LIE n°11 de la DRSD

La contre-ingérence dans le monde de la recherche de défense

La lettre d'information économique
Décembre 2022

Sommaire

Éditorial du Directeur du Renseignement et de la Sécurité de la Défense

Mesdames, Messieurs,

Occupant une place prépondérante à l'international, la recherche française rayonne par son excellence dans de nombreux domaines et contribue par essence à la souveraineté technologique nationale. La réputation de ses laboratoires, écoles et instituts de recherche engendre à ce titre une grande attractivité pour les scientifiques et étudiants étrangers.

Nécessaire au fonctionnement de la recherche, cette ouverture à l'international attire également des acteurs étrangers ciblant directement les savoirs et savoir-faire de pointe français. Ce constat est structurellement et conjoncturellement renforcé en ce qui concerne la recherche de défense française, pivot de la base industrielle et technologique de défense (BITD).

Le lien étroit entre la recherche « de défense » et la souveraineté nationale, qui vise au maintien et au renforcement des capacités de défense françaises, expose davantage les secteurs scientifiques aux applications militaires et duales à ces menaces d'ingérence. De plus, la conjoncture géopolitique et géoéconomique actuelle, illustrée par la résurgence de tensions internationales majeures, allant jusqu'au conflit armé, conduit le ministère des Armées à préserver encore davantage qu'hier le potentiel d'innovation.

Cette tâche incombe à la DRSD dans le cadre de sa mission de protection du potentiel scientifique et technique (PPST) de la défense nationale. C'est à ce titre qu'elle s'emploie à détecter les activités d'espionnage technologique et autres manœuvres susceptibles d'affaiblir la recherche de défense. S'inscrivant dans une manœuvre interministérielle de protection des savoirs, la DRSD exerce sa mission en coordination entre ses échelons centraux et ses composantes locales pour assurer une protection « au contact » du monde académique.

Cette lettre d'information économique s'adresse donc en particulier aux grandes écoles et unités de recherche qui conçoivent et produisent les succès de demain, ainsi qu'à la multitude d'acteurs qui concourent à la promotion et à la qualité de la recherche de défense française.

Cette lettre entend aussi donner la parole à ces maillons et relais indispensables de sa mission de protection. Certains sont intégrés à l'échelon académique en lui-même, à travers notamment les directions et chaînes de sécurité qui participent de la protection opérationnelle. D'autres assurent à l'échelon ministériel (DGA) et interministériel (MESRI) une action de planification stratégique. Tous s'inscrivent dans une manœuvre globale de protection de la souveraineté technologique nationale.

À l'heure où certains compétiteurs assument de manière décomplexée des stratégies d'influence et de rattrapage technologique offensives, il importe plus que jamais de préserver la recherche de défense française de ces ingérences parfois manifestes, d'autres fois dissimulées, mais toujours déstabilisatrices. Soyez assurés de l'appui de la DRSD dans l'anticipation des atteintes et des contraintes décrites dans les pages qui suivent.

Au seuil de l'année à venir, assurément riche de nombreux défis collectifs, je vous adresse mes vœux les plus chaleureux.

Général de corps d'armée Philippe Susnjara
Directeur du Renseignement et de la Sécurité de la Défense

La protection de la recherche de défense, un enjeu au cœur de la mission de contre-ingérence de la DRSD

Des secteurs très convoités

Dans le contexte actuel de compétition économique et technologique, tous les secteurs scientifiques jugés stratégiques peuvent être les cibles de stratégies d'influence et d'actes d'ingérence émanant de l'étranger. Parmi les secteurs particulièrement convoités figurent ceux amenés à révolutionner les armées sur le plan cinétique (propulsion, nucléaire, matériaux avancés, etc.) mais aussi les futurs piliers de la révolution de l'information (mathématiques, informatique, physique quantique, etc.), aux applications plus duales mais tout aussi discriminantes pour les armées de demain.

Des vulnérabilités connues

La culture d'ouverture et la perception universaliste de la recherche française, y compris dans le domaine de la défense contribuent à fragiliser un secteur particulièrement exposé. En effet, l'ouverture à l'international des campus français (40% des doctorants en France sont étrangers), les nombreuses coopérations scientifiques internationales et l'exposition consentie des travaux de recherche dans le cadre de nombreux programmes français et européens, sont autant d'éléments susceptibles d'être exploités par des acteurs malveillants. Bien qu'absolument nécessaires au foisonnement de la recherche française, ces caractéristiques, auxquelles s'ajoutent la recherche de financements et le besoin de rayonnement, rendent la recherche *a fortiori* de défense particulièrement vulnérable.

« Construire les nids pour attirer les phénix »

L'immixtion d'acteurs étatiques dans des champs autres que celui de l'affrontement militaire traditionnel voire, plus récemment, économique transforme peu à peu le monde de la recherche en nouveau champ de conflictualité.

Certains États, conscients du besoin de financement des universités et des centres de recherche français n'hésitent pas à financer certaines chaires voire à racheter certains instituts pour y accroître leur influence. Il s'agit également de propositions de bourse dans des domaines ou sur des thématiques convoités par l'État financeur, ou encore de propositions de voyages d'études afin d'établir le contact avec certains chercheurs français. Ces financements poursuivent souvent un objectif double : promouvoir un narratif officiel attractif et faciliter de futures ingérences. Enfin, le Service constate la mise en œuvre, par certains compétiteurs, de programmes institutionnalisés de recrutement de chercheurs étrangers - dont des Français - destinés à favoriser la recherche scientifique nationale.

La protection de la recherche de défense, un enjeu au cœur de la mission de contre-ingérence de la DRSD

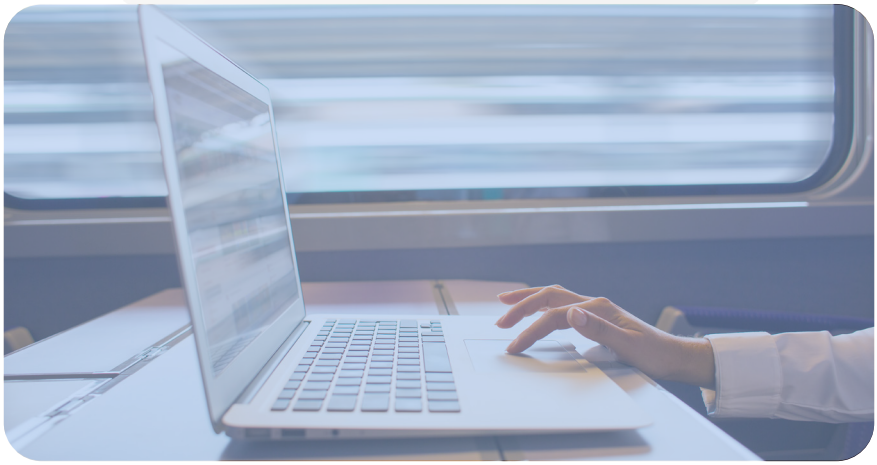
Des ingérences de plus en plus offensives

Outre ces stratégies d'influence, la compétition technologique mondiale pousse les États étrangers à procéder à des actes d'ingérence de plus en plus offensifs. En effet, les commanditaires n'hésitent plus à contraindre leurs ressortissants à commettre des actes illégaux dans un but de rattrapage technologique ou de sabotage. Concrètement, ces actes se manifestent par des vols ou piratage de données dans les laboratoires par des chercheurs permanents (professeurs ou doctorants) ou non-permanents (stagiaires, alternants, etc.) disposant de droits d'accès physiques et informatiques parfois trop étendus et exploitant le manque de vigilance d'un secteur parfois peu au fait des risques d'espionnage technologique.

Les cyberattaques constituent un mode opératoire auquel ont régulièrement recours les acteurs étatiques étrangers, qu'il s'agisse d'intrusions informatiques par voie électronique ou par l'insertion physique de supports numériques contenant des charges malveillantes. Principale menace cybernétique en 2021 (voir en ce sens la Lettre d'information économique n°10 de mai 2022) et pour les années à venir, les rançongiciels (*ransomwares*) ciblent les établissements de recherche publics comme privés. La maturité inégale dans le domaine de la cyber-sécurité est en effet une vulnérabilité du domaine académique, y compris pour la recherche de défense. Enfin, ces ingérences peuvent aller jusqu'à la déstabilisation de chercheurs français adoptant des positions non conformes à l'idéologie de certains compétiteurs. Ces derniers peuvent alors faire pression sur les chercheurs via leurs réseaux diplomatiques ou par le biais de « citoyens engagés » sur les réseaux sociaux, parfois soutenus par des « fermes à trolls » pour entacher la réputation et l'intégrité des victimes.

L'exposition renforcée en déplacement

La reprise des déplacements nationaux et internationaux expose à nouveau les chercheurs français à ces risques. En effet, le Service a constaté une recrudescence de vols d'ordinateur mais également de prises de vues non autorisées lors du travail dans les transports. Pour protéger le fruit de ses recherches, il convient de limiter la sensibilité des données transportées en déplacement mais également d'adopter une posture de vigilance et de discrétion (filtres de confidentialité, etc.) dans les lieux à risque, qu'il s'agisse des transports, hôtels ou restaurants (voir en ce sens la Lettre d'information économique n°10 de mai 2022).



L'Institut de recherche biomédicale des armées (IRBA) : ouverture scientifique et enjeux de sécurité

PHCSCN Frédéric Dorandeu - Directeur adjoint de l'IRBA

Le pharmacien chef des services de classe normale (PHCSCN) Frédéric DORANDEU est directeur adjoint de l'Institut de recherche biomédicale des armées (IRBA). Exerçant par ailleurs la fonction d'officier supérieur des sécurités et officier de sécurité de l'IRBA, il est également professeur agrégé du Val-de-Grâce, titulaire de la chaire de recherche appliquée aux armées et conseiller technique du Directeur central du SSA pour les questions de défense médicale contre les risques chimiques.

L'Institut de recherche biomédicale des armées (IRBA) est un établissement de la Défense placé sous l'autorité de la Direction centrale du service de santé des Armées (DCSSA). Il est né de la fusion des quatre établissements de recherche du SSA pour constituer un site unique à Brétigny-sur-Orge (Essonne) [1]. L'établissement occupe une superficie de 9 hectares et compte plus de 11 000 m² de laboratoires confinés ou ne requérant pas de systèmes de confinement. L'IRBA possède également des équipes distantes à Clamart, Marseille, Toulon et Mont-de-Marsan en raison des environnements particuliers nécessaires à leurs études.

Dédié à la recherche spécifique aux milieux d'emploi des forces ainsi qu'aux aspects biomédicaux liés aux risques nucléaires, radiologiques, biologiques et chimiques (NRBC), l'institut assure des activités de recherche, des actions d'expertise et des formations. Cette polyvalence, combinant connaissance scientifique et milieu militaire, assure sa spécificité ainsi que sa place unique dans le paysage de la recherche en France, illustrant sa devise « la connaissance au service des forces ». Pour la défense NRBC, l'IRBA est un acteur important, mais mal connu, de la fonction stratégique « connaissance – anticipation ».

La position géographique de l'IRBA au sud de l'Île-de-France offre une proximité vis-à-vis des états-majors de Balard et une insertion dans le pôle d'excellence de Paris-Saclay regroupant de nombreuses équipes à la pointe de la recherche scientifique française. Pour garantir une recherche, une expertise et un conseil au commandement de premier plan, l'ouverture vers l'international est également absolument nécessaire sur un grand nombre de domaines d'intérêt. Peu de nations sont, en effet, capables d'aborder seules des questions médico-scientifiques clés pour le soutien du combattant. C'est particulièrement le cas dans le domaine de la protection contre les effets des armes NRBC. Les équipes de recherche de l'IRBA sont ainsi très impliquées dans des consortiums internationaux ou des groupes de travail de l'OTAN, capacitaires ou scientifiques.

L'IRBA rassemble un effectif d'environ 430 personnes, composé de militaires (environ 40%) et de civils (environ 60%), répartis en chercheurs, ingénieurs, techniciens, et en personnels d'encadrement, de soutien et d'appui scientifique. Les équipes scientifiques de l'IRBA représentent environ 250 personnes. À cela s'ajoute une quarantaine de doctorants et post-doctorants. En 2021, le dynamisme des équipes de recherche s'exprimait également à travers plus de soixante projets de recherche, 190 publications scientifiques, 150 expertises, 70 partenariats.

Les équipes de recherche de l'IRBA peuvent bénéficier de laboratoires et de plateformes expérimentales d'exception qui permettent notamment de recréer les conditions auxquelles sont exposés les combattants sur le terrain : laboratoires d'étude de la perception (vision, audition, perception de l'espace), des contraintes environnementales (centrifugeuse humaine, appartement climatique et sommeil, plateforme bioclimatique, etc.).

Le défi majeur est ainsi de conserver l'ouverture indispensable aux activités de recherche tout en préservant les intérêts de la défense ou le potentiel scientifique et technique de la Nation. Outre des mesures particulières de sécurisation de nos installations grâce notamment à une brigade de gendarmerie de l'armement, les personnels sont régulièrement sensibilisés en interne et au travers des excellentes interactions avec la DRSD.

En conclusion, l'IRBA est un établissement militaire et scientifique unique par ses activités, moyens expérimentaux et thématiques de recherche. En complément des formations et sensibilisations permanentes de ses personnels, l'IRBA se doit d'être doté des moyens informatiques sécurisant son fonctionnement et assurant une parfaite protection de ses productions et savoirs et lui permettant de communiquer par des canaux classifiés si la situation l'exige.

[1] Le Centre de recherches du SSA (Grenoble), l'Institut de médecine tropicale (Marseille), l'Institut de médecine navale (Toulon) et l'Institut de médecine aérospatiale (Brétigny-sur-Orge).

Risques et menaces dans la recherche de défense

Interview du Dr François Plais - Directeur des opérations du CIEDS

Diplômé de SUPELEC et docteur en Sciences de l'Université Paris XI–Saclay, François PLAIS a débuté sa carrière au Laboratoire Central de recherches de Thales avant de rejoindre le groupe Alcatel et sa filiale de composants optoélectroniques en tant que responsable d'un secteur en *Front-End.* Arrivé en 2006 à l'École Polytechnique, il a participé au démarrage de l'activité de valorisation de la recherche, avant de prendre la responsabilité du Service Recherche Partenariale et Propriété Intellectuelle en 2014. Il est depuis 2021 Directeur des opérations du CIEDS.

DRSD : ***Bonjour, le Centre interdisciplinaire d'Etudes pour la Défense et la Sécurité (CIEDS) est un nouvel acteur important sur le territoire de Paris-Saclay. Pourriez-vous rappeler son positionnement structurel et ses domaines d'activité au sein de l'écosystème français de la recherche et de l'innovation de défense ? Quelles sont les applications actuelles et futures de vos domaines de recherche pour les Armées ?***

François Plais : Le CIEDS a été créé en 2021 par l'Institut Polytechnique (IP) de Paris pour animer et fédérer les activités de recherche « défense & sécurité » au sein des écoles membres d'IP Paris. L'Ecole polytechnique et l'ENSTA Paris, sous tutelle du ministère des Armées, ainsi que Telecom Paris et Telecom Sud Paris ont, de longue date travaillé avec la Direction générale de l'armement (DGA) sur des études intéressant la défense. Le CIEDS va amplifier ces relations. Les moyens financiers supplémentaires apportés par l'Agence d'innovation de la défense (AID), les industriels de la BITD et un travail commun systématique entre équipes – chercheurs, responsables « innovation » de l'AID, experts techniques de la DGA, industriels et personnels des forces – vont permettre de co-construire et mieux accompagner des projets ambitieux.

L'enjeu principal est de poursuivre une recherche fondamentale tout en renforçant le transfert et la valorisation des travaux. La pluridisciplinarité d'IP Paris et la capacité des laboratoires à modéliser, simuler puis expérimenter sur tous les domaines des sciences de l'ingénieur ouvrent la voie à des modélisations et calculs, en fonctionnalisation de matériaux pour la protection ou la détection, liste non exhaustive.

Par son ancrage dans la recherche, la formation et la valorisation de l'innovation de défense, le CIEDS est un pont entre la recherche et l'industrie, deux secteurs aux fonctionnements et aux enjeux souvent perçus comme résolument différents. Partagez-vous ce constat ? Quel est votre point de vue sur les difficultés rencontrées mais aussi les synergies pouvant être construites ?

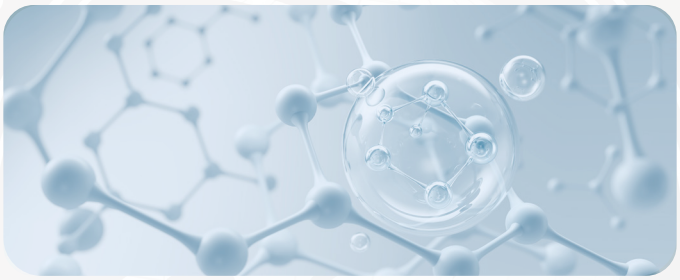
Oui, les secteurs de la recherche académique et de l'industrie ont des motivations différentes, produire des connaissances pour l'un et produire des actifs économiques pour l'autre. Les expérimentations pour mieux travailler ensemble sont nombreuses mais sur le terrain, au jour le jour, il est souvent difficile d'aplanir ces différences. La situation du CIEDS est particulière car une tierce partie, l'État, avec une impérieuse nécessité de sécurité et de souveraineté technologique, nous oblige collectivement à dépasser ces différences. Le ministère des Armées et l'AID vont nous aider à développer les synergies nécessaires à nos ambitions.

Le CIEDS contribue directement au potentiel de défense français en prenant part à de nombreux projets de recherche et d'innovation de défense. Êtes-vous pour cela en contact avec les services de la DRSD ? Si oui, pouvez-vous évoquer le cadre et l'objectif de ces contacts ?

Oui, nous sommes en contact avec la DRSD et son pôle de Paris-Saclay depuis la création du CIEDS. Plusieurs rencontres se sont tenues pour sensibiliser collectivement les chercheurs aux risques, mais aussi faciliter les prises de contact plus circonstanciées, au sein des laboratoires de recherche, en lien avec un projet particulier ou un contexte de partenariat sensible. Nous apprécions la démarche didactique et pragmatique de la DRSD dans ces circonstances.

Le monde de la recherche est un écosystème contraint à une importante visibilité afin de faire rayonner les travaux des chercheurs. Comment conciliez-vous cette nécessaire visibilité avec les enjeux de protection de propriété intellectuelle et particulièrement ceux de projets de défense suscitant un vif intérêt de la part d'acteurs étrangers ?

C'est un dilemme que l'on connaît bien en valorisation de la recherche, tous secteurs applicatifs confondus parce que les laboratoires de recherche sont soumis à des injonctions contradictoires. D'un côté, mener une recherche académique d'excellence conditionnée par des publications de résultats aux frontières de la connaissance, attirer des talents, lever des fonds hyper compétitifs, et irriguer la « science ouverte ». D'un autre côté, réserver la primeur de connaissances tacites, de résultats innovants, d'inventions non divulguées, de dossiers techniques secrets à des utilisateurs ou des licenciés exclusifs. Nos grands modèles universitaires à l'international montrent qu'on peut concilier les deux sous réserve de ne pas sacrifier l'un à l'autre, et donc d'avoir les moyens de toutes ses ambitions. En clair, on peut réserver des résultats et rester discret sur leurs applications, en particulier pour la Défense, si dans le même temps l'attractivité et la renommée de nos établissements et de nos chercheurs sont assurées sur des sujets voisins compatibles avec le paradigme de la science ouverte.



Quels risques et vulnérabilités spécifiques à la recherche de défense française (financements, coopérations, déplacements, nomadisme, etc.) identifiez-vous ?

Il m'est difficile vu mon parcours d'apporter une réponse globale. Les faiblesses de la recherche partenariale en France – avec les industriels, sur tous secteurs – ne me semblent *a priori* pas plus importantes sur le secteur de la défense. Mais il faut maintenir un effort soutenu sur un temps long, pour des technologies de ruptures très spécifiques, comme l'hyper vélocité, la furtivité large bande, la détection ultime, des programmes peu compatibles avec un mode de financement sur appels à projets qui devient majoritaire en France au détriment des subventions récurrentes. De plus, les appels à projets concernent principalement des projets collaboratifs, nationaux ou internationaux, ce qui ajoute une couche de complexité juridique. Un autre souci est notre capacité à recruter au bon niveau et en priorité sur la zone Europe, dans un milieu académique très compétitif et dans un contexte de relative désaffection des sciences dures chez nos jeunes.

Pour réduire les risques et maîtriser les vulnérabilités que vous venez d'aborder, quelles mesures recommanderiez-vous, que ce soit sur le plan humain, technique ou organisationnel ?

Au CIEDS, nous nous efforçons d'inclure dans les budgets des projets des salaires attractifs aux candidats doctorants et post-doctorants, et plus globalement de financer à un bon niveau des projets de 3 à 4 ans pour permettre aux laboratoires de travailler sur la durée. Notre objectif est également d'apporter un soutien sur le plus long terme aux chercheurs pour leur permettre de poursuivre les travaux dans la continuité et aller idéalement jusqu'au transfert vers l'industrie et les forces.

La recherche intéressant la défense dans les établissements d'enseignement supérieur et de recherche « civils »

Dr Frédéric Marie - Responsable PPST au Service du
Haut Fonctionnaire de Défense et de Sécurité du MESR

Titulaire d'un Magistère des sciences de la matière de l'université Lyon 1 et ENS Lyon, docteur en physique nucléaire, Frédéric MARIE est également auditeur de la 50ème session nationale de l'IHEDN « Armement et économie de défense ». Mis à disposition du CEA auprès du MESR entre 2005 et 2008, il a exercé à la DGRI les fonctions de chargé de mission « énergie nucléaire », chargé de mission « tutelle CEA » et celle de coordonnateur défense et sécurité. Il est aujourd'hui responsable du pôle PPST au Service du Haut Fonctionnaire de Défense et de Sécurité du MESR.

Le ministère de l'Enseignement supérieur et de la Recherche est le plus gros contributeur au dispositif interministériel de protection du potentiel scientifique et technique de la Nation (PPST) avec aujourd'hui près de 700 zones à régime restrictif (ZRR) créées au sein des établissements d'enseignement supérieur et de recherche. Sous sa tutelle, on peut compter : toutes les universités, la plupart des organismes de recherche (CNRS, INRIA, INRAE, INSERM, CNES, CIRAD, IRD, IPP, etc.) et beaucoup de grandes écoles d'ingénieurs (ENS, réseau des INSA et écoles Centrales, les UT, ENSI, l'IOGS, etc.), c'est-à-dire celles qui ne sont pas sous la tutelle des ministères en charge des armées, des finances et de l'agriculture.

Aujourd'hui, ce sont plus de 165 laboratoires de recherche qui sont protégés des captations étrangères, dans tous les domaines des sciences dures. Les ZRR hébergées dans tous ces établissements ont permis en 2021 au service du Haut-fonctionnaire de défense et de sécurité du MESR d'examiner plus de 14 000 dossiers de recrutement de chercheurs, étudiants et prestataires.

Mais tout l'enjeu pour le MESR est de permettre aux établissements de concilier une pluralité de partenariats scientifiques internationaux, y compris avec des grandes institutions de pays dits « sensibles », car ce sont eux qui garantissent l'excellence de nos recherches, avec le nécessaire contrôle des risques d'ingérence étrangère qui passe par les avis ministériels sur les accès en ZRR et les programmes de coopération internationale.

À de rares exceptions près, les recherches au sein des opérateurs civils du MESR se caractérisent par leur caractère amont et transversal, avec des TRL[1] plutôt bas et des applications potentielles civiles quand elles sont anticipées. Mais ce que l'on constate, c'est le caractère souvent dual de ces recherches. C'est-à-dire que si les chercheurs des laboratoires français ont souvent en ligne de mire des applications civiles potentielles de leurs recherches, ces mêmes recherches amont peuvent en parallèle déboucher sur des applications dans le domaine militaire (qu'il soit conventionnel ou non).

Il suffit d'observer l'appétence de certains étudiants étrangers pour certaines recherches bien identifiées au sein de nos laboratoires d'excellence pour se convaincre que ce sont clairement les applications futures de défense ou de sécurité qui sont visées et qui font l'objet de toutes les convoitises. Un élément de preuve en est apporté quand on analyse les risques de la PPST qui sont invoqués lors des avis négatifs du MESR. Ainsi en 2021, le risque d'atteinte aux intérêts de défense (conventionnelle) de la Nation est présent dans 80% des avis défavorables émis pour raisons scientifiques et techniques, à égalité avec le risque d'atteinte au potentiel économique de la Nation.

Aujourd'hui, tous les domaines scientifiques porteurs sont duaux : technologies de l'Espace, les sciences de l'information, l'électronique embarquée, l'intelligence artificielle, les matériaux innovants, l'énergie, etc. et les progrès scientifiques sont si rapides dans certaines disciplines, que les questions éthiques posées par les mésusages potentiels de certaines technologies par certains pays ou tout simplement par certains individus, deviennent prégnantes et doivent nous conduire à anticiper dès à présent ces risques et à les prendre en compte. C'est ce que nous faisons au MESR, dans l'analyse des risques de la PPST et des atteintes aux intérêts fondamentaux de la nation.

Au 21ème siècle, à l'ère du tout numérique et des réseaux sociaux, le maillon faible de la chaîne de vulnérabilité face aux risques de captation et d'ingérence reste l'être humain : le chercheur, l'ingénieur, l'étudiant, le collaborateur. Avec les services compétents de l'Etat, Il nous revient de poursuivre l'acculturation des communautés scientifiques à l'évolution des vulnérabilités de la recherche et à la mise en œuvre des bonnes pratiques, sans entraver l'esprit de création et de partage, mais sans naïveté.

[1] Le *Technology Readiness Level* est un système de mesure pour l'évaluation du niveau de maturité d'une technologie

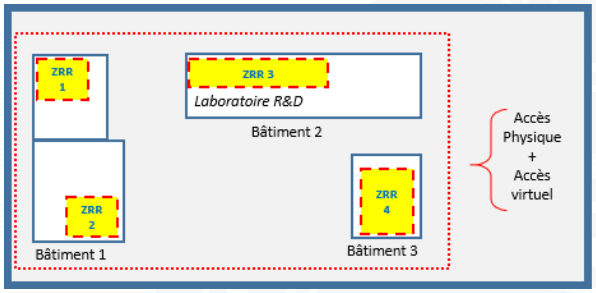
La zone à régime restrictif (ZRR) : un dispositif flexible offrant une protection ciblée, sur mesure et adaptable

Mme Mathilde Baudu - Chargée de Protection du Potentiel Scientifique (DGA/SSDI)

Ingénieure chimiste de formation, Mme Mathilde BAUDU occupe le poste de chargée de Protection du Potentiel Scientifique au Service de la sécurité de défense et des systèmes d'information (SSDI) de la Direction générale de l'Armement.

La zone à régime restrictif (ZRR) est le principal outil concourant à la protection du PPST. Ce dispositif vise à protéger l'accès aux savoirs, aux savoir-faire et aux technologies des entités publiques ou privées présentes sur le territoire national. Pouvant être mises en place tant par des acteurs industriels que par des établissements de recherche, les ZRR offrent une protection ciblée, sur mesure et adaptable.

En effet les entités qui choisissent d'adhérer à ce dispositif sont libres de définir leur niveau de protection en fonction de leurs moyens et de leurs besoins, en liaison étroite avec les services spécialisés. La réglementation impose simplement qu'une ZRR soit un espace clos doté, à chacun de ses accès extérieurs, d'une signalétique informant du statut de cet espace et des conséquences pénales auxquelles s'expose une personne y entrant sans autorisation.



Exemple de ZRR ciblées et circonscrites au juste besoin de protection

Le dispositif offre une protection juridique contre les actes malveillants ayant des conséquences sur la compétitivité de l'entité (utilisation frauduleuse d'informations, vol ou captation de données sensibles, pratiques anticoncurrentielles, intrusion dans les systèmes d'information, etc.).

Concrètement, la ZRR permet de circonscrire une zone de travail particulièrement sensible à la captation d'informations (moyens de production, zone de calcul, bureaux d'étude) en maîtrisant les entrées et les sorties à l'intérieur de cette derrière.

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, sera ainsi soumis à autorisation. Cette dernière sera accordée ou non après étude de l'opportunité par les services spécialisés. Adaptatif, ce dispositif suit la vie de l'activité sensible à protéger.

Si les dispositions de travail évoluent, la ZRR peut être révoquée, réduite ou agrandie, mais aussi dupliquée suivant les besoins. Pour les entités relevant du ministère des Armées, ce sont la DGA et la DRSD qui accompagneront la mise en place des ZRR et conseilleront tout au long de la vie de ces dernières.

Enfin, le dispositif PPST constitue un outil de promotion de la maturité de l'entité dans la protection des informations sensibles qu'elle détient, conférant ainsi une réelle crédibilité pour initier des partenariats avec des acteurs exigeants sur le plan de la sécurité.

Cas concret de risque maîtrisé grâce à la mise en place d'une ZRR

Un brillant étudiant étranger effectuant un master 2 en cotutelle entre l'université de son pays d'origine et un institut français prestigieux a postulé pour effectuer son stage au sein d'une entreprise française disposant d'une ZRR et spécialisée dans un secteur sensible à forte dualité civilo-militaire. L'entrée en ZRR nécessitant une autorisation, l'étude du dossier par le ministère compétent a permis de détecter que cet étudiant était proche d'une entreprise étrangère concurrente. Le stage lui a donc été refusé.

Pour aller plus loin, des informations sont disponibles sur le site IXARM :
www.ixarm.com/fr/protection-du-potentiel-scientifique-et-technique-ppst

CAS CONCRET 1
d'ingérence ciblant la recherche de défense française

Usurpation du courriel d'un chercheur

Exposé des faits

Un organisme de recherche français a été victime de plusieurs tentatives de vol de données concernant des prototypes de logiciels qu'il conçoit. Le ou les auteurs ont usurpé l'adresse mail d'un de ses cadres pour récupérer des informations sensibles relatives aux travaux de recherche et développement (R&D) de défense. Après plusieurs tentatives, une plainte a été déposée mais l'enquête n'a pas permis d'identifier les auteurs localisés à l'étranger.

Des vulnérabilités connues

Cet organisme a été ciblé pour ses prototypes de logiciels. Il est fort probable que ces tentatives aient été commanditées par un concurrent étranger qui cherchait ainsi à bénéficier malhonnêtement des efforts de recherche entrepris par cette entité française. Si le vol de données avait réussi, il aurait rapidement mis à mal la pérennité de l'organisme de recherche. Une démarche interne doit être entreprise afin de mieux percevoir les risques et les vulnérabilités qui pèsent sur toute l'activité de R&D des logiciels afin d'en renforcer la protection pour déjouer toute nouvelle tentative du même type ou autre.

Principales recommandations de la DRSD

- *Sensibiliser chaque nouvel arrivant ainsi que régulièrement le personnel aux risques d'ingérences avec pour consigne de signaler immédiatement toute approche inhabituelle ;*
- *Mettre en place (ou compléter) une charte informatique encadrant l'usage sécurisé des outils informatiques, notamment en matière de partage et de stockage d'informations sensibles ;*
- *Vérifier et au besoin renforcer le niveau de protection des informations de R&D (protection physique, informatique et juridique) ;*
- *Identifier et catégoriser (classifier) toutes les informations sensibles pour mettre en place un dispositif de protection adapté ;*
- *Effectuer une veille concurrentielle pour identifier et évaluer les risques (menaces-vulnérabilités-conséquences) présents et à venir ;*
- *Vérifier si d'autres faits inhabituels liés aux tentatives de vol se sont produits. Si c'est le cas, les intégrer à l'analyse mentionnée ci-dessus.*

S'il s'agit de travaux de recherche en lien avec la « sphère défense » :

- *Informer la DRSD de ces faits qui entrent dans son champ de compétences en matière de contre-ingérence ;*
- *Solliciter son expertise (meilleure compréhension de la menace, conseils adaptés pour la protection des informations sensibles).*

La DRSD est en mesure de réaliser des actions de sensibilisation à la protection des informations et à la contre-ingérence économique au profit de la direction et du personnel de l'organisme de recherche.

La rapidité de réaction permet de limiter les conséquences : il est indispensable de signaler le moindre doute le plus rapidement possible.

CAS CONCRET 2
d'ingérence ciblant la recherche de défense française

Entrisme d'un professeur étranger

Exposé des faits

Au début de la crise sanitaire, en pleine période de pénurie d'effets de protection individuelle, un professeur originaire d'Asie du sud-est a proposé à la direction de son école d'effectuer des démarches pour la livraison importante de masques.
Ce professeur est réputé pour faciliter la venue en France de délégations et d'étudiants de son pays, dont certains ont déjà récupéré indûment des informations sensibles dans les établissements qu'ils visitaient ou fréquentaient.
Au travers de cette offre, il cherchait à s'attirer la sympathie des responsables de son école pour relancer l'accueil de ses compatriotes dans des laboratoires sensibles.

Des vulnérabilités connues

S'il s'agit d'être prudent sur l'implication directe de ce professeur dans la récupération d'informations par certains de ses compatriotes, il semble important de veiller à la protection des informations sensibles auxquelles pourraient avoir accès des ressortissants étrangers privilégiant les intérêts de leur pays d'origine au détriment de celui qui les accueille.
Quelle que soit leur nationalité, quel que soit le motif de leur présence dans des universités, des laboratoires de recherche ou des organismes dédiés à la recherche et à l'innovation (R&D), il est impératif de les encadrer avec le souci de préserver toute information contribuant à la valorisation des projets.

Principales recommandations de la DRSD

Quels que soient les profils des visiteurs et leur temps de présence :

- *Encadrer le personnel de passage (chercheurs, doctorants, stagiaires, etc.), c'est-à-dire préciser les règles qui s'imposent sur le site (zones de circulation autorisées ou non, horaires de présence autorisés ou non, port du badge apparent, autorisation ou non de prise de photographies, remise des appareils numériques avant l'accès à certaines zones protégées, accompagnement obligatoire ou non d'un représentant de l'établissement, etc.). Ces règles doivent être communiquées et appliquées par tous (personnel permanent et temporaire, visiteurs) avec un contrôle de leur mise en œuvre ;*
- *Identifier et limiter l'accès à toutes les informations dont la récupération pourrait être préjudiciable à l'entité et/ou ses représentants ;*
- *Veiller à la protection juridique de ces informations (propriété intellectuelle, clause de confidentialité, etc.) ;*
- *Veiller à attribuer des droits d'accès informatique limités aux besoins professionnels ;*
- *Réglementer l'usage d'objets numériques personnels, surtout dans les zones dédiées à la R&D ;*
- *Sensibiliser et former le personnel à l'ensemble des règles précitées ;*
- *Encadrer les délégations (avant : obtenir l'identité, la nationalité des personnes ; pendant : remise de badge spécifique, informer les collaborateurs ; et après : réunion post-délégation pour remonter des informations comme le questionnement intrusif de certains membres de la délégation).*

N'hésitez pas à contacter votre chaîne de sûreté/sécurité au sein de votre structure de recherche et votre agent DRSD référent afin de faire remonter toute ingérence ou atteinte (physique, économique, juridique, cybernétique, etc.) dont vous penseriez être victimes.
Soyez assurés que la DRSD et chacun des agents présents à votre contact se tiennent à vos côtés.

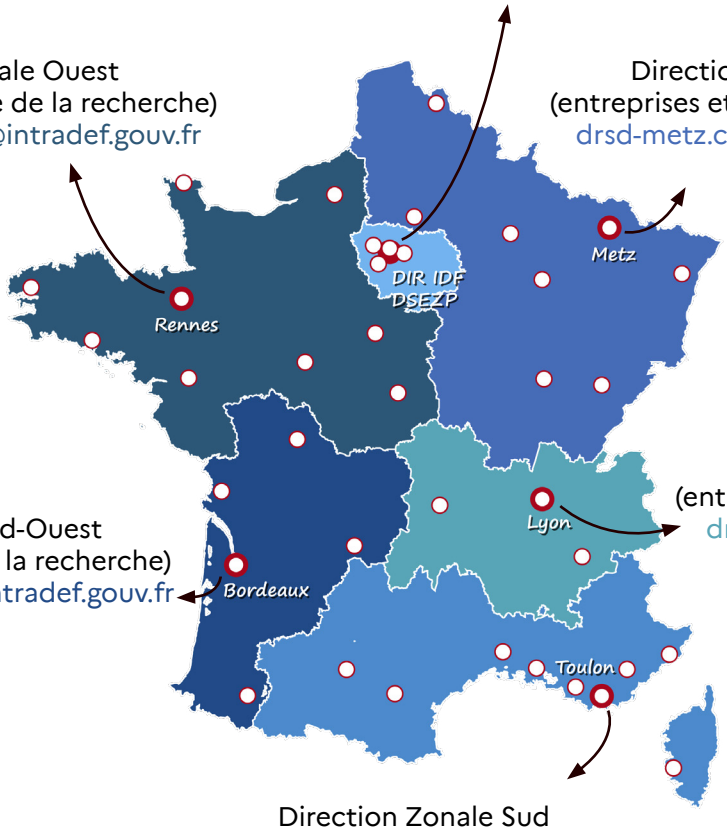
Gardons le contact

Direction Centrale
Section « Sensibilisation »
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Directions Zonales Ile-de-France
Entreprises : drsd-dsezp-4.cds.fct@intradef.gouv.fr
Instituts et écoles de recherche : drsd-idf.cmi.fct@intradef.gouv.fr

Direction Zonale Ouest
(entreprises et monde de la recherche)
drsd-rennes.cmi.fct@intradef.gouv.fr

Direction Zonale Nord-Est
(entreprises et monde de la recherche)
drsd-metz.cmi.fct@intradef.gouv.fr



Direction Zonale Sud-Est
(entreprises et monde de la recherche)
drsd-lyon.cmi.fct@intradef.gouv.fr

Direction Zonale Sud-Ouest
(entreprises et monde de la recherche)
drsd-bordeaux.cmi.fct@intradef.gouv.fr

Direction Zonale Sud
(entreprises et monde de la recherche)
drsd-toulon.cmi.fct@intradef.gouv.fr