause le fait que la notion de ZRR puisse être tout à fait pertinente pour protéger des laboratoires sensibles du CEA ou du ministère des armées, ou même de certaines entreprises. Nous allons cependant démontrer que sa déclinaison pour des laboratoires publics en informatique est tout à fait contre-productive.

La ZRR ne réduit aucun des risques majeurs mentionnés ci-dessus. Elle pourrait contribuer à réduire le cinquième risque, ce qui se traduirait par une augmentation absolument marginale de la PPST du laboratoire. En tant que protection juridique (aspect de la ZRR qui est souvent mis en avant), il serait intéressant de savoir combien de procès ont eu lieu (réponse : à ma connaissance aucun). De même, quels moyens concrets avons-nous pour traquer la propriété intellectuelle qui aurait été volée ? (réponse : aucun).

En regard de cet effet positif minuscule, il faut considérer l'ensemble des inconvénients qu'une ZRR amène à l'exercice de la recherche dans un laboratoire comme l'IRISA.

C'est d'abord (comme c'est bien documenté par ailleurs, par exemple par le LAAS) un handicap majeur pour les équipes de recherche en ZRR. Le délai de deux mois imposé par la ZRR sur tout recrutement est dramatique dans un contexte où, avec un taux de chômage historiquement faible en informatique, on s'arrache littéralement les talents. Ces difficultés de recrutement induisent en particulier une énorme distorsion de concurrence avec les équipes à l'étranger et pénalise la recherche française, car comme on l'a vu ci-dessus, notre richesse ce sont les cerveaux.

La notion de ZRR rappelle un peu trop la mentalité « ligne Maginot ». Un exemple récent d'absurdité de cette notion de bastion : les américains ont interdit aux chinois l'usage des processeurs Intel pour leur machine petaflopique. Résultat, accélération sur leur technologie et Gordon Bell Price(s) à la clé pour les chinois [7].

Une ZRR induit ensuite un *overhead* administratif disproportionné par rapport au service fourni, tant en local au niveau du laboratoire (il faut du personnel pour aider les agents à faire les dossiers, les suivre et gérer les délais et les refus), que de l'hébergeur

7. https://www.acm.org/media-center/2017/november/gordon-bell-prize-2017

(coût de gestion de la ZRR elle-même), qu'à celui du ministère où un nombre considérable de hauts fonctionnaires sont occupés à des tâches finalement bien peu utiles pour la nation dans un contexte de pénurie générale de moyens.

Alors que la notion de sensibilité des recherches est en réalité très graduelle et demanderait des réponses nuancées et adaptées, le coté binaire d'une ZRR est particulièrement inique : on y est et on en paye tout le prix, on n'y est pas et le laboratoire n'a plus aucune contrainte, c'est-à-dire se retrouve ouvert à tout vent.

6 Propositions

Si la notion de ZRR telle qu'elle est actuellement mise en œuvre n'induit que des inconvénients sans apporter de solution concrète à la problématique de la PPST des laboratoires publics en informatique, mon propos n'est en aucun cas de revenir à l'absence totale de PPST (i.e. des laboratoires ouverts à tout vent). Plutôt que d'appliquer dogmatiquement une solution qui marche dans un contexte donné (e.g. CEA) à un contexte complètement différent, voyons comment on peut *rationnellement* répondre de manière proportionnée aux risques effectifs compte tenu de leur probabilité d'occurrence.

6.1 Gestion des deux risques majeurs : pillage des cerveaux et des sujets de projets

Pour éviter le débauchage des chercheurs fonctionnaires, il faudrait diminuer l'attractivité des salaires qui leur sont proposés par des entreprises étrangères en augmentant considérablement leur salaire actuel. On parle ici au minimum d'un doublement, mais pour résister aux GAFA un facteur 3 à 5 serait nécessaire, ce qui est bien évidemment irréaliste [8].

Pour ce qui est des personnels contractuels (stagiaires, doctorants, post-doctorants, ingénieurs), il conviendrait de leur proposer assez de postes attractifs tant dans la recherche publique que dans l'industrie européenne. S'agissant d'éventuels agents introduits secrètement par une entité hostile au sein des équipes de recherche, pourquoi cette entité prendrait-elle un tel risque alors qu'il lui est si facile d'agir légalement en offrant un pont d'or aux personnes qui ont les compétences recherchées ?

Concernant les fuites liées à l'évaluation par des experts étrangers de projets collaboratifs, la solution évidente serait de donner aux laboratoires les moyens de mener par eux-mêmes ces projets sans être systématiquement contraints de rechercher des financements externes.

Le fait que très probablement le lecteur trouvera ces propositions tout à fait irréalistes montre bien *a contrario* que la valeur économique de la recherche des laboratoires publics n'est pas considérée par l'État comme si importante que cela et invalide donc la dimension économique de la matrice de risque PPST. Comme par construction les laboratoires d'informatique sont peu concernés par les dimensions « prolifération » et « terrorisme », il ne reste à gérer que la dimension « défense ». À cet égard, il est à noter

8. En revanche, éviter de dégrader leurs conditions de travail avec des règles absurdes serait déjà une action positive.

que dans la cas de l'IRISA, qui travaille étroitement avec la défense au travers de la DGA, la gestion du risque est parfaitement contrôlée par la DGA, qui en conséquence n'est absolument pas demandeuse d'un mécanisme ZRR systématique pour une équipe qui collaborerait avec elle.

6.2 Gestion du vol d'ordinateurs portables

Le vol d'ordinateurs portables hors de nos locaux est un problème qui ne peut être négligé. Nous appliquons donc pour cela la politique de sécurité des systèmes d'information (PSSI) des établissements, dans laquelle on trouve en particulier le chiffrement des postes de travail.

Si celui-ci est disponible maintenant de manière standard pour la plupart des systèmes d'exploitation (Windows, MasOS, Linux), il n'en reste pas moins que sa mise en œuvre dans un laboratoire comme l'IRISA n'est pas gratuite.

En effet, si on considère que les données sur un ordinateur portable sont sensibles au vol, il est probable qu'elles doivent aussi être sensibles à la perte (i.e. la destruction involontaire ou volontaire). Il est donc indispensable de prévoir des procédures efficaces de sauvegarde (*back-up*) et de restauration. Faire ceci en présence de disques chiffrés nécessite une gestion adéquate de ces deux contraintes.

De même, on souhaite pouvoir accéder à ces données sensibles dans le cas où le possesseur du PC viendrait à ne plus être en mesure de déverrouiller lui-même son disque, ce qui induit un mécanisme de séquestre des clés de chiffrement qui doit être planifié, suivi et sécurisé.

Ce surcoût, nous le payons déjà à l'IRISA car nous pensons qu'il est indispensable de traiter correctement ce problème.

6.3 Attaques informatiques venant de l'extérieur

Il n'est pas dans l'objet de ce document de détailler les mesures à mettre en œuvre pour atteindre une protection raisonnable de nos infrastructures informatiques (sécurisation des réseaux, usage de VPN, etc.). À l'IRISA nous le faisons déjà avec un fort niveau de compétence qui a permis d'éviter toute intrusion hostile dans notre réseau depuis plusieurs décennies. Nous n'avons à déplorer dans les dernières années que quelques défigurations de sites web d'équipes ou de projets qui n'avaient pas assez vite été mis à jour suite à la découverte de failles de sécurité dans des logiciels comme PHP ou Wordpress.

À nouveau, il faut noter que le fort niveau de sécurité dont nous bénéficions a un coût RH qui est loin d'être négligeable : il s'agit du développement et du maintien de la compétence des ingénieurs et techniciens de notre service informatique au plus près de nos équipes de recherche.

6.4 Vol de données de l'intérieur

L'ensemble de nos bâtiments étant placés sous contrôle d'accès, il est relativement difficile (mais pas impossible) pour une personne étrangère au laboratoire de s'y introduire frauduleusement. Mais aujourd'hui l'essentiel de nos données sensibles est sous

une forme numérique : il n'y a plus de coffre-fort IRL à l'IRISA. Ce risque doit donc être interprété d'abord comme un risque informatique, qu'il vienne des personnes internes ou externes au laboratoire, risque qui est d'ailleurs partiellement géré par notre service informatique (par exemple avec le monitoring du trafic réseau et la détection de schémas anormaux).

Cependant, à cet égard, nous avons certainement des progrès à faire concernant l'architecture de nos réseaux virtuels ; il n'est par exemple pas raisonnable que les données du directeur du laboratoire soient sur le même réseau que celles du moindre stagiaire présent dans nos murs.

Ceci n'est certainement pas insurmontable, mais nécessite la mise en place d'une infrastructure informatique bien pensée et de procédures RH en tirant partie. À nouveau cela ne peut être réalisé à coût zéro.

6.5 Rôle des ZRR

Comme on le voit les mesures prioritaires ici proposées n'ont que peu à voir avec les notions de ZRR. Des ZRR pourraient toutefois être utiles à la PPST effective des laboratoires, avec au choix deux interprétations mutuellement exclusives.

6.5.1 ZRR comme moyen de protection juridique uniquement

L'autorisation d'accès à la ZRR est décidée par le directeur de laboratoire, qui peut toutefois prendre conseil auprès de son FSD pour les cas qu'il juge délicats. L'intérêt de la ZRR est alors que la personne indélicate s'expose de plein droit et sans ambiguïté aux conséquences d'avoir violé les règles de la ZRR.

6.5.2 ZRR comme chambre forte

Alternativement, la ZRR pourrait être vue comme une chambre forte, selon les besoins, soit physique (espace délimité) soit logique (sous-réseau isolé), ou bien sûr une combinaison des deux. Ceci serait concrètement utile pour entreposer du matériel et du logiciel sensible (du point de vue défense ou terrorisme, par exemple une base de virus), et il serait alors parfaitement légitime d'en restreindre l'accès à des personnes dûment sélectionnées par un HFDS.

7 Conclusion

Contrairement à ce qui est généralement affirmé par les HFDS, la mise en place de ZRR n'apporte au mieux qu'une amélioration marginale de la PPST d'un laboratoire public de recherche en informatique, pour un coût qui est très loin d'être nul. Son efficacité est donc proche de zéro.

Parce que nous prenons au sérieux cette problématique de la PPST, nous avons dans ce document proposé des pistes qui nous semblent raisonnables pour une véritable PPST efficace.

On me rapporte que le LAAS se plaint de la lourdeur du dispositif, et fait état avec justesse d'une véritable distorsion de concurrence avec les autres laboratoires français

de recherche en informatique, mais aussi avec les laboratoires étrangers (nulle ZRR à l'EPFL, l'un des meilleurs laboratoire d'informatique au monde !). L'État va-t-il donc tirer tout le monde vers le bas en imposant plus de ZRR, au risque d'un lourd handicap vis-à-vis de la concurrence internationale, ou bien va-t-il enfin réaliser que ce qui fonctionne pour le CEA et d'autres ne peut être automatiquement transposé à des structures comme les nôtres ?

Ce document se focalise sur la recherche en informatique, que l'auteur a la prétention de bien connaître, mais il est fort probable que beaucoup des aspects mentionnés ici soient tout à fait pertinents pour d'autres disciplines.