RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

IH2EF INSTITUT DES HAUTES ÉTUDES DE L'ÉDUCATION ET DE LA FORMATION

DRSD : un service de renseignement qui protège la recherche en lien avec la Défense - Entretien

Publié le 14 octobre 2024

En mettant en lumière ses missions de surveillance, de prévention et de collaboration étroite avec les institutions académiques, cette discussion avec la Direction du renseignement et de la sécurité de la défense (DRSD) éclaire les stratégies mises en place pour sauvegarder le patrimoine scientifique et technique national face aux menaces d'ingérence.

Entretien réalisé en avril 2024.

Qu'est-ce que la DRSD?

La Direction du renseignement et de la sécurité de la défense (DRSD) est issue du deuxième bureau créé au sein de l'État-major de l'armée à la suite de la défaite de 1871 face à la Prusse. De nombreuses réorganisations et réformes des services de contre-ingérence au profit des forces armées et de l'industrie de défense sont intervenues dans les 152 ans d'histoire qui ont succédé à cette création. S'inscrivant notamment dans les pas de la sécurité militaire créée en 1961 renommée en Direction de la protection et de la sécurité de la défense (DPSD) en 1981, la DRSD (dont le changement de nom est intervenu en 2016 pour

mieux souligner la composante de sa mission renseignement) œuvre chaque jour afin de "renseigner pour protéger" (devise du service) la sphère défense élargie (personnels du ministère des Armées et des Anciens combattants et entreprises de la base industrielle et technologique de défense) contre les tentatives d'ingérences d'acteurs malveillants. Directement rattachée auprès du ministre des Armées et des Anciens combattants, son action s'inscrit également en étroite coordination avec l'ensemble des services de la communauté nationale du renseignement créée en 2007.

De quelles manières la DRSD œuvre-t-elle à protéger la recherche sensible et l'innovation au sein du secteur de la défense, en particulier dans les universités et les laboratoires de recherche?

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 développant des applications militaires et duales à des 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 et des Anciens combattants à préserver encore davantage qu'hier le potentiel d'innovation et la DRSD à prendre en compte cette dimension internationale de la recherche.

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

Comment la DRSD évalue-t-elle et répond-elle aux menaces potentielles pesant sur l'infrastructure de recherche liée à la défense en France, et quels défis rencontre-t-elle dans ce domaine ?

Ces menaces sont multiples mais la DRSD a coutume de les réunir en six catégories :

- humaines (débauchage de chercheur, pressions exercées à l'occasion d'un déplacement à l'étranger) ;
- physiques (intrusion au sein d'un laboratoire, survol de drone à des fins de reconnaissance) ;
- capitalistiques (approches d'incubateurs de start-up par des fonds étrangers activistes) ;

- juridiques (inclusions de clauses à portée extraterritoriale dans un partenariat universitaire) ;
- réputationnelles (campagne de dénigrements des recherches développées par un laboratoire) ;
- cyber (rançonnage d'un laboratoire ou exfiltration de données à des fins d'espionnage).

Pour caractériser ces menaces, la DRSD peut notamment compter sur son maillage territorial et sur la collaboration avec les autres services de l'État. La DRSD conduit deux actions simultanées permettant d'évaluer l'amplitude du risque. D'une part, elle conduit ses missions de détection de la menace en évaluant les capacités et les intentions de concurrents à cibler des domaines spécifiques, d'autre part, elle conduit des missions d'évaluation du niveau de protection, le cas échéant de vulnérabilités des sites potentiellement concernés. En jugeant du ratio menace/vulnérabilité, le Service parvient ainsi à mesurer autant que possible le risque d'occurrence des atteintes et leur impact. Les grands défis rencontrés tiennent à l'évolution des stratagèmes reposant davantage qu'hier sur la numérisation des données (hausse de la fluidité de l'information), l'emploi du droit et des normes à des fins concurrentielles (influence) et la grande mouvance des acteurs économiques innovants plus nombreux, plus insouciants et plus fragiles.

Pouvez-vous décrire la nature de la collaboration avec les institutions de l'enseignement supérieur et de la recherche ? Comment cette collaboration renforce-t-elle la sécurité des activités de recherche et de développement ?

Il existe en France une multitude d'acteurs qui concourent à la promotion et à la qualité de la recherche de défense française. Ce sont des maillons et relais indispensables de la mission de protection de la DRSD. 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 (direction générale de l'armement et agence de l'innovation de défense) et interministériel (ministère de l'enseignement supérieur et de la recherche), y compris déconcentré, une action de planification stratégique.

Cette collaboration avec les institutions de l'enseignement supérieur et de la recherche permet notamment de renforcer les actions de la DRSD dans l'identification des risques, l'évaluation des menaces liées à la recherche de défense française et ses missions de sensibilisation.

Comment la coopération internationale s'intègre-t-elle dans la stratégie de la DRSD pour protéger la recherche liée à la défense, et quels sont les avantages et les défis de cette coopération ?

Afin de répondre à cette question, nous vous proposons le cas concret suivant :

En novembre 2023, un laboratoire de recherche lié au ministère des Armées a accueilli une chercheuse étrangère issue d'une prestigieuse université de son pays d'origine. Le CV de celle-ci était très attrayant pour le laboratoire car elle y indiquait avoir participé à la rédaction d'un nombre important d'articles scientifiques publiés dans des revues internationales de premier rang. L'intérêt de ce profil était renforcé par son statut de boursière, ce qui lui permettait de bénéficier d'une subvention totale pour ses travaux.

Dès son arrivée, cette chercheuse a attiré l'attention de son entourage professionnel en procédant à un inventaire détaillé du matériel utilisé par l'équipe de recherche.

Elle s'est également montrée très insistante auprès de son encadrement pour disposer de la clé des locaux de recherche, ce qui lui a toujours été refusé.

Par ailleurs, cette chercheuse n'a pas travaillé sur les projets scientifiques qu'elle devait mener mais a montré beaucoup d'intérêt pour le projet de recherche d'un autre doctorant dont les travaux sont considérés par le directeur du laboratoire comme innovants, intéressant l'industrie de pointe et pouvant faire prochainement l'objet d'un dépôt de brevet.

Enfin, cette chercheuse s'est montrée extrêmement insistante envers deux membres du laboratoire en leur proposant de rejoindre un programme de recherche étranger et en évoquant une rétribution financière importante. Malgré de multiples relances de plus en plus insistantes, les deux chercheurs, sensibilisés par le Service aux risques liés aux partenariats avec ce pays, n'ont pas donné suite.

Intrigué, le directeur du laboratoire a pris attache avec l'ancien employeur de cette chercheuse, qui a confirmé avoir observé les mêmes comportements suspects. Du fait d'un constat unanime sur l'inadéquation de son profil et sur son comportement suspect, le laboratoire a désactivé dès mars 2024 son badge d'accès et procédé à l'annulation de sa convention d'accueil. Elle a quitté le territoire national depuis.

Si les ingérences conduites par des ressortissants étrangers dans le milieu de la recherche scientifique publique d'intérêt défense se multiplient, la nature offensive du cas d'espèce lui procure un caractère inédit.

Les différents rapports français semblent mettre en lumière que cette chercheuse était engagée dans une logique de captation de savoirs, savoir-faire et/ou technologies, en misant sur la rapidité et l'agressivité et représente donc une menace pour le potentiel scientifique et

technique de la France. Le Service considère donc que cette chercheuse pourrait être instrumentalisée par un service de renseignement étranger et servir d'intermédiaire en vue de débaucher des ingénieurs-chercheurs français ou de capter des informations et savoir-faire sensibles d'intérêt défense.

Comment la DRSD trouve-t-elle l'équilibre entre le besoin d'innovation dans la recherche de défense et la nécessité de mesures de sécurité pour protéger ces innovations de l'espionnage ou du vol ?

À l'instar de sa mission de contre-ingérence économique en milieu industriel, la DRSD tâche de concilier intelligence et vigilance pour préserver la continuité de l'activité scientifique. Il en va de l'intérêt du ministère des Armées de préserver la capacité d'innovation des laboratoires français. Il s'agit donc de trouver le juste équilibre pour freiner le moins possible le travail des chercheurs au quotidien tout en leur permettant de travailler dans des conditions sécurisées, pour eux comme pour le produit de leurs recherches.

L'encadrement des partenariats étrangers vise bien cela : permettre à ces partenariats d'avoir lieu, tout en garantissant un juste niveau de sécurité. De la même manière, le renforcement de mesures de sécurité au sein d'établissements ou de laboratoires - adaptées au juste besoin de protéger les valeurs sensibles - permet aux chercheurs, français comme étrangers, de travailler à l'abri de tentatives d'ingérences étrangères ou de pouvoir facilement détecter et alerter quand elles ont lieu.

Compte tenu de la menace croissante des cyberattaques, quelles mesures la DRSD met-elle en œuvre pour protéger les données de recherche numériques et les communications au sein de la communauté de recherche en défense ?

Les établissements de recherche français, y compris ceux contribuant au potentiel de défense français, représentent un milieu parfois peu sensibilisé aux ingérences étrangères et doté de moyens de protection souvent réduits, y compris sur le plan de la cybersécurité. Pour aider les unités de recherche à monter en maturité, les agents de la DRSD font la promotion des recommandations établies par l'Agence nationale de sécurité des systèmes d'information (ANSSI) au travers de guides en accès libre, mais aussi des prestataires en sécurité des systèmes d'information certifiés par cette dernière, y compris en matière de communication ou d'hébergement en nuage (cloud).

Enfin, des sensibilisations spécifiques dédiées à la menace cyber sont conduites par les agents de la DRSD, parfois épaulés par d'autres acteurs de la sécurité des systèmes d'information.

Quel rôle la DRSD joue-t-elle dans la sensibilisation et la fourniture de formations sur les questions de sécurité aux chercheurs et au personnel dans les environnements de recherche liés à la défense ?

La DRSD sensibilise chaque année des centaines de chercheurs aux ingérences touchant la recherche d'intérêt défense, mais aussi leurs collaborateurs et comités de direction. Une attention particulière est donnée aux départements de valorisation de la recherche ainsi que des relations internationales. De plus, en amont de déplacements à l'étranger, qui présentent des risques spécifiques de fuite, de perte et de vol de données, une sensibilisation dédiée peut être organisée. Sur sollicitation du laboratoire ou sur invitation de la DRSD, ces sessions de sensibilisation peuvent être organisées tout au long de l'année, y compris avec d'autres partenaires. La sensibilisation de tous les acteurs du monde de la recherche et de l'innovation est primordiale dans un objectif de sécurisation équilibrée de ce milieu. Chaque conscience éveillée est un rempart de plus face aux ingérences étrangères qui cherchent à tirer profit de l'excellence scientifique française.

En regardant vers l'avenir, quelles sont, selon vous, les menaces émergentes les plus significatives pour la sécurité de la recherche et des laboratoires de Défense, et comment la DRSD se prépare-t-elle à relever ces défis ?

Dans le contexte actuel de compétition économique et technologique accrue entre les différentes puissances étatiques mondiales, tous les secteurs scientifiques jugés stratégiques peuvent être les cibles de stratégies d'influence et d'actes d'ingérence émanant de l'étranger, dans l'ensemble des types d'ingérences précédemment évoqués.

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 duales et tout aussi discriminantes pour les armées de demain. Pour répondre à ces défis, la DRSD renforce continuellement ses capacités et ses liens avec les autres services de l'État mais aussi avec le monde universitaire.

Ces technologies, particulièrement sensibles, ont des applications duales qui permettent de lever des verrous technologiques et d'irriguer des programmes d'armement conventionnels et non-conventionnels. Plusieurs pays souhaitent accroître leurs capacités et démontrent donc un intérêt croissant pour des savoirs et savoir-faire dans ces domaines. Cela se traduit notamment par de nombreuses approches : proposition de partenariats, de collaborations scientifiques, sollicitations lors de conférences, etc.

Le grand défi à venir est la rapidité à savoir, comprendre et agir en matière de renseignement et d'alerte. Nous sommes passés de la protection du savoir par la dissimulation (masquer nos atouts comparatifs - cacher au concurrent) à la protection du savoir par la rapidité d'innovation (maintenir un niveau d'avancée supérieur - perpétuellement supplanter le concurrent). Ce cadre amplificateur d'événements économiques met le renseignement au défi de l'accès à temps à la donnée et à celui de l'obsolescence de l'information.

Pour réussir, il y a trois actions à conjuguer et la DRSD s'y emploie :

- partager l'intelligence : promouvoir une totale coopération interservices pour recouper et transmettre l'information obtenue ;
- partager l'événement : solliciter un échange fluide ; permanent et à temps des alertes et des faits entre les acteurs cibles (laboratoires, incubateurs, etc.) et le Service ;
- s'équiper de moyens de comprendre plus vite la masse de données collectées : la DRSD dispose d'un outil souverain de traitement des données hétérogènes réduisant le temps d'exploitation des données et facilitant le travail de l'analyste.

Enfin, quels sont les 2 conseils majeurs que la DRSD offrirait aux chercheurs travaillant sur des projets de défense sensibles pour assurer la sécurité de leur travail et prévenir l'accès ou les fuites non autorisés ?

Le premier conseil concerne les coopérations internationales et le nécessaire "cadrage" de celles-ci, qu'elles soient formalisées entre laboratoires ou universités, ou plus informelles, ad hoc, entre chercheurs. Deux points d'attention particulier sont nécessaires :

1. la vérification de l'équilibre du partenariat en termes de partage de la propriété intellectuelle d'une part et l'application de réciprocité dans les échanges d'étudiants étrangers, notamment en termes de volumes. Ainsi, il faut savoir dire "non" à des partenariats déséquilibrés ou pour lesquels la partie française ne gagne rien.
2. Le second conseil, plus général, consiste, pour toute personne travaillant en milieu scientifique ou industriel, à ne pas hésiter à faire part de tout événement, y compris d'ampleur réduite, qui serait perçu comme anormal voire insolite. Il s'agit d'un élément clé de la remontée d'incidents, qui va permettre à la structure de sécurité de l'université d'alerter les services de l'État, qui procéderont à la levée de doute et à l'accompagnement de la structure française ou de l'ingénieur/chercheur concerné.

Cet entretien est extrait du dossier Intelligence économique.