

BULLETIN OFFICIEL DES ARMÉES



Édition Chronologique n° 19 du 17 mai 2018

**PARTIE PERMANENTE
Administration Centrale**

Texte 1

DIRECTIVE N° 41/ARM/DGSIC
relative à la conduite de la mission de sécurisation et de refondation Intradef.

Du 20 avril 2018

DIRECTIVE N° 41/ARM/DGSIC relative à la conduite de la mission de sécurisation et de refondation Intradef.

Du 20 avril 2018

NOR A R M D 1 8 5 0 7 6 0 X

Références :

1. CSIC du 5 février 2018 : décision 32 relative à la mise en œuvre d'une mission de sécurisation et de refondation de l'Intradef (n.i. BO).
2. CSIC du 5 février 2018 : décision 21 relative à la désignation de la DIRISI comme Administrateur unique de l'intradef (n.i. BO).

Classement dans l'édition méthodique : BOEM 160.5.2.5.7

Référence de publication : BOC n° 19 du 17 mai 2018, texte 1.

1. CONTEXTE GÉNÉRAL ET ENJEUX.

Les systèmes de communications et d'information constituent aujourd'hui une part essentielle de la performance du ministère, tant opérationnelle qu'administrative. Ces systèmes numériques sont aujourd'hui au cœur d'une révolution qui touche tous les pans des sociétés modernes et en bouleverse les modes de fonctionnement et d'organisation. Cette révolution est marquée par l'accélération très forte des rythmes d'évolution, par une complexité technologique croissante, et par un besoin essentiel de sécurisation.

La performance du ministère des armées et des forces militaires n'y déroge pas ; elle s'appuie en particulier sur un socle - ensemble de services, réseaux et infrastructures communs - en forte connexion avec le monde extérieur, qui peut être qualifié de « Socle commun MinArm » ou « SOCLE IT ». C'est sur ce socle que s'appuient les différents systèmes et applications métiers, plus intimement liés aux spécificités des services et des missions, qu'elles soient opérationnelles, de soutien et d'administration.

Le socle commun non classifié de défense, également réseau d'entreprise du MinArm, est appelé Intradef. Il s'agit d'un bien commun ministériel indispensable à l'ensemble du ministère et indispensable au soutien des opérations.

Essentiel à la fois au soutien des opérations et au bon fonctionnement du ministère, et intégrant un fort besoin de sécurisation et de résilience, son architecture fondée sur un espace de confiance unique doit être rénovée en profondeur et sans tarder. Outre sa vulnérabilité intrinsèque, elle est inadaptée pour répondre aux besoins portés par l'ambition numérique du ministère, validée par la ministre le 17 novembre 2017.

Intradef est exposé en plein aux effets de la révolution numérique. Interdépendant du monde de l'Internet, d'une part pour échanger avec nos partenaires et d'autre part pour profiter de sa capillarité (accès en mobilité), il est de fait directement soumis à l'influence des transformations et aux menaces extérieures. Il doit pouvoir s'adapter rapidement au rythme des usages et technologies du monde civil qui s'imposent de fait, tout en conservant la résilience qu'exigent les missions fixées au ministère.

Maîtriser son tempo d'évolution est également devenu un défi du fait de sa taille – aujourd'hui de l'ordre de 200 000 machines, 300 000 comptes et plusieurs opérateurs - car il faut à la fois en faire évoluer l'architecture, ses constituants et ses interfaces techniques tout en étant capable de continuer d'héberger les composants les plus anciens (systèmes d'information « métiers » développés il y a plusieurs années), d'y intégrer les nouveaux

projets structurants, de s'inscrire dans une démarche interministérielle et d'accueillir les évolutions agiles de l'informatique moderne.

Maitriser ce tempo demande la mise en place d'une gouvernance et d'une organisation dédiées, adossées à des processus *ad hoc*, s'appuyant sur une démarche « Agile », une rationalisation technique poussée des interfaces, et une adhésion sans faille de l'ensemble de la fonction système d'information et de communication (SIC) pour concevoir, spécifier, acquérir et déployer un socle performant, sécurisé et résilient.

2. OBJET DU DOCUMENT.

Le présent document définit la directive de conduite de la mission de cohérence d'ensemble de sécurisation et de refondation de l'Intradef approuvée par la ministre (Ref.1). Il fixe les principes fondateurs d'une organisation pluri-organismes, faisant appel tant à des compétences techniques et managériales qu'à des compétences de gestion, de mise en œuvre et de déploiement placée sous l'autorité fonctionnelle renforcée du directeur générale des systèmes d'information et de communication (DGSIC).

Ce document fixe les attributions et les relations entre chaque acteur impliqué : l'état-major des armées (EMA), la direction générale de l'armement (DGA), le secrétariat général pour l'administration (SGA), la direction générale des SIC (DGSIC) et la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI).

3. PÉRIMÈTRE COUVERT.

Par une démarche adaptée de pilotage de la cohérence d'ensemble, la mission INTRADEF consiste à sécuriser au plus tôt dans la durée INTRADEF tout en le rendant progressivement apte à soutenir le défi de la transformation numérique.

Elle a pour objet d'apporter de la cohérence entre les programmes et briques constitutives du socle IT du ministère, sans se substituer aux instances de pilotage de ceux-ci.

Le périmètre de cohérence de la mission Intradef englobe l'ensemble des constituants dont les réseaux de transport et de desserte, les services communs Intradef, les services de sécurité d'administration et de supervision, les capacités d'hébergement et les interfaces d'accueil des applications métiers (dont la mise en cohérence fait l'objet d'une démarche connexe sous l'égide de la DGSIC). Il prend également en compte le socle numérique défense plateforme, et ses différents constituants.

Le schéma ci-dessous donne une vision du périmètre couvert :



Les constituants peuvent être classés en trois catégories :

- ce qui relève en propre du projet de transformation de l'Intradef sur son périmètre défini ;
- les projets/programmes fortement adhérents à Intradef (Descartes, STCIA, etc.) , dont le cours pourra être infléchi pour répondre à l'exigence de cohérence d'ensemble ;

- les projets autres (LID par ex.), pour lesquels des interfaces classiques sont à prévoir.

Sont hors du périmètre, mais impactés par la mission :

- l'ensemble des applications métier du ressort des ADS, hébergées sur le socle Intradef (cadre ATG (1) et le CCT (2) validés par la DGSIC) ;
- les systèmes d'élongation (Satcom, etc.), les réseaux et applications classifiés, ou encore les systèmes de type SCADA.

Les constituants sont donc les suivants :

- les différents systèmes constitutifs du réseau Intradef mis en œuvre directement par la DIRISI ou placés sous son autorité en tant qu'administrateur de l'Intradef (Réf. 2) :
 - les logiciels du poste de travail, les services communs à l'utilisateur (annuaire, messageries instantanées, mail, outils collaboratifs, portails, etc.) ;
 - les services d'infrastructure (annuaires techniques, DNS, synchronisation horaire, etc.) ;
 - les solutions de mobilité, d'accès ou d'échanges avec internet, les passerelles ;
 - les *datacenters* et socles d'accueil des applications métier ;
 - les outils d'administration et de supervision, etc.
- le socle technique commun interarmées (STCIA), portés par le programme « SIA » ;
- le projet INCAS (dans toutes ses versions) ;
- le projet MIM3 (préfiguration d'un réseau d'entreprise Internet professionnel) » ;
- les différentes opérations de réseaux :
 - les réseaux résilients maîtrisés de transport des flux, portés par le programme « DESCARTES », notamment les composants ISR et SCR ;
 - le réseau de transport SCU porté par « OPERA » de la DIRISI (prestation externalisée auprès d'un opérateur commercial), qui offre un service qui pourrait être rendu à terme par le réseau interministériel de l'État (RIE) ;
 - les dessertes locales des utilisateurs:
 - les projets de « dessertes » DIRISI (MODIP, etc.) mais aussi le « PPP Balard » ;
 - « RDIP » PPP contractualisé par la DGA pour les bases aériennes.
- les différentes opérations liées à la cybersécurité et à la cyberdéfense :
 - CIMS : carte d'identité multiservices ;
 - SOSIE, signature du ministère ;
 - les outils de sécurisation du poste et des réseaux : chiffreurs, chiffrement de fichiers (ACID, Primx, etc.), chiffrement de partitions, chiffrement de réseau, *Firewall*, antivirus, etc.

- les outils de LID.

Au-delà de cet ensemble de projets et d'opérations d'armement existants, il s'agit également de prendre en compte dans le périmètre de cohérence les différentes futures briques de défense plateforme pour permettre au socle Intradef d'accueillir rapidement des services numériques et d'accélérer ainsi la transformation numérique du ministère. Les services portés par ce projet d'ensemble concernent l'identité numérique, l'accès aisé aux données, l'échange normalisé et sécurisé Internet/Intradef, l'hébergement automatisé (INCAS), apte à supporter des développements rapides et à partager les données pour permettre leur analyse grâce, entre autres, aux outils de datascience et d'intelligence artificielle à venir, etc.

Toutefois, la mission mettra en place un dispositif d'accompagnement des directions d'application pour une bonne intégration (ou migration) sur le socle rénové Intradef (documentations, organisation *ad hoc*, etc.).

4. PRINCIPES.

Une démarche agile compatible des impératifs de continuité opérationnelle.

Il s'agit de mettre en place une organisation et un mode de fonctionnement déclinés des méthodes agiles, permettant, par construction, de faire continuellement évoluer le produit Intradef sur une trajectoire ambitieuse, tant en termes de sécurité que de niveau de services offerts à l'utilisateur. Sans que le besoin n'ait à être parfaitement arrêté de manière analytique dès le départ, cette démarche fixe les délais et les coûts pour maximiser la valeur d'un périmètre fonctionnel et technique qui se construit en continu (pilotage par les délais, produits ajustés au juste besoin, amélioration continue, pas d'effet tunnel, etc.), en s'ajustant au besoin du client. Un effort particulier devra être conduit pour que l'utilisateur, individu ou système applicatif, soit bien au cœur de la démarche.

Cette démarche agile doit pouvoir, en toutes hypothèses, garantir la continuité opérationnelle du fonctionnement du système.

Cette agilité concerne en premier lieu le mode de fonctionnement de l'équipe et la fluidité de ses relations avec les instances en charge de la conduite des affaires, qui elles ensuite selon leur spécificités relèvent des opérations d'armement, des projets classiques, voire des modes de développement agiles.

Une cohérence maintenue de bout en bout tout au long de la vie du produit.

La mise en place d'une capacité « socle numérique » nécessite de garantir la cohérence d'une architecture d'ensemble sécurisée et de sa mise en œuvre, d'assurer la cohérence et la continuité des actions qui vont de l'expression du besoin au retrait du service des équipements constitutifs, garantir la cohérence d'ensemble, technique, fonctionnelle, sécuritaire, calendaire et financière, entre les différents constituants du socle commun, qu'il s'agisse d'équipements physiques, de logiciels mais également de services tels que le soutien de ces produits. Il s'agira d'avoir également une stratégie d'acquisition concertée et combinée entre les projets constitutifs, qu'ils soient DIRISI ou DGA.

Une équipe mixte à tous les niveaux, etc.

Pour maximiser la création de valeur au bénéfice des utilisateurs de l'Intradef, la mission est organisée pour développer et maintenir un lien fort entre les acteurs des phases de « *BUILD - TEST - RUN* », dans une démarche agile et transverse entre les différentes organisations qui ont obligation de travailler harmonieusement et de façon fluide ensemble. Ce lien repose notamment sur une mixité des compétences et des services d'origine (DGA – DIRISI) des agents affectés au sein de la mission. Ainsi, le pilotage de la mission est confié à un ingénieur émanant de la DGA, secondé par un adjoint émanant de la DIRISI. Sans en faire un dogme absolu, le principe de mixité à tous les niveaux, de fluidité de l'équipe constituera une des clés du succès de la mission.

Le fonctionnement en équipe intégrée pourra prendre différentes formes : plateau mixte, intégration de RH DIRISI au sein des équipes projets DGA et de RH DGA au sein des équipes projets DIRISI.

Un pilotage volontaire et disruptif.

La conduite et le pilotage de cette mission intègre impérativement une conduite de projet forte et disruptive, avec la mise en œuvre d'une feuille de route dynamique incluant les phases de déploiement des incréments successifs, et permettant d'avoir autorité sur les différents constituants du socle commun.

Les instances de gouvernance actuelles notamment GIS/COVESIOC/CSIOC, revues de jalon/CSIAG, Codir/Copil de programmes et projets (DID, SIA, INCAS, etc.), Codir des intranets, etc. doivent intégrer cette directive et faciliter la conduite de cette mission.

Un *sponsoring* fort et suivi dans le temps.

La conduite de cette mission, bénéficiera d'un engagement fort du chef d'état-major des armées (CEMA), du SGA et du DGA, et des pleins soutiens et appuis du cabinet du ministre et du DGSIC.

5. MISSIONS.

Les principales transformations que la mission est chargée de conduire visent à :

- sur le plan de la sécurité et de l'administration du système :
 - sécuriser au plus tôt l'Intradef en traitant au plus vite toutes les vulnérabilités identifiées lors des audits ;
 - diminuer durablement la surface d'attaque ;
 - mettre en place des mécanismes de défense en profondeur du système ;
 - reprendre la maîtrise complète du système et en faciliter l'administration ;
 - tenir le plus grand compte de la tension qui affecte les ressources humaines (RH), en acceptant l'idée que celle-ci est durable et probablement croissante et en introduisant par conséquent une forte automatisation des processus pour dégager des marges de manœuvres RH.
- sur le plan des services rendus par l'Intradef à ses utilisateurs :
 - répondre à l'ambition numérique du ministère, en faisant d'Intradef un produit supportant l'accélération de l'évolution technologique ;
 - répondre aux évolutions des usages : mobilité, multicanal, télétravail, etc.
 - mettre en œuvre un cadre d'accueil normalisé, avec des interfaces standards, permettant de garantir le bon fonctionnement des services et applications métiers du ministère.
- sur le plan méthodologique :
 - expérimenter et à amener au ministère de nouvelles manières de concevoir et de piloter un socle des services informatiques, généralisables à l'ensemble de la fonction SIC ;
 - accompagner la transformation de la fonction SIC du ministère.

En corolaire, il s'agira d'assurer la cohérence d'ensemble de l'architecture de l'Intradef au cours du temps compte tenu de l'évolution des besoins et des technologies.

6. RESPONSABILITÉS.

6.1. L'équipe mixte de projet.

Conformément à la décision prise au CSIC du 5 février 2018, l'équipe mixte est placée sous la responsabilité de la DGA. Cette responsabilité est confiée à l'UM ESIO, au sein de la direction des opérations, auquel le chef de mission est rattaché.

Le chef de la mission INTRADEF (CM.INTRADEF) placé sous la responsabilité du DGA, est secondé par un adjoint rattaché au directeur central de la DIRISI.

Intraded étant un bien commun ministériel, le DGSIC y porte une attention toute particulière comme garant de la cohérence d'ensemble de la fonction SIC ministérielle et de la bonne coordination des différents services. Le CM.INTRADEF et son adjoint bénéficient d'un accès direct au DGSIC et sont systématiquement associés au CeCSIC.

Le rôle du CM.INTRADEF et de son adjoint est de piloter la mission de sécurisation et de refondation de l'Intraded, et d'assurer la cohérence d'ensemble (architecture, projets, déploiements).

À ce titre, ils ont pour mission :

- d'organiser, de constituer et de piloter une équipe intégrée mixte (EIM) pluridisciplinaire. Cette équipe mixte doit intégrer des ressources issues des équipes déjà en place sur les projets concourants à la constitution du socle pour notamment faciliter le pilotage et la cohérence d'ensemble ;
- de définir les modalités de fonctionnement de sa structure et de mettre en place les GT et comités *ad hoc* ;
- de décliner en plan d'action la vision stratégique et le besoin portés par la DGSIC;
- de mettre en place et de piloter une démarche agile permettant de garantir cette cohérence de bout en bout, tout au long de la vie du système ;
- de s'assurer de la maîtrise des délais de livraisons des nouvelles capacités, de maîtriser les risques d'ensemble,
- de s'assurer de la maîtrise des interfaces tant internes qu'externes, de maîtriser le cout global et le plan d'investissement annuel *BUILD* et *RUN* réunis ;
- de proposer les réorientations éventuelles des programmes et projets relevant d'instances de pilotage autres (exemple Descartes, STCIA, etc.) ;
- d'assurer sur le périmètre de l'infrastructure la conformité avec l'ATG et le CCT, dont il peut proposer les évolutions et les mises à jour,
- de piloter la conduite du changement, en inscrivant les évolutions de l'Intraded dans le respect strict du principe de continuité opérationnelle assurée par la DIRISI à l'échelle du ministère ;
- de présenter le plan d'investissement pluriannuel et établi en concertation qui sera soumis au visa DGSIC avant de le présenter en CMI;
- d'être comptable devant le COSTRAT et le CMI de la définition du format RH annuel de l'équipe mixte, en qualité comme en quantité, et atteste de son respect ;
- de mettre en place au profit de la gouvernance de la mission une vision permettant à celle-ci de mesurer les résultats obtenus (tableaux de bord de pilotage avec indicateurs de suivi) et d'orienter si

besoin, tant sur les plan capacitaire, technologique que financier, les travaux de la mission. Il présente annuellement à cet effet un tableau de bord avec indicateurs, et un dossier de suivi en vue du CMI.

6.2. Le porteur du besoin.

Le besoin ministériel est porté et validé par le DGSIC, il est élaboré en concertation avec l'ensemble des acteurs.

Le besoin sera élaboré en commun dans le cadre des instances ad hoc, notamment au travers du sous-comité 1 du codir des intranets, et des instances de gouvernance portant la transformation numérique du ministère. Les arbitrages et décisions relevant du CeCSIC.

La DGSIC identifiera au sein du ministère, des porteurs de besoin de services au profit de l'organisation mise en place par la mission et déclinée des méthodes agiles.

6.3. Les règles relatives à l'emploi.

Les dispositions et priorités relatives à l'emploi sont définies par le CEMA.

6.4. Opérateur en charge de l'exploitation.

L'opérateur DIRISI est en charge de l'exploitation et du maintien en condition opérationnel et de sécurité de l'INTRADEF et de la réponse aux besoins exprimés par le CPCO ou les EMO pour les opérations (ex : bulles projetables, adaptations réseaux, etc.). Il est également le gestionnaire logistique de bien et à ce titre occupe les fonctions de responsable du soutien en service.

6.5. Autorité qualifiée et autorité d'homologation.

Le CEMA est l'autorité qualifiée (AQ) unique de l'Intradef.

Son autorité d'homologation (AH) est définie par le COMCYBER (RAQ CEMA).

7. UNE GOUVERNANCE AD'HOC.

En raison des enjeux, un suivi régulier et un pilotage stratégique de la mission de sécurisation et de refondation Intradef seront mis en place au travers d'une gouvernance dédiée : CMI (ministre) – COSTRAT (cabinet) – CECSIC (DGSIC). Ce suivi régulier ne doit pas nuire au principe de subsidiarité dans les prises des décisions, nécessaire pour mener le projet de façon agile.

Cette gouvernance intègre les dispositions du décret DGNUM (révision des textes de la DGSIC pour en faire une direction générale du numérique et des systèmes d'information et de communication –DGNUM-) qui instaure une autorité fonctionnelle renforcée, en particulier sur les systèmes communs et transverses, un processus particulier de validation des plans d'investissement, et du contrôle de conformité.

7.1. Comité ministériel d'investissement.

Le CMI est l'instance supérieure de gouvernance du ministère en matière d'opérations d'investissement. À ce titre, le CMI est un organe de décision et de partage d'informations.

Il comprend le ministre, qui le préside, le CEMA, le DGA et le SGA, membres permanents (qui s'expriment dans le cadre de leurs responsabilités). Le chef du CGA et le directeur des affaires financières (DAF), secrétaire du CMI, sont invités permanents.

L'ordre du jour est fixé par le ministre, sur proposition du secrétaire du CMI.

Les dossiers d'orientation du socle commun et les grandes décisions structurantes sont systématiquement proposés à l'ordre du jour du CMI pour un passage annuel.

Le CMI est également une instance d'arbitrage à la demande du DGSIC.

Le DGSIC rend compte lors d'un CMI annuel de l'avancement des travaux, fait valider les grandes orientations nécessaires, les ressources et le plan d'investissement d'ensemble (flux annuel de ressources humaines et financières).

7.2. Comité stratégique.

Le COSTRAT est l'instance de gouvernance de haut niveau de cette mission essentielle au bon fonctionnement du ministère et au soutien des opérations.

Le COSTRAT est présidée par le directeur de cabinet du ministre ou son représentant.

Le DGSIC présente au cabinet la démarche d'ensemble et le CM INTRADEF fait le point d'avancement de ses travaux.

L'EMA, la DGA, le SGA, la DGSIC, le COMCYBER, le DC DIRISI, le CGA participent au COSTRAT.

Le secrétariat est assuré par l'EIM INTRADEF.

7.3. Comité exécutif du conseil des systèmes d'information et de communication.

Le CECSIC est chargé de superviser la conduite d'ensemble de la mission, la réalisation de ses objectifs et se porte garant de la vision stratégique.

Il valide le plan de management de la mission INTRADEF, notamment les dispositions prises pour répondre aux objectifs fixés à la mission (livraisons de nouvelles capacités, renforcement de la sécurité, meilleure intégration des produits livrés sur le socle exploité, etc.).

Il prépare et propose au COSTRAT les décisions stratégiques relatives aux évolutions significatives, jugées primordiales, des moyens financiers alloués et/ou des objectifs techniques, dont les objectifs de sécurité.

Il procède si besoin, sur demande du CM INTRADEF, aux arbitrages majeurs concernant le déroulement de la mission dans son ensemble dans les limites du cadre fixé de la mission de cohérence d'ensemble.

Sur proposition du CM INTRADEF, il valide les évolutions majeures nécessaires, et le lancement de nouveaux projets contribuant aux objectifs portés par INTRADEF. Il est l'instance de décision associée aux passages de jalons obligatoires, et de décision de déploiement et de mise en service opérationnelle de nouvelles capacités.

L'EMA, la DGA, le SGA, la DGSIC, le COMCYBER, le DC DIRISI, le CGA participent au CECSIC.

7.4. Pilotage opérationnel de la mission.

Pour garantir la réussite de la mission, un premier niveau de concertation et d'arbitrage est assuré par le DUM ESIO et le DC DIRISI.

Pour la ministre des armées et par délégation :

*Le vice-amiral d'escadre,
directeur général des systèmes d'information et de communication,*

Arnaud COUSTILLIÈRE.

(1) ATG : architecture technique générale.

(2) CCT : cadre de cohérence technique.