MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Guide pour la détermination des SI névralgiques

2022\CYBER\3\NP

Version : 1.0

Octobre 2022

Table des matières

1 Introduction

Le terme de SI névralgiques est utilisé dans le présent document, pour qualifier des systèmes qui sont à la fois critique d'un point de vue cyber mais aussi exposés à la menace cyber.

L'objectif de ce travail d'identification de SI névralgiques est de pouvoir mettre en place des mesures de protection appropriées pour des SI importants d'un point de vue cyber (car pouvant avoir des conséquences sur des systèmes d'armes par effet direct ou indirect) mais qui ne rentrent pas ou mal dans les catégories existantes :

- Les SIIV qui sont identifiés par un processus très formel et auxquels sont associés des mesures de sécurité de haut niveau difficilement généralisables.
- Les SI classifiés ou sensibles pour lesquels il existe aussi des cadres réglementaires mais qui mettent plus l'accent sur la confidentialité que sur la disponibilité ou l'intégrité qui sont des dimensions au moins aussi importantes pour les SA.

Les SI névralgiques peuvent donc couvrir tous les niveaux de sensibilité (NP, DR, S, TS) et n'intègrent pas les SIIV. Ils ne sont volontairement pas associés à un nouveau corpus réglementaire existant ou législatif spécifique mais leur sécurisation devra être basée sur une analyse de risques dédiée.

Ce document vise donc à couvrir l'ensemble de ces sujets :

- Comment identifier et prioriser les SI névralgiques ?
- Quelle méthode et quels éléments prendre en compte pour les analyses de risques ?
- Quelle démarche pour leur sécurisation ?
- Comment prendre en compte dans les contrats l'identification initiale et le suivi dans le temps ?

2 SI névralgiques

La définition retenue au sein du présent document est la suivante :

Un système d'information névralgique est un SI participant à la conception, la réalisation, la validation, l'entretien ou la production d'un système d'armes et dont la compromission par un attaquant pourrait produire sur le système d'armes des impacts jugés inacceptables.

Le terme névralgique a été choisi pour tenir compte de la criticité intrinsèque du système mais aussi de son exposition, afin de prioriser les travaux sur les systèmes les plus vulnérables. Cette démarche vient en complément des démarches existantes comme les SIIV par exemple. Il en résulte donc que les SIIV sont exclus de cette analyse des SI névralgiques.

Dans un premier temps, une typologie des systèmes a été réalisée afin de lister les catégories de systèmes concernés, mais aussi pour définir des priorités en identifiant les types de systèmes paraissant les plus à risque. Cette typologie est présentée en détail en Annexe 1 : Typologie des SI.

Ensuite, une grille d'évaluation a été proposée pour définir les critères de criticité et d'exposition. Le détail de cette grille est présenté en Annexe 2 : Critères de criticité et d'exposition.

Il faut noter que cette méthode est fournie à titre indicatif et qu'elle peut être adaptée ou remplacée par une méthode propre à chaque industriel.

3 Sécurisation des SI névralgiques

3.1 Menaces

Par définition les SI névralgiques sont potentiellement visés par des menaces ciblées de sources étatiques, mais en fonction du domaine il faut aussi considérer les sources de risques (SR) de type terroriste, activisme idéologique et crime organisé, ainsi bien sûr que toutes les menaces non ciblées.

3.2 Analyse de risques

Il est indispensable de mener une analyse de risques, en utilisant la méthode EBIOS RM sur chaque SI névralgique. Il est important de noter qu'une analyse de risques pertinente demande la mobilisation d'un ensemble de compétences variées, qui peuvent être différentes selon les ateliers, mais qui dépassent très largement les compétences purement cyber. Il est notamment indispensable que les entités « métiers » participent à l'analyse de risques. Le guide EBIOS (https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf) propose une liste type de participants pour chaque atelier. Il est utile de définir un RACI en début d'analyse de risques pour identifier les acteurs appropriés au sein de l'entreprise. Si on résume les participants aux différents ateliers :

Atelier 1 : cadrage et socle de sécurité	Direction, DSI, métiers, RSSI (au sens industriel), privacy

Atelier 2 : source de risque	Direction, métiers, sureté et CERT pour définir les objectifs visés RSSI pour définir des sources de risques , avec le soutien éventuel d'un expert SSI
Atelier 3 : scénarios stratégiques	Métiers, architectes fonctionnels, RSSI, experts cyber (pentesteurs)
Atelier 4 : scénarios opérationnels	RSSI, experts cybers (pentesteurs), architectes/experts IT
Atelier 5 : traitement du risque	Direction, DSI, métiers, RSSI

A l'issue de l'atelier 1, de premières mesures de sécurité peuvent être identifiées car issues de la réglementation applicable ou de la politique de sécurité interne.

Le déroulement des ateliers 4 et 5 s'effectue en général de manière concomitante. En effet, l'identification de scénarios opérationnels permet naturellement de réfléchir aux mesures qui permettent de les bloquer. En sortie du travail d'analyse de risques on obtient ainsi des scénarios de risques mais aussi un plan de réduction de ces risques.

3.3 Référentiel de mesures de sécurité

Il n'existe pas de référentiel spécifique pour les SI névralgiques. En effet :

- Selon leur nature, les SIN peuvent déjà relever de réglementation existantes (sensible, classifié, …) qui imposent déjà leur propre référentiel.
- Les référentiels les plus aboutis pour prendre en compte la panoplie des risques pesant sur les SIN sont les référentiels des SIIV ou la déclinaison française de NIS. L'application de ces référentiels consisterait à transformer les SIN en SIIV, ce qui est exclu.
- Les SI névralgiques sont de nature très hétérogène avec des besoins de sécurité qui peuvent être très différents, des technologies très variables parfois difficiles à faire évoluer.
- Les contextes réglementaires ou normatifs sont très différents selon les industriels (national / international, militaire / dual, …).

.

Cette réflexion sur les référentiels vient s'intégrer dans des travaux plus larges, sous pilotage étatique dans un premier temps, visant à définir de nouveaux référentiels :

- pour mieux intégrer les évolutions réglementaires,
- avec la volonté de simplifier le corpus réglementaire existant,
- pour définir des alternatives au initiatives internationales (CMMC, DCPP, …).

3.4 Principes de sécurisation des SIN

La conséquence des travaux d'analyse des différents référentiels est qu'en l'état, la sécurisation des SIN ne pourrait pas se faire en appliquant un référentiel unique.

Les principes suivants ont été retenus :

- Les SI névralgiques doivent suivre un processus d'homologation
- Le processus d'homologation doit s'adosser à des référentiels partagés et validés par le Minarm, à déterminer par chaque industriel en accord avec le MinArm : référentiel SSI de l'entreprise (ISO, PSSI opérateur, NIS, …), référentiels liés à la sensibilité du SI (IGI1300 ou II901), …
- Chaque opérateur devra décrire la démarche d'homologation de ses SIN dans son référentiel cybersécurité interne en précisant le ou les référentiels de sécurité utilisés.

Ces principes seront mis en œuvre chez les industriels lors de l'exécution de nouveaux contrats, par des travaux de sécurisation des SI identifiés comme névralgiques correspondant à des clauses contractuelles dédiées.

4 Management du risque sur les SI névralgiques

Le travail d'identification initiale des SIN pourra être intégré dans les futurs marchés à travers une clause dédiée, la liste des SIN devenant à ce titre une fourniture du contrat. Au cours de la vie d'un programme, lorsqu'un industriel doit mettre en place un nouveau SI, une analyse de risques, utilisant en entrée des éléments pertinents de l'analyse de risques du SA permettra de déterminer si le SI en question est un SIN ou pas. La liste des SIN névralgiques peut ainsi évoluer selon les phases du programme. La fréquence des échanges entre industrie et administration pour la mise à jour des SIN pourra être définie dans les clauses contractuelles et/ou entrer dans les échanges réguliers sur le niveau de sécurité ou le suivi des homologations.

Les annexes de sécurité des marchés seront elles aussi adaptées pour y intégrer les SIN et lister les attendus tels que décrits au §3.4 Principes de sécurisation des SIN (homologation, …).

L'identification des SIN devra être répercutée dans les contrats de sous-traitance, lorsque cela a un sens au vu des objectifs visés.

5 Liste des acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Informations
CMMC	Cybersecurity Maturity Model Certification
COMCYBER	COMmandement de la CYBERdéfense
DCPP	Defence Cyber Protection Partnership
DR	Diffusion Restreinte
DRSD	Direction du Renseignement et de la Sécurité de la Défense

EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
GT	Groupe de Travail
IGI1300	Instruction Générale Interministérielle n° 1300
II901	Instruction Interministérielle 901
ISO	International Organization for Standardization
LPM	Loi de Programmation Militaire
MOI	Maître d'Œuvre Industriel
MinArm	Ministère des Armées
NIS	Network and Information Security
NP	Non Protégé
OV	Objectif Visé
PSSI	Politique de Sécurité des Systèmes d'Information
RM	Risk Manager
RACI	Responsible Accountable Consulted and Informed
RETEX	Retour d'Expériences
SA	Systèmes d'Armes
S	Secret
SI	Système d'Informations
SIN	Système d'Informations Névralgique
SIIV	Système d'Informations d'Importance Vital
SR	Source de Risques
TS	Très Secret

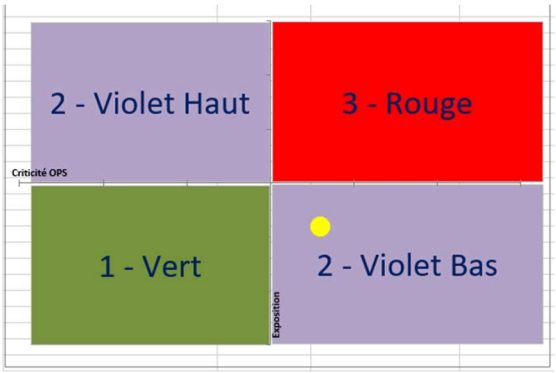
6 Annexe 1 : Typologie des SI

Typologie	Glossaire	Priorité
SI de développement des logiciels et microgiciels Fonctionnel : Développement logiciels et microgiciels	Ce type désigne les SI servant au développement (spécification, conception, codage, test, validation) des logiciels ou microgiciels utilisés dans les systèmes d'armes. Cela peut-être aussi bien un logiciel développé pour un système de soutien comme une PC de maintenance, ou un microgiciel embarqué dans une conduite de tir, un missile ou un moteur ou les modèles de simulation	P1
Moyen portable de maintenance et test Fonctionnel : Diagnostique et maintenance de SA	Ce type désigne les systèmes numériques servant à tester le bon fonctionnement des systèmes d'armes. Ils peuvent être utilisés en phase de maintien en condition opérationnelle mais aussi avant livraison aux armées.	P1
Plate-forme d'intégration ou validation Fonctionnel : Intégration et validation du SA	Ce type désigne les systèmes numériques servant à intégrer ou valider un nouveau développement de composant logiciel, électronique ou mécanique d'un système d'armes. Les plates-formes sont souvent hybrides, constituées de vrais composant du système d'armes, de composants émulés et de systèmes de stimulation et de mesure.	P1
Systèmes de livraison logiciels Fonctionnel : Livraison logiciel		P1
Banc de chargement Fonctionnel : Chargement logiciels ou configuration	Ce type désigne les systèmes numériques servant à la vérification de la configuration des logiciels et microgiciels, et à leur chargement dans les systèmes d'armes.	P2
Banc de test composant Fonctionnel : Diagnostique de composants	Ce type désigne les systèmes numériques servant à valider le bon fonctionnement d'un composant d'un système d'arme. Ils peuvent être utilisés en phase de maintien en condition opérationnelle mais aussi avant livraison aux armées.	P2
SI de conception et d'industrialisation Fonctionnel : Conception et industrialisation de pièces (mécaniques ou électroniques)	Ce type désigne les SI servant à la conception numérique des pièces mécaniques ou électroniques composant les systèmes d'armes, ainsi qu'aux machines et aux processus servant à les fabriquer (PLM, de CAO, calcul, …)	P1/P2

Typologie	Glossaire	Priorité
SI de production Fonctionnel : Production et assemblage	Ce type désigne les SI industriels servant à la fabrication et l'assemblage des systèmes d'armes. Cela comprend aussi bien les machines-outils que les systèmes d'information industriels servant à les contrôler. Il comprend les systèmes de métrologie utilisés lors de ces phases, les systèmes de planification des approvisionnements, des fabrications et des stocks (ERP, MES,...).	P1/P2
Moyens d'essai	Moyen de surveillance, de mesure, de communication avec les moyens sous tests (avions, navires, ...). Moyens d'exploitation des mesures, ...	P3
SI d'ingénierie système Fonctionnel : Ingénierie système	Ce type désigne les SI participant au travaux d'ingénierie système des systèmes d'armes : gestion des besoins du client, gestion des exigences fonctionnelles, décomposition fonctionnelle, gestion des spécifications fonctionnelles, gestion de programme,...	P3
Systèmes coopérants Fonctionnel : Fonction coopérante au bon fonctionnement ou à la maintenance du SA	Ce type désigne les systèmes de gestion d'infrastructure générale comme la gestion technique des bâtiments (GTB) et gestion technique centralisée (GTC) sur un périmètre plus large (par exemple : air comprimé, carburant, ...). Ce type désigne également les SI utilisé dans l'environnement d'un SA et pouvant avoir un impact sur la disponibilité d'un SA (exemple : SIL du SA permettant la gestion des stocks de pièce et des flux de réparation entre une MOI et les forces).	P4
Plate-forme de référence Fonctionnel : Diagnostique par reproduction d'évènements non conforme sur le SA	Ce type désigne un système représentatif du système d'arme ou d'une partie du système d'arme. Comme les plates-formes d'intégration ou de validation il est souvent hybride. Chez les industriels, souvent la même chose que les plate-forme d'intégration ou de validation.	P4
Moyens de formation Fonctionnel : formation	Simulateurs utilisés pour la formation.	P4
Intranet d'entreprise et SI transverse (SIC de l'entreprise) Fonctionnel : moyens supports aux SI métiers.	Ce type désigne soit les réseaux d'entreprise au sens fonctionnel (intranet bureautique, réseau de développement, réseau industriel) avec l'ensemble des systèmes techniques qui le font fonctionner (Active Directory, annuaire LDAP, SCCM, antivirus, ...), soit un SI identifié transverse à plusieurs fonctions mais dont la compromission par un attaquant pourrait produire sur le système d'armes des impacts jugés inacceptables.	Priorité variable en fonction des applications hébergées

7 Annexe 2 : Critères de criticité et d'exposition

Un SI névralgique étant un SI à la fois critique et exposé, la méthode proposée comprend deux parties, la détermination d'un niveau de criticité et la détermination d'un niveau d'exposition. Le résultat est matérialisé par deux valeurs qu'on peut représenter graphiquement de la manière suivante :



La zone rouge correspond aux SI à la fois critiques et exposés donc névralgiques. Les zones violettes peuvent contenir des SI à considérer comme névralgiques en seconde analyse.

Un fichier Excel est disponible pour aider à réaliser ce travail de catégorisation.

Les critères proposés sont les suivants :

Criticité opérationnelle :

- Dépendance des armées au Système d'Arme concerné
- Besoins SSI du SI de l'industriel au regard de l'impact sur le Système d'Arme.
- Complexité pour atteindre le Système d'Arme
- Sensibilité des données dans le SI de l'Industriel

Exposition :

- Ouverture du SI vers d'autres SI internes ou externes
- Données : échanges synchrones ou asynchrones
- Ecosystème : prestataires, hébergement, …
- Complexité du SI
- Localisation : par exemple exploitation possible ou pas des SPC
- Utilisateurs : nombre et sensibilisation

Pour chaque critère, des valeurs sont proposées dans des listes prédéfinies et associées à une note. La combinaison de ces notes permet d'obtenir une valeur pour chaque critère.

8 Suivi des versions

Version	Date	Commentaires
V1.0	28/10/22	Version initiale