Rapport d'activité 2012

HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

SOMMAIRE

ÉVOLUTION DES MISSIONS ET DU CONTEXTE

À la fin de l'année 2012 est élaboré un nouveau livre blanc pour la défense et la sécurité nationale. Cinq ans après le précédent, l'évolution des menaces tant dans le monde que sur le territoire national confirme le continuum établi entre la sécurité nationale et la défense nationale, qui a conduit à renforcer le rôle des hauts fonctionnaires de défense et de sécurité placés auprès des ministres pour « animer et coordonner la politique en matière de défense et de sécurité, de vigilance, de prévention de crise et de situation d'urgence et de contrôler la préparation des mesures d'application ».

Depuis 2010, le secrétaire général des ministères de l'éducation nationale (MEN) et de l'enseignement supérieur et de la recherche (MESR) est en charge de cette fonction et s'appuie pour la mener à bien sur deux adjoints respectivement pour l'éducation nationale et pour l'enseignement supérieur et de la recherche. En liaison avec le secrétariat général de la défense et de la sécurité nationale (SGDSN) auprès du Premier ministre, le service du HFDS a intensifié son activité en 2012 dans les objectifs prioritaires suivants :

1. Renforcer la capacité du ministère à prévenir et gérer les crises liées aux risques majeurs (violences et terrorisme, cybermenaces, risques sanitaires, catastrophes naturelles ou industrielles, etc.) compte tenu de ses responsabilités vis-à-vis de la population dont il a la charge et de l'importance de son cycle d'activité dans l'ensemble de la vie économique et sociale. À cet égard, en 2012 une circulaire des deux ministres en charge de l'éducation nationale et de l'enseignement supérieur et de la recherche définit l'organisation des missions de défense et de sécurité et de gestion de crise, en cohérence avec l'organisation générale de l'État face aux crises majeures ;

2. Renforcer la protection du potentiel scientifique et technique de la Nation qui a fait l'objet d'une nouvelle réglementation en 2012 pour mieux contrôler l'accès aux laboratoires sensibles afin de protéger les intérêts fondamentaux de la Nation, en délimitant des « zones à régime restrictif » et en identifiant des secteurs sensibles à protéger. Les modalités de mise en œuvre de ce contrôle sont définies en concertation avec les organismes de recherche et les établissements d'enseignement supérieur, en particulier avec les fonctionnaires de sécurité de défense ;

3. Animer la politique de sécurité des systèmes d'information qui soutiennent les grandes fonctions administratives ainsi que ceux qui se développent dans l'enseignement. Le plan d'action gouvernemental de 2011 et le RGS sont à mettre en œuvre par l'ensemble des ministères en liaison avec l'Agence de sécurité des systèmes d'information (ANSSI). C'est pourquoi le poste de « fonctionnaire de sécurité des systèmes d'information » momentanément vacant a été pourvu sans délai auprès du HFDS à la fin de l'année 2012 afin de planifier la mise en œuvre d'une politique de sécurité du ministère ;

4. Faire appliquer les dispositions relatives à la protection du secret de la défense nationale, notamment en optimisant la carte des habilitations qu'il s'avère nécessaire de délivrer. Tel a été le cas par exemple des 170 autorités de nos ministères qui, ayant accès au réseau sécurisé « Rimbaud », doivent se voir attribuer un téléphone cryptographique « Teorem » en 2012 ;

5. S'assurer des dispositions prises par les opérateurs pour la **protection des points d'importance vitale** dans le cadre des directives nationales de sécurité ;

6. Promouvoir la formation et l'éducation nécessaire en matière de défense et de sécurité, d'une part en direction des cadres et personnels ayant en charge la sécurité des services et des établissements, d'autre part en direction des personnels chargés de l'enseignement des compétences civiques et sociales. Le HFDS facilite la coopération avec l'ensemble des institutions en charge de défense et de sécurité.

PLAN DE DÉFENSE, GESTION DE CRISE ET CONTINUITÉ DES ACTIVITÉS

Organisation ministérielle et interministérielle de la gestion de crise

Les plans gouvernementaux de défense constituent une réponse interministérielle à des risques naturels, technologiques, sanitaires, terroristes ou à des attaques contre les systèmes d'information. Ils constituent un outil d'aide à la décision à partir de l'analyse de la menace, prévoient une répartition des rôles au sein de l'État tant au niveau national que déconcentré, et développent un référentiel commun de mesures planifiées et graduées de protection à mettre en œuvre.

Le plus connu est le plan « Vigipirate » qui a fait l'objet en 2012 de cinq communications par le HFDS sur les postures à adopter en application des décisions du Premier ministre. Ayant établi, à l'attention des chefs de services et d'établissements un document simplifié et adapté au contexte de l'éducation nationale et de l'enseignement supérieur, le HFDS a pu formuler des propositions au SGDSN dans le cadre d'un travail de refonte du plan.

Le service du HFDS s'est attaché à structurer et clarifier l'organisation des missions de défense de sécurité et de gestion de crise à tous les niveaux. Ainsi, une circulaire signée des deux ministres de l'éducation nationale et de l'enseignement supérieur et de la recherche destinée à l'ensemble des services déconcentrés et des établissements, a été publiée le 12 mars 2012, accompagnant la désignation des « recteurs délégués de zone ». Elle est en cohérence avec la circulaire du Premier ministre du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures.

Le service du HFDS a participé à des travaux relatifs à la planification : participation au comité directeur post accident nucléaire (CODIRPA), pour la mise au point d'un document validé qui est disponible sur le site de l'autorité de sûreté nucléaire (ASN)[1] ; élaboration d'une doctrine pour l'évacuation massive de populations, qui s'est traduite par la rédaction d'un document de référence «EVAGLO» qui sera diffusé au

1 Site de l'Autorité de sûreté nucléaire (ASN) : http://www.asn.fr/

niveau territorial courant 2013. Le service a également contribué au travail conduit par le SGDSN, dans le domaine de la professionnalisation des acteurs de la gestion de crise pour les fonctions « situation », « anticipation », et « communication », en tenant compte des expériences et réflexions menées avec ses correspondants des services déconcentrés (académies).

Le service maintient en état une salle de crise disposant des moyens de communication nécessaires, au profit des deux ministères en cas de besoin. Cette salle permet de concentrer l'information et d'être en liaison avec le centre interministériel de crise. Elle nécessite un renfort en personnel pour fonctionner en continu.

Sensibilisation des services déconcentrés, retours d'expérience et communication de crise

Le HFDS a organisé un séminaire relatif à la gestion de crise et aux risques majeurs au profit des directeurs de cabinet et d'autres proches collaborateurs des recteurs. Ce séminaire a permis, avec la participation d'intervenants extérieurs (ministères de l'intérieur, de la défense, collectivités territoriales), de sensibiliser ces cadres à l'organisation de la gestion de crise, au rôle que sont appelés à y jouer les services déconcentrés ainsi qu'aux questions de communication interne et externe et à l'importance des retours d'expérience et de la formation.

Le site collaboratif du HFDS « gestion des risques majeurs » réunit une centaine de correspondants académiques pour la gestion de crise et des risques majeurs. Il a permis, tout au long de l'année, la diffusion d'information en direction des participants au séminaire, amorçant une mutualisation des réflexions et des pratiques, tout en élargissant la liste de diffusion et les thématiques abordées. Les demandes spontanées d'inscription sur le site ont été significatives de l'intérêt de cet outil pour l'animation des acteurs locaux et de l'intérêt porté à cette thématique.

Communication de crise

Lors des exercices de crise, le service est présent, en cas de besoin, à la cellule interministérielle de crise communication, ou en cellule ministérielle de crise. En tant que membre du réseau interministériel des communicants en situation de crise, il a participé aux sessions de professionnalisation de la communication de crise organisées par le SGDSN ainsi qu'aux diverses réunions organisées sur le sujet. Il a participé aux réunions du comité éditorial sur la refonte du portail interministériel « risques majeurs ».

Dans le cadre de la mise au point d'outils de communication, en liaison avec le SGDSN et le service d'information du gouvernement (SIG), le MEN et le MESR ont adhéré au centre de contacts multicanal interministériel «InfoCrise» en signant une convention avec le SIG.
Une étude a été réalisée par le HFDS en lien avec la direction générale de

l'enseignement scolaire et la délégation à la communication, sur les possibilités et les coûts d'une éventuelle utilisation de ce service par le MEN à partir de l'exemple des incidents survenus en 2011 dans le déroulement du baccalauréat.
Les services déconcentrés peuvent également avoir recours au centre « InfoCrise » pour une situation de crise spécifique à l'éducation nationale ou à l'enseignement supérieur et de la recherche à l'échelle régionale. Une présentation de ce dispositif a été faite, en lien avec la délégation à la communication, aux chargés de communication des académies lors du séminaire qui les réunissait en août 2012.

Plan de continuité d'activités

La stratégie de sécurité nationale nécessite que les ministères, parallèlement aux mesures de protection, prévoient des plans de continuité d'activité (PCA), destinés à assurer le maintien des fonctions essentielles en cas de catastrophe ou de situation très dégradée.
Le plan de continuité d'activité (PCA), progressivement élaboré par chaque ministère, doit constituer un document stratégique de planification de la réaction à une menace ou une catastrophe grave pour en minimiser les impacts et assurer le maintien des fonctions essentielles. C'est ainsi que lors de la pandémie grippale en 2009, des plans de continuité ont pu être élaborés aux différents niveaux : central, académique et établissements.

En liaison avec le SGDSN et le comité de contrôle interne pour la maîtrise des risques, le service du HFDS a participé directement à l'élaboration de certains plans :
- afin d'assurer la continuité du travail gouvernemental dans le cas d'une crue centennale de la Seine, un plan a été défini en concertation avec les différentes directions et services concernés pour déterminer les fonctions à maintenir, les effectifs nécessaires et le site de secours. Ce plan devra être soumis aux instances de concertation en 2013 ;
- une réflexion a été menée en 2012 au sein du comité de contrôle interne pour la maîtrise des risques, pour sensibiliser et associer les directions de l'administration centrale des deux ministères à la démarche d'élaboration des plans de continuité pour les fonctions essentielles. L'exposition aux risques a pu notamment être mise en évidence lors des exercices nationaux « Nuit totale » et « Piranet 2012 » portant respectivement sur une rupture électrique et sur une rupture d'internet.

Afin de faciliter cette démarche, un guide méthodologique adapté au contexte de l'éducation nationale et de l'enseignement supérieur et de la recherche, est en cours d'élaboration.

PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DANS LES ÉCHANGES INTERNATIONAUX ET INTELLIGENCE ÉCONOMIQUE

La protection du potentiel scientifique et technique (PPST) vise à sécuriser des connaissances élaborées dans certains laboratoires de recherche en vue de prévenir leur captation et leur détournement à des fins nuisibles à la défense et la sécurité de la France. À cet effet le dispositif PPST s'appuie, en particulier, sur un contrôle des accès à des zones protégées (ZRR) et aux supports informatiques qui peuvent contenir ces connaissances ou les détourner.

Le mode de fonctionnement de la recherche intègre de nombreuses occasions d'échanges qui sont autant de possibilités offertes à ceux qui cherchent à capter indûment ces connaissances.

Ces échanges peuvent revêtir plusieurs formes :

- coopération scientifique et technique élaborée conjointement par une autorité ou un établissement français avec un organisme étranger ou international ;
- séjours de toute durée, effectués en délégation ou à titre individuel dans les organismes et les entreprises du secteur public ou privé ;
- transferts de technologies impliquées par ces coopérations, séjours et visites ;
- accès de résidents étrangers non titularisés à des centres français de recherche scientifique ou des entreprises pour y exercer une activité ;
- activité des français à l'étranger à l'occasion de missions d'ordre économique, scientifique et technologique.

Refonte de la réglementation pour protéger le potentiel scientifique et technique de la Nation

Le cadre juridique dans lequel s'inscrivent les missions de protection du potentiel scientifique et technique (PST) peut être défini à trois niveaux de réglementation, d'abord internationale, puis nationale, interministérielle, et enfin ministérielle.
Concernant le volet international doivent être appliqués les traités et conventions internationales telles que les résolutions du conseil de sécurité de l'organisation des Nations-Unies (ONU) et la position commune 2008/652 PESC du conseil de sécurité européenne contre les pays proliférants.

Au niveau national interministériel, jusqu'en 30 juillet 2012, l'instruction interministérielle 486 relative à la protection du patrimoine scientifique et technique français dans les échanges internationaux régissait ce dispositif portant sur la lutte contre la prolifération, le contrôle des coopérations internationales, le contrôle des visiteurs et stagiaires dans les établissements à régime restrictif (ERR) et les recommandations pour les français en mission à l'étranger.

Le nouveau cadre juridique relatif à la PPST repose désormais sur un décret du Premier ministre en date du 4 novembre 2011, suivi d'un arrêté du Premier ministre du 5 juillet 2012 et d'une circulaire du Premier ministre du 7 novembre 2012.

Ce nouveau dispositif s'adosse au code pénal en créant une nouvelle catégorie de zone protégée, les zones à régime restrictif (ZRR), afin de contrôler l'accès à leur contenu matériel et immatériel.

La mise en œuvre de ce dispositif s'appuie sur trois niveaux :
- le SGDSN en interministériel ;
- le service du HFDS au niveau ministériel ;
- l'établissement, université, organisme de recherche, ou école d'ingénieurs, au niveau local.

Le travail de création des ZRR a été initié et les premiers dossiers ont été adressés au SGDSN.

Coopérations internationales et stratégie nationale de recherche et d'innovation du MESR

Dans les cadres réglementaires énoncés ci-dessus, le service a instruit 3 133 dossiers :
- 104 coopérations scientifiques initiées par des universités ou des organismes de recherche ;
- 1 847 dossiers appartenant à des programmes de coopération initiée par le ministère des affaires étrangères (MAE) et le MESR ;
- 1 182 demandes de stages de master 2, doctorat, post doctorat, au sein des ERR.

Le service HFDS a participé à divers groupes de réflexion et comités de suivi organisés par :
- la DGRI, dans le cadre de la stratégie nationale de recherche et d'innovation (SNRI) ;

- le SGDSN, dans le cadre de travaux interministériels ;
- la DREIC et le service HFDS, en coopération avec la conférence des présidents d'université (CPU), la conférence des grandes écoles (CDEFI), Campus France, et le MAE, pour la réalisation d'un vade-mecum des coopérations internationales.

Actions de sensibilisation et de formation auprès de la communauté scientifique et des fonctionnaires de sécurité de défense

La mise en œuvre du dispositif nécessite de nombreuses actions d'information, de sensibilisation et de formation. À cet effet le service a organisé :

- avec l'agence de mutualisation des universités et établissements (AMUE), un séminaire à destination des personnels ingénieurs, administratifs, techniques, ouvriers et de services (IATOS) et enseignants chercheurs et chercheurs, portant sur la PPST le 30 mars 2012 ;
- avec le cabinet du ministre de l'enseignement supérieur, un séminaire de sensibilisation et d'information sur la PPST à destination de toute la communauté scientifique le 6 avril 2012 ;
- un séminaire à destination des FSD et des RSSI de tous les établissements, le 27 novembre 2012 ;
- un groupe technique de FSD pour préparer les documents ministériels.

Il a participé également à la sensibilisation des conseillers et attachés scientifiques en ambassade lors de la réunion organisée par le ministère des affaires étrangères et européennes le 28 juin 2012.

Lutte contre la prolifération des armes de destruction massive et de leurs vecteurs

Point d'entrée privilégié pour les concertations interministérielles en matière de lutte contre la prolifération des armes de destruction massive (NRBC-E : nucléaire, radiologique, biologique, chimique et explosifs) et de leurs vecteurs (balistique), le service a :

- donné des contributions aux groupes de réflexion sur la mise en œuvre de la convention du 10 avril 1972 sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines et sur leur destruction avec participation aux réunions organisées par le MAE ;
- participé au suivi du master en fusion par confinement inertiel (FCI), décret n° 80-247 relatif aux activités d'études et de recherche dans le domaine de la fusion thermonucléaire par confinement inertiel, avec participation aux réunions d'enseignants du master organisées par le SGDSN.

Autres activités en liaison avec le SGDSN et intelligence économique

Le service a participé à :

- un groupe de travail interministériel sur l'intelligence économique organisé à l'initiative du délégué interministériel à l'intelligence économique (D2IE) ;
- à deux groupes de travail d'accompagnement sécuritaire et de défense de contrats industriels passés avec des pays étrangers, organisés à l'initiative du SGDSN.

SÉCURITÉ DES SYSTÈMES D'INFORMATION

L'année 2012 a été marquée par des attaques informatiques de grande ampleur tant sur les systèmes d'information de l'État que de grandes entreprises. Elles peuvent porter atteinte à la souveraineté des États, au potentiel scientifique et technique, aux données personnelles des citoyens. Dans la poursuite du plan gouvernemental, et sous l'impulsion de l'ANSSI, la montée en puissance du dispositif de défense et de sécurité des systèmes d'information s'est poursuivie. Certaines mesures sont communes à l'ensemble des ministères, d'autres plus spécifiques au MESR, telles que l'insertion de la sécurité des systèmes d'information dans les formations supérieures.

Dans ce contexte et en cohérence avec les démarches interministérielles et nationales, le service du HFDS assure un rôle d'animation et de pilotage de la politique de sécurité des systèmes d'information. Il intervient dans l'organisation de la chaîne de sécurité et participe à une mission de contrôle.

Actions d'animation et de pilotage de la politique de sécurité des systèmes d'information

Le service a participé ou piloté un certain nombre d'actions visant à développer une meilleure sécurité des systèmes d'information dans les deux ministères :

- participation à l'élaboration d'une politique de sécurité des systèmes d'information de l'État (PSSIE) sous la direction de l'ANSSI en collaboration avec les ministères ;
- participation aux travaux de mise en place d'un réseau interministériel de l'État (RIE) créé par arrêté du 17 décembre 2012[2] selon un cahier des charges défini conjointement par tous les acteurs ministériels afin de répondre à un fort besoin de résilience et de sécurité ;
- participation au projet de déploiement de la « carte agent » ;
- participation aux réunions inter-

2. Lien vers l'arrêté du 17 décembre 2012 portant création portant création d'un service à compétence nationale dénommé « Réseau interministériel de l'État ».

ministérielles pilotées par l'ANSSI et aux groupes de travail organisés par le SGDSN, portant sur la protection du patrimoine « informationnel » ;

- participation à la prise en compte de la sécurité des systèmes d'information dans les formations supérieures, en commençant par les formations scientifiques et techniques, afin que l'ensemble des étudiants acquièrent un socle commun de connaissances et de bonnes pratiques en ce domaine. Un conseiller de défense et de sécurité, recruté en 2012 par le HFDS, a pour mission de participer à cette réflexion en lien avec la direction générale pour l'enseignement supérieur et l'insertion professionnelle (DGESIP) ;
- réalisation par un groupe de travail « PSSI des universités » co-animé par le service du HFDS, d'un référentiel d'outils de sensibilisation, de formation et de conduite d'entretien. Ces travaux ont reposé sur une analyse de risques pour l'enseignement supérieur et la recherche. Ils ont été validés par l'ANSSI à la demande du HFDS et ont été présentés à l'ensemble des établissements lors du séminaire national organisé en collaboration avec le réseau des télécommunications pour l'enseignement et la recherche (RENATER) et l'AMUE au premier trimestre 2012 ;
- participation au comité de pilotage des systèmes d'information et au comité directeur du schéma stratégique des systèmes d'information et de télécommunication (S3IT) du MEN et du MESR. Le S3IT 2013 est disponible en ligne[3] . La sécurité numérique a été retenue comme axe stratégique reposant sur un programme en quatre points : actualiser le schéma directeur SSI (SDSSI), se conformer au référentiel général de sécurité (RGS), être en capacité de gérer une crise informatique et sensibiliser, responsabiliser et protéger les utilisateurs ;
- information et validation des candidatures aux formations proposées par le centre de formation à la sécurité des systèmes d'information (CFSSI[4]) ;
- information et sensibilisation sur les enjeux, les menaces, le référentiel général de sécurité (RGS[5]) auprès des directions ministérielles et des RSSI (responsables de la sécurité des systèmes d'information) ; ainsi qu'à la demande d'organismes ou établissements publics : groupe national logiciel de l'enseignement supérieur et de la recherche, l'inspection générale de l'administration de l'éducation nationale (IGAENR), CNRS.

3. Lien vers le S3IT 2013

4. http://www.ssi.gouv.fr/fr/anssi/formation/

5. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/

Interventions de sécurité

Elles ont concerné :

- la coordination du traitement d'incidents avec les différentes entités concernées (CERTA, CERT-RENATER, service de supervision du réseau RENATER, maîtrises d'ouvrage, maîtrises d'œuvre,

autres ministères de tutelle des entités concernées) ;
- les alertes vers les établissements et organismes de recherche concernés par des attaques ciblant des secteurs d'activités sensibles, ou par des vulnérabilités touchant des technologies spécifiques ;
- l'élaboration d'un document d'organisation créant un centre opérationnel de sécurité des systèmes d'information ministériel (COSSIM), en application du retour d'expérience de l'exercice « Piranet 12 », les COSSIM intervenant en liaison avec le centre opérationnel de l'ANSSI dans les situations de crise ou de dysfonctionnements graves au plan national, ces derniers étant rarement circonscrits à un seul département ministériel.

Actions relevant du contrôle

Dans le cadre du contrôle de l'application de la politique de sécurité des systèmes d'information, le service a coordonné des inspections menées par l'ANSSI avec l'IGAENR à la demande du secrétaire général de la défense et de la sécurité nationale, d'un laboratoire de recherche sensible, d'un organisme de recherche opérateur d'importance vitale, d'un système d'information de gestion de ressources humaines du ministère, d'un centre d'hébergement des serveurs du ministère ainsi que d'un cabinet ministériel.

Le service a également contrôlé le déploiement des nouveaux terminaux téléphoniques chiffrants du réseau de l'État « Rimbaud-Teorem » à usage des autorités ministérielles habilitées. 170 terminaux « Teorem » ont ainsi été déployés à l'administration centrale du MEN-MESR et dans les services académiques.

Réseau des RSSI et des experts

Les responsables de la sécurité des systèmes d'information (RSSI), désignés par leur autorité qualifiée de la sécurité des systèmes d'informations (AQSSI), sont les interlocuteurs directs du fonctionnaire de sécurité des systèmes d'information (FSSI) au sein du service du HFDS.

Ce réseau des RSSI de l'enseignement supérieur continue de s'élargir avec, entre autres, les désignations de RSSI dans les CROUS, à l'initiative du CNOUS, suite à la sollicitation du HFDS ainsi que du directeur de RENATER.

Le service du HFDS veille à l'articulation des réseaux SSI au niveau interministériel et notamment au niveau zonal en relayant les informations des observatoires zonaux de la sécurité des systèmes d'information (OZSSI) mis en place en 2009 auprès des préfets de zone.

Les RSSI interviennent au côté des FSD dans la mise en œuvre de la protection du potentiel scientifique et technique.

PROTECTION DU SECRET

La mission de protection du secret de la défense nationale (PSDN) est confiée au fonctionnaire de sécurité de défense (FSD) rattaché au service du HFDS.
En 2012, elle a concerné le traitement des dossiers de demande d'habilitation, l'enquête sur les lieux abritant des éléments couverts par le secret de la défense nationale, les dossiers transversaux suivis particulièrement au titre de la PSDN.

Traitement des dossiers de demande d'habilitation

Il se fait en liaison avec les FSD des organismes de recherche, des universités, des écoles d'ingénieurs, et les directions de l'administration centrale du MEN et du MESR d'une part, avec la direction centrale du renseignement intérieur (DCRI) ou le SGDSN d'autre part.

Le nombre de dossiers est habituellement reconductible d'une année sur l'autre mais en 2012, le déploiement des téléphones « Teorem » dans les académies a conduit à mettre en adéquation le catalogue des emplois et les habilitations des titulaires.

Le catalogue des emplois

Le catalogue des emplois, mis à jour en 2010, a généré de nouvelles habilitations dans les structures qui étaient en retard, sans créer pour autant d'engorgement dans le service.

L'attribution des téléphones chiffrants « Teorem » a entraîné également une évolution et un renouvellement des habilitations des personnels concernés. Au total, sur 450 habilitations ou renouvellements d'habilitation instruits en 2012, la quasi totalité l'ont été dans le cadre du catalogue des emplois.

Ce catalogue respecte l'objectif national de ne pas augmenter le nombre des personnes habilitées. L'augmentation des consultations des services spécialisés (DCRI) constatée depuis fin 2011, est liée principalement aux fonctionnaires titulaires qui font l'objet d'une procédure automatique et aux contrôles élémentaires liés à l'opération «Teorem».

Les délais, incluant la durée de traitement des dossiers par la direction centrale du renseignement intérieur (DCRI) sont variables, allant de six mois environ pour une habilitation au niveau « secret défense » (SD), à trois semaines ou trois mois pour le niveau « confidentiel défense » (CD).

Les procédures des habilitations

Après la refonte complète du dispositif et la publication de l'arrêté du 30 novembre 2011, le texte et ses annexes ont été analysés pour en formaliser l'application. Ce travail a été préparé au sein d'un groupe de travail de FSD qui s'est réuni plusieurs fois en quelques mois.

En lien avec le groupe des FSD, des logigrammes et des procédures ont été définies par le service du HFDS, afin de permettre ensuite la mise en place d'une procédure dématérialisée destinée aux gestionnaires des dossiers d'habilitation. Cette phase s'est inscrite également dans la procédure interministérielle de la dématérialisation des habilitations prévue début 2013 pour le MEN et le MESR.

Lieux abritant des éléments couverts par le secret de la défense nationale

L'enquête commencée en 2010 sur les lieux abritant des éléments couverts par le secret de la défense nationale a été poursuivie en 2012.

Cette enquête a confirmé la nécessaire prise de conscience des responsables d'établissements en matière de protection d'informations sensibles et classifiées.

Les fiches de procédures concernant les perquisitions aux établissements concernés leur ont été renvoyées, en raison de fréquents changements concernant les titulaires des fonctions liées à la sécurité et à la sûreté.

Les échanges dans ce domaine ont donné lieu à la rédaction de 1 200 courriers, décisions, notes, etc.

Pour cette mission, le HFDS continue de s'appuyer sur le réseau des FSD. L'animation de celui-ci repose sur l'établissement de relations suivies, sur l'aide fournie à chacun dès qu'il en exprime le besoin, et sur leur participation à l'élaboration des règles de fonctionnement mutuel.

Les FSD des universités ont depuis deux ans une meilleure connaissance des documents classifiés dans leurs établissements.

Dossiers transversaux suivis particulièrement par le service pour la protection du secret de la défense nationale

Le service suit le dossier ITER (international thermonuclear experimental reactor), traité en groupe de pilotage interministériel au secrétariat général des affaires européennes (SGAE), mais c'est bien le service du HFDS pour le MESR qui est chargé de suivre les implications et la mise en œuvre de l'IGI 1300 et du code de la défense sur la PSDN concernant la recherche.

La direction générale de la recherche et de l'innovation (DGRI) du MESR suit, avec le service du HFDS, les questions techniques scientifiques relevant de sa compétence.

Une visite technique de certains locaux du CNRS a été effectuée en collaboration avec les FSD du CNRS et du service du HFDS et la participation d'agents de la DCRI, à la demande du service du HFDS, afin de déterminer les conditions d'une éventuelle zone protégée.

Un nouvel agent est venu renforcer le service pour procéder à l'inventaire exhaustif des documents classifiés « CD » et « SD » conformément à l'article 51 de l'IGI 1300. Il s'occupe aussi de l'enregistrement et du départ des nouveaux documents classifiés.

SECTEURS D'ACTIVITÉ D'IMPORTANCE VITALE

Le code de la défense renforce la protection des installations d'importance vitale. En application de ces dispositions, plusieurs opérateurs dépendant du ministère de l'enseignement supérieur et de la recherche antérieurement à 2012 ont établi des plans de sécurité d'opérateur (PSO) au regard des directives nationales de sécurité du MESR et du ministère des affaires sociales et de la santé. Des analyses de risques en 2012 ont été mises au point site par site afin d'affiner les hypothèses et les solutions à prévoir en matière de défense et de sécurité.

L'instruction générale interministérielle n° 6600/SGDSN/PSE/PPS du 26 septembre 2008 relative à la sécurité des activités d'importance vitale, a permis la notification de nouveaux points d'importance vitale (PIV). En cours de mise à jour, la nouvelle version pourra tenir compte des retours d'expérience des divers projets aboutis et validés.
De nouveaux plans particuliers de protection (PPP) ont été finalisés en liaison avec les préfectures et le décret n° 2012-491 du 16 avril 2012 relatif à l'accès aux points d'importance vitale a été notifié aux opérateurs concernés.

ESPACE

L'espace représente un enjeu stratégique majeur pour la France, à la fois en tant que vecteur d'indépendance nationale, et en raison de son impact économique considérable. C'est bien sûr une priorité très forte du service HFDS du ministère de l'enseignement supérieur et de la recherche.

Son activité s'exerce dans quatre directions :

- maîtrise de la sécurité des sites et installations implantées sur le territoire national et participant au domaine spatial français et européen ;
- maîtrise des informations sensibles liées aux activités des opérateurs français ;
- maîtrise des risques liés aux exportations de matériels et de technologies ;
- maîtrise des dispositions de sécurité accompagnant les grands projets.

Les activités remarquables pour 2012 ont été, principalement de :

- poursuivre le processus d'homologation des installations sol du projet Galileo ;
- mettre à jour la directive nationale de sécurité (DNS) Espace ;
- poursuivre le processus de désignation des opérateurs d'importance vitale et points d'importance vitale (OIV/PIV) pour les installations sol Galileo, notamment pour le Galiléo security management center (GSMC) ;
- présider les commissions d'homologation du projet pléiades « Haute résolution » et émettre un intermediate authorization to operate (IATO) système ;
- représenter le MESR aux réunions mensuelles de la Commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG) ;
- représenter le MESR aux réunions mensuelles de la Commission interministérielle des biens à double usage (CIBDU).

FORMATION EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Le HFDS coordonne des actions de formation et d'éducation en matière de défense et de sécurité, d'une part en direction des cadres et personnels ayant à mettre en œuvre les plans de défense pour la sécurité des personnes et des établissements, d'autre part en direction des personnels chargés de l'enseignement des compétences civiques et sociales. Le HFDS facilite à cette fin la coopération avec l'ensemble des institutions en charge de défense et de sécurité.

L'enseignement des questions de défense et de sécurité est prévu par le code de l'éducation (article L312-12). La loi de modernisation de la sécurité civile de 2004 l'élargit en prévoyant une formation aux risques et un apprentissage des gestes de premiers secours (article L313-1).

Enseignements et formations doivent par conséquent se traduire par des connaissances, attitudes et compétences indispensables tant pour assurer la sécurité des établissements que pour l'éducation des jeunes. L'éducation à la défense et à la sécurité, réaffirmé dans les protocoles défense-éducation nationale successifs, concerne également l'enseignement supérieur depuis 2007.

En 2012, une attention est portée à l'importance de former la communauté de l'enseignement supérieur et de la recherche aux problématiques de défense et de sécurité. La nouvelle réglementation sur la PPST implique que des efforts de sensibilisation auprès des chercheurs soient entrepris. Aussi le service du HFDS s'attache-t-il à mobiliser le concours de partenaires extérieurs en charge de la défense et de la sécurité pour développer les activités de sensibilisation, d'éducation et de formation auprès de ces différents publics.

Formation des cadres et personnels responsables de dispositifs de défense et de sécurité

Le service du HFDS est chargé d'instruire les candidatures aux sessions régionales et nationales de l'institut des hautes études de la défense nationale

(IHEDN). Il participe au jury de sélection de la session nationale de l'IHEDN.

Il participe au comité de pilotage de l'école supérieure de l'éducation nationale et de l'institut national des hautes études de la sécurité et de la justice (ESEN/INHESJ) sur la formation des équipes mobiles de sécurité.

Il a permis la participation d'enseignants au séminaire « Cohésion nationale et citoyenneté » de Paris.

En collaboration avec l'AMUE, le service a organisé deux journées de formation sur : « Les enjeux de la sécurité dans les établissements d'enseignement supérieur », en mars et novembre 2012, à destination des présidents, vice-présidents d'université, directeurs d'établissements d'enseignement supérieur et de recherche, directeurs généraux des services et directeurs des systèmes d'information (150 participants au total).

Un séminaire de deux jours a été organisé, en collaboration avec l'AMUE et l'IHEDN, les 4 et 5 décembre à l'école militaire sur : « La mission de défense et de sécurité dans les établissements d'enseignement et de recherche ». Le public visé était le même que pour les journées de formation à la SSI.

Il instruit les candidatures aux formations proposées par le CFSSI.

En collaboration avec la DCRI et avec l'association nationale des jeunes auditeurs de l'IHEDN, il a co-organisé des conférences sur la cybersécurité auprès d'étudiants de l'université Panthéon-Assas Paris II, de l'institut d'études politiques de Paris et du centre de formation en alternance (CFA) Stephenson (Paris 18e) : 500 étudiants ont été sensibilisés.

Soutien à l'enseignement de la défense et de la sécurité

Le service du HFDS siège à la commission esprit de défense. Il a aidé à l'organisation de la journée nationale annuelle des trinômes académiques du 23 mars 2012, en lien avec le délégué pour l'enseignement de la défense auprès de la direction générale de l'enseignement scolaire du MEN et la direction de la mémoire, du patrimoine et des archives du ministère de la défense. La journée était consacrée à : l'« utilisation des ressources audiovisuelles pour développer les formations à la défense », avec visite des différents ateliers de l'établissement de communication et de production audiovisuelle de la défense (ECPAD). Plus généralement, il soutient l'activité des trinômes académiques : animation du trinôme de Paris, intervention au colloque interrégional de Bordeaux, soutien à la journée défense du trinôme de l'académie de Lille.

Il a participé aux travaux de la commission armée-jeunesse (CAJ) au sein de laquelle le HFDS désigne des représentants du MEN et du MESR et a participé au séminaire : « Décider pour réussir officiers et jeunes cadres ».

Il a été co-rapporteur du séminaire 2013 de la CAJ : « Comment développer la résilience avant 12 ans ? ».

Il a participe au comité de pilotage de la journée des réservistes 2012 au conseil supérieur de la réserve militaire.

Aide au développement des compétences sociales et civiques

Le service du HFDS participe au comité de pilotage interministériel, animé par la direction générale de l'enseignement scolaire (DGESCO), pour l'éducation à la responsabilité face aux risques (éducation nationale, intérieur, santé).

Dans le cadre du plan ministériel de l'égalité des chances, il suit l'expérimentation des cadets de la défense dans les académies de Guyane, Lille, Martinique, Nancy-Metz, Nantes, Nice, Poitiers, Rennes, Rouen.

Il se charge de la promotion des prix « armées-jeunesse » et « Trophée du Cidan » dont il participe aux jurys, ainsi qu'au prix de l'association des villes-marraines.

OBJECTIFS 2013

Protection du potentiel scientifique et technique

Dotée d'un nouveau support de textes officiels, cette protection a pris un tournant décisif à l'été 2012. Un travail important doit être mené avec rigueur et opiniâtreté pour implanter ce nouveau dispositif dans les unités de recherche concernées.
Ce travail en profondeur implique des actions coordonnées par le service en liaison avec les fonctionnaires de sécurité de défense (FSD) des organismes de recherche et des universités. Un important et long travail d'information et de concertation avec chaque unité de recherche est nécessaire pour définir le tracé et le fonctionnement adapté de la zone à régime restrictif (ZRR). La création de ces zones est l'étape indispensable et prioritaire de cette année.

Sécurité des systèmes d'information

L'objectif premier est de finaliser la politique de sécurité des systèmes d'information (PSSI) en cohérence avec le contexte interministériel (PSSIE, RGS, RIE). Elle s'articulera autour de priorités partagées avec les responsables des services techniques informatiques et les grandes directions maîtres d'ouvrage.

La mise en conformité du SI existant avec le RGS reste en 2013 une tâche prioritaire qui est à mener en parallèle des projets nouveaux. Seule l'action convergente des grands acteurs (CEPSI, STSI, AMUE, MOA, RSSI), sous l'autorité de l'AQSSI, peut permettre d'atteindre cet objectif.

Le service du HFDS veillera aux moyens de communication sécurisés au niveau interministériel et zonal et relaiera les informations des OZSSI (observatoires zonaux de la sécurité des systèmes d'information) mis en place en 2009 auprès des préfets de zone.

Le FSSI s'attachera aussi à développer la fonction RETEX (analyse des incidents et diffusion des enseignements) des ministères en s'appuyant sur le réseau des RSSI.

Plans de défense, gestion de crise et continuité des activités

Les exercices nationaux programmés en 2013 par le SGDSN (SECNUC, SEISME…) seront l'occasion d'associer les services académiques et permettront de renforcer ainsi la perception de l'organisation et de la dynamique de gestion de crise. Ils permettront également de développer les plans de continuité des activités essentielles qu'il convient d'anticiper.

Le service s'investira, en s'appuyant sur les travaux de la mission du contrôle interne, dans le plan de continuité du processus de gestion des examens du baccalauréat et du BTS.

Une fois élaboré il constituera un exemple de bonne pratique utilisable vers d'autres fonctions essentielles, et sera la base de réflexion pour définir un plan de continuité global pour les services de l'administration centrale.

Espace

Dans ce domaine, outre la participation aux travaux récurrents pilotés par le SGDSN ou le MAE, le service s'attachera à :

- poursuivre le processus de désignation des opérateurs d'importance vitale (OIV) et des points d'importance vitale (PIV) pour les installations sol Galileo, au titre de la DNS Espace ;
- suivre l'évolution des PIV ;
- finaliser l'homologation du système Pléïades.

Formation en matière de défense et de sécurité

L'année 2013 visera à :

- resserrer la coopération avec les grandes directions générales des deux ministères pour la formation des cadres et des personnels ;
- développer des actions avec les instituts et associations en charge de défense et de sécurité (par exemple le Conseil supérieur de la formation et de la recherche stratégique auquel le MEN a décidé d'adhérer) ;
- entretenir et développer les partenariats avec l'AMUE et soutenir les différents établissements dans leurs actions de sensibilisation.

Le HFDS s'attachera à développer des relations de confiance, à la recherche permanente d'une meilleure efficacité, avec ses correspondants :

- fonctionnaires de sécurité de défense (FSD) des établissements d'enseignement supérieur et de recherche et des organismes de recherche ;
- responsables de la sécurité des systèmes d'information (RSSI) des services académiques et des établissements ;
- correspondants pour la gestion de crise et des risques majeurs auprès des recteurs d'académie.

LISTE DES ABRÉVIATIONS

AMUE
agence de mutualisation des universités et établissements

ANS
autorité de sûreté nucléaire

ANSSI
agence nationale pour la sécurité des systèmes d'information

AQSSI
autorités qualifiées pour la sécurité des systèmes d'information

CEA
commissariat à l'énergie atomique

CAJ
commission armées-jeunesse

CD
confidentiel défense

CDEFI
conférence des directeurs d'écoles françaises d'ingénieurs

CERTA
centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques

CODIRPA
comité directeur post accident nucléaire

CFSSI
centre de formation à la sécurité des systèmes d'information

CIBDU
commission interministérielle des biens à double usage

CIEEMG
commission interministérielle pour l'étude des exportations de matériels de guerre

CFA
centre de formation des apprentis

CNES
centre national d'études spatiales

CNRS
centre nationale de recherche scientifique

CNOUS
centre national des œuvres universitaires et scolaires

COSSIM
centre opérationnel de sécurité des systèmes d'information ministériels

CPU
conférence des présidents d'université

CROUS
centre régional des œuvres universitaires et scolaires

DCRI
direction centrale du renseignement intérieur

DGESCO
direction générale de l'enseignement scolaire

DREIC
direction des relations européennes et internationales et de la coopération

DNS
directive nationale de sécurité

DGRI
direction générale de la recherche et de l'innovation

ECPAD
établissement de communication et de production audiovisuelle de la défense

ERR
établissement à régime restrictif

ESEN
école supérieure de l'éducation nationale

FSD
fonctionnaire de sécurité de défense

FSSI
fonctionnaire de sécurité des systèmes d'information

GSMC
Galiléo security management center

HFDS
haut fonctionnaire de défense et de sécurité

IATOS
personnels ingénieurs, administratifs, techniques, ouvriers et de service

IGAENR
inspection générale de l'administration de l'éducation nationale et de la recherche

IATO
intermediate authorization to operate

IHEDN
institut des hautes études de la défense nationale

INHESJ
institut national des hautes études de la sécurité et de la justice

INSERM
institut national de la santé et de la recherche médicale

IN2P3
institut national de physique nucléaire et de physique des particules

ITER
international thermonuclear experimental reactor

MAE
ministère des affaires étrangères

MEN
ministère de l'éducation nationale

MESR
ministère de l'enseignement supérieur et de la recherche

NRBC-E
nucléaire, radiologique, biologique, chimique et explosifs

OIV
opérateur d'importance vitale

OZSSI
observatoires zonaux de la sécurité des systèmes d'information

PCA
plan de continuité d'activité

PIV
point d'importance vitale

PPMS
plans particuliers de mise en sûreté

PPP
plan particulier de protection

PPST
protection du potentiel scientifique et technique

PSDN
protection du secret de la défense nationale

PSO
plan opérateur sécurité

PSSI
politique de sécurité des systèmes d'information

PSSIE
politique de sécurité des systèmes d'information de l'État

PST
potentiel scientifique et technique

RENATER
réseau national des télécommunications pour l'enseignement et la recherche

RIE
réseau interministériel de l'État

RGS
référentiel général de sécurité

RSSI
responsable de la sécurité des systèmes d'information

SAIV
secteur d'activité d'importance vitale

SD
secret défense

SGAE
secrétariat général des affaires européennes

SIG
service d'information du gouvernement

S3IT
schéma stratégique des systèmes d'information et de télécommunication

SGDSN
secrétariat général de la défense et de la sécurité nationale

SNRI
stratégie nationale de recherche et d'innovation

ZRR
zone à régime restrictif

HAUT FONCTIONNAIRE
DE DÉFENSE
ET DE SÉCURITÉ

- Ministère de l'éducation nationale
- Ministère de l'enseignement supérieur et de la recherche

99, rue de Grenelle 75357 Paris SP 07

Tél : 01 55 55 87 00
Fax : 01 55 55 85 87

hfds@education.gouv.fr
hfds@recherche.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE