MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Guide pour la détermination des composants cyber-critiques

Référence : 2022\CYBER\8\NP

Version : 1.00

Table des matières

1 Objectif du présent document

Ce document se veut être un guide pratique destiné :

- aux industriels qui devront déterminer la liste des composants critiques d'un point de vue cyber au sein d'un système,
- à l'autorité Maitre d'Ouvrage du MINARM qui en contractualisera la demande,
- et aux services de la DGA en charge de la récupération des listes et de leur exploitation.

Dans la suite du document ces composants sont appelés cyber-critiques ou CCC (Composants Cyber Critiques) pour simplifier la rédaction.

Ce document comporte deux parties principales :

- La première définit la méthode d'analyse d'un système et de réduction de périmètre,
- La seconde définit les critères de criticité à utiliser.

2 Définitions

Cette section rassemble les définitions qui ont été retenues dans le cadre de ce guide.

Composant Cyber-Critique d'un système d'armes : un composant qui contient ou manipule de l'information numérique, et qui pour la réalisation d'une mission du système, soit assure des fonctions critiques ou les protège, soit peut introduire compte-tenu du design du système des vulnérabilités cyber sur des fonctions critiques. Une fonction critique est une fonction dont l'altération numérique ou la compromission aurait des conséquences inacceptables sur la capacité du système d'armes à assurer la mission principale pour laquelle il a été conçu. Un composant cyber-critique peut-être un sous-système, des constituants matériels, logiciels ou micro logiciels, ou les données de configuration qui leur sont associées. Ces composants cyber-critiques peuvent être achetés sur étagère, modifiés ou réalisés sur spécification.

Produit, Système d'Armes (SA) : Équipement ou système livré, employé par les Forces (sera décomposé en éléments plus petits lors de l'analyse jusqu'à atteindre le niveau Composant).

- **Approche Top-Down :** Approche partant d'un système délimité en termes de périmètre technique et en termes de phase de vie (cf. ISO [1]15288/EIA [2]632).

  La Figure 1 ci-dessous explicite les différentes notions développées dans les paragraphes suivants. Elle illustre en particulier la décomposition d'un système complexe et ses interactions avec son environnement.

[1] International Standard Organisation
[2] Electronic Industries Association

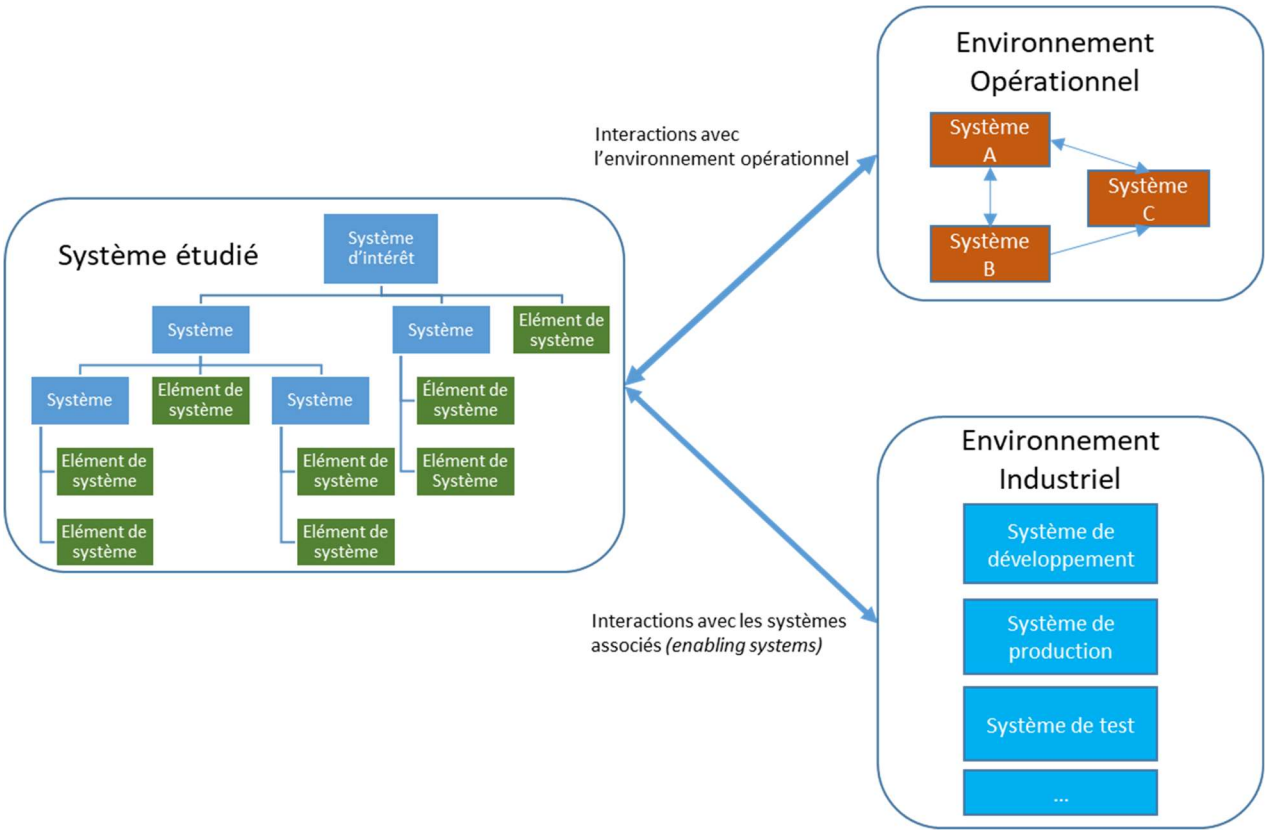

Figure 1 : Arborescence d'un système complexe et ses systèmes associés (enabling systems)

On constate notamment que le système d'intérêt (objet de l'étude) est composé de différents éléments qui eux-mêmes sont décomposés en éléments. Il est important de noter que cette arborescence est définie par l'architecture système pour satisfaire un besoin. En filigrane, la composition du système peut varier en fonction des phases de vie et en fonction des missions du système. De la même façon, l'écosystème dans lequel le système s'insère/est déployé peut-être évolutif en fonction des phases de vie.

Enfin, la norme introduit la notion de "enabling systems" (systèmes associés) qui sont les systèmes permettant au système objet de l'étude de réellement exister, cf. Figure 1. Par exemple, en supposant que le système soit un véhicule, on trouvera parmi les "enabling systems", les systèmes de conception, l'usine de fabrication qui en elle-même revêt un caractère de complexité…

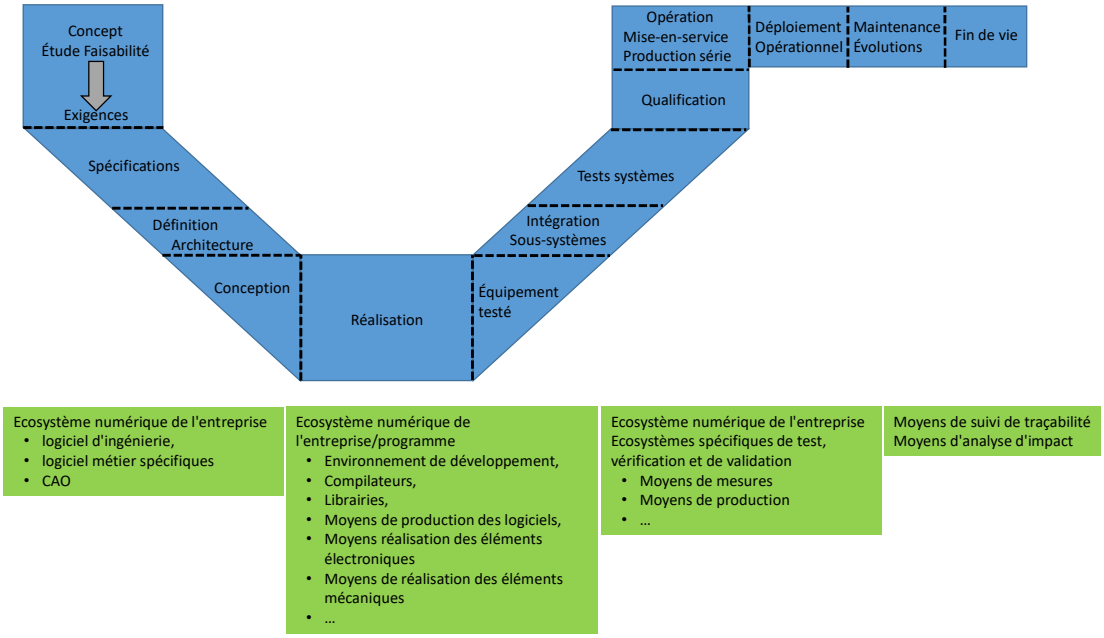

Figure 2 : Principales phases de vie d'un système et typologie de moyens associés

- **Approche Bottom-up :** Dans cette approche, on part des analyses de risques réalisées sur des constituants du système (sous-systèmes, équipements, …) qui peuvent directement identifier des composants cyber-critiques.

Dans un premier temps, il est proposé de concentrer les travaux sur le système d'intérêt, donc de ne pas traiter les « enabling systems ». Par contre, le présent document aborde l'ensemble des phases du cycle de vie du système. En effet, dans certains cas le niveau de criticité cyber de certains composants peut varier selon la phase du cycle de vie.

3 Exploitation et élaboration des listes de composant critiques

3.1 Exploitation des listes

Les listes fournies par les industriels seront concaténées et exploitées par la DGA. Cette liste ne sera pas rediffusée en l'état et seules des informations anonymisées pourront être diffusées.

La définition utilisée pour les composants cyber-critiques dans le présent document (cf le chapitre 2) montre bien qu'on analyse le composant dans l'environnement du système d'arme considéré. Il est important de noter que la présence d'un composant dans une liste de CCC ne constitue pas a priori un jugement de valeur sur ce composant. Notamment, le fait qu'un composant soit dans la liste ne signifie pas qu'il est vulnérable ou robuste d'un point de vue cybersécurité. Sa présence dans une liste ne doit donc pas être utilisée comme critère de choix.

L'exploitation de ces listes par la DGA vise à améliorer le niveau de protection contre le risque "cyber", suivant trois axes :

- **Orientations technologiques** : l'analyse des CCC peut permettre, par exemple, d'orienter des travaux de veille ou d'expertise sur des composants souvent signalés comme critiques, ou de proposer le développement de nouveaux composants souverains ou maîtrisés,
- **Traitement des vulnérabilités :**
    a. Si une vulnérabilité est découverte sur un composant, soit par des actions de veille ouverte soit à travers des travaux d'évaluation, l'information peut être envoyée vers les industriels ayant déclaré ce composant comme critique, et ceci en respectant les éventuels accords de confidentialités existant entre les différents acteurs industriels ou étatiques et les fabricants des composants critiques,
    b. La liste peut aussi permettre d'identifier rapidement les SA où le composant est considéré comme critique et donc de pouvoir faire un premier état des lieux en cas d'identification d'une vulnérabilité importante sur un composant,
- **Partage de bonnes pratiques** : pour certains composants il peut exister des guides de configuration ou d'utilisation sécurisée qui pourraient être partagés entre les différentes parties, et ceci en respectant les éventuels accords de confidentialités existant entre les différents acteurs industriels ou étatiques et les fabricants des composants critiques.

Pour les activités d'ingénierie industrielle, en phase de conception, l'analyse de criticité cyber des composants pourra être un élément complémentaire pour réaliser des choix d'architecture (minimisation de la criticité).

3.2 Élaboration des listes

Dans les premières étapes de déploiement du guide, il est souhaitable que chaque industriel l'expérimente sur un exemple même réduit pour avoir un retour d'expérience sur la méthode décrite dans ce document. Cela pourra permettre de proposer des évolutions à la méthode ou au présent guide mais aussi de calibrer le temps nécessaire à leur élaboration.

En mode nominal, les travaux d'élaboration des listes de composants cyber critiques seront intégrés sous forme de prestation dans les futurs marchés soit sur des systèmes existants soit sur des systèmes futurs. La ou les listes de CCC seront alors des fournitures de ces marchés.

4 Méthode d'analyse et de réduction de périmètre

4.1 Introduction

Compte tenu de la taille et de la complexité des systèmes d'armes, il est nécessaire de disposer d'une méthode pour identifier les composants cyber critiques qu'il peut contenir. En effet, le

système peut avoir des formes différentes selon ses cas d'emploi et d'usage et donc tous les éléments ne sont pas forcément utilisés à tout instant, ces systèmes sont également composés de COTS dont il est parfois difficile de savoir ce dont ils sont faits : les ressources pour effectuer ce travail seraient importantes spécialement dans le cas de systèmes en MCO.

Il est donc nécessaire de trouver une solution permettant d'appréhender la complexité du système de façon contrôlée à l'instar de ce qui est fait en ingénierie des systèmes (cf. ISO 15288 / EIA 632). Pour fixer une limite au niveau de décomposition système, il proposé de s'arrêter au niveau des constituants sur étagère, c'est-à-dire répondant à un besoin générique, pré conçus par le fournisseur et pas suivant des spécifications du donneur d'ordres (COTS, MOTS, GOTS, [3]…).

Pour mener cette analyse, il est fortement conseillé de disposer d'une analyse fonctionnelle du système et d'une analyse EBIOS RM. Cette dernière, notamment par la détermination des valeurs métiers, des événements redoutés, des scénarios stratégiques ou opérationnels permet en effet d'identifier clairement les chaines fonctionnelles et les constituants les plus critiques d'un point de vue cyber au sein d'un système.

4.2 Logique de l'analyse et réduction du périmètre

La méthode repose sur la combinaison de deux approches :

- Une approche top-down basée sur une analyse partant du système jusqu'à ses constituants,
- Une analyse bottom-up permettant d'identifier des composant cyber-critiques par conception.

4.2.1 Analyse top-down

La logique d'établissement de la liste des CCC repose sur une réduction du périmètre initial de l'étude se concentrant sur les fonctions critiques du système (chaînes fonctionnelles critiques qui auront été identifiées par la méthode EBIOS RM ou l'analyse fonctionnelle + critères de criticités retenus). Cette étude s'appuiera avantageusement sur la décomposition "PBS[4]" du Système d'Armes. Bien entendu, une fois les chaines fonctionnelles critiques traitées dans un premier temps, l'analyse pourra également prendre en compte des fonctions réputées moins critiques mais pouvant être source de menace dans un second temps. L'objectif étant de couvrir dans le temps tout le périmètre du système d'arme. L'analyse top-down, prend en compte les livrables existant du programme. Le but étant d'utiliser ces livrables pour mener cette analyse et en extraire les composants cyber-critiques.

[3] COTS : Commercial Off The Shelf, MOTS : Military Off The Shelf, GOTS : Government Off The Shelf)
[4] PBS : Product Breakdown Structure

Cette analyse sera récursive et doit s'appliquer à chaque niveau du PBS (Système → sous-système → équipement).

Pour des systèmes développés avec une analyse système type vues OTAN, il est conseillé d'utiliser les vues NSV[5] et NOV[6] du NAF[7].

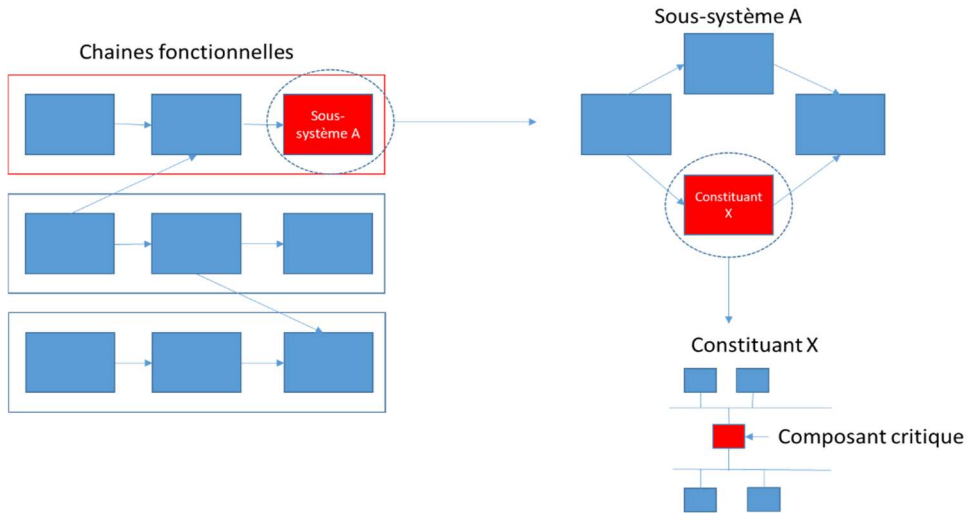

Figure 3 : Place d'un sous-système d'intérêt dans une chaîne fonctionnelle et décomposition du sous-système

4.2.1.1 Systèmes en cours de développement

Cette approche top-down est "naturelle" pour un système nouveau en cours de conception au travers la mise en place des PBS[8]et de toute l'arborescence système ainsi qu'au travers la mise en place de l'OBS[9] par la nomination d'ingénieurs en chef, de responsables de lots, d'autorités techniques, de responsable techniques/métier, d'architectes…

Le système à concevoir étant inconnu et le problème à adresser complexe, le but est d'utiliser une segmentation du système pour faciliter sa conception. Une des voies la plus utilisée pour éviter d'imposer la totalité des exigences à l'ensemble des éléments du système, consiste à identifier les phases de vie du système et notamment les phases de vie du système en opération. L'identification des phases de vie permet de décrire simplement les différentes configurations du système et permet également de décrire de façon plus ou moins macroscopique le comportement du système par rapport à son environnement.

On voit donc qu'intrinsèquement, la mise en place de cette structure indique la décomposition du système et chaque responsable produit sera alors à même de faire l'analyse sur son périmètre.

[5] NSV : NATO Systems View
[6] NOV : NATO Operation View
[7] NAF : NATO Architecture Framework
[8] Product Breakdown Structure
[9] Organisation breakdown structure

Le système est vu dans son écosystème avec les systèmes supports. EBIOS-RM utilise cette notion d'écosystème pour établir les scénarii stratégiques.

L'objectif est d'avoir un périmètre d'analyse "gérable" pour une analyse en un temps raisonnable. Il faut donc utiliser une description du système d'armes global de haut niveau pour aboutir à quelques sous-systèmes et ce par phase de vie afin de ne pas superposer tous les environnements à la fois.

Dans le cas d'un système en conception, et pour les composants identifiés cyber-critiques, il conviendra de mettre en place des spécifications possiblement renforcées dans les contrats de sous-traitance et convenir des moyens de contrôle de la supply chain et d'appliquer les modalités de vérification des livraisons de ces composants (au sens où l'on cherche à garantir l'absence d'éléments malicieux dans le composants cyber critique).

4.2.1.2 Pour un système déjà existant et déployé

Pour un système déjà en opération, toutes ces informations peuvent être présentes dans le dossier fonctionnel livré lors de la MSO[10] du système.

Cependant il peut être nécessaire de vérifier que la définition du système réel n'a pas évolué depuis sa MSO et dans le cas contraire de mettre à jour les documents d'architecture (différences entre les états "as delivered" par rapport aux états "as maintained" et "as operated").

De même une actualisation de l'analyse de risques (voire la réalisation d'une nouvelle analyse EBIOS RM) peut être nécessaire pour bien identifier les éléments critiques. Pour chacune de ces phases de vie, Figure 4, la délimitation du système est primordiale pour limiter le nombre d'éléments à analyser.

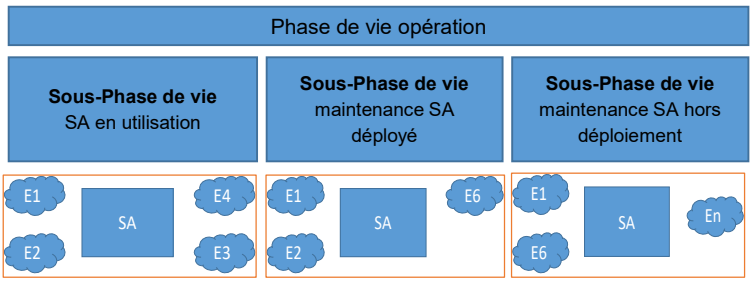

Figure 4 : Phases de vie associées au SA

Il est donc possible d'avoir une vision complète en "superposant" les différentes listes obtenues par phase de vie. Il est possible qu'une entité extérieure au périmètre d'analyse pour une phase de vie soit le sujet de l'analyse pour une autre. Exemple : un sous-système de maintenance serait exclu de l'analyse pour une phase d'utilisation militaire du système d'arme (emploi de la

[10] MSO : Mise en Service Opérationnelle

munition par exemple), alors que c'est le périmètre d'intérêt pour la phase de vie maintenance d'un système déployé.

D'autre part, on peut se baser sur les grands blocs du système d'arme. Par exemple, pour un missile, on peut d'emblée faire une analyse sur la munition elle-même et une analyse sur le système de mise en œuvre du porteur. Par la suite, on peut avoir une analyse du système de mise en œuvre lors de la constitution de la munition ou lors de son accostage sur le porteur. Enfin, le système de gestion de la mission de la munition peut également faire l'objet d'un troisième axe d'analyse.

Dans cette approche, il peut être demandé à chaque autorité technique, au titre des dossiers à livrer, une liste des composants critiques (sous la forme d'une annexe du DD[11] par exemple).

Dans certains cas, par exemple pour des systèmes de conception ancienne, l'ensemble de ces éléments peut être difficile voire impossible à obtenir en tout cas avec un effort raisonnable. La démarche devra alors être adaptée au cas par cas après discussion entre les parties prenantes étatiques et industrielles. L'approche bottom-up décrite ci-dessous pourra sans doute être plus appropriée .

4.2.2 Approche Bottom-Up

La seconde approche est basée sur une démarche "bottom-up" où pour chaque équipement, il est possible que les concepteurs identifient d'emblée ces composants cyber-critiques au vue de l'analyse de risque effectuée sur cet équipement dans le cas d'un système en cours de conception.

Dans le cas d'un système existant, la démarche bottom-up permet de prendre en compte des REX d'attaques ayant eu lieu envers le système d'arme en opération via une analyse du chemin d'attaque (cf. scénarii opérationnels d'EBIOS-RM). Dans ce cas, les éléments sur la chaine d'attaque sont à considérer comme potentiellement cyber critiques et notamment le composant ayant été attaqué en premier dans cette chaine (les autres étant soit des composants non critiques car ils ne sont que la conséquence de la première brèche, soit également des composants cyber-critiques s'ils ont été également attaqués alors qu'ils participent à la défense en profondeur).

Cette approche bottom-up permet de prendre en compte des alertes remontées par des CSIRT[12] ou des centres de veille Etatiques (CALID[13] par exemple), ou des informations de sources ouvertes issues des travaux de veilles technologiques et cyber.

[11] DD : Dossier de Définition
[12] CSIRT : Cyber Security Incident Response Team
[13] CALID : Centre d'Analyse et de Lutte Informatique Défensive

4.2.3 Prise en compte des mesures de réduction de risques

Les deux démarches font apparaitre une difficulté potentielle concernant des équipements qui seraient identifiés critiques dans les analyses et pour lesquels des mesures sont prises pour rendre le niveau de risque à un niveau acceptable pour le projet.

Plusieurs approches peuvent être retenues :

- On ne conserve dans la liste fournie à l'administration que les composants pour lesquels le niveau de risque reste, malgré les mesures prises, à un niveau jugé trop important pour le projet.

  Une autre option est de conserver dans une liste additionnelle (pas forcément fournie à l'administration) les composants initialement critiques dont la criticité a pu être revue à la baisse.

- On considère que si un composant a été jugé critique lors d'une étape de l'analyse il faut le conserver dans la liste au cas où les mesures ajoutées pour le protéger seraient contournées ou défaites par un attaquant, remettant le composant en première ligne. On se protège aussi ainsi de futures évolutions de conception qui pourraient modifier ou supprimer ces mesures, si on a perdu la raison pour laquelle elles ont été prévues.

5 Critères de criticité

La méthode de réduction de périmètre du chapitre précédent permet de délimiter le ou les périmètres d'analyse. L'application de critères permet d'identifier, parmi les composants potentiels, ceux qui sont les plus critiques. Les deux démarches peuvent être liées, une analyse de criticité macroscopique pouvant aider à la réduction de périmètre.

Ce chapitre présente une méthode de détermination de la criticité recommandée par le groupe de travail. L'utilisation d'une méthode commune permettra plus facilement d'analyser les résultats produits par les différents industriels. Il est possible d'utiliser une autre méthode sous réserve de fournir les éléments permettant d'assurer un minimum de cohérence avec celle décrite ici.

L'analyse de criticité d'un composant s'effectue selon trois dimensions :

- L'impact opérationnel
- Le niveau de confiance
- Le niveau de vulnérabilité potentiel

Chaque dimension comprend plusieurs sous-critères notés entre 0 et 3, la valeur 3 correspondant à une criticité maximum. Une note globale peut être calculée, si besoin avec l'emploi de

pondération entre critères. Il semble cependant plus intéressant de conserver le triplet de valeurs qu'une moyenne pondérée.

Un fichier Excel dont la forme est fournie en annexe 1 permet d'automatiser les calculs.

5.1 L'impact opérationnel

Cet impact comprend 4 composantes. La première est l'impact sur la mission, les trois autres, les impacts en confidentialité, intégrité et disponibilité.

Les valeurs possibles pour l'impact mission sont les suivantes :

pas d'impact immédiat	0
gênes mais les objectifs de la mission peuvent être remplis	1
certains objectifs de la mission ne peuvent plus être remplis	2
la mission ne peut plus être assurée	3

Pour analyser cet impact on considèrera l'impact direct sur le système étudié, sans prendre en compte l'importance relative de la mission dans une activité de plus haut niveau. Par exemple si une attaque cyber sur composant empêche un aéronef de décoller, si le SA étudié se limite aux aéronefs en question, le composant se verra affecter la valeur 3 (la mission ne peut plus être assurée) qu'il s'agisse d'une mission de routine ou d'une mission de guerre. On ne prendra pas non plus en compte le fait qu'il peut exister d'autres moyens par ailleurs…

Pour les impacts en CID, les notes sont les suivantes :

Impact confidentialité	pas d'impact	0
	accès à des données non ciblées	1
	Accès total aux données ou accès à des données ciblées	3
Impact intégrité	pas d'impact	0
	modification de données non ciblées	1
	modification possible de toutes les données ou de données ciblées	3
Impact disponibilité	pas d'impact	0
	pertes temporaires de services	1
	pertes massive de services	2
	pertes totales de services	3

Quand on parle d'accès **total,** de modification de **toutes** les données, de pertes **totales**, il ne faut pas s'attacher forcément au sens littéral mais plutôt à l'idée de pertes ou de modifications massives.

Pour ces critères il est proposé de retenir le maximum des notes sur les trois critères. En effet un composant qui conduirait à une perte totale de service (note 3) est plus critique qu'un composant qui aurait trois notes à 1.

La note finale pour la dimension "impact opérationnel" sera la somme de l'impact mission et du max des impacts en CID, elle peut donc varier entre 0 et 6.

Note finale « impact opérationnel » = {Impact Mission} + {Max (C, I, D)}.

5.2 Le niveau de confiance

Pour tenter d'objectiver cette notion de confiance qui peut être vue comme très subjective, on propose deux sous critères :

- Le niveau d'assurance sécurité du composant
- Le niveau de contrôle et de souveraineté du fournisseur

Le niveau d'assurance sécurité peut prendre les valeurs suivantes :

réalisé à façon par un opérateur de confiance et évalué	0
avec évaluation de sécurité par un laboratoire indépendant	1
avec évaluation fonctionnelle	2
sur étagère	3

Pour le niveau de contrôle et de souveraineté du fournisseur, les valeurs sont dérivées de la méthode EBIOS RM :

Filiale du groupe donneur d'ordre, industriel de la défense (France), ou partenaire historique.	0
Informations sur une conduite généralement éthique du prestataire, de ses parties prenantes et de son écosystème.	1
Faible niveau de connaissance du prestataire, de ses parties prenantes et de son écosystème	2
Connaissance étendue de pratiques répréhensibles du prestataire, de ses parties prenantes et de son écosystème (risque d'espionnage industriel, d'ingérence étatique).	3

La note globale est obtenue par addition des deux critères et peut donc varier entre 0 et 6.

Note finale « Niveau de confiance » = {niveau d'assurance sécurité du composant} + {niveau de contrôle et de souveraineté du fournisseur}

5.3 Les vulnérabilités potentielles

L'objectif n'est pas ici de prendre en compte les vulnérabilités réelles du composant, ce qui serait trop complexe et trop long mais plutôt la facilité d'exploitation des vulnérabilités potentielles à travers deux critères :

- Le vecteur d'attaque ou l'exposition
- La complexité de mise en œuvre

Pour le vecteur d'attaque on prendra les valeurs suivantes :

besoin d'un accès physique au système	0
accès distant possible via un système contrôlé	1
accès à distance	2
accès depuis le domaine public	3

Pour la complexité de mise en œuvre :

pas "d'exploit" connu	0
exploits non publics	1
exploits publics documentés	2
exploits publics documentés et outillés	3

Ce critère de criticité doit bien entendu être estimé en fonction des informations disponibles. Le fait qu'il n'existe pas d'exploits connus sur un composant ne signifie pas qu'il est exempt de vulnérabilités mais simplement que celles-ci ne sont pas ouvertement disponibles, ce qui potentiellement rend la tâche de l'attaquant plus compliquée.

La note globale est obtenue par addition des deux critères et peut donc varier entre 0 et 6.

Note finale « Vulnérabilités potentielles » : {vecteur d'attaque ou l'exposition} + {complexité de mise en œuvre}

5.4 Tri par criticité

Une fois les valeurs estimées dans les trois dimensions indiquées ci-dessus, plusieurs méthodes sont possibles pour trier les composants par criticité.

- **Méthode 1** : somme pondérée des trois valeurs [impact opérationnel], [confiance] et [vulnérabilité]. Les composants les plus critiques ont la valeur la plus élevée. Concernant les pondérations, il est proposé de prendre 3 pour l'impact opérationnel, 1 pour la confiance, et 2 pour la vulnérabilité

- **Méthode 2** : projection sur deux axes : [impact opérationnel] d'une part, [confiance] et [vulnérabilité] de l'autre. Les composants les plus critiques sont alors dans le quadrant supérieur droit.
- **Méthode 3** : toute autre méthode d'analyse multicritères.

Chaque méthode peut avoir son intérêt et il est donc préconisé de conserver les valeurs des trois composantes pour permettre une analyse ultérieure selon plusieurs filtres.

À titre d'illustration, on peut aussi utiliser un graphique de type "radar" pour afficher les différentes valeurs : dans le cas fictif de la Figure 5, le composant 1 apparait comme étant le plus critique.

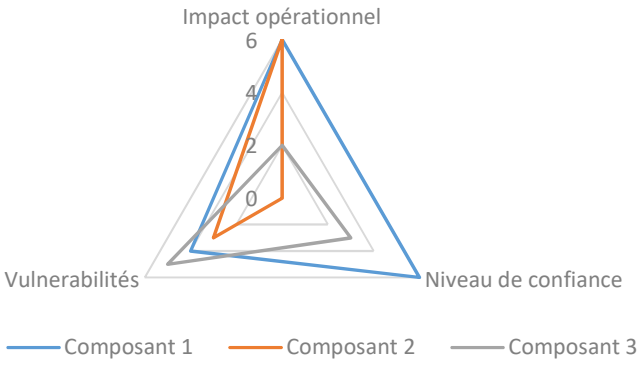

Figure 5 : Représentation 'radar'

6 Format de liste

Il est proposé de fournir la liste des composants critiques d'un système d'armes sous forme d'un fichier Excel. Pour permettre une exploitation aisée, il est recommandé d'utiliser un format commun, même si tous les champs de sont pas renseignés. Cette liste peut être classifiée si nécessaire.

L'Annexe 2 propose une liste de champs.

7 Suivi des versions

Version	Date	Commentaires
V1	28/10/2022	Version initiale

8 Annexe 1 : exemple de feuille notation des composants cyber-critiques

Coefficients	impact ops	3
	confiance	1
	vulnérabilité	2

				Composant 1	Composant 2	Composant 3
Impact opérationnel	impact mission	pas d'impact immédiat	0	3	3	1
		gênes mais les objectifs de la mission peuvent être remplis	1			
		certains objectifs de la mission ne peuvent plus être remplis	2			
		la mission ne peut plus être assurée	3			
	Impact confidentialité	pas d'impact	0			1
		accès à des données non ciblées	1			
			2			
		Accès total aux données ou accès à des données ciblées	3			
	Impact intégrité	pas d'impact	0			1
		modification de données non ciblées	1			
			2			
		modification possible de toutes les données ou de données ciblées	3			
	Impact disponibilité	pas d'impact	0	3	3	1
		pertes temporaires de services	1			
		pertes massive de services	2			
		pertes totales de services	3			
	Total	{Impact Mission} + {Max (C, I, D)}.		**6**	**6**	**2**
Niveau de confiance	Assurance sécurité du composant	réalisé à façon par un opérateur de confiance et évalué	0	3	0	1
		avec évaluation de sécurité par un laboratoire indépendant	1			
		Avec évaluation fonctionnelle	2			
		sur étagère	3			
	Niveau de contrôle et de souveraineté du fournisseur	Filiale du groupe donneur d'ordre, industriel de la défense (France), ou partenaire historique.	0	3	0	2
		Informations sur une conduite généralement éthique du prestataire, de ses parties prenantes et de son écosystème.	1			
		Faible niveau de connaissance du prestataire, de ses parties prenantes et de son écosystème	2			
		Connaissance étendue de pratiques répréhensibles du prestataire, de ses parties prenantes et de son écosystème (risque d'espionnage industriel, d'ingérence étatique).	3			
	Total	{niveau d'assurance sécurité du composant} + {niveau de contrôle et de souveraineté du fournisseur}		**6**	**0**	**3**
Vulnérabilités	Vecteur d'attaque	besoin d'un accès physique au système	0	3	3	2
		accès distant possible via un système contrôlé	1			
		accès à distance	2			
		accès depuis le domaine public	3			

	Complexité	pas d'exploit connu	0	1	0	3
		exploits non publics	1			
		exploits publics documentés	2			
		exploits publics documentés et outillés	3			
	Total	{vecteur d'attaque ou l'exposition} + {complexité de mise en œuvre}		**4**	**3**	**5**
	total général			**5,3**	**4**	**3.2**

9 Annexe 2 : liste des champs

- MOI
- **Programme** (tel que connu par la DGA)
- **Sous-système** (selon le PBS)
- Identification du composant *(nom commercial)*
- **NNO** (numéro de nomenclature OTAN), **CPE** (Common Platform Enumeration) si existant
- Numéro d'article
- Référence
- Fournisseur
- Date d'introduction dans la liste
- Notes de criticité :
- Impact opérationnel
- Niveau de confiance
- Vulnérabilités