RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

cnes
CENTRE NATIONAL
D'ÉTUDES SPATIALES

GUIDE D'HYGIÈNE CYBERSÉCURITÉ
DES SYSTÈMES ORBITAUX

Studio Graphique CNES, 2025-123

Préface

Lionel Suchet

Président Directeur Général
par intérim

Le rôle essentiel de l'espace dans le fonctionnement quotidien des activités individuelles, scientifiques, économiques et souveraines des États n'est plus contesté.

Ces dernières années, la numérisation de notre monde et l'arrivée de nombreux « nouveaux » acteurs ont considérablement fait évoluer les manières de concevoir, de construire, de lancer, d'opérer et d'utiliser un système orbital, et ce dans un contexte géopolitique où conflits et tensions sont de toute nature. C'est donc plus récemment que nous avons pu mesurer les conséquences de notre dépendance vis-à-vis de services, d'infrastructures et de systèmes spatiaux, notamment par l'observation de la forte augmentation en volume et en complexité des cyberattaques les visant.

Ainsi, l'enjeu stratégique que représente l'espace n'échappe plus à personne, et surtout pas aux acteurs mal intentionnés. Plusieurs cas dans l'actualité de ces dernières années ont démontré l'exposition des systèmes orbitaux et la capacité de certains acteurs malveillants à exploiter leurs vulnérabilités.

Ces nouvelles menaces nécessitent une réponse adaptée : on ne peut plus considérer nos systèmes spatiaux protégés par leur isolement ou par une technologie qui serait réservée à une poignée d'organisations.

C'est pourquoi le Centre National d'Études Spatiales, en complément des mesures déjà prises depuis de nombreuses années, s'est engagé dans une démarche d'anticipation en plusieurs temps pour contrer une menace floue et dissymétrique. Ce guide, rédigé en association avec nos partenaires industriels, institutionnels et académiques, est la première des étapes : les recommandations qu'il présente accompagnent la nouvelle Loi sur les Opérations Spatiales et, grâce à vos contributions, préparent nos futures activités, propres et sectorielles. Il est donc essentiel que ce recueil de bonnes pratiques éprouve le terrain et évolue pour répondre aux défis qui nous obligent.

Nous sommes convaincus que c'est ainsi que nous pourrons développer nos pratiques en cybersécurité spatiale, renforcer le positionnement de la France dans ce domaine, garantir l'efficacité et la pertinence de notre soutien aux activités spatiales de nos partenaires institutionnels et industriels, et amener le secteur spatial au meilleur niveau.

TERMES
DÉFINITIONS
ABRÉVIATIONS

Sigle / Abréviation	Définition
AIT	Assemblage, Intégration et Test
ANFR	Agence Nationale des Fréquences
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CCSDS	Consultative Committee for Space Data Systems
CERT	Computer Emergency Response Team
CESTI	Centres d'Evaluation de la Sécurité des Technologies de l'Information
CNES	Centre National d'Etudes Spatiales
COTS	Commercial Off The Shelf
CSIRT	Computer Security Incident Response Team
CSPN	Certification de Sécurité de Premier Niveau
CTI	Cyber Threat Intelligence
CVE	Common Vulnerability Exposure
DAST	Dynamic Application Security Testing
EAR	Export Administration Regulations
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager
EOL	End Of Life
EOS	End Of Support
EUSL	European Space Law
FIR	Force d'Intervention Rapide
HSM	Hardware Security Module
IDPS	Intrusion Detection and Prevention System
IGC	Infrastructure de Gestion des Clefs
IGI	Instruction Générale Interministérielle
IoC	Indicator Of Compromise
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ISP	Instruction de Sécurité Programme
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITU	International Telecommunication Union
KMS	Key Management Service
LOS	Loi relative aux Opérations Spatiales

LPM	Loi de Programmation Militaire
MCO	Maintien en Condition Opérationelle
MCS	Maintien en Condition de Sécurité
MFA	Multifactor Authentication
MINARM	Ministère des Armées
NIS	Network and Information Security
OT	Operational Technology
OTAR	Over-the-air-rekeying
PAS	Plan Assurance Sécurité
PCA	Plan de Continuité d'Activité
PGSC	Politique Générale de Sécurité et de Cybersécurité
PKI	Public Key Infrastructure
PPST	Protection du Patrimoine Scientifique et Technique
PQC	Post-Quantum Cryptography
PRA	Plan de Reprise d'Activité
PSSI	Politique de Sécurité des Systèmes d'Information
RETEX	Retour d'Expérience
RF	RadioFréquence
ROOT CA	Certificate Authority Root
RSSI	Responsable Sécurité des Systèmes d'Information
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SDR	Software-defined Radio
SDS	Software-defined Satellite
SI	Système d'Information
SIEM	Security Information Management System
SOC	Security Operation Center
SPC	Signaux Parasites Compromettants
SSA	Space Situational Awareness
STIX	Structured Threat Information Expression
TAXII	Trusted Automated eXchange of Indicator Information
TC	Télécommande
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
TM	Télémétrie
TRANSEC	Transmission Security
VPN	Virtual Private Network
ZRR	Zone à Régime Restrictif

Sommaire

01 INTRODUCTION

1.1 I CONTEXTE

La maîtrise du niveau de cybersécurité des systèmes orbitaux est aujourd'hui au cœur des discussions et des préoccupations des États. Depuis quelques années, il a été observé une accélération du nombre d'attaques ciblant les infrastructures spatiales. La guerre en Ukraine a confirmé cette tendance. Cet évènement, qui a été démarré par l'attaque d'un opérateur spatial, constitue une démonstration évidente de l'expansion du champ de conflictualité au domaine spatial.

Les premiers cas d'attaques de type cyber sur des systèmes orbitaux, recensés dans le domaine public, datent de la fin des années 1970. Le nombre moyen d'attaques connues par an est estimé à 5 jusqu'en 2020. Depuis l'année 2020, le nombre d'attaques publiquement référencé a connu une augmentation significative, avec plus de 46 cyberattaques en 2022, environ 80 attaques en 2023, et plus de 110 attaques identifiées au cours de l'année 2024.

La complexité de ces attaques a grandement augmenté ces dernières années, amenant les attaquants à s'intéresser de manière croissante à la disruption de missions spatiales, sur lesquelles reposent le bon fonctionnement des infrastructures critiques des États.

Les enjeux géopolitiques, économiques et technologiques, liés à la sécurisation de l'espace amènent les institutions à consolider un état de l'art réglementaire qui peut être considéré aujourd'hui comme fragmenté. Il est nécessaire d'offrir aux parties prenantes des systèmes orbitaux des recommandations et bonnes pratiques, à la fois pertinentes et suffisamment spécifiques, pour améliorer et homogénéiser le niveau de résilience de l'ensemble des acteurs formant l'écosystème spatial.

1.2 I OBJECTIFS & ENJEUX DU GUIDE

Le CNES met en place un guide d'hygiène cybersécurité à l'attention des acteurs impliqués, directement ou indirectement, dans le bon fonctionnement d'un système orbital. L'application de ces bonnes pratiques permettra d'assurer une protection minimale, de réduire le risque d'attaque ou de réduire l'impact d'une attaque avérée. Ce guide d'hygiène se fonde sur l'état de l'art en matière de bonnes pratiques. Il est inspiré de la littérature existante et a été amélioré grâce aux retours d'expérience fournis par des acteurs de l'écosystème spatial français.

Ce guide a vocation à suggérer un ensemble de bonnes pratiques aux parties prenantes d'un système orbital et n'est pas contraignant. Il doit être perçu comme un guide permettant de faciliter l'identification de mesures qui pourraient être mises en place par une organisation. Il conviendra à chaque acteur impliqué, directement ou indirectement, dans un système orbital, d'identifier les bonnes pratiques de ce guide qui lui sont utiles et applicables, afin d'améliorer son niveau de sécurité. Le guide se veut généraliste et ne prétend pas couvrir l'exhaustivité des besoins de sécurité des acteurs concernés.

Son application peut venir compléter ou enrichir l'application de règlementations nationales telles que la « Loi relative aux Opérations Spatiales » (LOS), ou européennes telles que la « Loi Spatiale Européenne » (EUSL) à venir.

Ce guide est aujourd'hui présenté dans sa première version. Il sera mis à jour régulièrement afin de refléter l'état de l'art en termes de bonnes pratiques et prendra en compte les retours des lecteurs entre deux versions du guide.

1.3 | PÉRIMÈTRE D'APPLICATION DU GUIDE D'HYGIÈNE

Le guide d'hygiène cybersécurité des systèmes orbitaux s'adresse à l'ensemble des acteurs de l'écosystème qui contribuent à l'opération ou à la conception des systèmes orbitaux. **Dans le cadre de ce guide, le "système orbital" est composé d'un ensemble de segments (segment spatial, segment sol, segment signal), des infrastructures et de l'ensemble des acteurs des chaînes de valeur et d'approvisionnement impliqués, directement ou indirectement, dans la bonne réalisation de la mission.** Les acteurs impliqués dans le segment utilisateur, bien qu'indirectement concernés, peuvent également identifier des bonnes pratiques applicables au sein de ce guide.

Les acteurs intervenant dans cet écosystème jouent des rôles différents, tels que l'opérateur, le constructeur et autre systémier ou intégrateur. Ces acteurs se reconnaissent parfois selon des typologies plus transverses telles que le New Space, les TPE/PME ou les acteurs majeurs industriels. Les bonnes pratiques identifiées dans ce guide sont génériques et applicables quelle que soit la typologie des acteurs.

Le cycle de vie d'un système orbital débute par une phase de conception et se termine par une phase de décommission. La durée du cycle de vie amène les acteurs intervenant sur chacune des phases à s'interroger sur leur niveau de sécurité. Ce guide concerne les 6 différentes phases d'un programme spatial, à savoir : Phase A (Conception, Design), Phase B (Développement, Intégration, Vérification et Validation), Phase C (Conception détaillée du système), Phase D (Réalisation et tests, AIT), Phase E (Transport, Préparation au lancement, Lancement, Mise à poste, Validation en orbite, Exploitation), Phase F (Maintien à poste, Réalisation de la mission, Fin de vie).

Le guide s'applique aux systèmes d'information des acteurs intervenant sur la chaîne opérationnelle du satellite allant des phases préliminaires de « design », jusqu'à l'opération et la fin de vie du satellite.

FIGURE 1 : **PÉRIMÈTRE DU GUIDE D'HYGIÈNE**

Ce guide se veut généraliste et propose des bonnes pratiques applicables à l'ensemble des systèmes d'information impliqués tout au long du cycle de vie d'un système orbital, que ce système soit orienté IT (Information Technology) ou OT (Operational Technology).

1.4 I GUIDE DE LECTURE

Ce guide d'hygiène sur la cybersécurité des systèmes orbitaux repose sur une liste de bonnes pratiques à mettre en œuvre. **Les bonnes pratiques sont regroupées par famille**. Un **ensemble de thématiques** a été identifié pour chaque famille.

Chaque famille se découpe de la façon suivante :

Description : Description générale et contextualisation de la bonne pratique.

Recommandation ou bonne pratique : Mesure permettant d'assurer un niveau de cybersécurité minimal du système orbital.

Document support (fichier excel) : tableur listant l'ensemble des bonnes pratiques identifiées dans ce guide. Il permet un suivi d'applicabilité et d'implémentation de chacune d'entre elles par phase du cycle de vie du système orbital.

Document annexe d'études de cas (document support fourni en annexe dans le cadre de la version 2 du guide) : Il s'agit d'illustrer, à l'aide d'exemples ou de scénarios, les conséquences liées à l'absence de mise en œuvre de bonnes pratiques. Cette description s'appuie généralement sur des cas de cyberattaques publiquement connus.

Dans le cadre de ce guide, **« l'organisation » désigne l'entité en charge de mettre en place les bonnes pratiques identifiées.** La réalisation d'une action peut se faire à différents niveaux (constructeur, opérateur, sous-traitant, fournisseur). Ce niveau de détail sera considéré dans une version ultérieure du guide.

02 GUIDE D'HYGIÈNE ET BONNES PRATIQUES

2.1 | MÉTHODOLOGIE D'ÉLABORATION DU GUIDE

La méthodologie appliquée pour **l'élaboration de ce guide s'est déroulée en 3 phases :**

1. **Compréhension de l'état de l'art réglementaire** par l'identification de toutes les recommandations nationales ou internationales connues.
2. **Phase d'entretiens avec les acteurs internes au CNES** impliqués dans les différentes phases du cycle de vie d'un système orbital.
3. **Atelier de réflexion collective** avec les acteurs externes au CNES afin de consolider les bonnes pratiques identifiées et de s'assurer de la complétude de la démarche et de la bonne compréhension des besoins provenant d'acteurs avec des positionnements différents.

2.2 | LISTE DES FAMILLES DE BONNES PRATIQUES

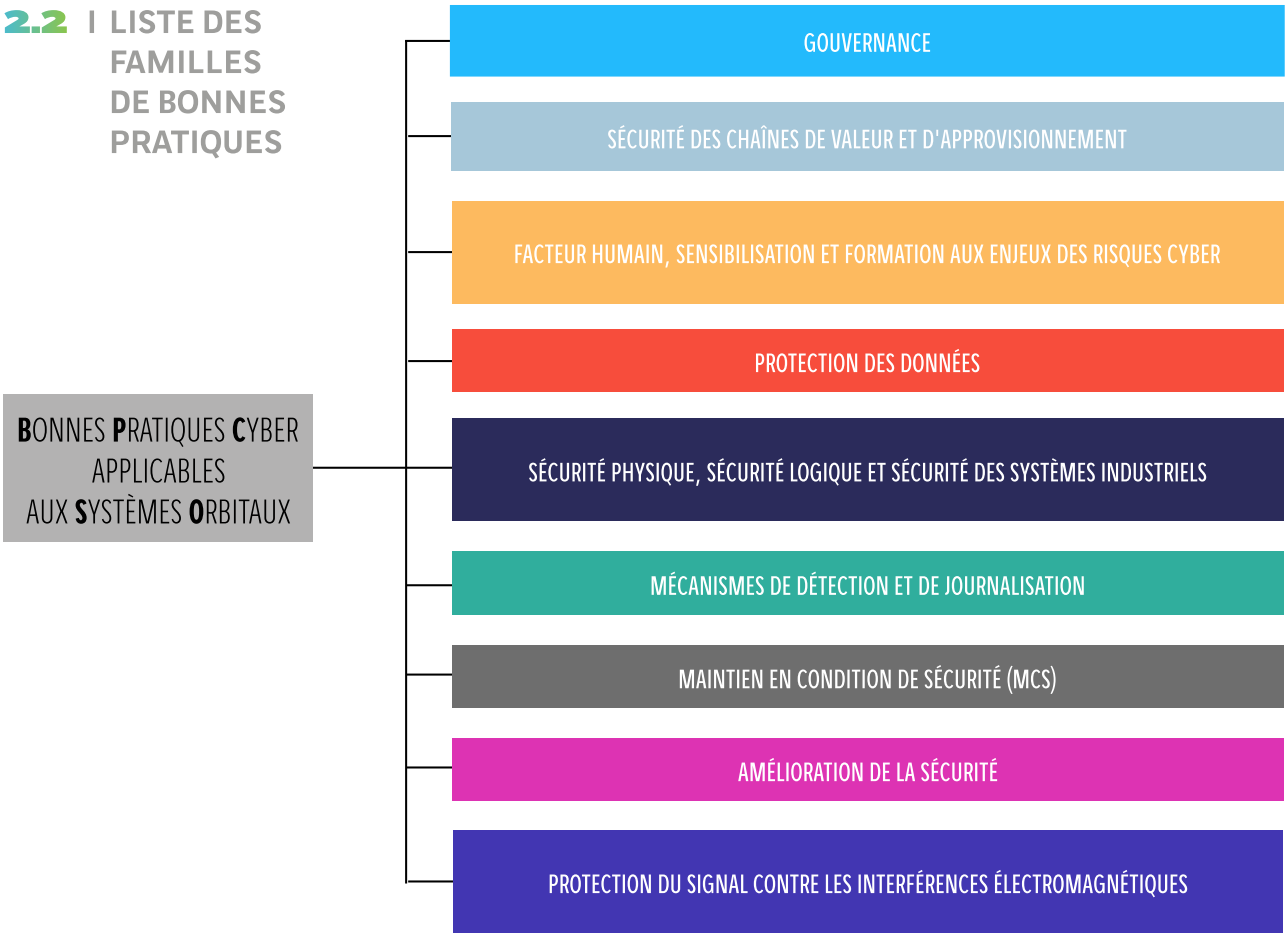


FIGURE 2 : **FAMILLES DE BONNES PRATIQUES**

2.3 I GOUVERNANCE

L'ANSSI rappelle que le risque numérique est devenu un risque stratégique pour les organisations. La gouvernance a pour objectif de fournir le cadre stratégique et organisationnel nécessaire pour anticiper, prévenir et répondre au risque numérique, dans les différentes phases d'un système orbital, de sa conception à son opération, et jusqu'à sa fin de vie.

Une bonne gouvernance du risque numérique passe par la mise en place d'une **structure organisationnelle avec des responsabilités claires et un budget dédié.** L'objectif est de définir la stratégie de sécurité numérique de l'organisation au travers d'une feuille de route, de s'assurer de la mise en œuvre d'une politique de sécurité du système d'information et de piloter la performance.

L'analyse de risque est un point de départ permettant l'identification d'une grande partie des mesures de sécurité à mettre en place. Elle peut s'appuyer sur la mise en œuvre d'une méthode d'analyse de risque notamment EBIOS Risk Manager.

Une **démarche d'homologation** d'un système d'information peut être un préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation. L'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque acceptable pour le système d'information considéré. L'homologation est délivrée par une autorité d'homologation.

La conformité réglementaire est un enjeu fort et demande une maîtrise des exigences imposées par un écosystème, un état ou un donneur d'ordre.

Maîtriser sa sécurité demande une adaptation quotidienne par des actions de prospectives permises par des **échanges avec l'écosystème** au travers de groupes de discussions tels que les CERT, CSIRT ou ISAC.

2.3.1 I STRUCTURE ORGANISATIONNELLE DE LA CYBERSÉCURITÉ

SYS-ORBIT-GOUV_100 : L'organisation **définit une structure organisationelle afin d'assurer la gouvernance cyber** et de sa bonne application. La gouvernance cyber consiste en l'ensemble des décisions que l'organisation doit prendre pour garantir la sécurité de ses systèmes d'information.

SYS-ORBIT-GOUV_101 : L'organisation **désigne les individus responsables de la sécurité de l'information**, qui incarneront et exprimeront les besoins de sécurité dans les comités décisionnels. Il convient de **définir précisément les rôles et responsabilités associés** (responsable de la sécurité des systèmes d'information, responsable de la sécurité produit, responsable stratégique, responsable opérationnel, auditeur interne, architecte sécurité des systèmes d'information des programmes, etc.). La structure organisationnelle de la cybersécurité peut différer en fonction de l'organisation concernée et des phases du cycles de vie du système orbital.

SYS-ORBIT-GOUV_102 : L'organisation **octroie un budget cybersécurité dédié à chaque projet, dont le montant est en cohérence avec les recommandations ou exigences réglementaires (techniques, opérationnelles et organisationnelles) applicables au SI.** Le budget prévu par l'organisation doit inclure des moyens financiers, matériels, logiciels et humains en phase avec les besoins identifiés par le projet.

2.3.2 I POLITIQUE DE SÉCURITÉ

SYS-ORBIT-GOUV_103 : Dans le cadre de sa gouvernance cyber, **l'organisation met en place une Politique de Sécurité des Systèmes d'Information (PSSI) qui reflète sa vision stratégique en matière de cybersécurité**. Cette **PSSI peut être déclinée** pour être adaptée à différents niveaux d'application : PSSI globale pour l'organisation, PSSI applicable aux partenaires ou sous-traitants, PSSI Exploitation applicable au contexte opérationnel du système orbital, PSSI Projet etc.

En phase avec la Politique Générale de Sécurité et Cybersécurité (PGSC) de l'organisation, la PSSI couvrira différents sujets tels que la protection des données, la formation du personnel, la gestion des accès et des identités, le chiffrement des données, les mécanismes de réponses aux incidents, la sauvegarde des données, l'exportation, la gestion de la chaîne d'approvisionnement et de valeur.

SYS-ORBIT-GOUV_104 : L'organisation **crée une cartographie de son patrimoine informationnel et la met à jour de manière régulière.** Selon le besoin, différentes cartographies du patrimoine informationnel peuvent être effectuées : cartographie de l'écosystème de l'entreprise sous la responsabilité du RSSI, cartographie orientée produit du ressort du responsable sécurité produit, cartographie orientée système orbital, cartographie orientée services support etc.

SYS-ORBIT-GOUV_105 : L'organisation **détermine le niveau de classification de son patrimoine informationnel en fonction du niveau de sensibilité des données** et en accord avec les recommandations et exigences applicables (PPST, LPM, IGI n°1300, II n°901).

SYS-ORBIT-GOUV_106 : L'organisation met en place une Instruction de Sécurité Programme (ISP) permettant de garantir la sécurité des informations échangées. Cette instruction comprend une annexe contenant le niveau de classification des informations et se déclinant en plan contractuel de sécurité qui couvre les échanges des différents systèmes d'information de l'organisation ou du système orbital.

2.3.3 | APPROCHE PAR L'ANALYSE DE RISQUE

SYS-ORBIT-GOUV_107 : L'organisation met en place **un processus de gouvernance des risques, basé sur une méthode d'analyse de risque conforme aux normes internationales (ISO27005 ou EBIOS Risk Manager par exemple),** en accord avec les recommandations des agences nationales ou internationales de sécurité. Il convient de protéger le contenu de l'analyse de risque et notamment les scénarios d'attaques identifiés ou les risques résiduels.

SYS-ORBIT-GOUV_108 : L'organisation cadre et définit le périmètre technique et métier du système d'information du système orbital concerné par l'analyse de risque. Elle possède une vision globale de son système d'information et est capable de le cartographier.

SYS-ORBIT-GOUV_109 : L'organisation évalue l'état actuel de la menace, les sources de risques et les objectifs visés concernant le système orbital à protéger.

SYS-ORBIT-GOUV_110 : Dans le cadre de cette démarche régulière d'analyse de risque, l'organisation **met en place un processus de veille quotidienne,** qui permet de surveiller et d'identifier les nouveaux risques. Cette veille régulière permet d'affiner les mesures mises en place.

SYS-ORBIT-GOUV_111 : L'organisation identifie des scénarios de risques qu'ils soient stratégiques ou opérationnels.

SYS-ORBIT-GOUV_112 : L'organisation met une place une démarche de traitement des risques identifiés (prévention, réduction, transfert, acceptation).

2.3.4 | DÉMARCHE D'HOMOLOGATION

SYS-ORBIT-GOUV_113 : Lorsque cela est nécessaire, l'organisation met en place une **démarche d'homologation** de ses systèmes d'information. L'homologation doit être adaptée aux enjeux de sécurité du système de l'organisation. L'organisation doit se rapprocher de l'autorité d'homologation compétente.

2.3.5 | CONFORMITÉ RÉGLEMENTAIRE

SYS-ORBIT-GOUV_114 : L'organisation **identifie les exigences règlementaires contraignantes applicables** en matière de cybersécurité. Il convient de s'intéresser notamment à la LOS (Loi relative aux Opérations Spatiales), à la LPM (Loi de Programmation Militaire), à la directive NIS2 (Network and Information Security) ou à la future loi spatiale européenne (European Space Law - EUSL).

SYS-ORBIT-GOUV_115 : L'organisation **implique les différentes parties prenantes sur les sujets de sécurité, notamment les opérateurs techniques des systèmes orbitaux**, afin d'assurer une cohérence globale et une acceptation des enjeux liés à la conformité réglementaire.

SYS-ORBIT-GOUV_116 : L'organisation **anticipe les questions relatives au contrôle à l'export** de ses données et documents, notamment pour les cas de double-usage (civil et militaire). Selon les **usages associés aux systèmes orbitaux, la portée extraterritoriale** des réglementations étrangères doit également être prise en compte (par exemple US ITAR ou EAR).

2.3.6 | GESTION DE CRISE ET RÉSILIENCE EN CAS D'INCIDENT

SYS-ORBIT-GOUV_117 : L'organisation **définit de manière anticipée les rôles et responsabilités** au sein de son équipe permettant le **retour à un fonctionnement nominal à la suite d'une crise**.

SYS-ORBIT-GOUV_118 : L'organisation met en place, en avance de phase, un ensemble de procédures permettant d'assurer sa **résilience et son retour à un fonctionnement nominal à la suite d'une crise**, avec notamment : un **PCA** (Plan de Continuité d'Activité) et un **PRA** (Plan de Reprise d'Activité).

SYS-ORBIT-GOUV_119 : L'organisation **prévoit la mise en place d'une équipe dédiée à la réponse à incident**, de type **CERT** interne (Computer Emergency Response Team) ou **FIR** (Force d'Intervention Rapide).

SYS-ORBIT-GOUV_120 : L'organisation anticipe la communication de crise et la posture publique à tenir en cas de crise afin d'atténuer ou de maîtriser **les impacts potentiels sur sa réputation et son image de marque.**

SYS-ORBIT-GOUV_121 : En cas d'attaque, l'organisation **informe les autorités compétentes** en fonction du niveau de sensibilité de ses activités (ex. : ANSSI, CNES, Ministère des Armées).

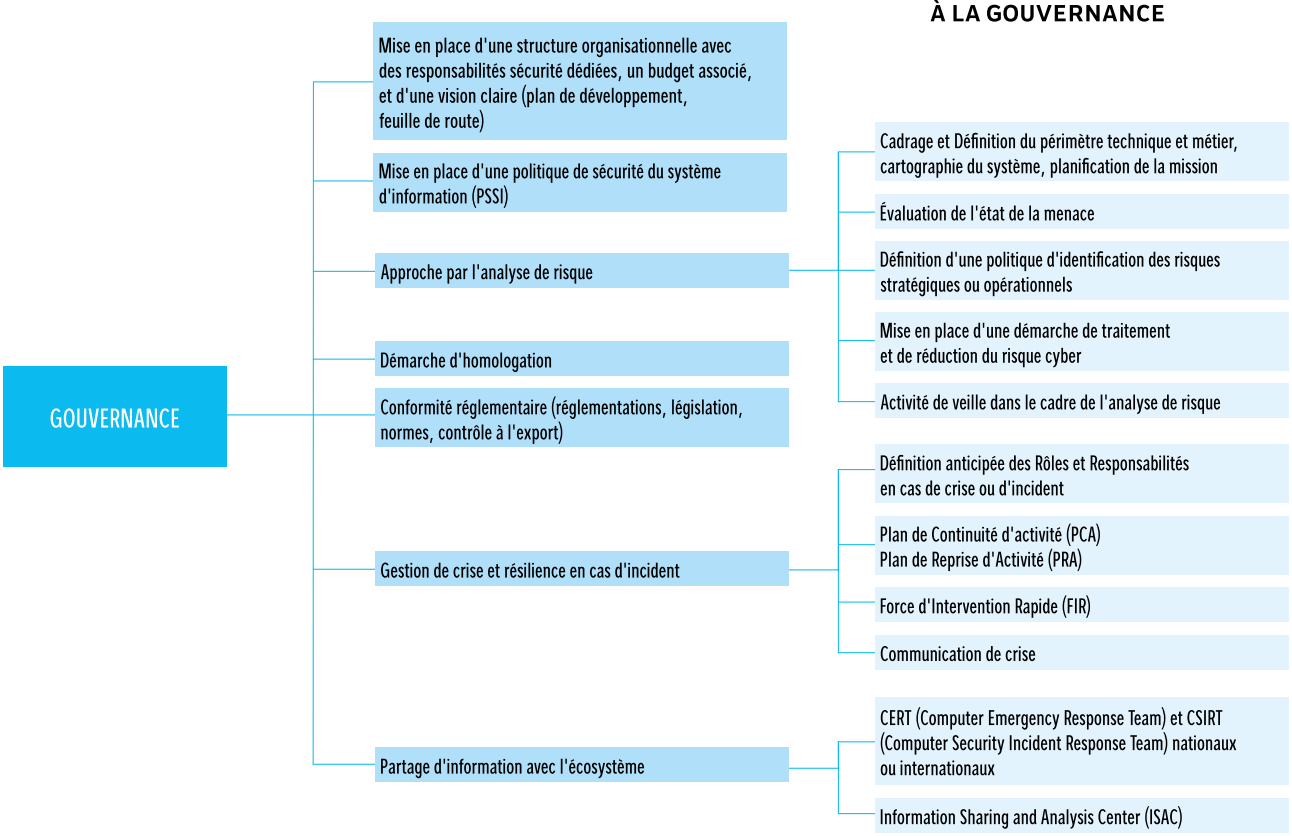
2.3.7 | PARTAGE D'INFORMATION AVEC L'ÉCOSYSTÈME

SYS-ORBIT-GOUV_122 : L'organisation s'implique et partage de l'information, des bonnes pratiques et des retours d'expériences (RETEX) au sein d'entités nationales ou internationales dédiées de type CERT, CSIRT ou ISAC. Il peut être intéressant de partager de l'information avec d'autres secteurs (aviation, maritime, bancaire etc.).

KOUROU VU PAR LE SATELLITE PLÉIADES

FIGURE 3 :

THÉMATIQUES ASSOCIÉES À LA GOUVERNANCE



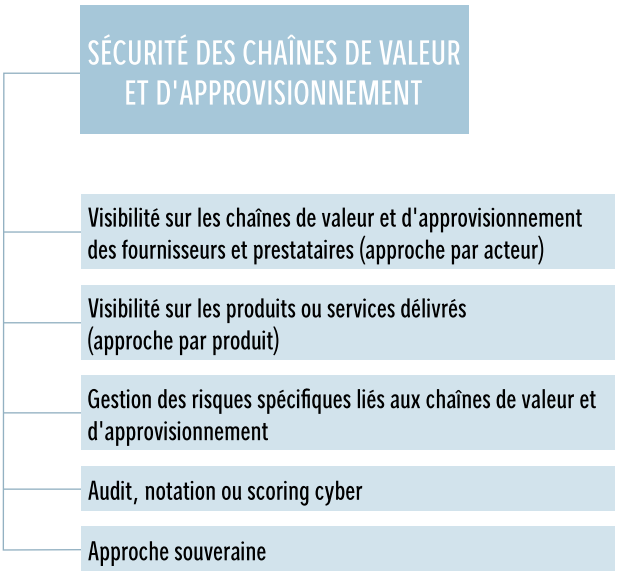
CENTRE SPATIAL GUYANAIS
VU PAR LE SATELLITE SPOT-6
©Airbus/, 2015

2.4 | SÉCURITÉ DES CHAÎNES DE VALEUR ET D'APPROVISIONNEMENT

Les chaînes de valeur et d'approvisionnement associées au développement et aux opérations d'un système orbital font intervenir un grand nombre d'acteurs, souvent répartis géographiquement.
La multiplicité des acteurs impliqués augmente la surface d'attaque et le niveau d'exposition à la menace cyber.
Parmi les nouveaux types d'attaques, on peut retrouver les risques d'espionnage ou de compromission d'un composant dans les phases amont du cycle de vie.

FIGURE 4 :

THÉMATIQUES ASSOCIÉES À LA SÉCURITÉ DES CHAINES DE VALEUR ET D'APPROVISIONNEMENT



La complexité croissante des chaînes de valeur et d'approvisionnement résulte de l'ouverture de la technologie utilisée par les systèmes orbitaux au secteur commercial et de l'intégration de technologies grand public, notamment avec l'utilisation des COTS.

2.4.1 | VISIBILITÉ SUR LES CHAÎNES DE FOURNISSEURS ET PRESTATAIRES

SYS-ORBIT-CHAINE_200 : L'organisation **cartographie ses chaînes d'approvisionnement et de valeur et identifie le niveau d'implication de chaque intervenant dans le bon fonctionnement du système orbital**, notamment : identification des rang-1 et de rang-n, compréhension du rôle de chacun, situation géographique, type d'interaction, niveau de dépendance etc.

SYS-ORBIT-CHAINE_201 : L'organisation **détermine des obligations contractuelles étendues et réalisables pour ses fournisseurs et prestataires**. Parmi celles-ci peuvent exister, entre autres, l'éventualité d'un audit, l'obligation de notifier l'organisation lors d'un changement de fournisseur ou prestataire, le droit de communiquer en cas d'attaque ou la notification en cas d'obsolescence d'un produit.

SYS-ORBIT-CHAINE_202 : L'organisation **établit une procédure de vérification du respect des obligations contractuelles,** pour chaque fournisseur et prestataire. Cette procédure de vérification peut passer par des audits enquêtes et tests, par le biais de CESTI par exemple, afin de déterminer si les mesures de sécurité établies lors du contrat sont respectées.

SYS-ORBIT-CHAINE_203 : L'organisation **communique clairement les attentes, les exigences et contraintes applicables à ses fournisseurs et prestataires** par plusieurs biais (éléments contractuels, cahier des charges, clauses techniques, labels à respecter etc.). L'organisation différencie les exigences liées à la gestion ou à la sécurité de l'information, des exigences techniques. Les exigences peuvent différer en fonction du rang du fournisseur ou du prestataire. S'il s'agit d'un fournisseur de rang-1, par exemple, des exigences telles que l'obligation de faire remonter les informations de leurs propres fournisseurs peuvent être demandées.

2.4.2 | VISIBILITÉ SUR LES PRODUITS OU SERVICES DÉLIVRÉS

SYS-ORBIT-CHAINE_204 : L'organisation peut choisir de confier à un tiers tout ou une partie d'une activité qui pourrait être réalisée en interne en s'appuyant pour cela sur un **Plan d'Assurance Sécurité** (PAS). Ce document présente les règles, garanties et mesures de sécurité mises en place par un prestataire pour protéger les données et les systèmes informatiques de son client.

SYS-ORBIT-CHAINE_205 : L'organisation **s'informe sur la provenance des composants** de tout produit et service délivré par un fournisseur ou prestataire, et est en mesure d'assurer sa traçabilité.

SYS-ORBIT-CHAINE_206 : L'organisation identifie les **services et produits pour lesquels une vigilance accrue est nécessaire en fonction de leur origine géographique.** Notamment, l'organisation **identifie les différents pays et régions** en provenance desquels les produits et services délivrés par les fournisseurs pourraient présenter des risques.

2.4.3 | GESTION DES RISQUES LIÉS AUX CHAÎNES DE VALEUR ET D'APPROVISIONNEMENT

Les chaînes de valeur et d'approvisionnement, par leur étendue et leur complexité, peuvent représenter des risques pour l'organisation. L'organisation doit réaliser une **analyse de risque spécifique** permettant d'identifier, d'évaluer et de gérer les menaces cyber provenant de cet écosystème.

SYS-ORBIT-CHAINE_207 : L'organisation réalise une **analyse de risque pour identifier les menaces spécifiques liées à la chaîne de valeur et à la chaîne d'approvisionnement.** L'organisation prend en compte des informations telles que le contexte géopolitique ou le niveau de menace estimé par les services de sécurité nationaux.

SYS-ORBIT-CHAINE_208 : L'organisation accorde une attention particulière aux risques associés à l'usage de COTS. Elle réalise une cartographie précise de ses COTS, détermine des critères pour les choisir, tels que la capacité à patcher ou le suivi des vulnérabilités, et les communique à ses fournisseurs, en s'assurant de maintenir ces exigences de sécurité dans la durée. Parmi les vulnérabilités associées aux COTS peuvent se trouver, entre autres, des portes dérobées, logicielles ou matérielles, de l'obfuscation de code, des branches de code mort, l'intégration de composants ou librairies contrefaits ou obsolètes etc.

SYS-ORBIT-CHAINE_209 : L'organisation **accorde une attention particulière à la protection de sa propriété intellectuelle, notamment si sa chaîne de valeur inclut des organisations étrangères.**

2.4.4 | AUDIT, NOTATION OU « SCORING » CYBER

SYS-ORBIT-CHAINE_210 : L'organisation **évalue le niveau de sécurité de ses fournisseurs et prestataires.** L'organisation peut mettre en place un **système d'évaluation de son niveau de confiance envers ses fournisseurs et prestataires** en s'appuyant sur un ensemble de critères et sur une **méthodologie, aboutissant à un score final**. L'organisation peut définir son propre système d'évaluation, ou déléguer cette tâche à un tiers, via, par exemple, la mise en place d'un programme de certification (par exemple CSPN, ISO27001 ou autre programme sectoriel), avec un référentiel commun. Un bon score est une marque de confiance qui permettrait d'alléger les contrôles réalisés par l'organisation.

SYS-ORBIT-CHAINE_211 : L'organisation **réalise des audits de ses fournisseurs et prestataires de façon régulière.** L'organisation incite aussi ses fournisseurs et prestataires de rang-n à responsabiliser eux-mêmes leurs fournisseurs et prestataires de rang-1. Pour ce faire, l'organisation peut informer ses fournisseurs et prestataires de l'état de la menace qui pèse sur elle, des enjeux de sécurité et des évènements redoutés identifiés dans son analyse de risque.

SYS-ORBIT-CHAINE_212 : L'organisation envisage l'utilisation de produits **labellisés par les agences de**

sécurité. Il est nécessaire de discuter, en amont, avec le fournisseur ou prestataire, des labels qui seront acceptés et utilisés par l'organisation.

SYS-ORBIT-CHAINE_213 : L'organisation **définit un plan de développement et de sécurité fournisseur** pour améliorer la collaboration et accroître les mesures de sécurité mises en place par un fournisseur. Pour ce faire, l'organisation doit comprendre les bonnes pratiques mises en place chez le fournisseur et peut lui en proposer d'autres (en se basant sur ce guide par exemple).

SYS-ORBIT-CHAINE_214 : L'organisation s'assure que **chaque acteur de la chaîne de valeur et d'approvisionnement réalise une appréciation des risques** sur son système d'information et son écosystème.

SYS-ORBIT-CHAINE_215 : Selon le besoin, l'organisation s'assure que **certains fournisseurs ou prestataires répondent à un processus d'homologation**.

2.4.5 | APPROCHE SOUVERAINE

SYS-ORBIT-CHAINE_216 : En fonction de la mission du système orbital et des risques associés, **l'organisation encourage une approche souveraine** dans ses approvisionnements et dans le choix de ses fournisseurs.

SYS-ORBIT-CHAINE_217 : En fonction de la mission du système orbital et des risques associés, l'organisation veille à respecter **les restrictions ou exclusions imposées par les autorités nationales ou internationales dont elle dépend**.

2.5 | FACTEUR HUMAIN, SENSIBILISATION ET FORMATION AUX ENJEUX CYBER

L'erreur humaine est généralement reconnue comme une des principale vulnérabilités pour un scénario d'attaque sur un système d'information. L'exploitation d'une erreur humaine se fait par des moyens détournés comme l'ingénierie sociale ou l'envoi d'emails de phishing. Le risque lié au facteur humain peut être atténué par une organisation qui forme et sensibilise ses employés aux enjeux et risques liés à la cybersécurité.

2.5.1 | SENSIBILISATION AU RISQUE CYBER

SYS-ORBIT-HUMAIN_300 : L'organisation **établit un programme de sensibilisation sur les meilleures pratiques en matière de cybersécurité**. Elle met notamment l'accent sur la création et la gestion de mots de passe forts, la reconnaissance des tentatives de phishing et l'utilisation prudente des technologies numériques de façon générale. Il est pertinent de s'inspirer de cas d'attaques réels.

SYS-ORBIT-HUMAIN_301 : L'organisation **sensibilise l'ensemble de son personnel** aux enjeux de sécurité, aux règles et bonnes pratiques à appliquer et aux comportements à adopter. Il est nécessaire d'actualiser régulièrement les sessions de sensibilisation. Les sessions de sensibilisation peuvent également être réalisées de façon autonome (par l'intermédiaire de MOOC par exemple).

SYS-ORBIT-HUMAIN_302 : L'organisation met en place des mesures permettant **d'évaluer l'efficacité du niveau de sensibilisation** de son personnel à l'aide de simulation de phishing par exemple.

2.5.2 | FORMATION CYBERSÉCURITÉ

SYS-ORBIT-HUMAIN_303 : L'organisation met en place des **formations qui permettent aux différents profils de l'organisation d'améliorer leur connaissance en matière de cybersécurité en adéquation avec leur(s) poste(s) et leur(s) responsabilité(s)**. Ce processus de formation peut être validé par l'obtention de certifications.

SYS-ORBIT-HUMAIN_304 : En accord avec la PSSI correspondante, **l'organisation incite son personnel à signaler les activités suspectes**, les tentatives d'hameçonnage ou toute anomalie de sécurité potentielle. Les mécanismes mis en place pour remonter les incidents doivent être simples et responsabilisants.

SYS-ORBIT-HUMAIN_305 : L'organisation met en place des **formations concernant la gestion de crise cyber**. Les employés sont formés à réagir aux différents cas d'attaques et aux comportements à adopter en cas de crise cyber.

SYS-ORBIT-HUMAIN_306 : Selon le besoin, l'organisation envisage des **activités de formation basées sur des cas pratiques à l'aide de plateformes de simulation ou de bancs de tests** (de type « cyber-range » par exemple) permettant aux équipes de sécurité de s'entraîner sur des cas réalistes et de développer leur expertise.

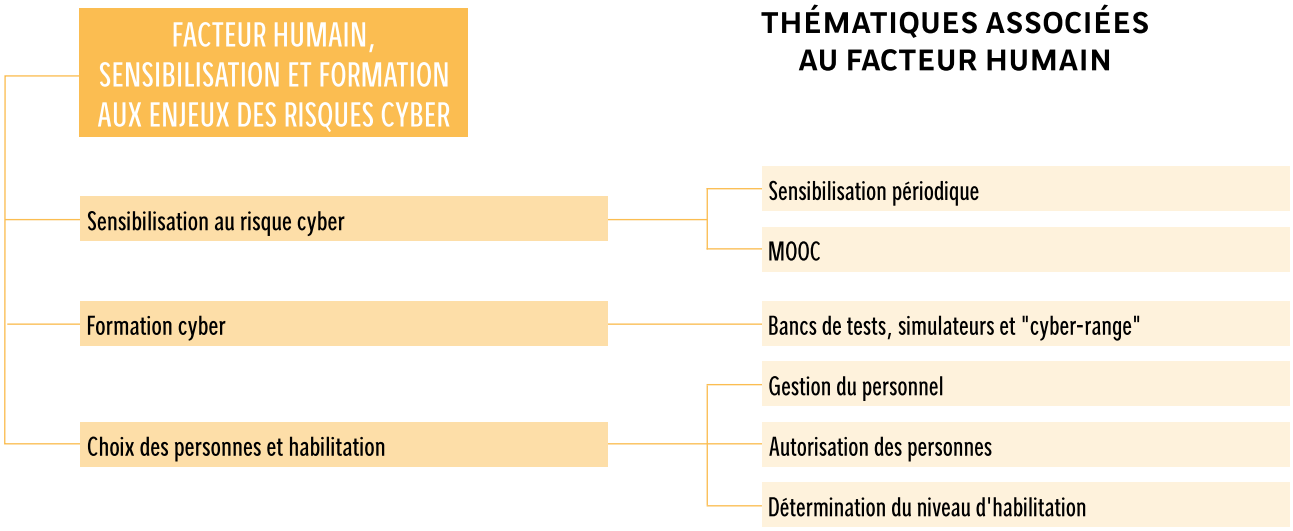
2.5.3 | CHOIX DES PERSONNES ET HABILITATION

SYS-ORBIT-HUMAIN_307 : En fonction des besoins associés au système d'information du système orbital, **l'organisation protège l'accès aux savoirs et savoir-faire stratégiques en sélectionnant les personnes** sur la base de critères, tels que le droit d'en connaître. Elle constitue une équipe de travail responsable et sensibilisée aux enjeux de sécurité du système.

SYS-ORBIT-HUMAIN_308 : L'organisation détermine l'avis de sécurité des individus intervenant sur les systèmes d'information en fonction de la sensibilité des informations auxquelles ils auront accès et du besoin d'en connaître (ex. Instruction générale interministérielle n° 1300).

FIGURE 5 :

THÉMATIQUES ASSOCIÉES AU FACTEUR HUMAIN



JOURNÉE ÉVÈNEMENT RTNC 2024 AU CENTRE DE CONGRÈS PIERRE BAUDIS À TOULOUSE

2.6 | PROTECTION DES DONNÉES

La multiplication des cas d'attaques des systèmes orbitaux amène les acteurs à prendre des mesures de sécurité adéquates. La protection des données, à travers l'utilisation de mécanismes tels que le chiffrement ou la signature, permet d'assurer des fonctions de confidentialité, d'intégrité ou de traçabilité.

2.6.1 CARTOGRAPHIE DES DONNÉES ET DÉFINITION DES BESOINS DE PROTECTION

SYS-ORBIT-PROTEC_400 : L'organisation **cartographie ses données**. Elle **distingue les différents types de données** (données métiers, données systèmes, algorithmes, images, données bord, TM/TC etc.) et **définit les besoins de protection pour chaque type** (confidentialité, intégrité, disponibilité, authenticité, anti-rejeu) **en fonction de leur sensibilité** et en correspondance avec les résultats de l'analyse de risque.

SYS-ORBIT-PROTEC_401 : L'organisation met en place des **processus de protection des données suivant les grands principes de sécurité** tels que la confidentialité, l'imputabilité, la traçabilité, l'intégrité, l'authenticité ou encore la gestion des accès en fonction des **besoins identifiés dans l'analyse de risque**.

SYS-ORBIT-PROTEC_402 : L'organisation accorde une attention particulière à la **protection de son patrimoine informationnel** et, lorsque cela est nécessaire, décline cette protection de façon opérationnelle ou projet par projet.

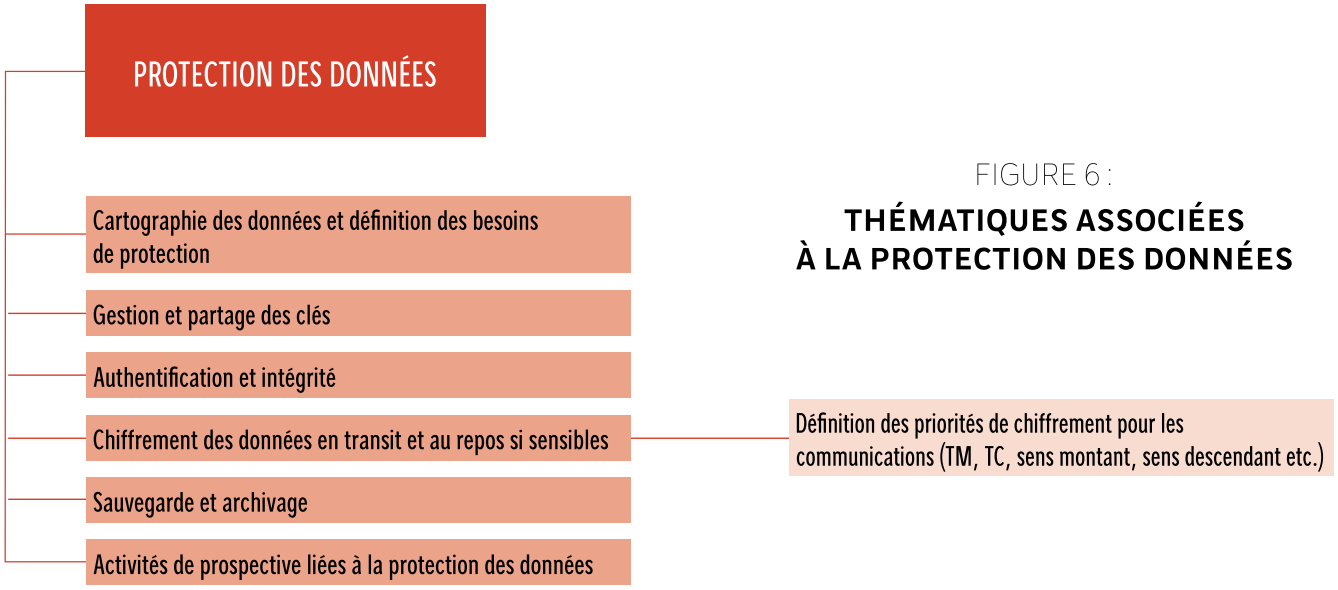


FIGURE 6 :
THÉMATIQUES ASSOCIÉES À LA PROTECTION DES DONNÉES

SYS-ORBIT-PROTEC_403 : L'organisation met en place une politique de gestion des accès à distance en privilégiant l'utilisation de connexions sécurisées, comme les réseaux privés virtuels (VPN), et en implémentant des mécanismes d'authentification forte de type authentification multifacteur (MFA).

2.6.2 GESTION ET PARTAGE DES CLES

SYS-ORBIT-PROTEC_404 : L'organisation **sélectionne des algorithmes de cryptographie adaptés aux besoins identifiés dans l'analyse de risque**. Elle veille à respecter les recommandations des agences de sécurité (telles que l'ANSSI ou le CCSDS). Les implémentations « maison » doivent respecter les recommandations actuelles et les standards en vigueur.

SYS-ORBIT-PROTEC_405 : L'organisation **s'assure de la bonne gestion des privilèges des utilisateurs des systèmes d'information.**

SYS-ORBIT-PROTEC_406 : Afin d'assurer l'authenticité et le chiffrement des données du système orbital, **l'organisation s'assure de la sécurisation du partage initial des clefs de chiffrement**. Dans certains cas, le partage des clefs doit être renouvelé au cours du cycle de vie. L'organisation s'assure également de **l'échange sécurisé du certificat racine** (aussi appelé « Root CA ») de la chaîne de confiance et de la bonne filiation des certificats utilisés en aval de la chaîne de confiance.

SYS-ORBIT-PROTEC_407 : Un **environnement d'exécution sécurisé** (TEE : Trusted Execution Environment) peut reposer sur l'usage de module matériel sécurisé (HSM : hardware security module) qui permet de **générer et de stocker des clefs cryptographiques** et dont le fonctionnement ne peut pas être altéré.

SYS-ORBIT-PROTEC_408 : L'organisation **met en place une Infrastructure de Gestion des Clefs** (IGC ou PKI), couvrant les différents types de clefs, symétriques et asymétriques, **et assurant leur gestion dans le temps**. Le schéma général peut ressembler au suivant : production, séquestration, révocation, distribution, crypto-period et rotation des clefs.

SYS-ORBIT-PROTEC_409 : Dans certains cas spécifiques identifiés, l'organisation peut **suivre le concept OTAR** (over-the-air-rekeying) pour renouveler ses clefs de chiffrement pendant les phases d'opération du système orbital.

SYS-ORBIT-PROTEC_410 : L'organisation anticipe les obsolescences des algorithmes et clefs de chiffrement et s'assure de les remplacer ou les mettre à jour en se basant sur l'état de l'art.

2.6.3 AUTHENTIFICATION ET INTEGRITE

SYS-ORBIT-PROTEC_411 : Si nécessaire, l'organisation s'assure de **l'authentification des entités** se connectant sur le système d'information du système orbital et de **l'authenticité des messages** échangés, par le biais de mécanismes cryptographiques (de type clef publique, clef privée par exemple).

SYS-ORBIT-PROTEC_412 : Si nécessaire, **l'organisation s'assure de l'intégrité des messages échangés avec ou au sein du système orbital** par le biais de primitives cryptographiques (fonction de hachage par exemple).

2.6.4 CHIFFREMENT DE DONNÉES

SYS-ORBIT-PROTEC_413 : Si nécessaire, l'organisation **opte pour une approche de chiffrement de bout-en-bout** afin de protéger l'entièreté d'une chaîne de communication.

SYS-ORBIT-PROTEC_414 : En accord avec l'analyse de risque et en fonction du niveau de sensibilité de l'information, **l'organisation chiffre les différentes liaisons du système orbital qui le nécessitent** (sol-bord, bord-sol, TM, TC etc.)

2.6.5 SAUVEGARDE ET ARCHIVAGE

SYS-ORBIT-PROTEC_415 : L'organisation définit une politique de sauvegarde des données permettant de planifier des sauvegardes à froid ou à chaud, afin d'assurer une conservation des données en cas d'attaque ou de panne.

SYS-ORBIT-PROTEC_416 : En accord avec la politique de sauvegarde, l'organisation **réalise des sauvegardes régulières, i.e. des copies périodiques des informations**, dans l'objectif d'être capable de restaurer des données endommagées (par un cryptolocker par exemple). Elle s'assure également de tester les sauvegardes régulièrement.

SYS-ORBIT-PROTEC_417 : L'organisation **identifie les données qu'elle doit conserver sur un temps long et met en place un système d'archivage** permettant d'y répondre. L'archivage doit être réalisé sur des moyens séparés de ceux utilisés pour la sauvegarde et doit pouvoir être testé régulièrement.

2.6.6 ACTIVITÉS DE PROSPECTIVE LIÉES À LA PROTECTION DES DONNÉES

SYS-ORBIT-PROTEC_418 : L'organisation **s'inspire de l'état de l'art et des bonnes pratiques actuelles** en matière de chiffrement. L'organisation doit être **capable de s'adapter aux évolutions technologiques liées à la cryptographie**. Selon le besoin du système orbital, il conviendra d'être capable de s'adapter aux futures disruptions technologiques telles que le quantique et les algorithmes de chiffrement post-quantique (PQC).

SUIVI DU LANCEMENT DU PREMIER VOL VA262 FM1 ARIANE 6 EN SALLE JUPITER 2, CENTRE DE CONTRÔLE (CDC) DU CENTRE SPATIAL GUYANAIS (CSG), LE 09 JUILLET 2024

2.7 | SÉCURITÉ PHYSIQUE

La sécurité physique est généralement acceptée comme l'ensemble des mesures de sécurité conçues pour limiter l'accès aux personnes autorisées et pour protéger des dommages corporels et matériels.

2.7.1 | MISE EN PLACE DE PROCÉDURES DE CONTRÔLE D'ACCÈS PHYSIQUE OU À DISTANCE

SYS-ORBIT-PHY_500 : L'organisation identifie les points d'accès physiques des installations et sites du système orbital. Cela inclut notamment les accès aux prises réseaux dans des lieux ouverts au public, comme par exemple des salles de réunion, l'accueil, les couloirs etc.

SYS-ORBIT-PHY_501 : L'organisation **définit et cartographie les zones sensibles** dans le but d'adapter les contrôles d'accès physiques et distants selon la sensibilité de l'activité abritée. Les locaux abritant des activités de recherche ou de production stratégiques reçoivent le statut de zones protégées, qualifiées de ZRR, dont l'accès est contrôlé pour assurer la protection du potentiel scientifique et technique de la nation (PPST) afin de lutter contre les tentatives de captation ou de détournement.

SYS-ORBIT-PHY_502 : L'organisation prévoit un **contrôle strict des entrées** et sorties de ses sites en fonction de leur sensibilité. **L'organisation tient un registre des accès au site**.

SYS-ORBIT-PHY_503 : L'organisation contrôle les accès physiques aux serveurs, locaux techniques et zones sensibles par la **mise en place de mesures d'imputabilité** (comme l'installation de serrures sécurisées ou badges par exemple). Les accès aux prises réseaux dans des lieux de passage doivent eux aussi être désactivés ou restreints. Ce contrôle d'accès sous-entend également la **gestion des clés physiques et des cartes d'accès**. En fonction des besoins de l'organisation, les mesures de protection physique des zones peuvent être adaptées.

SYS-ORBIT-PHY_504 : L'organisation procède régulièrement à une revue des comptes et des droits associés, comme les droits d'accès des personnes afin d'éviter les accès non autorisés. L'organisation veillera notamment à supprimer les droits d'accès du personnel ayant quitté l'organisation.

SYS-ORBIT-PHY_505 : Selon le niveau de risque, **l'organisation peut prévoir les cas où son personnel serait forcé à travailler sous la contrainte** (prise d'otage, terrorisme). Cela peut se traduire par la création de mots de passe d'alerte dédiés au travail sous la contrainte.

2.7.2 | GESTION TECHNIQUE DES SITES

SYS-ORBIT-PHY_506 : L'organisation s'assure d'avoir une **approche globale de la sécurité**, en tenant compte des interactions avec les éléments afin que les **contraintes techniques des sites** (intrusion physique, incendie, climatisation, filtration d'air, hygrométrie) **aient le moins de conséquences directes ou indirectes** possibles sur la sécurité du système d'information du système orbital.

2.7.3 | APPROCHE DE LA SÉCURITÉ LORS DES DIFFÉRENTES PHASES DU SYSTÈME ORBITAL

SYS-ORBIT-PHY_507 : L'organisation s'assure que la **sécurité du système d'information du système orbital est assurée lors de chacune des phases du cycle de vie,** et notamment lors des phases d'AIT, de transport ou de lancement qui peuvent être perçues comme des phases à risque.

SYS-ORBIT-PHY_508 : L'organisation s'assure que l**e stockage physique des composants sensibles se fait de façon sécurisée** afin d'éviter toute intervention d'entités non autorisées.

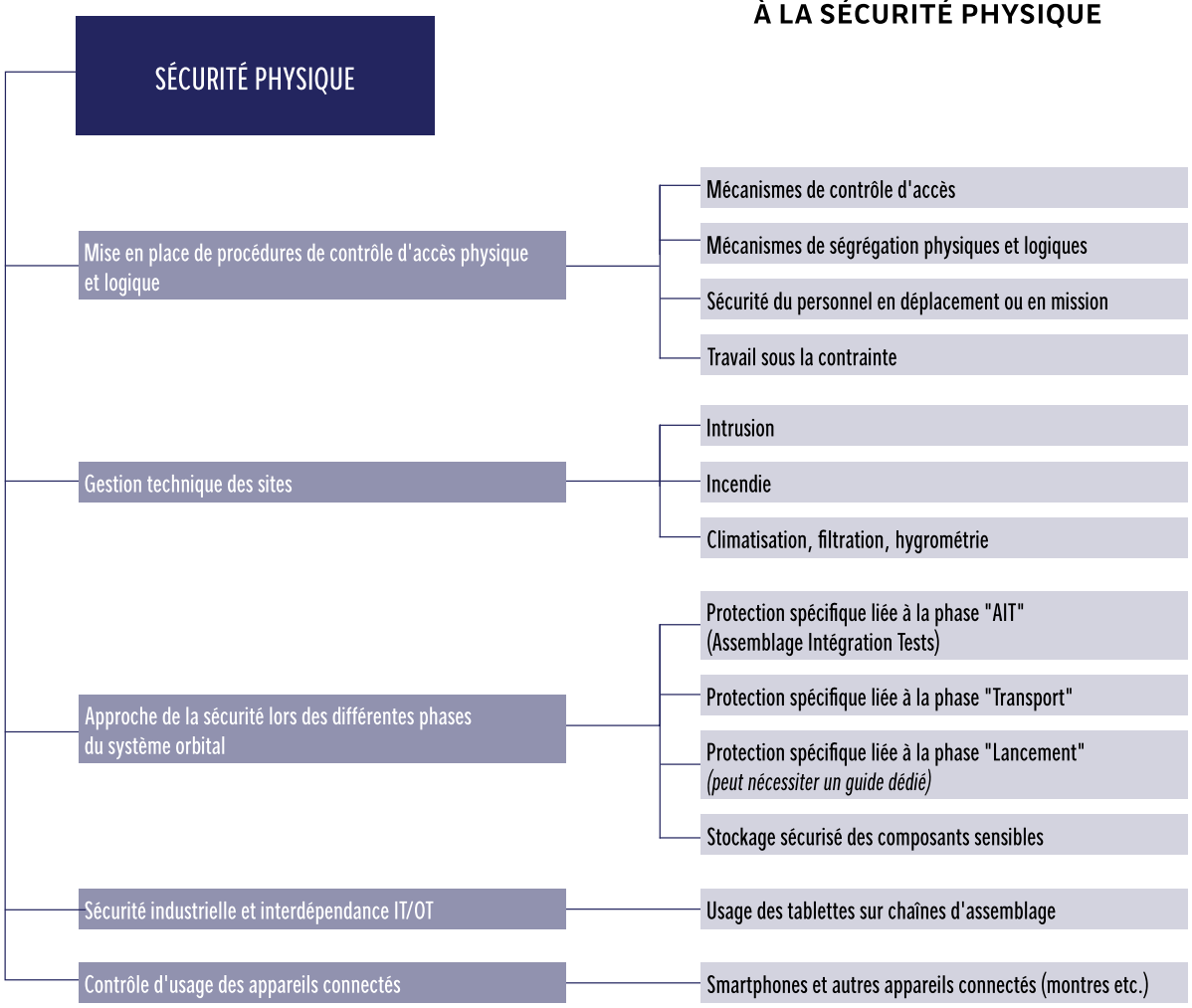
2.7.4 SÉCURITÉ INDUSTRIELLE ET INTERDÉPENDANCE IT/OT

SYS-ORBIT-PHY_509 : L'organisation **s'assure de la ségrégation des systèmes industriels (appelés OT et comprenant les moyens de contrôles et de commandes des installations techniques, SCADA etc.) des systèmes d'information classique (IT)**, notamment elle s'assure que les systèmes d'information IT ne puissent pas perturber le bon fonctionnement des systèmes industriels.

2.7.5 CONTRÔLE D'USAGE DES APPAREILS CONNECTÉS

SYS-ORBIT-PHY_510 : L'organisation s'assure que seuls les appareils mobiles dûment autorisés peuvent être raccordés aux systèmes d'information IT ou OT, et qu'ils **ne peuvent pas interférer ou perturber, directement ou indirectement, les systèmes d'information industriels**, et les systèmes d'information du système orbital en général.

FIGURE 7 :
THÉMATIQUES ASSOCIÉES À LA SÉCURITÉ PHYSIQUE



2.8 I MÉCANISMES DE DÉTECTION ET JOURNALISATION

La détection permet d'identifier au plus tôt des comportements s'apparentant à une cyberattaque ou une tentative d'attaque et de réagir le plus rapidement possible.
La journalisation permettra de rassembler un ensemble d'éléments d'information, d'assurer une traçabilité des accès et des actions afin d'offrir des éléments d'investigation en cas d'incident.

2.8.1 I SÉLECTION ET MISE EN ŒUVRE D'OUTILS DE DÉTECTION

SYS-ORBIT-DETECT_600 : L'organisation met en place un IDPS afin de détecter les cybermenaces et prévenir des intrusions.

SYS-ORBIT-DETECT_601 : L'organisation met en place un SIEM permettant de collecter, d'analyser, de corréler et de réagir aux évènements de sécurité dans le but d'identifier des menaces au plus tôt et de minimiser l'effort lié au filtrage de faux positifs.

2.8.2 I JOURNALISATION, GESTION DES LOGS ET CORRÉLATION

SYS-ORBIT-DETECT_602 : L'organisation met en place des mécanismes de journalisation des évènements à l'aide de fichier de logs. Les logs enregistrés pourront être corrélés afin d'utiliser différents faisceaux d'information (par exemple sécurité physique et sécurité numérique) pour identifier et comprendre de potentiels incidents de sécurité.

2.8.3 I ACTIVITÉ DE CYBER THREAT INTELLIGENCE (CTI) ET ANTICIPATION DE LA MENACE TECHNIQUE

SYS-ORBIT-DETECT_603 : L'organisation envisage des activités de CTI (Cyber Threat Intelligence) lui permettant d'acquérir des indicateurs techniques sur l'évolution du niveau de menace et d'adapter sa sécurité en fonction des activités observées. Ce monitoring peut être réalisé à l'aide d'un SOC (Security Operation Center) ou à l'aide de sondes dédiées. En fonction des résultats de l'analyse de risque, l'organisation engage des **réponses adaptées et des moyens de remédiation du risque**. Dans le futur, l'intelligence artificielle est envisagée comme un moyen d'amélioration de la qualité des outils de détection. Les activités de CTI peuvent demander de faire **appel à des spécialistes** de la menace et de ses indicateurs.

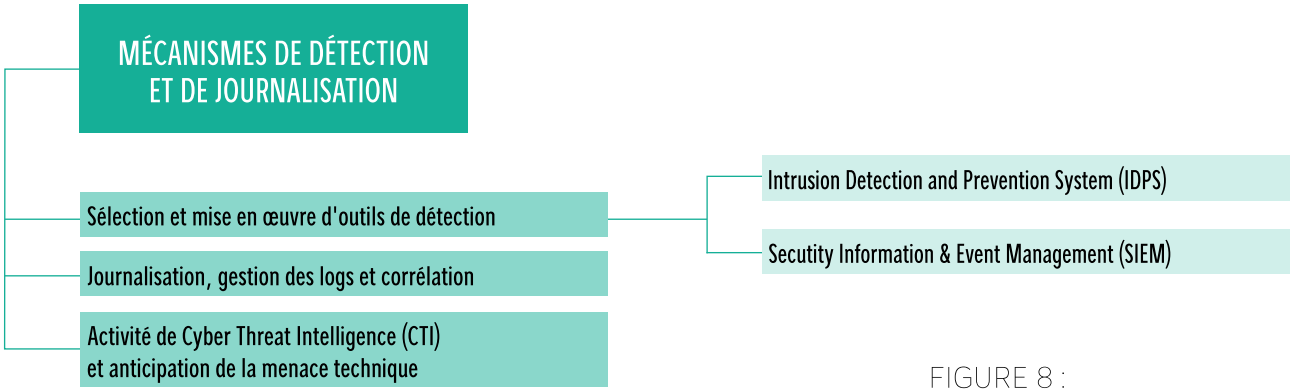
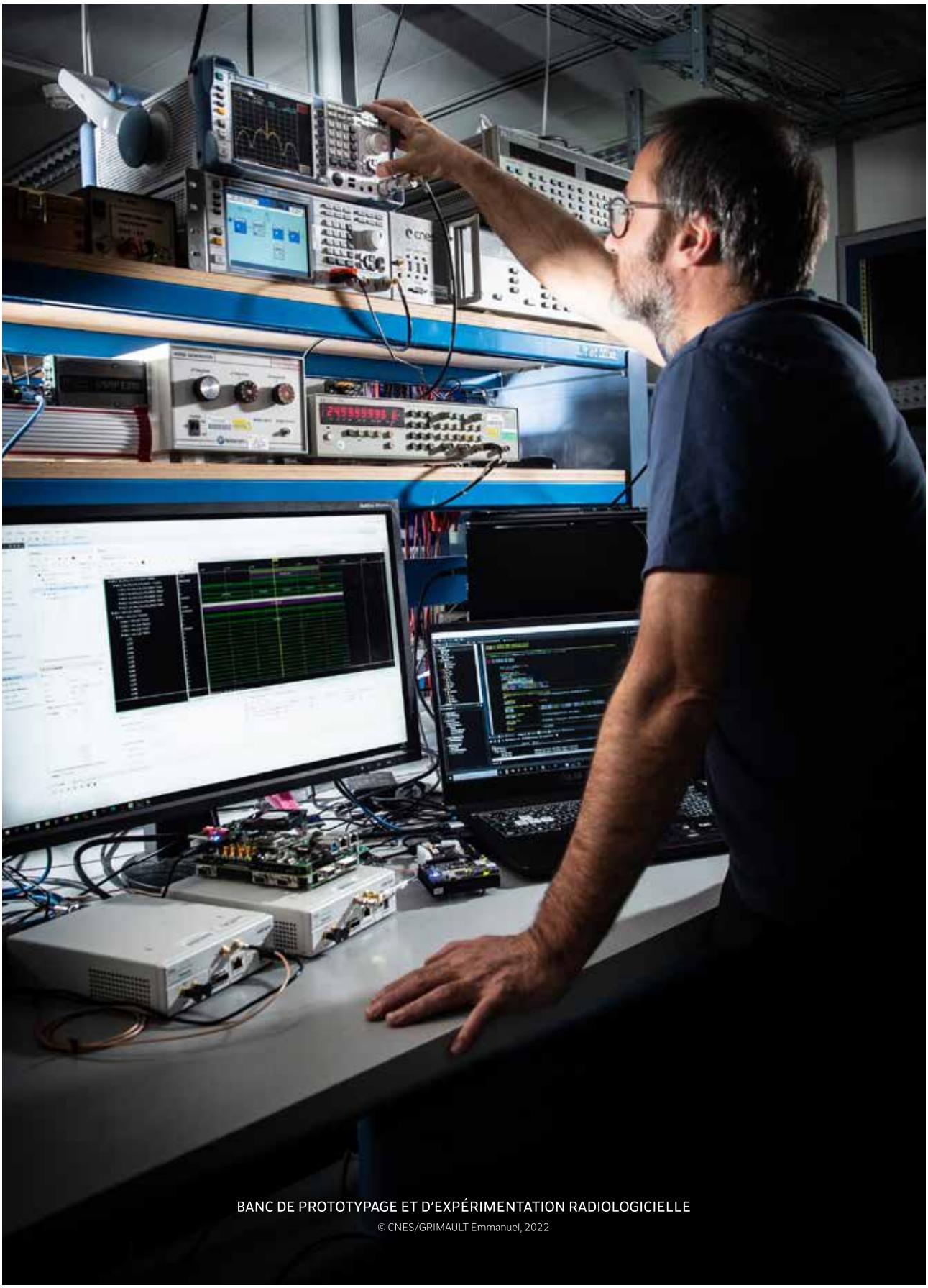


FIGURE 8 :
THÉMATIQUES ASSOCIÉES AUX MÉCANISMES DE DÉTECTION ET JOURNALISATION



BANC DE PROTOTYPAGE ET D'EXPÉRIMENTATION RADIOLOGICIELLE

2.9 | MAINTIEN EN CONDITION DE SÉCURITÉ (MCS)

La sécurité des systèmes orbitaux est un processus qui doit être maintenu dans le temps, tout au long du cycle de vie du système orbital. Le Maintien en Condition de Sécurité, ou MCS, permet de maintenir le système orbital dans un état de sécurité optimal en prenant en compte l'évolution de la menace ainsi que les nouvelles vulnérabilités découvertes sur le système orbital.

FIGURE 9 :

THÉMATIQUES ASSOCIÉES AU MAINTIEN EN CONDITION DE SÉCURITÉ

2.9.1 | PHASES DE TESTS ET SURVEILLANCE DE LA CHAINE LOGICIELLE

SYS-ORBIT-MCS_700 : L'organisation définit ses **stratégies** de **Maintien en Condition de Sécurité** (MCS) et de **Maintien en Condition Opérationnelle** (MCO).

SYS-ORBIT-MCS_701 : L'organisation accorde une **attention particulière aux logiciels de type COTS et met en place des processus permettant de maîtriser la chaîne logicielle par des mécanismes de traçabilité** (par l'utilisation d'une nomenclature logicielle ou d'une approche de type SBOM). L'organisation accorde aussi une attention particulière à la potentialité de piégeage des logiciels libre.

SYS-ORBIT-MCS_702 : Lors de livraisons de logiciels par un fournisseur, l'organisation s'assure que son fournisseur **signe ses livraisons et offre des mécanismes permettant de vérifier l'intégrité** du code ou du logiciel fourni.

2.9.2 | GESTION DES MISES À JOUR DES SYSTÈMES ORBITAUX

SYS-ORBIT-MCS_703 : Selon le besoin, l'organisation peut développer et mettre en place un **double digital** du système orbital **en amont des mises à jour** à effectuer lors de la phase d'exploitation. L'objectif est de prévenir des imprévus techniques qui peuvent subvenir suite à une mise à jour.

SYS-ORBIT-MCS_704 : En accord avec les actions identifiées dans l'analyse de risque, l'organisation **réalise des tests de non-régression** des fonctionnalités pouvant être impactées par une mise à jour. Elle **conserve des états de restauration** dans le cas où la mise à jour engendrerait un dysfonctionnement ou une régression.

2.9.3 | GESTION DES OBSOLESCENCES

SYS-ORBIT-MCS_ 705 : L'organisation anticipe les obsolescences matérielles et logicielles des composants du système orbital. Concernant les logiciels, l'organisation peut se renseigner sur les dates de fin de maintenance d'un logiciel. Concernant le matériel, l'organisation peut anticiper les obsolescences matérielles par la provision d'équipements de rechange ou « spare ». L'utilisation d'équipement de rechange peut permettre d'anticiper la fin de production d'un équipement par un fabriquant ou un systémier.

SYS-ORBIT-MCS_706 : L'organisation a**nticipe les phases associées à la fin de vie** (« end of life » EOL) **ou à la fin du support** (« end of support » EOS) d'une partie ou de l'ensemble du système orbital.

Il convient d'anticiper les phases EOL ou EOS en envisageant, par exemple, l'effacement de données sensibles, la révocation de certificats, l'effacement des clés de vol avant mise en orbite cimetière. En fonction du besoin, il conviendra de prévoir de lancement d'un projet permettant d'assurer la continuité de la mission.

2.9.4 | AUDIT ET GESTION DES VULNÉRABILITÉS

SYS-ORBIT-MCS_707 : L'organisation conduit des tests d'intrusion et des scans de vulnérabilités dont la nature et la fréquence sont déterminées par l'analyse de risque. En fonction du besoin, l'organisation effectue des corrections (changement de configuration, **mises à jour, application des patchs, etc.**).

SYS-ORBIT-MCS_708 : L'organisation **met en place des mesures de protection des résultats de tests** afin d'éviter qu'ils soient utilisés par des acteurs malveillants.

SYS-ORBIT-MCS_709 : L'organisation **produit une analyse d'impact des vulnérabilités** détectées, en prenant en compte son niveau d'exposition aux menaces, en vue de déterminer les actions appropriées. En fonction de la PSSI associée au système d'information analysé, **l'organisation applique des correctifs et des patchs** correspondants afin de prévenir l'exploitation de ces vulnérabilités par des acteurs malveillants. Certains contextes opérationnels d'un système orbital ne sont pas favorables à l'application de correctif ou de patch.

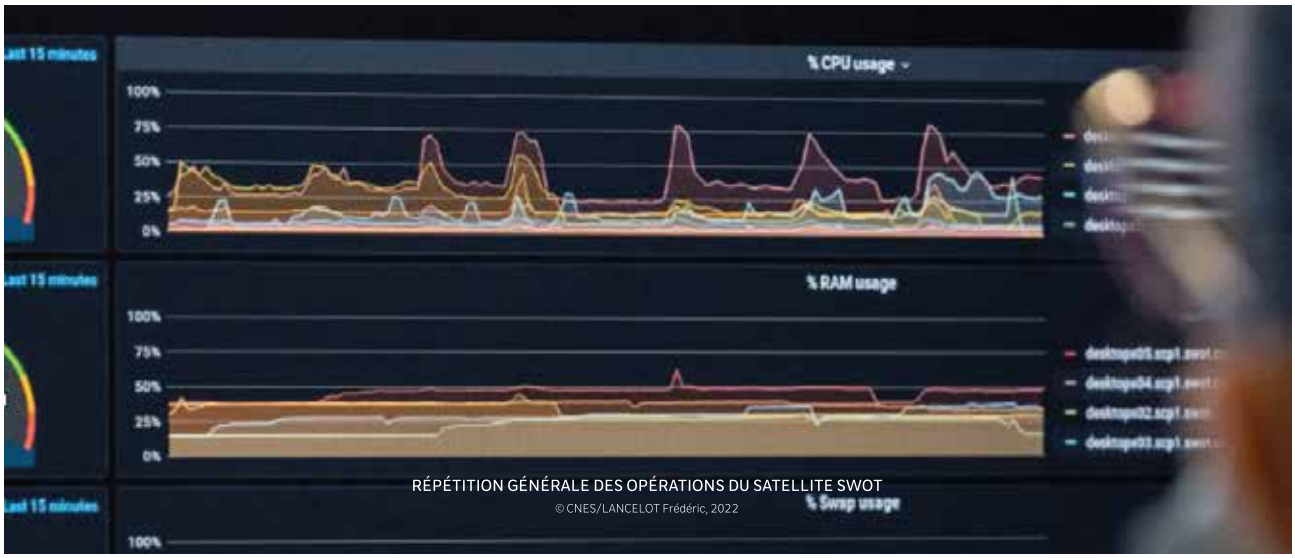
SYS-ORBIT-MCS_710 : L'organisation protège les résultats des audits et les vulnérabilités, afin de ne pas compromettre le système d'information dans le cas d'un vol de données.

SYS-ORBIT-MCS_711 : Lors de l'application de correctifs et de patchs, l'organisation s'assure de ne pas introduire de régression dans le système en réalisant des **tests de non-régression**.

2.9.5 | VEILLE TECHNIQUE

SYS-ORBIT-MCS_712 : L'organisation réalise une veille sur les vulnérabilités (IoC, CVE) permettant de maintenir à jour les différents composants logiciels ou matériels, ainsi que les capteurs de détection cyber (notamment la base antivirale).

SYS-ORBIT-MCS_713 : L'organisation adopte des outils et frameworks lui permettant de faciliter le partage d'indicateurs techniques de type IoC (en utilisant par exemple des frameworks comme OpenCTI et des protocoles comme STIX/TAXII etc.). ▮



RÉPÉTITION GÉNÉRALE DES OPÉRATIONS DU SATELLITE SWOT
© CNES/LANCELOT Frédéric, 2022

2.10 | AMÉLIORATION DE LA SÉCURITÉ

La sécurité des systèmes orbitaux passe par la mise en place d'une défense proactive tout au long de leur cycle de vie. L'amélioration continue de la sécurité s'appuie sur des approches de type « zero-trust » qui consistent à appliquer des couches successives de sécurité, sans confiance implicite d'un service ou d'un composant, même interne au système.

2.10.1 | CONNAISSANCE APPROFONDIE DU SYSTÈME ET MISE EN PLACE DE DIFFÉRENTS NIVEAUX DE PROTECTION

SYS-ORBIT-AMELI_800 : L'approche par la **défense en profondeur** permet à l'organisation **d'identifier des mécanismes permettant de ralentir toute attaque ou de décourager les attaquants par l'investissement à consacrer pour mener une attaque**. Cette approche, inspirée du domaine militaire, consiste à ralentir la progression d'un ennemi par la mise en place d'obstacles successifs, l'objectif étant de dissuader un attaquant aux vues de l'investissement nécessaire pour mener à bien une cyberattaque.

SYS-ORBIT-AMELI_801 : L'approche de type « **zero-trust** » permet à l'organisation d'appliquer à tous les segments de son système orbital plusieurs niveaux de protection dans le but d'**éviter toute confiance implicite**, c'est-à-dire que la confiance dans l'identité d'une personne ou d'un composant doit toujours être vérifiée, en effectuant des contrôles réguliers, dynamiques et granulaires. Une authentification mutuelle, par exemple, peut être mise en place entre chaque composant du système.

SYS-ORBIT-AMELI_802 : L'approche basée sur **l'utilisation d'une chaîne de confiance basée sur une racine de confiance** (ex. « secure boot ») permet à l'organisation de sécuriser les systèmes d'information du système orbital le plus en amont possible, dès leur phase d'initialisation.

2.10.2 | DÉVELOPPEMENT SÉCURISÉ

SYS-ORBIT-AMELI_803 : L'organisation **cherche à intégrer la sécurité de façon agile dans son processus de développement** avec l'approche type « devsecops ».

SYS-ORBIT-AMELI_804 : L'organisation **respecte et encourage l'utilisation de règles de codage** permettant de limiter les failles et exploitations logicielles possibles. L'application des règles de codage doit pouvoir être contrôlée régulièrement par l'organisation.

SYS-ORBIT-AMELI_805 : L'organisation s'assure de la sécurisation de ses forges logicielles et de sa gestion de configuration pour protéger la confidentialité ou l'intégrité de son code source.

SYS-ORBIT-AMELI_806 : Lors des phases de conception ou de maintenance, selon le besoin, l'organisation réalise, ou coordonne avec ses fournisseurs, des **campagnes de tests sur ses logiciels**. Les tests orientés sécurité peuvent être de différente nature, **dynamiques** (de type Dynamic Application Security Testing ou DAST) ou **statiques** (de type Static Application Security Testing ou SAST).

2.10.3 | DURCISSEMENT ET REDONDANCE

SYS-ORBIT-AMELI_807 : En accord avec l'analyse de risque, **l'organisation assure une redondance des systèmes ou sous-systèmes critiques du système orbital** afin d'éviter les points de défaillance uniques.

SYS-ORBIT-AMELI_808 : En accord avec l'analyse de risque, **l'organisation cloisonne et implémente des mécanismes de ségrégation spatiale et temporelle** entre les différentes parties du système d'information du système orbital.

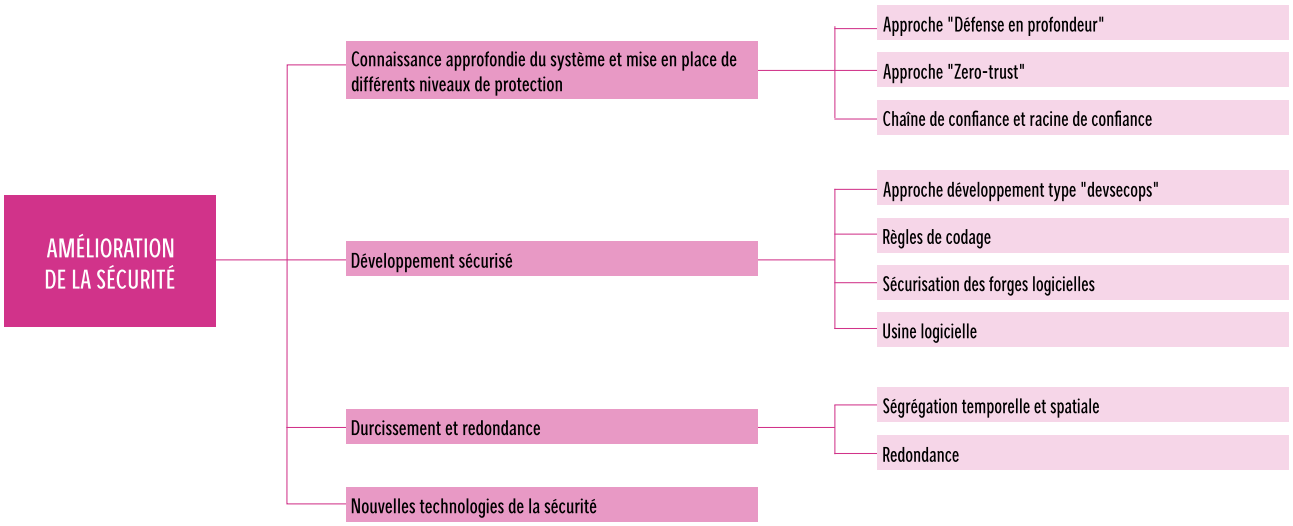
SYS-ORBIT-AMELI_809 : L'organisation applique des règles de filtrage sur le système d'information du système orbital pour s'assurer que seuls les flux strictement nécessaires sont autorisés.

SYS-ORBIT-AMELI_810 : En accord avec l'analyse de risque, **l'organisation envisage de mettre en place des techniques de durcissement matériel ou logique, qui permettent de réduire la surface d'attaque du système**.

2.10.4 | NOUVELLES TECHNOLOGIES DE LA SÉCURITÉ

SYS-ORBIT-AMELI_811 : Lorsque cela est possible, **l'organisation envisage de nouvelles technologies de cybersécurité** pour protéger son système orbital, et notamment celles basées sur la **dynamicité du système** (reconfiguration en orbite, technologies de type « software defined » SDR ou SDS).

FIGURE 10 :
THÉMATIQUES ASSOCIÉES À L'AMÉLIORATION DE LA SÉCURITÉ

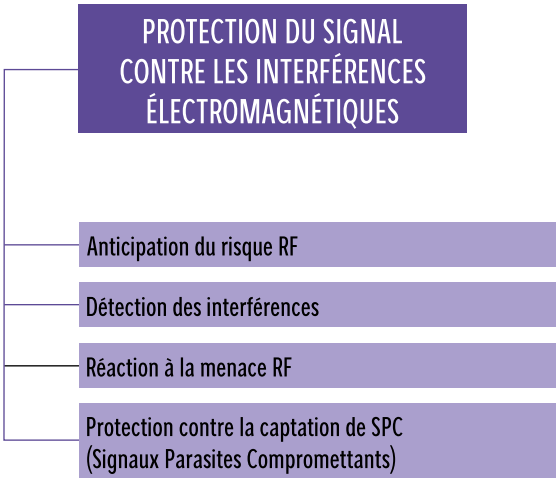


2.11 | PROTECTION DU SIGNAL CONTRE LES INTERFÉRENCES ÉLECTROMAGNÉTIQUES

Les actions d'interférences électromagnétiques sont des perturbations générées par une source externe qui peuvent affecter les communications et services fournis par un circuit électrique, en dégradant ses performances ou en empêchant son bon fonctionnement. Ces attaques s'intensifient depuis ces dernières années et sont accentuées par les tensions géopolitiques (nombreux cas de leurrage ou de brouillage).

FIGURE 11 :

THÉMATIQUES ASSOCIÉES À LA PROTECTION DU SIGNAL CONTRE LES INTERFÉRENCES ÉLECTROMAGNÉTIQUES



Les systèmes orbitaux peuvent être impactés par ce type de menaces. Bien qu'il soit souvent complexe et onéreux de prendre en compte cette menace, il convient de s'interroger sur la capacité du système à évoluer dans un environnement de plus en plus sujet à ces attaques.

Le risque radiofréquence sur les signaux des systèmes orbitaux, qu'ils soient bord-sol, sol-bord ou bord-bord, demande aux organisations d'anticiper les impacts associés et de concevoir des mécanismes de robustesse ou de résilience. En fonction de la mission, des orbites utilisées, et des spécificités du système orbital, l'opérateur peut sélectionner les bonnes pratiques qu'il considère applicables.

Le risque lié aux signaux parasites compromettants est également appelé menace TEMPEST. La menace TEMPEST ne porte pas uniquement sur le spectre radiofréquence (et peut cibler des domaines tels que l'acoustique, le visuel, le vibratoire, etc.). Dans le cadre de cette première édition, nous nous focaliserons sur le domaine radiofréquence uniquement.

2.11.1 | ANTICIPATION DU RISQUE RF

SYS-ORBIT-SIGNAL_900 : L'organisation effectue une **analyse de risque** destinée à **identifier les besoins de sécurité associés au risque d'interférence électromagnétique**. L'organisation identifie les différents signaux et types de données en fonction des canaux de communication utilisés et en fonction des usages (en nominal, en secours, etc.). En fonction du besoin, l'organisation **met en œuvre un ensemble de mesures de type TRANSEC** (étalement du spectre, utilisation de plusieurs fréquences, « burst encoding », sauts de fréquence) pour les signaux concernés permettant de répondre à des attaques de type « spoofing » ou « jamming » notamment.

SYS-ORBIT-SIGNAL_901 : En fonction des résultats de l'analyse de risque, l'organisation **envisage l'utilisation de systèmes et d'infrastructures de secours ainsi que des voies de communication alternatives** (antennes, fréquences alternatives par exemple) pour assurer la continuité des communications en cas d'interférence.

2.11.2 I DÉTECTION DES INTERFÉRENCES

SYS-ORBIT-SIGNAL_902 : Selon les résultats de l'analyse de risque, **l'organisation met en place des mécanismes de surveillance du spectre électromagnétique** tels que la surveillance de points critiques de télémétrie, l'état d'accrochage de porteuse ou autres paramètres RF liés au signal.

SYS-ORBIT-SIGNAL_903 : En fonction des résultats de l'analyse de risque et des moyens à disposition, l'organisation **peut mettre en place ou utiliser des capacités de surveillance de l'environnement spatial** (SSA) par l'identification et le suivi des objets spatiaux afin d'anticiper une menace dans l'espace.

2.11.3 I RÉACTION A LA MENACE RF

SYS-ORBIT-SIGNAL_904 : L'organisation **communique les fréquences ou communications impactées par des interférences aux institutions compétentes** (Bureau des fréquences du CNES, MINARM, ANFR, ITU etc.).

2.11.4 I PROTECTION CONTRE LA CAPTATION DE SIGNAUX PARASITES COMPROMETTANTS

SYS-ORBIT-SIGNAL_905 : En fonction des résultats de l'analyse de risque, **l'organisation anticipe les risques d'interception et d'exploitation des Signaux Parasites Compromettants (SPC)** des systèmes d'information du système orbital, comme ceux liés aux radiations d'une carte électronique ou d'un écran, avec, par exemple, la mise en place de mesures de type TEMPEST (durcissement du système orbital, audit des bâtiments sol, utilisation d'une enceinte faradisée au sol pour la mise à la clé...). Ces mesures peuvent être mises en place lors du traitement des secrets au niveau du segment sol ou du segment spatial, ainsi que lors des mises à la clé. ▮

INAUGURATION D'UNE NOUVELLE STATION STC, DE RÉCEPTION POURSUITE SUR LE SITE D'ISSUS-AUSSAGUEL.
© CNES/GNAWAN, 2023


cnes

Version 1 **- Février 2025**

DCS-2024.0004634

cyber4space@cnes.fr

https://cnes.fr/entreprises/centre-cyber-spatiale

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES