BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 23 du 14 juin 2018

PARTIE PERMANENTE
Administration Centrale

Texte 1

INSTRUCTION GÉNÉRALE D'EMPLOI N° 2009/DEF/DGSIC/--
Cartographie à des fins de cybersécurité.

Du *25 novembre 2015*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION..

INSTRUCTION GÉNÉRALE D'EMPLOI N° 2009/DEF/DGSIC/-- Cartographie à des fins de cybersécurité.

Du 25 novembre 2015

NOR D E F E 1 5 5 2 6 4 9 J

Classement dans l'édition méthodique : BOEM 160.4

Référence de publication : BOC n° 23 du 14 juin 2018, texte 1.

SOMMAIRE

ANNEXE(S)

1. CADRE GÉNÉRAL D'EMPLOI.

1.1. **Contexte.**

La cartographie des systèmes d'information à des fins de cybersécurité ou cartographie cyber vise à donner une vision de synthèse du périmètre des SI du ministère à des fins de prise de décisions stratégiques dans le domaine de la cybersécurité.

1.2. **Enjeux et objectifs.**

La cartographie cyber repose sur la description systématique de chacun des SI opéré ou utilisé par le ministère à travers une sélection limitée d'informations jugées pertinentes pour évaluer l'état de cybersécurité et l'interdépendance des systèmes d'information du ministère. Elle ne se substitue pas aux outils existants et aux cartographies à la main des opérateurs de systèmes d'information, mais vient au contraire s'appuyer sur eux pour donner une vision transverse (administrative, fonctionnelle, technique) et intelligible du périmètre d'analyse.

Il ne s'agit pas d'un outil de conduite opérationnelle des systèmes d'information mais d'un outil à vocation d'analyse stratégique qui s'adresse aussi bien à la chaîne de cyberdéfense que de cyberprotection.

La cartographie cyber peut également répondre aux demandes des différents décideurs du ministère sur le périmètre qu'ils ont en charge et doit ainsi permettre de répondre aux attendus suivants :

- disposer d'une vision métier / mission des différents systèmes pour évaluer les impacts ;

- connaître l'état de chaque système par rapport au dispositif d'homologation ;

- disposer des informations nécessaires à l'évaluation de la situation en cas d'incident de sécurité (liens avec d'autres SI, …) ;

- identifier les composants techniques principaux du système ;

- connaître le niveau et le principe de mise à jour des composants logiciels.

1.3. **Principes.**

Le ministère de la défense dispose déjà au travers de SICL@DE d'un outil de cartographie des systèmes d'information. La démarche de sécurisation et de suivi de la sécurité d'un système faisant intégralement partie de la démarche projet, il apparaît pertinent de ne pas redévelopper un outil spécifique, mais de s'appuyer sur cet outil et ses processus qui intègrent déjà un volet sécurité.

Ainsi, les données nécessaires à la mise en œuvre de la fonction cartographie des SI à des fins de cybersécurité seront intégrées dans SICL@DE (lorsqu'elles n'y figurent pas déjà). Le processus de contrôle de ces dernières sera intégré aux modalités de vérification, de contrôle et d'approbation des projets et de suivi des systèmes en service tout au long de leur cycle de vie.

1.4. **Périmètre.**

L'ensemble des systèmes d'information sont concernés, qu'il s'agisse de SI dit classiques [IOC (1), SIAG (2) ou SIST (3)] ou de systèmes industriel (SINDS) ou de systèmes d'information embarqués ou enfouis dans des systèmes d'arme (SIESA).

Ces systèmes devront être cartographiés avec des informations pertinentes dépendant de la phase dans laquelle ils se trouvent (conception ou projet, pré-production ou en service).

2. DESCRIPTION FONCTIONNELLE.

Les principaux attendus de la cartographie des systèmes d'information à des fins de cybersécurité sont de capitaliser l'information et de disposer d'une visualisation stratégique à des fins d'analyse.

2.1. **Capitaliser l'information.**

La cartographie cyber remplit un rôle de consolidation de données sur l'ensemble des systèmes d'information opérés ou mis en œuvre par le ministère. Elle concilie les trois exigences suivantes :

- constituer un recensement des systèmes d'information du ministère ;

- disposer sur chacun de ces systèmes d'une information structurée, systématique et correspondant à plusieurs types d'approche à des fins d'analyse liées à la cybersécurité, et d'élaboration d'indicateurs de gouvernance ;

- décrire pour chaque système d'information ses interactions avec d'autres systèmes ou son intégration à un système de systèmes.

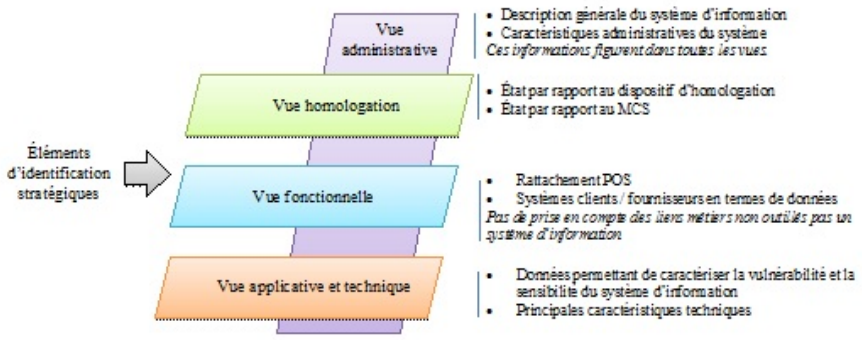
Les informations relatives à un système d'information peuvent se répartir en 4 vues conceptuelles dont la composition est détaillée en annexe :

- une vue administrative : elle recense les caractéristiques essentielles d'un système d'information nécessaires à toute analyse. Cette vue constitue la carte d'identité du système d'information ;

- une vue homologation : elle permet d'apprécier la maitrise du processus d'homologation et du processus de maintien en condition de sécurité du système d'information ;

- une vue fonctionnelle : elle fournit une appréciation des impacts métiers d'une vulnérabilité ou d'un incident sur le système d'information considéré ;

- une vue applicative et technique : elle regroupe les éléments à même de caractériser la vulnérabilité et la sensibilité du système et détaille ses principales caractéristiques techniques.



2.2. **Disposer d'une visualisation stratégique à des fins d'analyse.**

Sur la base de cette information consolidée, la cartographie cyber devient alors un outil d'aide à la décision et permet ainsi de répondre aux besoins selon deux modes :

- l'analyse porte sur une question transverse : le caractère systématique de description de chaque système d'information permet alors d'identifier l'ensemble des systèmes d'information concernés, compte tenu de leurs caractéristiques.

- l'analyse porte sur un système d'information : la cartographie permet d'identifier l'ensemble des systèmes externes potentiellement impactés par une vulnérabilité sur ce dernier.

3. ACTEURS, ACCÈS AUX DONNÉES ET RESPONSABILITÉS.

3.1. **Acteurs.**

3.1.1. ***La direction générale des systèmes d'information et de communication.***

Conformément à l'instruction ministérielle 900, le fonctionnaire de la sécurité des systèmes d'information du ministère (FSSI) recense et veille à ce que les besoins de protection des SI soient exprimés et satisfaits. À ce titre, il dispose d'un accès à l'ensemble des données de la cartographie cyber contenues dans SICL@DE.

3.1.2. ***L'officier général cyberdéfense.***

Au titre de ses missions, l'officier général cyberdéfense (et ses mandataires) dispose d'un accès à l'ensemble des données de la cartographie cyber contenues dans SICL@DE.

3.1.3. ***L'Officier de la sécurité des systèmes d'information d'organisme.***

Des officiers de la sécurité des systèmes d'information sont désignés au sein de l'état-major des armées, du secrétariat général pour l'administration, de la direction générale pour l'armement, de la direction de la protection et de la sécurité de défense et de la direction générale de la sécurité extérieure. Des délégations peuvent être réalisées pour que le portefeuille applicatif de chaque responsable soit adapté (délégation par armée …).

Outre l'exploitation des données à des fins de gouvernance, ils sont chargés de contrôler le bon remplissage de ces dernières (cf. annexe).

3.1.4. ***Responsable chargé du projet / Responsable technique du système.***

Selon la phase du projet, le responsable chargé du projet et le responsable technique du système sont responsables respectivement de l'atteinte ou du maintien des objectifs, y compris ceux relatifs à la sécurité. Ils sont chargés, éventuellement avec l'aide du responsable de la sécurité du système d'information (RSSI) lorsqu'il est désigné, de renseigner et de mettre à jour les données de la cartographie cyber pour le SI dont ils ont la charge.

3.2. **Accessibilité des données.**

Une partie des données n'est accessible qu'à un nombre restreint de profils sous SICL@DE du fait de leur sensibilité. Ces données sont identifiées en annexe dans la description de la composition des différentes vues. Seuls le responsable chargé du projet, le responsable technique du système, le responsable SSI du système (lorsqu'il dispose d'un accès à SICL@DE), les OSSI, le FSSI et l'officier général cyberdéfense (et/ou leurs mandataires) sont autorisés à accéder à l'intégralité de ces données.

3.3. **Saisie des données.**

Le responsable chargé du projet et le responsable technique du système, éventuellement appuyés par le responsable de la sécurité du système d'information projet ou aval lorsqu'il est désigné, sont chargés de saisir et de mettre à jour les données présentées en annexe sur SICL@DE.

3.4. **Contrôle / vérification des données.**

Le contrôle et la vérification des données sont réalisés soit ponctuellement soit lors des revues ou examens prévus par l'instruction ministérielle 2008 (4). L'annexe précise le jalon à partir duquel chaque donnée doit être vérifiée ou contrôlée.

3.4.1. ***Contrôles ponctuels.***

Les contrôles ponctuels sont réalisés par et à la convenance des OSSI (cf. point 3.1.1). Le FSSI (ou ses mandataires), au titre de sa mission de contrôle, peut effectuer des contrôles inopinés et informer les OSSI des résultats afin que des mesures adéquates soient prises.

3.4.2. ***Lors du passage des jalons.***

La revue des projets est assurée selon des modalités mise en place par les commissions relatives à chaque segment (COVESIOC, CSIAG et CSIST) conformément à l'instruction ministérielle 2008. Lors de ces revues, notamment au passage d'un jalon, la présence effective des données figurant en annexe est vérifiée. Concernant les données en accès restreint, les responsables SSI d'organisme sont sollicités et apportent leur concours.

Tout projet dont la fiche est incomplète ne peut se voir autorisé à passer au jalon suivant sauf dérogation accordée par le responsable de la sécurité des systèmes d'information d'organisme concerné.

Pour le ministre de la défense et par délégation :

L'ingénieur général hors classe de l'armement,
directeur général des systèmes d'information et de communication,

Marc LECLÈRE.

---

(1) SIOC : système d'information opérationnel et de commandement.

(2) SIAG : systèmes d'information d'administration et de gestion.

(3) SIST : Système d'information scientifique et technique.

(4) Instruction ministérielle 2008/DEF/DGSIC du 10 juillet 2013 fixant les modalités d'approbation et de suivi des systèmes d'information et de communication.

ANNEXE I.

À L'INSTRUCTION GÉNÉRALE D'EMPLOI N° 2009 DEF/DGSIC/-- DU 25 NOVEMBRE 2015.

DÉTAIL DES VUES DE LA CARTOGRAPHIE CYBER.

1. VUE ADMINISTRATIVE.

La vue administrative rassemble le socle minimal d'informations pour caractériser un système d'information et disposer des informations administratives le concernant. Cette vue, qui constitue la carte d'identité d'un système d'information est composée des champs suivants :

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information est obligatoire
Nom du SI	Général ⇨ Identification ○ Sigle	• Permet d'identifier de façon unique chaque système. • SICL@DE est le système de référence de nommage des SI.	**Jalon 1**
Type de SI	Général ⇨ Caractérisation ○ Segments(s) ▪ Segment principal	• Permet d'identifier le domaine d'appartenance du SI (SIOC, SIAG, SIST, ICS, SIESA).	**Jalon 1**
Nature de SI	Général ⇨ Caractérisation ○ Typologie ▪ Type de fiche	• Passerelle d'interconnexion, application spécifique, portail de communication, service réseau ...	**Jalon 1**
État du SI	Planning ⇨ Calendrier du projet ○ Phase courante ○ Liste des tâches et actions	• La « phase courante » située dans « 05-Planning – Calendrier du projet » associée avec la liste des tâches et actions permet de déterminer l'état du SI. • Exemple 1 : un SI en phase de réalisation peut disposer d'une tâche déploiement. À l'issue, il commence donc à être utilisé (mais ne bascule pas en phase Utilisation). • Exemple 2 : La MSO correspondant à un jalon en phase de réalisation, mais dans la tâche utilisation. À l'issue, le SI passe en phase d'utilisation.	**Jalon 1**

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information est obligatoire
Type d'opérateur du SI	Technique ⇨ Exploitation o Opérateur technique		**Jalon 4**
Réseau support	Technique ⇨ Architecture technique o Type de réseau		**Jalon 2**
Confidentialité	Sécurité ⇨ Confidentialité o Besoins d'en connaître o Réglementation applicable o Mention de manipulation		**Jalon 1**
Criticité	Non retenu pour l'instant du fait de sa sensibilité		**Sans objet**
Zone fonctionnelle – POS	Général ⇨ Caractérisation o Zone fonctionnelle de rattachement o Liste des positionnements sur le POS ▪ Zone fonctionnelle		**Jalon 0**
Adresse de description du SI	Documents	• Permet d'identifier, quand elle existe, l'espace où est conservée la documentation de référence sur le SI.	**Sans objet**

2. VUE HOMOLOGATION.

Répondant aux besoins spécifiques de la chaîne cyberprotection, cette vue rassemble les éléments nécessaires à une analyse critique des SI par rapport au processus d'homologation ainsi qu'au processus de maintien en condition de sécurité.

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Statut de l'homologation	Sécurité ⇨ Homologation o État homologation ▪ Statut d'homologation	• Permet d'apprécier l'état du système par rapport au processus d'homologation.	**Jalon 1**
Date de fin homologation	Sécurité ⇨ Homologation o État de la démarche ▪ Date ▪ Durée	• Permet d'anticiper le renouvellement des homologations. • Cette date est calculée à partir de la date de début d'homologation et de sa durée.	**Jalon 4**
Procédure	Sécurité ⇨ Homologation o État homologation ▪ Type d'homologation	• Standard, simplifiée ou sommaire.	**Jalon 1**
Autorité d'homologation	Organisation ⇨ Autres acteurs o Autorité d'homologation		**Jalon 1**
RGS	Sécurité ⇨ Autres éléments SSI o RGS	• Permet d'identifier si le système d'information est soumis au référentiel général de sécurité.	**Jalon 1**

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Données à caractère personnel sensible	Sécurité ⇨ Autres éléments SSI o Données à caractère personnel sensibles	• Permet d'identifier les SI traitant de telles données.	**Jalon 2**
Date du dernier audit	Accès SSI restreint ⇨ Audits et état de sécurité o Date du dernier audit		**Jalon 4**
État de sécurité du SI	Accès SSI restreint ⇨ Audits et état de sécurité o État de sécurité du SI	• Permet d'identifier rapidement les conclusions d'un audit sur un SI concernant son état de sécurité (bon, mauvais, non évalué, ...).	**Jalon 4**
Date évaluation de l'état de sécurité	Accès SSI restreint ⇨ Audits et état de sécurité o Date évaluation de l'état de sécurité	• Permet d'apprécier le caractère récent ou non de l'état de sécurité du SI mentionné ci-dessus.	**Jalon 4**
État du MCS	Sécurité ⇨ Homologation o État du MCS	• Aucun MCS, MCS interne mais présentant des insuffisances, MCS externe mais efficace, ...	**Jalon 4**
Enrôlement LID	Sécurité ⇨ Autres éléments SSI o Enrôlement LID	• Permet de savoir si le SI a été enrôlé au CALID	**Jalon 4**
Impacts directs	Accès SSI restreint ⇨ Informations générales o Impacts directs		**Jalon 1**
Impacts indirects	Accès SSI restreint ⇨ Informations générales o Impacts indirects		**Jalon 1**
Autorité qualifiée	Sécurité ⇨ Gouvernance de la sécurité o Autorité qualifiée		**Jalon 1**

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
OSSI	Sécurité ⇨ Gouvernance de la sécurité o OSSI	• Permet d'identifier l'OSSI de chaîne.	**Jalon 4**
RSSI projet	Organisation ⇨ Acteurs de la maîtrise d'ouvrage o RSSI-P		**Jalon 2**
RSSI aval	Organisation ⇨ Acteurs de la maîtrise d'ouvrage o RSSI-A		**Jalon 4**
OP / Responsable fonctionnel	Organisation ⇨ Acteurs de la maîtrise d'ouvrage o RF		**Jalon 0**
DP / responsable conduite de projet (phase projet)	Organisation ⇨ Acteurs de la maîtrise d'ouvrage o RCP		**Jalon 0**
Responsable technique du système RTS (phase utilisation)	Organisation ⇨ Acteurs de la maîtrise d'ouvrage o RTS		**Jalon 4**

3. VUE FONCTIONNELLE.

Cette vue permet d'apprécier les impacts métiers associés à une vulnérabilité ou un incident sur le SI. Fondée majoritairement sur l'exploitation du POS, elle décrit le SI selon ses clients ainsi que les activités soutenues par le SI.

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Quartier fonctionnel – POS	Général ⇨ Caractérisation o Liste des positionnements sur le POS ▪ QF		Jalon 0
Bloc fonctionnel - POS	Général ⇨ Caractérisation o Liste des positionnements sur le POS ▪ BF		Jalon 1
Autorité d'emploi	Général ⇨ Responsabilités o Autorité d'emploi		Jalon 1
Clients du SI	Technique ⇨ Utilisation o Clients du SIC		Jalon 1
Administrateur fonctionnel	Organisation ⇨ Autres acteurs o Liste des contacts ▪ Administrateur fonctionnel		Jalon 4
Existence d'un PCI/PRI	Sécurité ⇨ Plan de continuité/Reprise o PCI-PRI – PCA-PRA ▪ PCI/PRI engagé		Jalon 4
Appartenance à un système de système	Général ⇨ Identification o Fiche mère	• La fiche mère permet de regrouper plusieurs fiches. • Fonctionnalité limitée à deux niveaux	Jalon 1
Fonction essentielle supportée par le SI	Accès SSI restreint ⇨ Fonctions et activités supportées o Fonctions supportées	• Liste d'activités en référence à la PSSI du Mindef	Jalon 1
Activités supportées par le SI	Accès SSI restreint ⇨ Fonctions et activités supportées o Activités essentielles supportées	• Identification des activités supportées par le SI à un degré plus fin que la PSSI. Dans un premier temps, champ en texte libre	Jalon 1

4. VUE TECHNIQUE ET APPLICATIVE.

Cette vue regroupe les éléments à même de caractériser la vulnérabilité et la sensibilité du SI et de détailler ses principales caractéristiques techniques. Ne sont retenus que des éléments techniques permettant de faire apparaître les caractéristiques majeures du SI. L'obtention d'information plus détaillées se fera auprès de l'opérateur.

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Imputabilité	Sécurité ⇨ Autres éléments de sécurité o Imputabilité		**Jalon 1**
Réactivité	Sécurité ⇨ Autres éléments de sécurité o Réactivité		**Jalon 1**
Disponibilité - DIMA[5]	Sécurité ⇨ Confidentialité o DIMA		**Jalon 1**
Disponibilité retenue par l'ARR	Sécurité ⇨ Confidentialité o Disponibilité retenue		**Jalon 4**
Disponibilité – PDMA[6]	Sécurité ⇨ Confidentialité o PDMA		**Jalon 1**

[5] DIMA : durée d'indisponibilité maximale acceptée.
[6] PDMA : perte de données maximale acceptée.

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Intégrité	Sécurité ⇨ Confidentialité ○ Niveau d'intégrité		**Jalon 1**
Interconnexions du SI - Liens entrants	Technique ⇨ Architecture technique ○ SIC interconnectés	• Liste de SI avec protocoles associés • Le protocole peut être ajouté dans la case précisions. • Permet d'identifier la potentielle diffusion d'une vulnérabilité	**Jalon 2**
Interconnexions du SI - Liens sortants	Technique ⇨ Architecture technique ○ SIC interconnectés	• Liste de SI avec protocoles associés • Le protocole peut être ajouté dans la case précisions. • Permet d'identifier la potentielle diffusion d'une vulnérabilité	**Jalon 2**
Interconnexions du SI - Liens bi-directionnels	Technique ⇨ Architecture technique ○ SIC interconnectés	• Liste de SI avec protocoles associés • Le protocole peut être ajouté dans la case précisions. • Permet d'identifier la potentielle diffusion d'une vulnérabilité	**Jalon 2**
Déploiement serveur	Technique ⇨ Architecture technique ○ Type d'architecture serveur		**Jalon 3**
Déploiement client	Technique ⇨ Architecture technique ○ Type d'architecture client		**Jalon 3**
Niveau d'hébergement	Technique ⇨ Exploitation ○ Hébergement DIRISI ▪ Niveau de service retenu		**Jalon 4**

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Mutualisation de la ressource de type terminal	Technique ⇨ Architecture technique ○ Mutualisation du client		**Jalon 3**
Mutualisation de la ressource de type serveur	Technique ⇨ Architecture technique ○ Mutualisation du serveur		**Jalon 3**
Certificats	Sécurité ⇨ Autres éléments SSI ○ Type d'IGC	• Avec certificat ; Sans certificat ; en précisant le type d'IGC	**Jalon 3**
Localisation géographique nominale du système	Technique ⇨ Architecture technique ○ Liste des matériels ▪ Lieu géographique des serveurs Technique ⇨ Exploitation ○ Hébergement serveur DIRISI ▪ Site(s) DIRISI Technique ⇨ Exploitation ○ Site(s) hors DIRISI	• non pertinent pour les réseaux	**Jalon 4**
Localisation géographique de secours du système	Technique ⇨ Exploitation ○ Site de secours	• non pertinent pour les réseaux	**Jalon 4**

Critère	Position dans SICL@DE	Remarques	Jalon à partir duquel la présence de l'information doit être contrôlée
Administration technique	Organisation ⇨ Autres acteurs o Liste des contacts ▪ Administrateur technique		**Jalon 4**
Opérateur du système	Organisation ⇨ Autres acteurs o Liste des contacts ▪ Opérateur du système		**Jalon 4**
Exploitant du système	Organisation ⇨ Autres acteurs o Liste des contacts ▪ Exploitant du système		**Jalon 4**
Logiciel	Technique ⇨ Architecture logicielle o Liste des logiciels ▪ Nom du logiciel		**Jalon 4**
Version majeure	Technique ⇨ Architecture logicielle o Liste des logiciels ▪ Version majeure		**Jalon 4**
Briques logicielles	Technique ⇨ Architecture logicielle o Liste des logiciels ▪ Type logiciel	• Permet d'apprécier l'obsolescence de certaines briques.	**Jalon 4**
Matériels	Documents	• Sous forme d'un schéma descriptif d'architecture joint à la fiche SICL@DE.	**Jalon 4**