MINISTÈRE
DES ARMÉES
*Liberté*
*Égalité*
*Fraternité*

# Intégration de la cybersécurité dans le déroulement d'une opération d'armement

Référence : 2022\CYBER\1\NP

# 1 Objectif du document

Ce document a pour objectif de préciser comment la cybersécurité doit s'intégrer dans le déroulement d'une opération d'armement **sous la conduite des directeurs de projet**. Ce déroulement s'appuie sur une logique de phases, jalons et activités décrite et encadrée par l'IM1618.

# 2 Synthèse et recommandations

Ce document de synthèse repose sur une analyse détaillée des activités cyber pour chaque phase de la 1618, transcrites sous la forme d'un jeu de planches très opératives, appelées « calque 1618 ». Lors de ce travail, de grands principes ont émergé pour la prise en compte de la cybersécurité dans la conduite des opérations d'armement :

- La cybersécurité est avant tout :
  - **Une performance d'ensemble comme une autre.** Elle doit être explicite, justifiable et prise en compte dès le stade de préparation des opérations d'armement, dans le travail de convergence entre besoin opérationnel et sa formalisation dans le DUB (Document Unique de Besoin) et dans l'architecture de la solution. À ce titre, elle est soumise à arbitrages et compromis pour aboutir à la réalisation de Systèmes d'Armes opérables à des risques, coûts et délais acceptables. Cette performance d'ensemble doit être pleinement caractérisée et évaluée tout au long du cycle de vie des systèmes.
  - **Une capacité opérationnelle à part entière.** En effet, un point de vue suffisamment spécifique (technologie, compétence …) et complexe (nombre d'acteurs, variabilité de la menace…), sans oublier son inclusion dans le grand tout du fait de l'interconnexion de la plupart des systèmes d'armes, elle nécessite des compromis à instruire au fil de l'eau dans une vision globale. Ceci justifie en propre **une logique de développement et la mise en place d'une organisation ad'hoc au sein de chaque projet, pérenne jusqu'au retrait de service,** qui doit être formalisée dans des **Plans de Management**. Une vision « cybersécurité » de niveau capacitaire, transverse aux différentes opérations, doit également être entretenue au niveau étatique.

La cybersécurité intervient d'une manière transverse sur les sujets suivants :

- **Contextualisation.** En phase de préparation, une **analyse de risques cyber à l'échelle capacitaire** doit être menée afin d'éclairer l'expression de besoin cyber des systèmes qui composent la capacité étudiée et constituer **un élément de référence dans les choix d'optimisation** pouvant être faits lors de la conception des systèmes d'armes.
- **Préparation des contrats.** Les exigences de cyber sécurité doivent entrer dans le **schéma de contractualisation (DUB, PJD et DJD) entre le MOA et le(s) MOI**. Le PJD, annexe incontournable du contrat de réalisation au même titre que le DUB, détaille les activités de justification et les moyens associés. Le niveau de complexité du Système d'Armes, objet de l'opération d'armement, peut conduire le MOA à notifier des travaux d'études et de

prototypage afin de réduire les risques liés à l'atteinte des objectifs de performance en cybersécurité en phase de réalisation et, consolider les parties de DUB et PJD correspondantes. La menace cyber étant évolutive, il est nécessaire de prévoir dans les contrats de réalisation et de soutien un mécanisme d'ajustement des objectifs tout au long du développement, et également des périodes de reingéniering permettant de prendre en compte les évolutions des menaces et du contexte capacitaire.

- **Définition des responsabilités état-industrie.** Elles doivent être rigoureusement respectées tout au long de l'opération d'armement tout en organisant de la visibilité réciproque et des travaux en commun. S'agissant de cybersécurité, il est important de rappeler que **l'homologation SSI d'un système d'armes est de responsabilité Étatique**. Cette autorité doit donc être associée à la gouvernance de la capacité cyber et pouvoir orienter les choix effectués au fil de la réalisation. Le MOI contribue au processus d'homologation cyber par la fourniture d'un dossier technique, alimenté par le DJD ou des prestations spécifiques comme de l'assistance technique à des essais cyber, pour autant qu'il ait la couverture contractuelle pour le faire. L'obtention formelle de l'homologation cyber ne peut constituer une obligation de résultat pour le MOI. Enfin, selon le niveau d'intégration du Système d'armes dans son environnement capacitaire, **l'Administration pourra être amenée à prendre une responsabilité de maitre d'œuvre d'ensemble** sur l'architecture cyber et de conduire les travaux d'ingénierie et d'essais correspondants. Les MOI peuvent alors être sollicités pour réaliser des travaux dans le cadre de contrats d'assistance à maitrise d'ouvrage.

- **Contraintes d'exportation**. Ces contraintes doivent être **identifiées et cadrées au plus tôt dans la conduite de l'opération d'armement** et dans tous les cas avant le gel des principes d'architecture du système d'armes et de la notification du contrat de réalisation. La dimension cyber doit être prise en compte dans ces travaux.

- **Contraintes de coopération.** Un accord multinational de type G to G doit être mis en place dans le cas de programmes menés en coopération précisant les modalités de traitement des aspects cybersécurité (réglementation, homologation)

- **Identification en amont des éléments clé :** biens essentiels (valeurs métier), patrimoine technologique, contextes opérationnels d'utilisation (sur le cycle de vie complet) et systèmes en interfaces. Cette démarche permet de converger sur une cible de cyber sécurité robuste qui sera confortée par une analyse préliminaire de risque dès qu'une architecture de solution est connue.

- **MSO des systèmes d'armes.** Elle doit pleinement prendre en compte les performances de cybersécurité qui doivent être déclinées dans les activités de formation, d'entrainement opérationnel, de montée en puissance, et de prise en main par les acteurs exploitants ou utilisateurs (exercices LID, PCI/PRI, …).

- **Stratégie de MCS (partie intégrante de la stratégie de soutien)**. Elle doit être établie pour nourrir le DUB, en amont de la passation du contrat de réalisation. Au-delà des activités classiques liées au maintien en condition de sécurité des systèmes, elle doit s'attacher à faire **appliquer des règles strictes de gestion de configuration** permettant de partager entre tous les acteurs du soutien l'état des différents systèmes déployés. Dans la phase opérationnelle,

le maintien en condition de sécurité, intégrant la **gestion des vulnérabilités**, est un enjeu majeur pour garantir le niveau de performance des systèmes d'armes.

- **Revues jalons.** Ces revues**,** autant étatiques qu'industrielles, doivent inclure de façon obligatoire **un volet cybersécurité explicite.**
- **Veille des menaces.** De responsabilité étatique, elle revêt une importance particulière pendant toutes les phases du cycle de vie afin d'alimenter les analyses de risques et de pouvoir à tout moment connaitre et maitriser les performances attendues.

# 3 Suivi des versions

| Version | Date | Commentaires |
|---|---|---|
| V1.00 | 28/10/2022 | Version initiale |
| | | |
| | | |