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

# Spécification de la cybersécurité en tant que performance

## Synthèse et recommandations

Référence : 2022\CYBER\9\NP

Version : 1

# 1 Introduction

Pour ajuster le niveau de cybersécurité d'un système d'armes au juste besoin il est indispensable de passer d'une logique de conformité (à des référentiels, des exigences, …) à une logique de maîtrise des risques cyber. Le présent document s'inscrit pleinement dans cet objectif, en proposant une manière de spécifier la cybersécurité sous forme d'une performance, au même titre que les autres performances fonctionnelles du système.

Cette démarche nouvelle devra être affinée par le retour d'expérience sur les futurs programmes d'armement.

# 2 Enseignements

Cette démarche a été élaborée au sein d'un groupe de travail qui réunissait des participants industriels et étatiques, qui a validé que **l'objectif de spécifier la cybersécurité sous forme d'un ensemble de performances est atteignable** et permettrait de répondre à un certain nombre de difficultés identifiées dans la conduite des programmes d'armements, comme par exemple : l'inflation de documents réglementaires applicables, les exigences cyber trop nombreuses et non contextualisées, …

Les spécifications pourraient donc comprendre à la fois des exigences décrivant des performances à atteindre et des exigences techniques permettant d'attester une conformité, l'équilibre entre les deux pouvant dépendre du type de programmes (plus d'exigences de performances pour des programmes de type PTD[1] par exemple). Les exigences techniques pourraient dans ce cadre représenter un socle négociable sous réserve de la démonstration de la tenue des performances.

Pour pouvoir se dérouler dans les meilleures conditions, cette démarche nécessite un travail d'ingénierie système itératif entre MOI et MINARM.

La transition entre la démarche actuelle et cette nouvelle approche s'effectuera de manière progressive pour accompagner la montée en maturité des différents acteurs. En complément, il est indispensable de mettre en place un RETEX sur l'application de cette démarche pour permettre sa consolidation à la lumière des remontées des différents programmes ou projets.

La déclinaison de ces concepts vers la chaine sous traitance devra faire l'objet d'une réflexion complémentaire.

[1] Projets de technologie de défense (nouveau nom des études amonts)

# 3 Démarche

D'un point de vue ingénierie, la cyber sécurité est avant tout **une performance d'ensemble comme une autre**.

Elle doit être

1. Explicite,
2. Justifiable, Vérifiable, Mesurable (ce dernier point nécessite encore des réflexions pour le domaine cyber),
3. **Prise en compte dès le stade de préparation** ainsi que dans le travail de convergence entre besoin opérationnel, sa formalisation dans le DUB (Document Unique de Besoin) et l'architecture de la solution.
4. À ce titre, elle est soumise à des arbitrages et des compromis pour aboutir à la réalisation de Systèmes d'Armes opérables à des risques, coûts et délais acceptables.
5. Cette performance d'ensemble doit être pleinement caractérisée et évaluée tout au long du cycle de développement.

## *3.1 Travaux préliminaires*

**La réalisation d'une analyse fonctionnelle en entrée du processus semble indispensable**. Réalisée par les équipes étatiques, elle peut dériver d'une analyse fonctionnelle de niveau capacitaire. Dans tous les cas, la dimension cyber doit être prise en compte pour intégrer les fonctions associées (par exemple générer et distribuer des éléments secrets, …).

Durant cette phase, des études préliminaires de type ETO ou PTD, sont utiles pour permettre d'affiner ces analyses avec les MOI.

Pour les étapes suivantes, **il est préconisé d'utiliser les concepts de la méthode EBIOS RM**.

## *3.2 Analyse et expression du besoin par le MINARM*

Dans une première étape, les premiers ateliers de la méthode EBIOS RM doivent être réalisés par le MINARM en s'appuyant, lorsqu'ils existent, sur les résultats des analyses de risques de niveau capacitaire. Ce travail **doit impérativement être déroulé par une équipe comprenant des experts « métiers »** (DGA et opérationnels) sous pilotage d'un expert cyber.

Dans une deuxième étape, si la démarche contractuelle le permet, le MOI sera intégré à ces travaux. Un travail de convergence entre MOI et MINARM doit en effet être mené durant la phase pré-contractuelle, ce qui implique la participation du MOI aux différents ateliers EBIOS RM et une détermination itérative des éléments de sortie qui vont alimenter la STB ou le DUB.

A partir des éléments de l'analyse fonctionnelle, les premiers ateliers EBIOS RM vont permettre d'identifier, les valeurs métiers[2], les événements redoutés avec leur gravité, les sources de risques et les objectifs visés, le socle réglementaire applicable et des scénarios stratégiques. Le niveau de performances cyber sera défini à partir des actions élémentaires réalisables par les sources de menaces. Ces actions élémentaires seront définies à partir des scénarios, dans un atelier EBIOS RM. Les actions élémentaires sont cotées selon leur niveau de complexité, par exemple en s'appuyant sur les travaux des GEMP[3] Cyber.

On pourra ainsi énoncer des performances sous la forme suivante :

> Capacité du système à résister à des attaques, constituées d'actions élémentaires, portant sur les valeurs métiers (informations, fonctions, processus), le niveau des attaques à contrer étant lié à la gravité des événements redoutés identifiés.

Ce qui peut s'exprimer sous forme de tableau :

| Valeur métier | type | Fonction associée | Evénement redouté | gravité | Performance Cyber |
|---|---|---|---|---|---|
| VMx | Information, ou donnée ou processus | FXX | ERX | CRITIQUE<br>GRAVE ou SIGNIFICATIF<br>MINEUR | ELEVE<br>MOYEN<br>BASIQUE |

Ou de manière plus textuelle :

> La protection de la {valeur métier, fonction} X, doit pourvoir résister à des attaques, constituées d'actions élémentaires, de niveau {élevé, moyen, basique}.

Lorsque nécessaire, un niveau de dégradation tolérable peut être défini.

La définition des niveaux d'attaque doit être partagée avec le MOI.

## *3.3 Analyse du besoin par MOI et contractualisation*

**En phase de contractualisation et à partir d'une primo-architecture de la solution envisagée, le MOI consolide la liste des scénarios stratégiques fournis en entrée, et définit les scénarios opérationnels** et leur vraisemblance associée en convergence d'analyse avec le MINARM.

Le traitement du risque est alors exprimé sous forme de mesures permettant d'atteindre la performance spécifiée qui s'exprime in fine par un niveau de risque résiduel acceptable, pour des scénarios d'attaques donnés. Dans la phase pré-contractuelle, Il est donc nécessaire de disposer au

[2] Au sens EBIOS RM : composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé (anciennement « biens essentiels » dans la méthode EBIOS 2010).

[3] GEMP : Groupe d'Evaluation de la Menace Prospective

minimum de principes d'architecture. Ces principes, les scénarios opérationnels et les actions élémentaires retenus devront être annexés au contrat. L'architecture finale du système résulte d'un compromis entre les différentes performances qu'il sera utile de tracer dans un dossier justificatif.

**La performance cyber doit être justifiable par le MOI** : Il est essentiel qu'au moment de la contractualisation, MINARM et MOI aient identifié les essais à mener et les moyens nécessaires à la démonstration des scénarios opérationnels à tenir (PJD cyber).

Dans certains cas, si la notion de performance cyber est particulièrement difficile à définir, ces moyens d'essais devront permettre de mesurer la dégradation de ses performances opérationnelles en fonction du niveau d'agression cyber.

### *3.4 Justification du niveau de performances atteint*

L'évaluation de l'efficacité des mesures de sécurité et la confiance dans leur implémentation est un élément à prendre en compte pour calculer la vraisemblance nette d'un scénario opérationnel et devrait faire à l'avenir d'échange entre MINARM et MOI pour partager des méthodes ou des pratiques communes allant au-delà de l'application de mesures techniques préétablies.

Toute évolution des scénarios stratégiques ou des performances proposées par Le MINARM après la signature du contrat devra être instruite pour analyser l'impact sur l'architecture qui avait été retenue et en identifier les implications contractuelles.

## 4 Suivi des versions

| Version | Date | Commentaires |
|---|---|---|
| V1.10 | 17/06/2021 | Version initiale |
| | | |
| | | |