

BULLETIN OFFICIEL DES ARMÉES



Édition Chronologique n° 81 du 21 mai 2019

TEXTE RÉGLEMENTAIRE PERMANENT

Texte 1

INSTRUCTION N° 3696/ARM/EMA/PERF/REG

portant organisation du centre d'analyse en lutte informatique défensive.

Du 25 avril 2019

INSTRUCTION N° 3696/ARM/EMA/PERF/REG portant organisation du centre d'analyse en lutte informatique défensive.

Du 25 avril 2019

NOR A R M E 1 9 5 3 8 4 3 J

Référence(s) :

- [Code du 22 mai 2019 de la défense \(Dernière modification le 1er janvier 2019\)](#)
- [Arrêté du 20 mars 2015 portant organisation de l'état-major des armées et fixant la liste des commandements, services et organismes relevant du chef d'état-major des armées ou de l'état-major des armées.](#)
- [Arrêté du 27 juillet 2016 fixant la liste des formations administratives relevant du chef d'état-major des armées.](#)
- [Instruction N° 600/ARM/EMA/ESMG/CDA du 24 octobre 2017 relative à l'organisation et au fonctionnement de l'état-major des armées.](#)
- [Instruction N° 101000/ARM/CAB du 24 décembre 2018 relative à la politique de lutte informatique et défensive du ministère des armées.](#)
- [Décision 208/ARM/EMA/PERF/REG du 20 juillet 2018 portant création de l'organisme interarmées « centre d'analyse en lutte informatique défensive ».](#)

Classement dans l'édition méthodique :

BOEM [110.3.5.5.1](#).

Référence de publication :

BOC n°81 du 21/5/2019

Préambule

La présente instruction a pour objet de préciser les missions du centre d'analyse en lutte informatique défensive (CALID) ainsi que son organisation et son fonctionnement.

Le CALID a été créé en tant qu'organisme interarmées (OIA) par la [décision n° 208/ARM/EMA/PERF/REG/NP du 20 juillet 2018](#).

1. MISSIONS

Le CALID est responsable du volet spécialisé et de l'expertise opérationnelle de cyberdéfense. Il est le centre de surveillance, de détection et d'alerte du ministère des armées en la matière.

Il fournit la première capacité d'intervention et d'analyse des événements de lutte informatique défensive.

2. RATTACHEMENT ET SUBORDINATION

Conformément à la [décision n° 208/ARM/EMA/PERF/REG/NP du 20 juillet 2018](#), le CALID est un organisme interarmées constitué en formation administrative au sens de l'article R. 3211-1 du code de la défense.

Le CALID relève organiquement de l'officier général « commandant de la cyberdéfense » (OG COMCYBER). Cette autorité organique est déléguée au chef de l'état-major de la cyberdéfense conformément à l'[instruction n° 600/ARM/EMA/ESMG/CDA relative à l'organisation et au fonctionnement de l'état-major des armées du 24 octobre 2017](#).

3. DIRECTION ET ORGANISATION INTERNE

Le CALID est commandé par un officier supérieur qui reçoit l'appellation de « commandant du CALID ». Il dispose d'un adjoint qui le supplée en cas d'absence ou d'empêchement, et à qui il peut déléguer certaines de ses responsabilités ou attributions.

Le commandant du CALID exerce la responsabilité de commandant de formation administrative.

Le CALID se situe administrativement sur les sites de Paris et Rennes. Il se compose de la manière suivante :

- d'un pôle « commandement » ;
- d'un bureau « performance et activité » ;
- d'un état-major opérations ;
- d'un pôle « cybersurveillance » ;
- d'un pôle « capacités et investigations numériques » ;
- d'un pôle « anticipation ».

Le pôle « commandement » assiste le chef du CALID et son adjoint dans les domaines RH/chancellerie et soutien.

Le bureau « performance et activité » appuie le commandement dans la montée en puissance du CALID et le pilotage interne à l'unité. Il met en œuvre le contrôle de gestion, le contrôle interne et s'assure de la cohérence au sein du CALID en termes capacitaire (RH, processus, outils).

L'état-major opérations, situé à Paris, est responsable de la planification et de la conduite des opérations de cyberdéfense au niveau tactique. Il coordonne des actions spécialisées visant à faire face à un incident ou une attaque informatique conformément aux ordres reçus du COMCYBER. Il a aussi en charge les actions de

préparation opérationnelle du CALID et de sa participation aux exercices de la chaîne CYBER.

Le pôle « cybersurveillance » assure une surveillance des réseaux du ministère de la défense et la détection des attaques informatiques remontées par les capteurs et outils spécialisés. À ce titre, il est, via la « cellule H24 », le point focal du recueil des alertes de cybersécurité émises au sein du ministère. Il est aussi chargée de l'appui à la montée en puissance des *security operation centers*⁽¹⁾ (SOC) des armées, direction et services du ministère de la défense et de l'orientation des stratégies de surveillance et de détection du ministère de la défense.

Le pôle « capacités et investigations numériques » est en charge de réaliser les analyses expertes permettant de comprendre et caractériser une attaque informatique, ainsi que de proposer des actions de remédiation nécessaire. Il soutient par ailleurs les réseaux « métier » du CALID, notamment le réseau d'investigations numériques du CALID, et œuvre à fournir à l'ensemble des divisions les solutions technologiques leur permettant de réaliser leur mission.

Le pôle « anticipation » est en charge de l'appréciation continue de la menace, ainsi que de la capitalisation des indices de compromission liés aux menaces et permettant la caractérisation des attaques, qu'il est aussi chargé de partager avec les SOC du ministère et les partenaires identifiés par le COMCYBER.

4. RESSOURCES HUMAINES

4.1. Effectifs.

Le CALID regroupe les militaires d'active et de réserve ainsi que du personnel civil de la défense.

Le référentiel en organisation (REO), mis à jour annuellement par les unités sous tutelle du COMCYBER et décrit sur le système d'information ressources humaines (SIRH) par le bureau organisation de l'état-major des armées (EMA/B.ORG), précise la répartition des effectifs au sein de la formation.

En application des décisions de l'état-major des armées (EMA), les directions des ressources humaines de chaque armée sont chargées d'honorer quantitativement et qualitativement les postes décrits au REO.

4.2. Administration.

Le personnel militaire du CALID est administré selon les règles en vigueur dans leur armée ou service d'origine :

- par le groupement de soutien de la base de défense (GSBdD) de Saint-Germain-en-Laye pour l'armée de terre affecté à Paris ;
- par le GSBdD de l'École militaire pour le personnel de la Marine et de l'armée de l'air affecté à Paris ;
- par le GSBdD de Rennes pour le personnel de l'armée de terre et de l'armée de l'air affecté sur Rennes ;
- par le GSBdD de Lorient pour le personnel de la Marine affecté sur Rennes.

Le personnel civil du CALID est géré par le centre ministériel de gestion (CMG) de Rennes.

Le bureau personnel civil de l'état-major des armées agit en qualité d'autorité locale d'emploi et d'autorité centrale d'emploi en direction du personnel civil du CALID.

Pour le personnel militaire, le commandant du CALID propose les postes éligibles à la nouvelle bonification indiciaire (NBI) à l'EMA et en décide la répartition finale.

S'agissant du personnel civil, le commandant du CALID fait part de ses propositions de postes éligibles à la NBI au bureau personnel civil. Ce bureau, en fonction de l'enveloppe constante de points, procède aux arbitrages nécessaires.

4.3. Discipline et notation.

En tant que commandant de formation administrative, le commandant du CALID prend part aux travaux d'avancement pour tout le personnel, quelle que soit la catégorie, conformément aux directives particulières.

L'exercice des pouvoirs disciplinaires au sein du CALID est déterminé par l'[arrêté fixant au sein des organismes qui relèvent du chef d'état-major des armées, la liste des autorités militaires de premier niveau et des autorités militaires de deuxième niveau du 10 février 2017](#).

La discipline à l'égard du personnel civil est régie par les dispositions des articles 66 et 67 de la [loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'État](#).

Elles sont complétées, selon le statut, par les textes suivants :

- le [décret n° 84-961 du 24 octobre 1984 modifié relatif à la procédure disciplinaire concernant les fonctionnaires de l'État](#) ;
- les articles 43 à 44 du [décret n° 86-83 du 17 janvier 1986 modifié relatif aux dispositions générales applicables aux agents contractuels de l'État pris pour l'application de l'article 7 de la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'État](#) ;
- le [décret n°87-1008 du 17 décembre 1987 modifié fixant le régime disciplinaire du personnel à statut ouvrier du ministère de la défense](#).

La notation des militaires (active et réserve) et civils affectés au CALID est réalisée selon les prescriptions des directives annuelles élaborées par les chefs d'état-major d'armée, les directeurs de service et par le directeur des ressources humaines du ministère de la défense.

Le commandant du CALID est noté en premier ressort par le chef d'état-major de l'EMCYBER et en deuxième ressort par l'OG COMCYBER.

Les autres personnels militaires officiers affectés au CALID sont notés en premier ressort par le commandant du CALID et en deuxième ressort par le chef d'état-major de l'EMCYBER.

Le personnel militaire non officier affecté au CALID est noté en premier ressort par les chefs de pôles, et en deuxième ressort par le commandant du CALID.

Le personnel civil du CALID est noté en premier ressort par le supérieur hiérarchique direct (SHD) et en dernier ressort par l'autorité hiérarchique placée immédiatement au-dessus du SHD.

4.4. Vie courante, concertation et dialogue social.

En dehors de la cellule situation CYBER assurant la permanence opérationnelle H24 du CALID, le personnel travaille en heures ouvrables, adaptables selon un rythme lié aux opérations.

En heures non ouvrables, une partie du personnel assure les astreintes permettant de tenir le contrat opérationnel fixé par le COMCYBER.

Le commandement du CALID est chargé d'instaurer un dialogue interne et les échanges d'informations avec les armées, conformément aux textes en vigueur, notamment [l'instruction N° 3394/DEF/SGA/DRH-MD/SDFM relative à la désignation des membres des instances de représentation du personnel militaire et des membres des commissions participatives locales du 23 septembre 2016 relative à la désignation des membres des instances de représentation du personnel militaire et des membres des commissions participatives locales.](#)

Il adresse un rapport sur le moral au chef d'état-major de la cyberdéfense, ainsi qu'un rapport de fin de commandement à la même autorité.

5. SOUTIEN

5.1. Base de défense de rattachement et organismes de soutien.

L'administration générale et le soutien commun (AGSC) du CALID sont exercés par le GSBdD de l'École militaire et le GSBdD de Rennes.

5.2. Budgets et finances.

Le CALID adresse au COMCYBER ses prévisions de besoin pour l'année à venir dans le cadre de l'élaboration de l'UO CYBER du BOP 0178-0061 « Environnement opérationnel interarmées ». Le COMCYBER arbitre les expressions de besoin préparées par le CALID et s'assure de l'engagement des dépenses.

5.3. Infrastructure.

À Paris le CALID occupe une partie de la Tour Mercure conformément à la convention financière relative à l'occupation de la Tour Mercure par le CALID.

5.4. Gestion logistique des biens.

5.4.1. Généralités-règles de gestion logistique des biens.

La base de défense (BdD) de rattachement (le service parisien d'administration centrale (SPAC) pour l'Île-de-France) pourvoit le CALID en matériels nécessaires à son fonctionnement et assure leur maintenance.

La gestion logistique des biens est assurée par les services de soutien locaux.

5.4.2. Matériel et services informatiques.

Le renouvellement du parc informatique bureautique du CALID est de la responsabilité de la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI), financé sur le budget opérationnel de programme (BOP) DIRISI. Les augmentations du parc et les moyens informatiques « métier » (matériels et logiciels) nécessaires aux missions du CALID sont financés par son budget métier (cf. point 6.2.).

Le soutien informatique est assuré par la DIRISI. Les modalités sont à définir dans des contrats de services à établir avec les DIRISI locales de rattachement, en liaison avec le gestionnaire de compte en DIRISI centrale.

5.4.3. Téléphonie mobile.

La téléphonie mobile d'usage courant en métropole (mobiles, abonnements, paiement des communications) est réalisée pour le CALID par le GSBdD de rattachement (le SPAC pour l'Île-de-France).

6. PRÉVENTION, MAÎTRISE DES RISQUES ET ENVIRONNEMENT

En qualité de chef d'organisme, le commandant du CALID a l'obligation de veiller à la sécurité et à la santé physique et mentale des personnels relevant de son autorité quel que soit le lieu géographique où les agents exercent leur activité.

À ce titre, il désigne parmi le personnel placé sous son autorité un chargé de prévention des risques professionnels, qui est chargé de l'assister et de le conseiller dans la mise en œuvre des dispositions réglementaires relatives à la santé et sécurité au travail au ministère de la défense.

Par ailleurs, avec l'appui du bureau « prévention, maîtrise des risques et environnement » de l'état-major des armées, le CALID en tant qu'organisme interarmées suit les prescriptions du coordonnateur central à la prévention de l'EMA.

Le commandant du CALID participe ou se fait représenter aux travaux des comités d'hygiène, de sécurité et des conditions de travail (CHSCT) compétents pour le personnel civil de son organisme et à la commission consultative d'hygiène et de prévention des accidents (CCHPA) pour le personnel militaire.

Sous couvert de l'arrêté relatif à la médecine de prévention, il est chargé d'organiser la surveillance médicale du personnel placé sous son autorité et de prendre en considération les avis et propositions du médecin de prévention.

7. SÉCURITÉ-PROTECTION

La protection des emprises est assurée par les commandants de formation administrative et les responsables de protection de site pour les sites multiformations et par le secrétariat général de la défense et de la sécurité nationale (SGDSN) qui héberge le CALID pour l'emprise parisienne.

Un officier de sécurité et un correspondant sécurité des systèmes d'information sont désignés au sein du CALID.

8. CONTRÔLE INTERNE

Le commandement du CALID est responsable de la mise en œuvre du dispositif de contrôle interne de premier niveau pour les domaines d'activités au sein du CALID. Le commandant du CALID organise son dispositif de contrôle interne en conséquence. Il rend compte du degré de maîtrise des risques via un rapport sur l'activité et selon une comitologie adaptée.

Le chef d'état-major de la cyberdéfense en qualité d'autorité organique déléguée du CALID est désigné responsable du contrôle interne de deuxième niveau (principalement dans le domaine métier « cyber », même s'il doit pouvoir en connaître dans les autres domaines d'activités). Le chef d'état-major de la cyberdéfense est l'échelon de cohérence qui apprécie l'effectivité et la robustesse du dispositif de contrôle interne en vigueur au sein du CALID. Il peut également conseiller et apporter une assistance méthodologique et technique au CALID dans la mise en œuvre du contrôle interne de niveau 1.

9. INSPECTION ET CONTRÔLE EXTERNE

9.1. Contrôle de gestion.

Après consultation préalable du CALID, le chef d'état-major de la cyberdéfense élabore une directive particulière lui assignant les objectifs spécifiques d'activité pour l'année, et lui fixant les échéances et les modalités de contrôle.

9.2. Réunions de commandement.

Les résultats obtenus dans la mise en œuvre de la directive prévue au point 9.1. sont mesurés à l'aide d'indicateurs et présentés annuellement lors d'un conseil de commandement présidé par l'OG COMCYBER ou son représentant.

10. DISPOSITIONS DIVERSES

La présente instruction est publiée au *Bulletin officiel des armées*.

Notes

⁽¹⁾ Conformément à l'[instruction n° 101000/ARM/CAB relative à la politique de lutte informatique défensive du ministère des armées du 24 décembre 2018](#).

Pour la ministre des armées et par délégation :

*Le vice-amiral,
adjoint au sous-chef d'état-major « performance »,*

Hervé CHENAL.