MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Direction de la Protection des Installations Moyens et activités de la Défense (DPID)

Paris, le 06 décembre 2022
N°DEP-00561/ARM/DPID/NP

NOTE

A l'attention des destinataires « *in fine* »

OBJET : mise en œuvre de la circulaire interministérielle n°3145

RÉFÉRENCE : Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation n° 3415/SGDSN/AIST/PST du 7 novembre 2012.

D. ABROGÉS : - Instruction ministérielle n° 298 du 5 mars 2014.
- note n°DEP-00437/2022/ARM/DPID/NP du 29 juillet 2022

ANNEXES : cinq.

Le document en annexe se substitue, dans une version provisoire, à l'instruction ministérielle n°298 du 5 mars 2014. Même si de nombreux travaux se poursuivent, il était nécessaire de disposer sans plus attendre d'un document actualisé afin d'accompagner et dynamiser le recours au dispositif de **protection du potentiel scientifique et technique de la nation** (PPST).

Cette note a donc vocation à être révisée très régulièrement, notamment en fonction des conclusions des travaux interministériels en cours sur les évolutions législatives et réglementaires du dispositif. En particulier, le sujet des projets de coopération, abordé dans l'instruction n°298, sera traité dans une version ultérieure.

Le potentiel scientifique et technique de la nation est constitué de l'ensemble des biens matériels et immatériels propre à l'activité scientifique fondamentale ou appliquée et au développement technologique. **Il constitue l'un des intérêts fondamentaux de la nation française**[1], au même titre que la sécurité et l'intégrité du territoire.

La protection du potentiel scientifique et technique de la nation est assurée par l'existence de **zones à régime restrictif** (ZRR) mentionnées à l'article R. 413-5-1 du code pénal et par la définition de **secteurs scientifiques et techniques protégés** en raison de l'intérêt qu'ils présentent pour la nation ou pour ceux qui les convoitent.

[1] Art. 410-1 du code pénal.

14 rue Saint Dominique
75007 PARIS SP 07
victoire1.roussel@intradef.gouv.fr
Dossier suivi par : ASC1 Roussel

Le dispositif de protection du potentiel scientifique et technique de la nation vise à prévenir la captation de savoirs et savoir-faire stratégiques des établissements au regard des **quatre risques suivants** :

- les atteintes aux intérêts économiques de la France (R1) ;
- le détournement de technologies conventionnelles susceptibles de renforcer l'arsenal militaire d'un autre pays ou d'affaiblir les capacités de défense de la nation (R2) ;
- la prolifération des armes de destruction massive et de leurs vecteurs, dans les domaines nucléaire, balistique, chimique ou biologique (R3) ;
- le détournement de savoirs susceptibles d'être utilisés à des fins d'activités terroristes, menées sur le territoire national ou à l'étranger (R4).

La protection du potentiel scientifique et technique est structurée au niveau interministériel par la circulaire de référence qui fixe les orientations générales en la matière. La présente note vient décliner et compléter ce texte, en précisant les modalités d'application relevant du ministère des Armées, notamment celles relatives à la politique de mise en place des zones à régime restrictif et au contrôle des accès associé.

Elle s'adresse aux armées, directions et services (ADS) ministériels, aux établissements publics sous tutelle du ministère, en particulier ceux d'enseignement supérieur et de recherche, et les entreprises dont l'activité relève du secteur de la défense et avec lesquelles, le ministère a conclu un contrat ou une convention spécifique.

Les modalités particulières qui concernent uniquement les entités liées par contrat ou par convention au ministère des Armées sont signalées par un encadré dans le corps du texte.

La protection du potentiel scientifique et technique de la nation est un dispositif simple, adapté aux moyens de l'établissement et qui présente de multiples avantages (protection administrative et juridique, sanctions renforcées contre les actes malveillants, appartenance à une communauté de confiance favorable aux partenariats industriels etc.). Dans un contexte de compétition stratégique exacerbée, l'adhésion à ce dispositif par les établissements concernés est une priorité.

Le vice-amiral Denis Bertrand
Directeur de la protection des installations,
moyens et activités de la défense,
haut fonctionnaire correspondant de
défense et de ~~sécurité adjoint~~

ANNEXE 1

Organisation de la protection du potentiel scientifique et technique au sein du ministère des Armées

Le ministre des Armées fixe les orientations générales du ministère en matière de protection du potentiel scientifique et technique de nation. Conformément au code de la défense, il peut déléguer certaines de ses compétences aux autorités suivantes.

1. Le haut fonctionnaire correspondant de défense et de sécurité

Le chef du cabinet militaire exerce les fonctions de **haut fonctionnaire correspondant de défense et de sécurité** (HFCDS) et agit au nom du ministre, pour ce qui relève du domaine de la protection du potentiel scientifique et technique de la nation.

Le HFCDS est assisté par la direction de la protection des installations, moyens et activités de la défense (DPID) dont le directeur est HFCDS adjoint. À ce titre, ce dernier dispose des prérogatives relevant du haut fonctionnaire correspondant de défense et de sécurité en matière de protection du potentiel scientifique et technique de la nation.

Le directeur de la protection des installations, moyens, activités de la défense (DPID) :

- prépare les orientations générales du ministère des Armées en matière de protection du potentiel scientifique et technique de la nation ;
- en suit la bonne exécution par les autorités compétentes définies ci-dessous[2] et la Direction du renseignement et de la sécurité de la défense (DRSD) ;
- assure les liaisons avec le Secrétariat général de la défense et de la sécurité nationale (SGDSN) ;
- adresse chaque année au SGDSN un bilan des activités liées à la protection du potentiel scientifique et technique de la nation ;
- peut diligenter des audits ou contrôles au sein des établissements ayant adhéré au dispositif de protection du potentiel scientifique et technique de la nation.

Dans le cadre de tutelles multiples au sein du ministère des Armées, il règle **les différents susceptibles de survenir** entre les autorités concernées.

2. Les autorités compétentes recevant délégation de pouvoirs du ministre des Armées

Les autorités suivantes reçoivent délégation du ministre des Armées[3] pour **déterminer le besoin de protection** du potentiel scientifique et technique de la nation :

2.1 Le chef d'état-major des armées (**CEMA**), pour les organismes interarmées implantés en métropole autres que ceux relevant des autorités mentionnées au §2.3, et pour les formations, services et établissements placés sous l'autorité ou l'autorité d'emploi des commandements supérieurs des forces armées ;

---

[2] Les autorités compétentes sont les autorités ayant reçu délégation du ministre des Armées pour déterminer le besoin de protection du potentiel scientifique et technique de la nation, pour créer, par arrêté, une zone à régime restrictif (ZRR) et pour émettre un avis sur les demandes d'accès aux ZRR.

[3] Art. D. 2362-2 du code de la défense.

2.2 Le délégué général pour l'armement (**DGA**), le secrétaire général pour l'administration (**SGA**), les chefs d'état-major d'armées, le directeur général des relations internationales et de la stratégie (**DGRIS**), le directeur général du numérique (**DGNUM**), le directeur général de la sécurité extérieure (**DGSE**), le délégué à l'information et à la communication de la défense (**DICOD**), le directeur du renseignement et de la sécurité de la défense (**DRSD**), le chef du contrôle général des armées (**CGA**) et le sous-directeur des bureaux des cabinets pour les formations, services, établissements et entreprises relevant de leur responsabilité respective ;

2.3 Le directeur du renseignement militaire (**DRM**), le directeur central du service de santé des armées (**DCSSA**), le directeur central du service des essences des armées (**DCSEA**), le directeur central de la direction interarmées des réseaux d'infrastructures et des systèmes d'information de la défense (**DIRISI**), le directeur central du service du commissariat des armées (**DCSCA**) et le directeur du service interarmées des munitions (**DSIMu**) pour les formations, services et établissements relevant de leur responsabilité respective ;

2.4 Le directeur de la protection des installations, moyens et activités de la défense (**DPID**) pour les formations, services, établissements et entreprises ne relevant de la responsabilité d'aucune des autorités mentionnées *supra*.

L'autorité ayant déterminé le besoin de protection a délégation du ministre des Armées[4] pour **créer par arrêté, une zone à régime restrictif** (ZRR) et **émettre un avis sur les demandes d'accès** aux ZRR.

Chaque autorité compétente est responsable de déterminer le besoin de protection, créer une zone à régime restrictif et émettre un avis sur les demandes d'accès aux ZRR pour les entreprises avec lesquelles elle a conclu un contrat ou une convention spécifique. Pour les entreprises relevant de plusieurs autorités compétentes, un choix est arrêté par concertation entre autorités. En cas de désaccord, la DPID est chargée d'arbitrer le différent.

3. Le directeur du renseignement et de la sécurité de la défense

La direction du renseignement de la sécurité et de la défense est le service de renseignement dont dispose le ministre des Armées pour assumer ses responsabilités en matière de sécurité du personnel, du matériel et des installations sensibles.

Le directeur du renseignement et de la sécurité de la défense apporte son concours au haut fonctionnaire correspondant de défense et de sécurité ainsi qu'aux autorités compétentes dans :

- la caractérisation de la menace et de l'exposition aux risques R1 à R4 des activités conduites par l'organisme et une proposition du besoin de protection du potentiel scientifique et technique de la nation qui est arrêté par l'autorité compétente en concertation avec la DRSD ;

[4] Art. D. 2362-4 et D. 2362-4-1 du code de la défense.

- le traitement des demandes de création, de modification et de suppression de zones à régime restrictif ;
- le traitement des demandes d'accès aux zones à régime restrictif ;
- le contrôle de l'application des dispositions de protection du potentiel scientifique et technique de la nation dans les établissements publiques du ministère, ainsi que l'accompagnement et le suivi dans les entreprises privées de défense.

ANNEXE 2

Création, modification ou suppression d'une zone à régime restrictif[5]

1. Création d'une zone à régime restrictif

Lorsqu'il existe un risque de captation d'informations, de savoirs et de savoir-faire sensibles susceptibles de porter atteinte au potentiel scientifique et technique de la nation, **l'établissement et l'autorité compétente pour déterminer le besoin de protection s'entendent** sur la nécessité de créer une ou plusieurs zones à régime restrictif.

S'agissant d'une entreprise privée, la détermination du besoin de protection résulte d'une concertation entre l'autorité compétente et l'entreprise concernée. La DRSD est associée, autant que besoin, tout au long du processus. Pour les entreprises qui ne sont pas liées par contrat au ministère des Armées, **une convention spécifique** formalise la concertation.

Afin de déterminer la nécessité de créer une zone à régime restrictif, le ministère des Armées met à la disposition des établissement **un questionnaire**[6], permettant d'évaluer la sensibilité de l'organisme et du potentiel scientifique et technique détenu au regard des risques encourus.

Ce questionnaire d'évaluation du besoin de protection est à renseigner par le chef d'établissement. Une fois complété, le document doit porter la mention de protection *Diffusion Restreinte* et être retourné par voie électronique à l'aide d'un moyen de chiffrement, ou, à défaut, par CD ROM ou clef USB, à l'autorité compétente et à la DRSD. Dans le cas où des précisions seraient nécessaires, l'autorité compétente et la DRSD peuvent procéder à **une visite de l'établissement.**

Si l'étude du questionnaire et l'analyse de risques conduite confirment le besoin de protection, l'autorité compétente fournit à l'établissement **un dossier de création de zone à régime restrictif**[7]. Il s'agit alors de **déterminer précisément le périmètre physique** de la ZRR. Ce dernier doit être adapté au juste besoin et ne cibler que les zones nécessitant une protection autour des seuls locaux ou bâtiments abritant du potentiel scientifique et technique.

Le dossier de création est à retourner, de préférence sous forme dématérialisée, à l'autorité compétente et à la DRSD. Il doit porter *a minima* la mention de protection *Confidentiel Industrie* [8] et si nécessaire, être classifié.

Préalablement à la signature de l'arrêté de création de la zone à régime restrictif, la DRSD confirme à l'autorité compétente que **l'espace est bien clos et délimité**[9].

---

[5] La création, modification et suppression d'un local sensible suit la même procédure.

[6] Un modèle est disponible sur le site Internet IXARM.

[7] La liste des pièces à fournir est disponible sur le site Internet IXARM.

[8] Mention de confidentialité spécifique définie à la fiche 7.5 de l'instruction ministérielle n°900 relative à la protection du secret et des information *Diffusion Restreinte* et sensibles.

[9] Un espace clos n'est pas nécessairement fermé à clef mais ses limites ne doivent pas pouvoir être franchies par inadvertance.

Une fois ces différentes étapes réalisées, l'autorité compétente informe le SGDSN de son intention de créer une ZRR au profit de l'établissement concerné. Celui-ci procède alors à **l'enregistrement de la ZRR** au répertoire national des zones à régime restrictif et fournit à l'autorité compétente **le numéro d'identifiant correspondant**.

L'autorité compétente signe ensuite **l'arrête portant création de la ZRR**. Celui-ci précise le nom et l'adresse de l'établissement, le numéro d'identifiant et le plan de masse de la zone à régime restrictif.

La décision de création de la zone à régime restrictif est enfin notifiée à l'établissement et communiquée au ministère de l'Intérieur, au préfet territorialement compétent, au SGDSN, à la DPID et à la DRSD.

Dans le cadre où la démarche de création de zones à régime restrictif a été initiée par le ministère des Armées pour une entreprise privée, le chef de l'entreprise **peut refuser de profiter du dispositif de protection du potentiel scientifique et technique**. La décision de refus motivée doit être transmise par écrit à l'autorité compétente.

Le ministère des Armées peut toutefois **imposer cette démarche** en cas de risques ou menaces liés au détournement de technologies (R2), à la prolifération (R3) ou au terrorisme (R4).

2. Modification d'une zone à régime restrictif

Lorsque l'établissement souhaite modifier le périmètre de la ZRR, le responsable d'établissement adresse **un courrier explicatif** à l'autorité compétente avec copie à la DRSD. La modification du périmètre de la ZRR est traitée **de manière similaire** à celle de la création de la ZRR. Ainsi, la DRSD doit confirmer le contour du tracé envisagé avant que l'autorité compétente signe un nouvel arrêté.

En cas de changement de la structure juridique ou capitalistique, de redressement ou de liquidation judiciaire de l'établissement, le chef d'établissement concerné doit informer l'autorité compétente et la DRSD. Si de nouveaux risques découlent de ces évolutions, l'autorité compétente peut proposer **des mesures additionnelles de protection**, qu'elle communique alors au responsable de la ZRR.

La DRSD peut également transmettre à l'autorité compétente un avis, dans lequel elle indique **les mesures correctrices** qu'elle juge nécessaire pour remédier aux failles de sécurité éventuellement induites par le changement de structure juridique ou capitalistique de l'établissement. Cet avis ne lie pas l'autorité compétente.

3. Suppression

Le chef d'établissement adresse un courrier à l'autorité compétente, avec en copie la DRSD, s'il envisage de demander la suppression d'une ZRR. Ce courrier doit préciser **les raisons motivant la suppression**.

La DRSD communique à l'autorité compétente **tout élément susceptible de justifier ou non** la suppression de la ZRR au regard de la sensibilité de l'activité exercée par l'établissement. L'autorité compétente évalue alors le bien-fondé de la demande et en cas d'accord, signe **un arrêté portant suppression de ladite ZRR.**

Si elle le juge nécessaire, l'autorité compétente peut organiser, avec le concours de la DRSD, **une visite** de la ZRR concernée.

Tableau synthétisant le processus de création d'une ZRR

	Acteurs		
Étapes de création d'une ZRR	Établissement	Autorité compétente	DRSD
Renseigne le questionnaire d'évaluation	**Responsable**	Destinataire	En copie
Détermine le besoin de protection	**Responsable**	**Responsable**	Contributeur
Remplit et transmet le dossier de création de ZRR	**Responsable**	Destinataire	En copie
Instruit le dossier de création de ZRR	-	**Responsable**	-
Signe l'arrêté de création de la ZRR	Destinataire	**Responsable**	En copie

Annexe 3

Les mesures de protection du potentiel scientifique et technique de la nation

1. Mesures de protection contre l'intrusion physique

Il appartient au chef de la ZRR ou le cas échéant, au chef de l'établissement de mettre en œuvre **les mesures nécessaires** pour protéger le potentiel scientifique et technique de l'établissement.

Il doit se conformer **aux obligations juridiques** définies par l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation qui supposent :

- l'installation, à l'extérieur du périmètre de la ZRR **d'une signalétique** informant du statut de ZRR et des conséquences pour les personnes qui sont entrées frauduleusement dans cette zone ;
- la mise en place **d'un contrôle d'accès** (voir annexe 4) ;
- la détermination de mesures de sécurité applicables **aux visites**[10] ;
- la définition et la mise en œuvre **d'une politique de sécurité des systèmes d'information** (PSSI).

A ces fins, il met en place **un règlement intérieur** comportant les éléments suivants :

- modalités d'accès en ZRR, notamment pour le personnel permanent, les stagiaires et les prestataires de service ;
- modalités de gestion des visiteurs ;
- présence de locaux sensibles ;
- mesures de contrôle interne (port du badge) ;
- amplitude horaire ;
- circuit de notoriété ;
- règles d'hygiène informatique ;
- compte rendu d'incident à envoyer à l'autorité compétente, à la DRSD et la DPID.

2. Mesures de protection contre l'intrusion informatique

L'établissement doit mettre en œuvre **une politique de sécurité des systèmes d'information** (PSSI) conforme aux exigences fixées par l'instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles[11].

Dans ce cadre, **tout système d'information participant à la protection des zones à régime restrictif** (en particulier ceux relatifs au contrôle d'accès, à la détection d'intrusion et à la vidéosurveillance) et **tout système destiné au traitement, au stockage ou à la transmission des informations relevant du potentiel scientifique et technique de la nation** doivent faire l'objet d'une **homologation de sécurité**[12] avant leur mise en service.

---

[10] Voir le chapitre 6 du titre 2 de la circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.

[11] Instruction interministérielle relative à la protection des systèmes d'information sensibles n°901/SGDSN/ANSSI du 28 janvier 2015.

[12] Article 8 de l'IM 901.

Une attention particulière doit également être portée aux **moyens informatiques mobiles**, tels que les outils de capture audio, les téléphones mobiles ou encore les tablettes. L'introduction ou l'utilisation de ces moyens à l'intérieur d'une ZRR et, *a fortiori*, d'un local sensible doit être soumis à l'autorisation du chef de la ZRR.

3. Mesures de protection propres au local sensible[13]

Les locaux sensibles font l'objet **d'une protection renforcée**, justifiée par l'entreposage de produits ou l'exécution d'activités pouvant induire un risque de prolifération (R3) ou de terrorisme (R4).

Les locaux sensibles sont nécessairement situés dans une ZRR et les mesures de protection, déterminées par le chef de l'établissement, doivent respecter **les normes techniques ministérielles suivantes** :

- les systèmes de contrôle d'accès physique doivent permettre d'assurer **la traçabilité de tous les passages** et de procéder à une authentification du porteur du titre d'accès, avec unicité de passage ;
- les locaux doivent être protégés contre les intrusions physiques par la mise en place **d'une détection périmétrique** avec levée de doute par déplacement d'un agent ou d'un système de vidéosurveillance, de détection volumétrique et de report d'alarme assuré en permanence.

[13] Au sens dans la circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.

Annexe 4

Contrôle d'accès en zone à régime restrictif

1. La formulation des demandes d'accès

Les visiteurs n'ont pas à formuler de demande d'accès en zone à régime restrictif[14]. L'autorisation d'accès est accordée par le chef de la ZRR.

Les personnes devant remplir une demande d'accès[15] sont :

- les stagiaires
- les doctorants
- les personnes nouvellement recrutées ou le cas échéant mutées en interne
- les intérimaires
- les prestataires extérieurs
- les personnes bénéficiant d'une formation professionnelle

Une personne des catégories ci-dessus souhaitant accéder à une ZRR en fait la demande auprès du chef de la zone à régime restrictif. Elle remplit alors **un formulaire de renseignement**[16] et le transmet au chef de la ZRR. Ce dernier vérifie ensuite que le dossier est bien complet[17] et renseigne la partie du formulaire concernant l'établissement et la ZRR. Si besoin, le chef de la ZRR peut transmettre le dossier au responsable de l'unité de recherche ou de production pour que des éléments de contexte, nécessaires à l'analyse de la demande, soient apportés.

Dans le cas où une personne souhaite accéder à plusieurs zones à régime restrictif relevant d'un même établissement, **un seul dossier** est à constituer.

L'officier de sécurité de l'établissement ou à défaut, le chef de la ZRR, transmet la demande d'accès à la DRSD sous format électronique chiffré *via* le système d'information SOPHIA ou par courrier recommandé. Dans ce dernier cas, il joint un CD-ROM ou une clef USB contenant la demande d'accès, non chiffrée.

Les personnes bénéficiant **d'une habilitation au titre de la protection du secret de la défense nationale en cours de validité** et délivrée par les autorités administratives françaises n'ont pas à effectuer de demande d'accès en ZRR. L'attestation d'habilitation tient lieu d'avis ministériel favorable tacite. Pour ces personnes, l'accès à la zone à régime restrictif est soumis à la vérification par le chef de la ZRR du besoin réel d'y accéder, sur présentation du certificat de sécurité.

Les personnes présentes au moment de la création d'une zone à régime restrictif sont également autorisées, par dérogation, à exercer leur activité au sein de cette zone sans constituer de demande d'accès. Cette dérogation n'est valable que pour une durée de six mois[18] à compter de la date de création de la ZRR.

---

[14] Voir le chapitre 6 du titre 2 de la circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.

[15] Art. R413-5-1 du code pénal.

[16] Le formulaire est disponible auprès de l'autorité compétente ou sur le site Internet IXARM.

[17] Seuls les dossiers complets avec les formulaires correctement renseignés permettent l'instruction des demandes d'accès en ZRR.

[18] Le temps de constituer le dossier de demande réglementaire.

Enfin, dans le cas particulier où une personne souhaite pénétrer dans une ZRR afin d'accéder à **des informations et supports classifiés** (ISC), **seule la demande d'habilitation** est à réaliser. La décision tient alors lieu d'autorisation d'accès[19].

2. L'instruction des demandes d'accès

A la réception du dossier de demande d'accès, la DRSD conduit **une enquête administrative pour le renseignement et la sûreté** (EARS)[20] afin de préciser l'opportunité de la demande d'accès à une ZRR ou à un local sensible. Cette enquête est conclue par un avis, dénommé **avis de contrôle élémentaire au titre d'une zone à régime restrictif** qui est transmis à l'autorité compétente *via* SOPHIA. Dans certains cas exceptionnels[21], l'autorité compétente peut recourir à **une demande de traitement accéléré** pour les accès.

Les avis restrictifs et défavorables rendus par la DRSD sont accompagnés **d'une fiche confidentielle**, exposant les motifs justifiant l'avis. Lorsqu'elle est communiquée au format papier, la fiche confidentielle est restituée à la DRSD. Dans l'instruction de certains dossiers, **des demandes complémentaires** peuvent être adressées par l'autorité compétente au service enquêteur afin notamment d'approfondir les questions pouvant survenir à la lecture de la fiche confidentielle.

L'autorité compétente doit ensuite rendre, dans **un délai maximum de deux mois** à compter de la réception du dossier par la DRSD, un avis ministériel, qui peut être de **trois types** :

- avis ministériel favorable ;
- avis ministériel favorable avec réserves ;
- avis ministériel défavorable.

L'avis émis par la DRSD **ne lie pas l'autorité compétente** qui peut rendre un avis ministériel différent, à la suite d'une analyse de risques basée sur les activités et les vulnérabilités, et qui précise, au travers des réserves, des mesures de réduction de risque à mettre en œuvre

L'autorité compétente adresse à la DRSD, *via* SOPHIA, **une copie** de l'avis ministériel qu'elle émet *in fine* au profit de l'établissement dès lors que cet avis est favorable avec réserves ou défavorable.

Les avis ministériels favorables, avec ou sans réserves, ne sont valables que pour l'accès à la ZRR pour laquelle ils ont été prononcés. Lorsqu'une demande d'accès a été faite pour plusieurs ZRR, l'avis ministériel peut être restreint à une ou plusieurs zones. **Les avis ministériels défavorables donnent obligatoirement lieu à un refus d'accès en zone à régime restrictif.**

---

[19] Lorsqu'une demande d'accès en ZRR est réalisée en parallèle d'une demande d'habilitation et qu'il s'avère que l'activité de l'intéressé est liée au besoin d'accéder à des ISC alors la DRSD se réserve le droit de réviser l'avis d'accès à la ZRR.

[20] Conformément à l'article R.114-1 du code de la sécurité intérieure.

[21] Les cas exceptionnels feront l'objet d'un accord entre l'autorité compétente et la DRSD et d'une définition précise.

Les avis ministériels favorables avec réserves peuvent prévoir des sensibilisations :

- **de l'intéressé**, pour lui préciser les vulnérabilités qu'il présente pour sa propre sécurité ou celle de son environnement, dans la limite de ce qui lui est communicable[22] ;
- **du chef de l'établissement** hébergeant la zone à régime restrictif pour l'alerter sur les vulnérabilités de l'intéressé.

Les sensibilisations à conduire auprès de l'intéressé sont réalisées, sauf disposition particulière agréée entre l'autorité compétente et la DRSD, par l'officier de sécurité de l'établissement lorsqu'il y en a un, ou dans le cas contraire par l'antenne locale de la DRSD. L'officier de sécurité peut en cas de besoin, s'appuyer sur l'antenne locale de la DRSD. Ces sensibilisations donnent lieu à **une attestation signée de l'intéressé** reconnaissant la réalisation de celles-ci.

3. Les décisions d'accès

Les décisions d'accès en ZRR sont prises par **l'établissement** hébergeant la zone à régime restrictif. Ces dernières sont limitées à cinq ans et sont renouvelables. Elles sont notifiées par écrit au demandeur et tiennent compte de l'avis ministériel rendu par l'autorité compétente. **L'autorité compétente est informée** dès lors que l'accès est refusé alors que l'avis ministériel est favorable, avec ou sans réserve(s).

Les décisions d'autorisation d'accès peuvent être formulées par courrier ou mail. Les décisions de refus d'accès sont quant-à-elles obligatoirement notifiées par **lettre recommandée avec accusé de réception** ou remises en main propre avec signature du bon de remise par l'intéressé[23].

Les décisions de refus d'accès en ZRR ne sont pas motivées. Elles peuvent faire l'objet de **recours** administratifs, recours gracieux et/ou hiérarchique ou de recours juridictionnels. Le recours administratif est à déposer auprès de l'établissement hébergeant la ZRR et le recours juridictionnel auprès du tribunal administratif relevant du lieu de résidence de l'intéressé[24].

Tout **nouvel élément significatif**[25] concernant les personnes accédant aux ZRR doit être porté à la connaissance de l'autorité compétente qui peut, le cas échéant, exiger le dépôt d'un nouveau dossier de demande d'accès en ZRR.

---

[22] Le chef de l'établissement hébergeant la ZRR peut prendre contact avec l'antenne locale de la DRSD pour connaitre les motifs justifiant la sensibilisation si ceux-ci sont communicables.

[23] Exceptionnellement, elles peuvent être transmises par courrier avec accusé de réception.

[24] Pour les personnes résidant à l'étranger, le recours juridictionnel est à déposer auprès du tribunal administratif de Paris.

[25] Par exemple, le passage du statut de stagiaire à doctorant etc.

4. Contrôle des accès logiques

L'accès aux informations scientifiques et techniques détenues dans une ZRR peut être uniquement virtuel, sous la forme d'un accès à distance par voie électronique[26]. Dans ce cas, tout accès, même distant **doit être autorisé** par le chef d'établissement **après avis ministériel, selon les mêmes modalités que celles prévues pour l'accès physique.**

Tout accès distant constitue une extension du système d'information (SI) protégé en ZRR. Ainsi, si les accès distants sont autorisés, **des mesures de protection logiques** doivent être mises en œuvre.

Les moyens d'accès à distance et les systèmes d'information traitant du potentiel scientifique et technique de la nation doivent, dans ce cadre, respecter les dispositions de **l'instruction interministérielle n°901** et ainsi faire l'objet **d'une homologation de sécurité**.

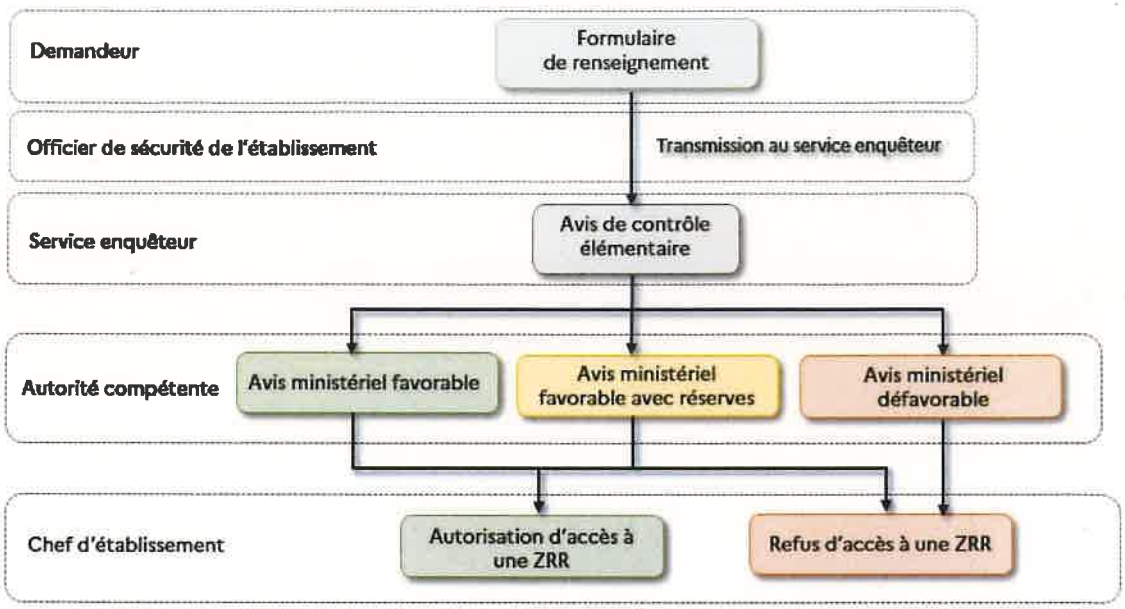
Le télétravail doit être évité car il n'est pas cohérent avec le dispositif de protection physique du potentiel scientifique et technique. Lorsque cela s'avère indispensable, et sous la responsabilité de l'autorité d'homologation, il peut être mis en œuvre dès lors que **les aspects suivants auront été étudiés sans révéler de faille de sécurité** et intégrés dans la démarche et la décision d'homologation de sécurité du SI :

- la séparation des usages : le poste de télétravail traitant du potentiel scientifique et technique doit être à usage unique ;
- la qualité de chiffrement du VPN (*virtual private network*) qui protège la confidentialité de la liaison électronique distante ;
- la qualité de chiffrement du disque interne du poste de télétravail ;
- le maintien en condition de sécurité du système d'information (antivirus, mises à jour du système d'exploitation et des logiciels) ;
- la maîtrise des supports connectés - voire leur interdiction - pour limiter les fuites de données et limiter l'introduction de logiciels malveillants ;
- la remontée des évènements de sécurité locaux du poste sur un serveur ;
- l'interdiction de faire du télétravail dans des lieux publics ;
- la sensibilisation fréquente des usagers quant à l'usage du poste au sein du foyer.

Si le système d'information traitant du potentiel scientifique et technique relève **d'une protection de niveau *Diffusion Restreinte*** (savoirs faire susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs), alors il convient d'utiliser, lorsqu'ils existent, des logiciels de chiffrement et des dispositifs agrées *Diffusion Restreinte* par **l'ANSSI**.

[26] Par exemple, la prestation de service d'infogérance, la réalisation de projet de recherche scientifique mené à distance, le télétravail etc.

Schéma synthétisant le processus de contrôle d'accès



Annexe 5

Visites, contrôles et inspections des zones à régime restrictif et locaux sensibles

1. Les visites d'assistance technique ou d'opportunité

Les visites d'assistance technique ou d'opportunité ont pour finalité d'accompagner le chef de la ZRR dans la mise en place de mesures de protection adaptées ou de s'en assurer. Elles peuvent être conduites par **l'autorité compétente avec le soutien des antennes locales de la DRSD**, qui s'adressent mutuellement la programmation respective des visites qu'elles souhaitent mener afin de permettre **une coordination** entre les deux administrations.

Les ZRR et locaux sensibles dont l'activité a été signalée comme porteuse de risques liés au détournement de technologies conventionnelles susceptibles de renforcer l'arsenal militaire d'un autre pays ou d'affaiblir les capacités de défense de la nation (R2), à la prolifération (R3) et au terrorisme (R4) peuvent faire l'objet **d'une visite d'assistance technique annuelle**.

Une visite d'assistance technique doit faire l'objet **d'un compte-rendu**, si nécessaire classifié au niveau *Secret* [27], portant la mention de protection *Spécial France*, dont une copie est adressée à la DRSD et à l'autorité compétente. Ce compte-rendu peut être **assorti d'un avis** quant à l'opportunité de créer une autre ZRR (ou local sensible) de modifier ou de supprimer une ZRR déjà existante ou **toute autre recommandation**.

La convention établie entre le ministère et l'organisme abritant du potentiel scientifique et technique de la nation, non lié par un contrat avec le ministère, prévoit que les services compétents du ministère des Armées sont autorisés à se rendre dans les locaux de l'organisme afin **de fournir des conseils, d'accompagner et de conseiller** le chef d'établissement ou son officier de sécurité dans la définition de mesures de protection et **de mener des actions de sensibilisation**.

2. Les inspections

La DRSD mène des inspections au sein des ZRR et locaux sensibles des établissements du ministère des Armées, sur saisine du haut fonctionnaire correspondant de défense et de sécurité, de la DPID, de l'autorité compétente ou de sa propre initiative.

Ces inspections portent sur **les moyens mis en œuvre** pour se conformer aux normes de sécurité des ZRR, des locaux sensibles et des réseaux informatiques supportant le potentiel scientifique et technique de la nation. Les éléments de protection physique, l'organisation de la gestion des informations et la réalisation des différents bilans et répertoires de visite peuvent donc faire l'objet d'un contrôle et de recommandations.

Chaque inspection de la DRSD fait l'objet **d'un compte-rendu adressé à l'établissement, à l'autorité compétente et à la DPID**.

---

[27] Dans le cadre des établissements non habilités au secret de la défense nationale, le compte-rendu de visite comporte une partie non classifiée qui peut alors être transmise à l'établissement considéré.

3. Le bilan annuel

La DRSD adresse **une synthèse annuelle** des atteintes au potentiel scientifique et technique de la nation au ministre des Armées, qui détaille notamment les éléments suivants :

- une typologie des atteintes ;
- le nombre d'atteintes par secteur scientifique et technique protégé ;
- une analyse des tendances selon les quatre risques (R1 à R4).

Cette synthèse est adressée à la **DPID et au SGDSN** avec copie aux autorités compétentes responsables des zones à régime restrictif.

4. Les compte-rendu d'incidents

Tout incident (vol, intrusion sans autorisation etc.) au sein d'une ZRR ou lié à la protection du potentiel scientifique et technique de la nation fait l'objet, par l'organisme abritant la ZRR, **d'un traitement adapté et d'une remontée d'informations** auprès de l'autorité compétente, de la DPID (département DAME) et de de l'antenne locale de la DRSD. Le format en sera défini prochainement. Dans l'attente d'un format détaillé, les chefs de zones à régime restrictif adresseront **un compte-rendu complet**, indiquant *a minima* les éléments suivants :

- la date de l'incident (jour, heure) ;
- le type d'incident (vol, intrusion, incendie etc.) ;
- la localisation de l'incident (adresse, local concerné etc.) ;
- une description précise de l'incident ;
- les éventuelles conséquences notamment sur le potentiel scientifique et technique ;
- les mesures prises à la suite de l'incident (administratives, correctives, palliatives, etc.) et celles prévues ;
- tout autre complément utile.

LISTE DE DIFFUSION

DESTINATAIRES :

- DGA
- DAJ
- EMA
- EMAT
- EMM
- EMAAE
- DGSE
- DRSD
- DGRIS
- SSA

COPIES :

- SGDSN, sous-direction non-prolifération, sciences et technologies (PST)
- SGA
- CGA