ICAO

SECURITY AND FACILITATION

Le partage de cyberinformations

Publié sous l'autorité du Secrétaire général
2024, version

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Table des matières

ABRÉVIATIONS ET SIGLES

ANSP	Fournisseurs de services de navigation aérienne
AAC	Autorité de l'aviation civile
CERT	Équipe d'intervention informatique d'urgence
CIShP	Politique relative au partage de cyberinformations
CSIRT	Équipe d'intervention face aux cyberincidents de sûreté
CTI	Renseignement sur les cybermenaces
FIRST	Forum of Incident Response and Security Teams (forum des équipes d'intervention en cas d'incidents liés à la sécurité informatique)
OACI	Organisation de l'aviation civile internationale
IoC	Indicateurs de compromis
DPI	Droits de propriété intellectuelle
ISAC	Centre d'échange et d'analyse d'informations
ISMS	Système de gestion de la sécurité de l'information
OSINF	Informations de sources ouvertes
OSINT	Renseignement de sources ouvertes
SOC	Centre des opérations de sûreté
TLP	Protocole des feux de circulation
TTP	Tactiques, techniques et procédures
UAS	Système d'aéronef non habité

RÉSUMÉ ANALYTIQUE

Les meilleures pratiques établies dans le domaine de la sécurité et de la sûreté de l'aviation témoignent de l'importance du partage d'informations et de son rôle dans la réduction des menaces et des risques pesant sur l'aviation civile. Le partage de cyberinformations est tout aussi important.

TCe dernier revêt un caractère crucial pour la gestion des cyberrisques dans l'aviation civile. Il concourt à une solide culture de la cybersécurité en encourageant la collaboration et en favorisant un climat de confiance. Par ailleurs, il contribue à l'appréciation de la situation, à la gestion opérationnelle et tactique des risques en la matière et à la planification stratégique.

Le présent document fournit des orientations aux États et aux parties prenantes du secteur pour l'élaboration d'un plan visant à partager des cyberinformations, y compris des recommandations sur la politique à adopter, les ressources à prévoir et les mesures concrètes à prendre aux fins de mise en œuvre et d'amélioration continue des pratiques dans ce domaine.

Il décrit également les préalables en la matière dans le secteur de l'aviation, et dresse la liste des différents types de cyberinformations qui se prêtent au partage. Il traite en outre des aspects relatifs à l'analyse et à l'assurance dans ce domaine, en insistant sur la nécessité d'évaluer la confiance qui peut être accordée à la source et la crédibilité du contenu.

Le présent document annule et remplace les orientations précédemment publiées par l'OACI sur l'utilisation du protocole des feux de circulation (TLP) dans l'aviation civile. Il énonce des règles applicables au partage de cyberinformations dans le secteur de l'aviation, d'après la norme TLP actualisée et selon le type d'informations communiquées, la date et l'heure de la communication et les destinataires (p. ex., organismes publics, exploitants ou prestataires de services).

De manière générale, l'accent est mis sur l'importance de partager des cyberinformations de différents types dans le secteur de l'aviation civile, non sans tenir compte des exigences à respecter en matière d'analyse, d'assurance et de marquage pour une diffusion efficace de ces informations aux parties prenantes concernées.

Les orientations données sont conformes à la stratégie pour la cybersécurité de l'aviation[1] de l'Organisation de l'aviation civile internationale (OACI) et au plan d'action pour la cybersécurité[2] qui y est associé, et répondent au besoin de partager des cyberinformations. Les informations qui figurent dans le présent document sont quant à elles conformes aux principes généraux de l'OACI sur l'échange d'informations intéressant la sûreté et la sécurité de l'aviation, tels qu'énoncés dans le *Manuel de sûreté de l'aviation* (Doc 8973 – Diffusion restreinte) et le *Manuel de gestion de la sécurité* (Doc 9859).

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

DÉFINITIONS

Assurance. Actions planifiées et systématiques nécessaires pour donner une assurance adéquate qu'un produit ou un procédé répond à des exigences données.

Vecteur d'attaque. Moyen d'accès utilisé par un pirate informatique pour lancer une attaque.

Authentification. Mesure qui permet de confirmer l'affirmation de l'identité d'un individu, d'un utilisateur, d'un programme, d'un processus, d'un système ou d'un appareil.

Disponibilité. Propriété de ce qui est accessible et utilisable à la demande par une personne, un utilisateur, un programme, un processus, un système ou un appareil autorisé.

Cybersécurité de l'aviation. Ensemble de technologies, de contrôles et de mesures, de processus, de procédures et de pratiques conçus pour assurer la confidentialité, l'intégrité, la disponibilité et la protection et la résilience globales des cyberactifs contre les attaques, les dommages, la destruction, les perturbations, les accès non autorisés et/ou l'exploitation.

Confidentialité. Propriété d'un actif qui n'est pas mis à disposition ni divulgué à une personne, un utilisateur, un programme, un processus, un système ou un appareil non autorisé.

Cyberactifs. Éléments numériques et physiques qui ont une valeur en termes d'activité, d'exploitation, de sécurité et de sûreté aériennes, d'efficacité et/ou de capacités de l'aviation, tels que les systèmes, les informations, les données, les réseaux, les appareils, les logiciels, le matériel, les processus, les firmware, le personnel pertinent/certifié et d'autres ressources électroniques.

Cyberattaque. Utilisation délibérée de moyens électroniques pour interrompre, modifier, détruire ou obtenir un accès non autorisé à des cyberactifs.

Cyberévénement. Tout occurrence observable dans un réseau ou un système.

Cyberincident. Un ou plusieurs cyberévénements qui ont une incidence négative sur la sécurité aérienne, et la sûreté, l'efficacité et/ou la capacité de l'aviation.

Cyberatténuation. Contrôles de sûreté qui visent à réduire le cyberrisque associé à une cybermenace ou à une vulnérabilité spécifique, en tenant compte de son incidence sur la sécurité aérienne et la sûreté, l'efficacité et/ou la capacité de l'aviation.

Cyberrésilience. Capacité d'un cyberactif à maintenir des fonctions essentielles dans des conditions défavorables ou sous la pression, et à s'en remettre.

Cyberrisque. Possibilité qu'un cyberévénement débouche sur un résultat indésirable.

Évaluation des cyberrisques. Processus continu de repérage, d'analyse et d'évaluation des cyberrisques.

Gestion des cyberrisques. Processus continu de repérage, d'atténuation, de traitement et de surveillance des cybermenaces et des cyberrisques, sur la base d'une évaluation des risques.

Cybermenace. Tout cyberévénement potentiel qui pourrait avoir une incidence négative sur la sécurité aérienne, et la sûreté, l'efficacité et/ou la capacité de l'aviation.

Sécurité des informations. Protection de la confidentialité, de l'intégrité et de la disponibilité des informations.

Partage d'informations. Processus par lequel des informations sont fournies par une entité à une ou plusieurs autres entités afin de faciliter la prise de décision, après évaluation des risques, et de promouvoir les pratiques exemplaires.

Intégrité. Propriété de l'exactitude et de l'exhaustivité d'un actif, qui confirme ce que l'actif prétend être.

Gravité. Indication qualitative de l'ampleur de l'effet négatif d'une condition de menace.

Acteur à l'origine de la menace . Entité partiellement ou entièrement responsable d'un incident, qui a une incidence – ou est susceptible d'en avoir -- sur une organisation ou un système.

1. INTRODUCTION

1.1 Intérêt du partage de cyberinformations

Le partage d'informations est essentiel pour soutenir la gestion des cyberrisques dans le domaine de l'aviation. Dans le monde interconnecté d'aujourd'hui, les cybermenaces font peser des risques notables sur le secteur de l'aviation civile. Des cyberattaques peuvent viser n'importe quel aspect du système de l'aviation, des systèmes de gestion du trafic aérien aux systèmes de données sur les passagers, ce qui peut entraîner des perturbations sur le plan opérationnel et mettre les passagers en péril. Par conséquent, une gestion efficace des cyberrisques appelle une approche collaborative qui passe notamment par l'échange d'informations entre les parties prenantes.

Les enseignements de l'expérience en matière de sûreté et de sécurité de l'aviation montrent bien qu'une culture du partage d'informations est de nature à réduire considérablement les risques que des acteurs malveillants font peser sur l'aviation civile. Il est établi que le partage d'informations constitue un outil précieux pour la sûreté et la sécurité dans le secteur de l'aviation. Cela vaut également pour la cybersécurité de l'aviation. En échangeant des cyberinformations, les parties prenantes peuvent avoir une meilleure compréhension des cybermenaces auxquelles elles sont confrontées, identifier les vulnérabilités et prendre des mesures appropriées pour prévenir ou atténuer les cyberattaques contre l'aviation civile.

Le partage d'informations joue aussi un rôle fondamental à l'appui d'une solide culture de la cybersécurité. Une telle culture aide à reconnaître les cybermenaces et à y répondre efficacement. Le partage d'informations en fait partie intégrante dans la mesure où il favorise la transparence, la collaboration et la confiance entre les parties prenantes. Bien mené, il permet à toutes de disposer des données nécessaires pour prendre des décisions en connaissance de cause, engager les actions qui conviennent, atténuer les cybermenaces et/ou réagir aux cyberincidents et s'en remettre.

Les cyberinformations ne consistent pas seulement dans des informations exploitables qui se rapportent spécifiquement au numérique, mais couvrent tout type de renseignement susceptible d'intéresser la lutte contre les cyberrisques dans l'aviation civile. Le partage de cyberinformations ne se limite pas au renseignement sur des questions propres à l'informatique. Il s'applique à toute information pertinente pour repérer et atténuer les cyberrisques dans le secteur de l'aviation civile. Par exemple, les informations concernant les atteintes à la sûreté matérielle, les menaces internes, le contexte géopolitique, la technologie ou encore les vulnérabilités de la chaîne logistique peuvent également aider les parties prenantes à mieux comprendre et atténuer les cybermenaces et les cyberrisques.

Le partage de cyberinformations soutient :

- **la planification stratégique**, pour renforcer les capacités en matière de cybersécurité dans le domaine de l'aviation. En échangeant des informations, les parties prenantes peuvent repérer des lacunes dans leurs capacités en matière de cybersécurité et élaborer des stratégies adaptées pour améliorer leur cyberrésilience. La planification stratégique permet de garantir que le secteur de l'aviation reste protégé et résilient face aux cybermenaces et que les parties prenantes soient prêtes à réagir à d'éventuels cyberincidents et à s'en remettre ;
- **l'appréciation de la situation**, tant dans le cadre des opérations quotidiennes qu'en cas de cyberincident. En échangeant des cyberinformations, les parties prenantes sont à même de mieux comprendre leurs positions respectives en matière de cybersécurité, l'état des cybermenaces et les vulnérabilités (faiblesses) que leurs systèmes peuvent présenter. Elles sont ainsi en mesure d'identifier les risques potentiels et de prendre

les dispositions qui conviennent pour prévenir les cyberincidents ou en limiter les conséquences ;

- **la gestion opérationnelle et tactique des cyberrisques**, pour anticiper ou contrer une cybermenace. En échangeant des informations, les parties prenantes peuvent détecter les cybermenaces et mettre au point les stratégies de gestion des risques qui conviennent ;
- **la gestion des crises** lors d'un cyberincident, un bon échange d'informations permettant aux parties prenantes de coordonner leur réponse et de prendre les mesures voulues afin d'atténuer les répercussions d'un incident.

Il est essentiel d'avoir à l'esprit que pour être efficace, le partage d'informations doit reposer sur la confiance qui règne entre les participants. Les présentes orientations visent à favoriser l'instauration de la confiance nécessaire pour encourager un groupe d'acteurs à surmonter leurs hésitations naturelles lorsqu'il s'agit d'échanger des informations. Cela passe par la définition d'un ensemble de règles et de procédures communes qui soient comprises, acceptées et respectées par tous. Pour faciliter les choses, il convient de rechercher un consensus à propos de la nature des cyberinformations partagées, des modalités de l'échange et des méthodes de diffusion.

Les présentes orientations s'ajoutent à l'action globale de l'OACI en matière de cybersécurité de l'aviation. Elles viennent à l'appui du cinquième pilier de la stratégie de cybersécurité de l'aviation de l'OACI, à savoir le partage de l'information, et du point 5.1 du plan d'action pour la cybersécurité, au titre duquel il est demandé à l'OACI d'élaborer des orientations concernant le partage de cyberinformations.

Le présent document incorpore et remplace les éléments indicatifs portant spécifiquement sur l'utilisation du protocole des feux de circulation (TLP) dans l'aviation civile, précédemment publiés par l'OACI. S'y trouvent également des directives sur la manière d'utiliser la norme TLP[3] dans sa version actualisée, mise au point par le FIRST (Forum of Incident Response and Security Teams), pour le partage de cyberinformations dans l'aviation civile.

1.2 Contexte du partage de cyberinformations

Avant d'aborder le partage de cyberinformations en soi, il est nécessaire de se pencher sur le cycle de vie global du cyberrenseignement.

Le cycle de vie du cyberrenseignement constitue un processus itératif fondamental dans le domaine de l'analyse du renseignement. Chacune de ses étapes remplit une fonction essentielle, en garantissant la transformation des informations, de leur état de données brutes à celui de produits de renseignement pour faciliter la prise de décision, améliorer la cybersécurité et soutenir les divers objectifs stratégiques de l'organisation.

L'échange d'informations (également appelé « diffusion » dans la figure 1 ci-dessous) fait partie du cycle de vie du cyberrenseignement, qui comprend les étapes suivantes :

1. Planification et orientation : la première étape de l'entreprise de collecte et d'analyse de cyberinformations consiste à planifier et à orienter le processus. Il s'agit d'en définir les objectifs, d'en déterminer la portée et l'ampleur, et d'identifier les parties prenantes qui doivent être impliquées. La planification et l'orientation passent également par l'élaboration de politiques et de procédures pour la collecte et l'analyse des informations, ainsi que par la définition des rôles et des responsabilités des acteurs concernés aux différentes étapes.

[3] https://www.first.org/tlp/

2. Collecte : la deuxième étape consiste dans la collecte proprement dite des cyberinformations. Il s'agit de recueillir des données auprès de différentes sources (voir section 3). La collecte peut être effectuée manuellement ou au moyen de processus automatisés. Il est essentiel de veiller à ce que les données recueillies soient pertinentes, exactes et opportunes.

3. Traitement : la troisième étape consiste à traiter les informations recueillies. Il s'agit de convertir les données collectées dans un format exploitable, de les analyser et de repérer des configurations ou des anomalies susceptibles d'indiquer une cybermenace. Cette étape peut nécessiter l'emploi d'outils de traitement des données, d'algorithmes et d'autres techniques d'analyse, notamment pour aider à la détection de cybermenaces ou à la découverte de vulnérabilités. Le traitement a également pour but de déterminer l'importance et le degré d'urgence des informations et d'établir les priorités d'intervention en conséquence.

4. Analyse et production : la quatrième étape consiste à analyser et à produire des rapports sur la base des données traitées. Il s'agit d'interpréter les données, de repérer des schémas ou des tendances et de déterminer les cyberrisques pour le système de l'aviation. Des informations peuvent ainsi être écartées si elles ne présentent pas un niveau de qualité ou de détail suffisant pour être analysées. Les analystes s'appuient sur leurs connaissances et leur expérience afin d'interpréter les données et de produire des rapports de renseignement qui soient pertinents pour le public visé et dont le contenu soit précis et exploitable. L'étape d'analyse et de production peut également comprendre l'élaboration de recommandations pour atténuer ou prévenir les cybermenaces.

5. Diffusion (partage de cyberinformations) et retour d'information : la dernière étape consiste à diffuser les rapports de renseignement auprès des parties prenantes concernées. Il peut s'agir de communiquer des cyberinformations à des parties prenantes internes, telles que les équipes chargées respectivement de l'informatique, de la cybersécurité et/ou de la sûreté/sécurité de l'aviation, ainsi qu'à des parties prenantes externes, telles que d'autres organisations s'occupant d'aviation ou des organismes publics. La diffusion suppose de s'assurer que les cyberinformations sont communiquées en temps utile et de façon sûre, et que les parties prenantes disposent des éléments de contexte nécessaires et en ont la compréhension requise pour les exploiter. Efficacement opérée, elle contribue au développement d'une culture du partage de cyberinformations dans le secteur de l'aviation civile et donne aux parties prenantes les moyens d'agir en vue de prévenir ou d'atténuer les cybermenaces.

Le retour d'information qui intervient à cette étape permet en outre d'évaluer l'efficacité et la pertinence du cycle de vie du cyberrenseignement, l'objectif étant de l'améliorer avec le temps.

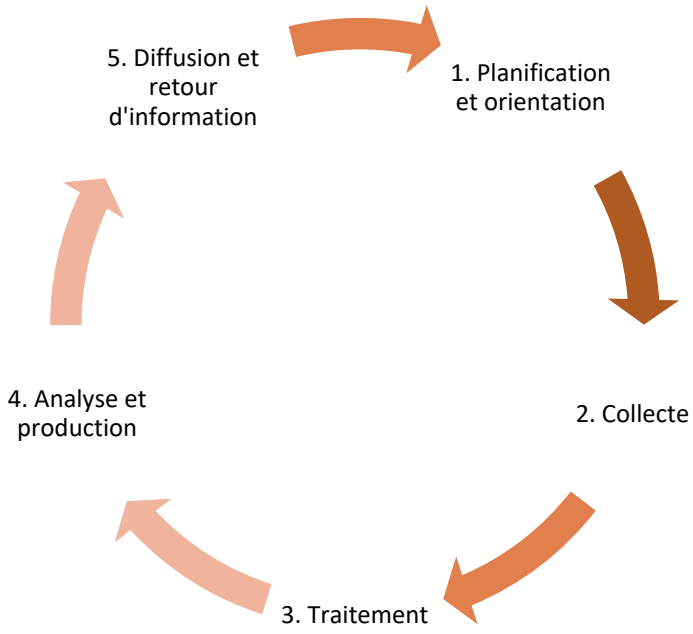

Figure 1. Cycle de vie du cyberrenseignement

2. POLITIQUE RELATIVE AU PARTAGE DE CYBERINFORMATIONS

La présente section contient des orientations sur la manière d'élaborer et de mettre en œuvre une politique relative au partage de cyberinformations au niveau organisationnel (p. ex. : entre les parties prenantes du secteur de l'aviation).

Ces orientations peuvent également servir aux États pour l'établissement de leurs plans en matière de partage de cyberinformations. Il faut toutefois noter que les programmes nationaux de partage de cyberinformations peuvent être intersectoriels et non spécifiques à l'aviation.

2.1 Politique relative au partage de cyberinformations (CIShP)

La CIShP doit définir :

- la raison du partage de cyberinformations ;
- le champ d'application, le contexte et les limites (p. ex. : sources des cyberinformations, limites liées aux droits de propriété intellectuelle (DPI), lois sur la protection de la vie privée) ;
- les membres du groupe concerné par le partage de cyberinformations au sein de l'organisation et leurs responsabilités respectives ;
- les règles de distribution (y compris secondaire[4]) des cyberinformations à l'intérieur et à l'extérieur de l'organisation, conformément aux règles de classement/catégorisation des informations et compte tenu des exigences réglementaires et juridiques pertinentes ;
- les procédures opérationnelles :
  - collecte des informations ;
  - dépersonnalisation, au besoin ;
  - validation du contenu ;
  - distribution ;
- le cycle d'examen de la CIShP et le contrôle des documents (enregistrement des modifications notables et procédures de validation).

La CIShP doit être approuvée par l'organisation dans le cadre du système de gestion de la sécurité de l'information (ISMS)[5]. Elle doit être réexaminée périodiquement (p. ex. : chaque année), après qu'un changement important lui a été apporté ou à la suite d'un cyberincident afin de tenir compte des enseignements tirés de l'expérience.

2.2 Exigences réglementaires et contractuelles[6]

Le CIShP doit être compatible avec toutes les réglementations applicables et tous les accords en vigueur qui se rapportent au partage de cyberinformations, notamment :

- les réglementations intersectorielles nationales, régionales et/ou internationales à caractère intersectoriel ;
- les réglementations nationales, régionales et/ou internationales spécifiques à l'aviation ;

[4] La distribution secondaire (la transmission par les destinataires initiaux) des informations est abordée dans la section 5 du présent document.
[5] Norme ISO 27001, chapitre A.5.14, *Transfert de l'information*.
[6] De plus amples informations (intersectorielles) figurent aux liens suivants :
NIST.SP.800-150 – Guide to cyber threat information sharing
ENISA, Cyber Security Information Sharing : An Overview of Regulatory and Non-regulatory Approaches
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

- les accords conclus avec les centres nationaux et/ou internationaux d'analyse et de partage de l'information (ISAC) et les équipes d'intervention informatique d'urgence/équipes d'intervention face aux cyberincidents de sûreté (CERT/CSIRT) (p. ex. : ISAC du secteur de l'aviation, équipe d'intervention informatique d'urgence pour la gestion du trafic aérien européen (EATM-CERT), CERT/CSIRT nationales).

2.3 Ressources

L'organisation doit déterminer les ressources nécessaires pour assurer la bonne mise en œuvre de la CIShP, à savoir :

- ressources humaines : tirer parti des équipes de cybersécurité existantes, comme celle du Centre des opérations de sûreté (SOC), et engager de nouvelles personnes au besoin ;
- ressources techniques : site web, courrier électronique, téléphone, SMS et plateformes d'échange sécurisées et/ou de confiance ;
- ressources financières : coûts liés à l'acquisition et/ou au développement de systèmes, à la formation du personnel, etc.

2.4 Mise en œuvre

La mise en œuvre de la CIShP comprend les phases suivantes :

- définition du cadre : détermination des sources d'information et des cyberinformations à partager dans le cadre de la CIShP ;
- établissement des outils à utiliser pour le partage de cyberinformations ;
- désignation d'un point de contact (PoC) pour le réseau de partage de cyberinformations et instauration de processus pour la tenue à jour des informations le concernant ;
- mise à l'essai des systèmes et des processus de partage de cyberinformations, et ajustement selon qu'il convient ;
- lancement du mécanisme de partage de cyberinformations (déploiement) ;
- suivi et contrôle continus ;
- examen et perfectionnement continus.

3. GESTION DES CYBERINFORMATIONS ET DE LEUR PARTAGE

3.1 Types de cyberinformations

Il est possible de partager les cyberinformations suivantes.

CYBERRENSEIGNEMENT

- **Renseignement sur les cybermenaces (CTI)** : inclut notamment des informations sur le paysage des cybermenaces et l'appétit des pirates informatiques.
  - **Stratégique** : aide une organisation à comprendre le type de cybermenace et les capacités et motivations des attaquants ;
    - permet de dresser un tableau général des intentions et des capacités attachées aux cybermenaces malveillantes ;
    - éclaire la prise de décision et/ou sert à l'alerte rapide ;
    - peut inclure des tendances (p. ex. : cibles, comportements des attaquants), des statistiques, des informations relatives aux cybermenaces (p. ex. : menaces persistantes avancées (APT), rapports de cyberincident, documents d'orientation, livres blancs/documents de recherche), etc.
    - *Exemple de CTI stratégique : rapport complet sur les nouvelles cybermenaces qui pèsent sur les infrastructures critiques d'un État, décrivant les vulnérabilités potentielles et les vecteurs d'attaque possibles. Ce rapport est généralement mis à profit par les décideurs de haut niveau pour élaborer des politiques et stratégies de long terme en matière de cybersécurité.*
  - **Opérationnel :**
    - contextualise les cyberincidents, permettant aux défenseurs de repérer tout danger éventuel ;
    - donne la possibilité de déterminer les répercussions possibles de cyberincidents sur les opérations (p. ex. : tactiques, techniques et procédures (TTP), motivations, impact, moment choisi) ;
    - aide à l'allocation des ressources et à la hiérarchisation des tâches.
    - *Exemple de CTI opérationnel : informations sur une campagne d'hameçonnage en cours qui cible l'aviation, y compris des détails comme les TTP utilisées par les acteurs à l'origine de la menace. Ces informations sont précieuses pour les équipes chargées des opérations de sûreté, qui peuvent ainsi détecter les cybermenaces immédiates et les contrer.*
  - **Tactique** : aide à la définition préventive d'une posture de sûreté capable de résister à des attaques (p. ex. : indicateurs de compromis (IoC), TTP, vulnérabilités).
    - *Exemple de CTI tactique : IoC liés à telle ou telle variante d'un logiciel malveillant. Il s'agit notamment d'adresses IP spécifiques, de hachage de fichiers et de modèles de comportement associés au logiciel malveillant. Ces informations tactiques sont utilisées par les analystes en cybersécurité de première ligne pour repérer et atténuer les cybermenaces en temps réel.*
- **Indicateurs de compromis (IoC)** : adresses IP malveillantes, URL malveillantes, noms de domaine malveillants ou hachage de logiciels malveillants, entre autres.

- Le partage de ces informations aide les destinataires à mieux protéger leurs systèmes/services.
- Lors du partage d'IoC, il n'est pas nécessaire de divulguer qui les a découverts.

- **Tactiques, techniques et procédures (TTP)** : scénarios d'attaque et méthodes préférées des pirates informatiques[7].

- **Vulnérabilités** :
  - **En tant qu'utilisateur d'un cyberactif** : les cyberinformations à communiquer se rapportent principalement au cyberactif (p. ex. : matériel, logiciel, service, protocole, norme) pour lequel la vulnérabilité a été découverte. Il n'est pas utile d'indiquer son identité.
    - Ces informations peuvent être mises à la disposition des autres afin de les aider à se protéger.
    - Il n'est pas nécessaire de préciser qui a détecté la vulnérabilité.
    - En ce qui concerne la divulgation responsable de vulnérabilités, le programme de gestion des vulnérabilités de l'organisation peut proposer un « tableau d'honneur » ou un processus similaire pour saluer les contributions des chercheurs à la découverte de vulnérabilités.
  - **En tant que propriétaire d'un cyberactif** : il convient de faire part des vulnérabilités aux utilisateurs.
    - Le propriétaire devrait proposer un correctif ou une modification.
    - À titre de pratique exemplaire, il est souhaitable d'informer les CERT/CSIRT (nationaux ou sectoriels) de ces vulnérabilités, afin de renforcer leur position face à tout cyberincident lié au cyberactif en question.
  - Une distinction peut être établie entre vulnérabilités potentielles, confirmées et exploitées pour déterminer la manière d'aborder la diffusion d'informations à leur sujet.

RAPPORT DE CYBERINCIDENT

- Informations sur un cyberincident touchant une organisation.
- Doit inclure, dans la mesure du possible : résumé, type, date et heure exactes de survenue, lieu de survenue, durée, chronologie (c'est-à-dire enchaînement des événements), IoC, TTP, contexte, vulnérabilité(s), répercussions (sécurité, sûreté, efficacité, capacités, activité, finances, réputation), gravité, motivation, cible, acteur à l'origine de la menace, services et organisation(s) touchés, etc.
- En règle générale, plus les informations fournies sont nombreuses, plus le rapport est exploitable.

CYBERATTÉNUATION

- Indication de méthodes pour :
  - remédier aux vulnérabilités ;
  - atténuer les cybermenaces ;
  - réagir aux cyberincidents et s'en remettre.

[7] MITRE ATT&CK a élaboré et tient à jour une taxonomie des TTP qui peut être consultée sur son site web : https://attack.mitre.org/.

- Indications les plus courantes : correctifs pour remédier aux vulnérabilités, mises à jour d'antivirus pour arrêter les exploits, instructions pour éliminer les acteurs malveillants des réseaux.

APPRÉCIATION DE LA SITUATION

- Télémétrie en temps réel des vulnérabilités exploitées, des menaces actives et des cyberattaques pouvant être nécessaires pour répondre à un cyberincident, à l'usage des décideurs.
- Peut également inclure des renseignements sur les cibles des attaques et l'état des réseaux informatiques publics ou privés d'importance critique.

MEILLEURES PRATIQUES

- Informations relatives à la manière dont les logiciels et les services sont élaborés et fournis : contrôles de sûreté, pratiques en matière de développement et de réaction aux incidents, correctifs logiciels et mesure de l'efficacité, notamment.

3.2 Émetteurs, destinataires et sources des cyberinformations

- Le partage de cyberinformations suppose un émetteur, un destinataire et une source (si les informations ne viennent pas directement de l'émetteur).
- Le tableau ci-dessous donne des exemples d'émetteurs, de destinataires et de sources de cyberinformations dans l'aviation civile.

Émetteurs/destinataires	• Usagers de l'espace aérien (p. ex. : entreprises de transport aérien, aviation générale, opérateurs de systèmes d'aéronef non habité (UAS)) • Fournisseurs de services de navigation aérienne (ANSP) • Exploitants d'aéroport • Autorités (p. ex. : autorité de l'aviation civile (AAC)) • Fournisseurs de services aéronautiques • Constructeurs • Chaîne d'approvisionnement aéronautique et non aéronautique • Autres
Sources	• Émetteurs/destinataires ci-dessus • Aéronefs (p. ex. : UAS, avions) • Renseignement de sources ouvertes (OSINT) • Fournisseurs de CTI • Associations et organisations internationales (p. ex. : associations d'entreprises de transport aérien, d'aéroports et d'ANSP) • Centres internationaux/nationaux/régionaux de cybersécurité de l'aviation et CERT/ISAC dans le domaine de l'aviation • Autres

- L'appendice A présente le flux recommandé pour les différents types de cyberinformations pouvant être mises en commun entre les différentes parties prenantes de l'aviation.

3.3 Évaluation, analyse et marquage TLP des cyberinformations par l'émetteur

3.3.1 Évaluation et analyse

Avant de partager des cyberinformations, l'émetteur doit procéder à une analyse pour :

- évaluer la fiabilité de la source (voir 3.3.1.1 et appendices B et D) ;
- estimer la plausibilité/crédibilité des informations (voir 3.3.1.2 et appendices C et D) ;
- déterminer la pertinence des informations pour l'organisation, la communauté de diffusion (organisation(s) destinataires (s)) et l'écosystème de l'aviation.

Il s'agit d'une étape essentielle du partage de cyberinformations. Sans cela, les éléments communiqués ne sont qu'un ensemble de données/constatations dépourvues de contexte.

Aux fins de cette analyse, il importe de rappeler que :

- des problèmes analytiques différents appellent des approches différentes ;
- les analystes doivent être conscients de leurs préjugés naturels et faire le maximum pour les surmonter afin de procéder à une analyse objective en utilisant les méthodes et outils qui conviennent.

Pour illustrer le rôle de l'évaluation et de l'analyse des cyberinformations, les figures 2 et 3 ci-dessous montrent ce qui diffère entre les informations de sources ouvertes et le renseignement de sources ouvertes, d'où il ressort clairement que l'utilité des informations augmente sensiblement lorsqu'elles sont dûment analysées et que leur fiabilité est vérifiée avant diffusion.

- **OSINF (informations de sources ouvertes)** – les informations recueillies sont partagées telles quelles.

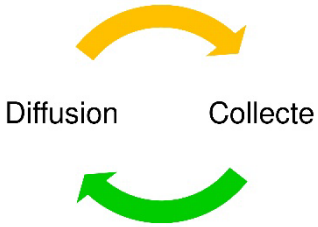

Figure 2. OSINF - Informations de sources ouvertes

- **OSINT (renseignement de sources ouvertes)** – les informations passent par le processus ci-dessous après leur collecte.

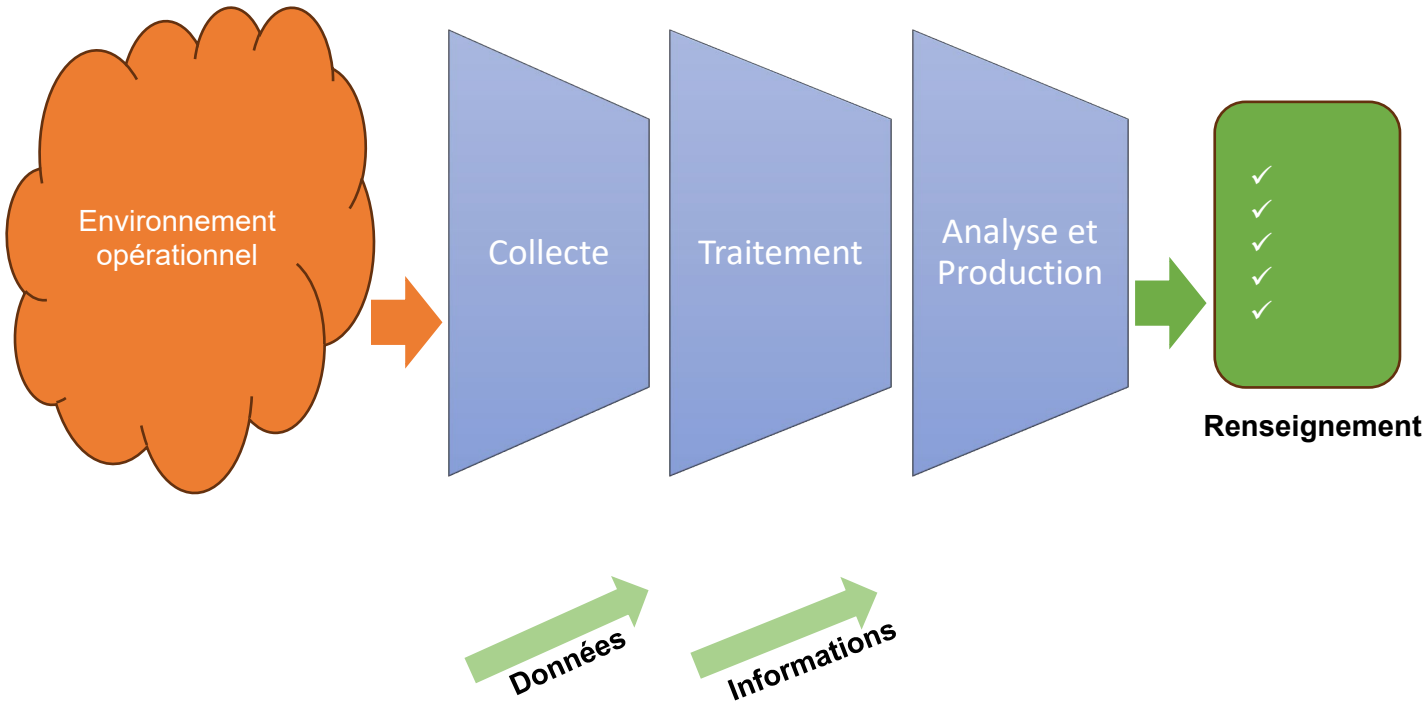

Figure 3. Production de cyberrenseignement[8]

3.3.1.1 Évaluation de la fiabilité de la source

Pour des décisions éclairées, il est crucial d'évaluer la fiabilité de la source des cyberinformations/du cyberrenseignement.

L'appendice B présente un exemple de cadre pour la définition de critères et propose un mécanisme d'évaluation pour mesurer la fiabilité d'une source de cyberinformations/cyberrenseignement.

Les coefficients de pondération et le barème de notation utilisés dans l'appendice B peuvent être adaptés aux exigences propres de l'organisation et à sa tolérance au risque.

L'appendice D fournit un autre exemple de mécanisme permettant d'évaluer à la fois la fiabilité de la source et la crédibilité des informations (voir 3.3.1.2 ci-dessous) au moyen d'une méthode différente : le code de l'Amirauté (système de l'OTAN).

Il convient que les organisations réévaluent et actualisent régulièrement les indices de confiance, étant donné que le paysage des cybermenaces et les sources de renseignement sur les menaces évoluent au fil du temps.

3.3.1.2 Analyse de la plausibilité/crédibilité des cyberinformations

Il est essentiel d'évaluer le niveau de plausibilité/crédibilité des cyberinformations/éléments de cyberrenseignement.

[8] Adapté de publication de doctrine interarmées 2-0, *Joint Intelligence* (2013).

L'appendice C présente un exemple de cadre pour la définition de critères et propose un mécanisme d'évaluation pour mesurer la plausibilité/crédibilité des cyberinformations/éléments de cyberrenseignement.

Les coefficients de pondération et le barème de notation utilisés dans l'appendice C peuvent être adaptés aux exigences propres de l'organisation et à sa tolérance au risque.

Il convient que les organisations réévaluent et actualisent régulièrement les notes de plausibilité/crédibilité à mesure qu'apparaissent de nouvelles informations/de nouveaux éléments de renseignement sur les cybermenaces et au fil de l'évolution du paysage des cybermenaces.

L'appendice D fournit un autre exemple de mécanisme permettant d'évaluer à la fois la fiabilité de la source (voir 3.3.1.1 ci-dessus) et la crédibilité des informations au moyen d'une méthode différente : le code de l'Amirauté (système de l'OTAN).

3.3.2 Marquage du protocole des feux de circulation (TLP) [9,10]

3.3.2.1 Utilisation du TLP dans l'aviation

La norme TLP comprend cinq marquages : RED, AMBER, AMBER+STRICT, GREEN et CLEAR.

Étant donné que le marquage **TLP:CLEAR** ne restreint pas la diffusion des informations reçues, à quiconque et quel que soit le support, et que le marquage **TLP:RED** limite la divulgation des informations au(x) destinataire(s) défini(s), sans la moindre possibilité de les relayer, ces deux marquages ne sont pas abordés dans la présente section. Les trois marquages pouvant appeler des précisions sur la manière de les appliquer dans le contexte de l'aviation sont les suivants :

- **TLP:GREEN**
- **TLP:AMBER**
- **TLP:AMBER+STRICT**

TLP:GREEN	- Les informations marquées TLP:GREEN peuvent être partagées au sein de la communauté de l'aviation. - Leur destinataire peut les transmettre à son tour à toute entité de l'aviation (AAC, ANSP, exploitants d'aéroport, usagers de l'espace aérien, constructeurs, fournisseurs de services aéronautiques, etc.). - Elles peuvent également être communiquées à des organismes de cybersécurité jouant un rôle dans l'aviation (centres nationaux de cybersécurité, CERT/CSIRT nationaux/régionaux/internationaux de l'aviation, ISAC du secteur de l'aviation, etc.). - Elles peuvent en outre être mises à la disposition d'organisations extérieures à l'aviation qui emploient des technologies similaires (p. ex. : informations liées aux

[9] Le protocole des feux de circulation (TLP) est une norme élaborée par le FIRST (Forum of Incident Response and Security Teams) pour faciliter la communication des informations au public concerné. Le présent document donne des orientations sur l'utilisation de la version 2.0 de la norme TLP, qui peut être consultée à l'adresse suivante : https://www.first.org/tlp/.

[10] Les orientations contenues dans le présent document annulent et remplacent les « Orientations relatives au Traffic Light Protocol » publiées par l'OACI en 2021.

	technologies opérationnelles ou de l'information), qui se heurtent à des cybermenaces similaires ou qui fournissent des services à l'aviation (p. ex. : systèmes ou services de télécommunication ou d'énergie). Il peut s'agir d'acteurs d'autres secteurs (p. ex. : exploitants, autorités, constructeurs) ou d'entités liées à la cybernétique (centres nationaux de cybersécurité, CERT/CSIRT d'autres secteurs, ISAC d'autres secteurs).

TLP:AMBER	- Les informations marquées TLP:AMBER peuvent être partagées sur la base du besoin d'en connaître au sein de l'organisation du destinataire et à ses clients. - Bien que la signification du terme « organisation » soit claire, celle de « clients » ayant le besoin d'en connaître, dans le domaine de l'aviation doit être interprétée comme suit : o Les AAC peuvent communiquer ce type d'informations : ▪ au sein de leur État : • aux parties prenantes nationales de l'aviation ; • aux centres nationaux de cybersécurité ; • aux CERT/CSIRT et ISAC nationaux de l'aviation. ▪ en dehors de leur État : • à d'autres AAC ; • aux CERT/CSIRT et ISAC nationaux/régionaux/internationaux de l'aviation. o Les parties prenantes de l'aviation (ANSP, exploitants d'aéroport, usagers de l'espace aérien, fournisseurs de services d'aviation) peuvent communiquer ce type d'informations : ▪ à leurs AAC nationales ; ▪ aux organisations qui soutiennent leurs prestations ; ▪ aux CERT/CSIRT et ISAC nationaux/régionaux/internationaux de l'aviation ; ▪ à leur clientèle, exception faite des passagers (p. ex. : agents de voyage, boutiques hors taxes). o Les constructeurs peuvent communiquer ce type d'informations : ▪ aux AAC nationales ; ▪ à leur clientèle (p. ex. : entreprises de transport aérien, aéroports) ; ▪ aux CERT/CSIRT et ISAC nationaux/régionaux/internationaux de l'aviation ; ▪ à leurs sous-traitants.

TLP:AMBER+STRICT	- Les informations marquées TLP:AMBER+STRICT peuvent être partagées sur la base du besoin d'en connaître au sein de l'organisation du destinataire.

3.3.2.2 Marquage TLP recommandé selon les cyberinformations

Il est recommandé de suivre les orientations ci-après pour marquer les cyberinformations aux fins d'aviation. Certaines considérations peuvent conduire à s'écarter de ces recommandations, notamment :

- Évolution du marquage TLP au fil du temps : plus restrictif lorsque les cyberinformations sont partagées pour la première fois, il peut être assoupli par la suite, à mesure que le risque associé aux informations diminue avec l'élargissement de leur diffusion.
- Points de vue respectifs des États et du secteur sur le marquage des cyberinformations : un État peut appliquer en la matière des règles différentes de celles d'une partie prenante de l'aviation, au nom de diverses considérations (p. ex. : contraintes de sécurité nationale).
- Contraintes nationales applicables au secteur : un État peut avoir un marquage spécifique pour certains types d'informations concernant des infrastructures nationales critiques (p. ex. : divulgation initiale d'IoC tels que des adresses IP suspectes).

CYBERRENSEIGNEMENT

- **Renseignement sur les cybermenaces (CTI)** :
  - **Stratégique :** dépend de la nature du CTI stratégique et du public visé (p. ex. : conseil d'administration, niveau C, analyste CTI, équipe bleue).
    - TLP:RED : élément de renseignement spécifique et très sensible sur une cybermenace précise visant une organisation. Ne s'adresse qu'à un nombre restreint de décideurs concernés.
    - TLP:AMBER : les cadres supérieurs, les membres du conseil d'administration ou les membres du comité de décision doivent être informés d'une cybermenace particulière qui cible l'organisation, intéresse l'aviation (p. ex. : chaîne logistique, parties prenantes liées) et/ou concerne les infrastructures nationales critiques.
    - TLP:GREEN : élément de renseignement devant être partagé avec toute une communauté pour garantir qu'il soit porté à la connaissance d'un large public et suivi d'effet (p. ex. : documents d'orientations, livres blancs, tendances, statistiques).
  - **Opérationnel :**
    - TLP:RED : pour le personnel opérationnel, technique et de sûreté qui doit agir sur la base d'éléments de renseignement portant précisément sur une cybermenace ou un cyberincident spécifique dont la cible est une partie prenante de l'aviation ou une infrastructure nationale critique (p. ex. : chaîne logistique, partie prenante liée).
    - TLP:AMBER : pour le personnel opérationnel, technique et de sûreté qui doit être informé d'une cybermenace ou d'un cyberincident spécifique dont la cible est l'organisation ou qui concerne l'aviation ou des infrastructures nationales critiques.
    - TLP:GREEN : élément de renseignement devant être partagé avec tout une communauté pour garantir qu'il soit porté à la connaissance d'un large public et suivi d'effet.

- **Tactique :**
  - TLP:RED : pour le personnel technique et de sûreté compétent qui doit réagir à une cybermenace précise dont la cible est l'organisation ou qui doit être informé d'un cyberincident en cours.
  - TLP:AMBER : pour le personnel technique et de sûreté qui doit être informé d'une cybermenace, d'un cyberincident en cours ou d'une vulnérabilité affectant l'organisation ou concernant l'aviation ou des infrastructures nationales critiques.
  - TLP:GREEN : élément de renseignement devant être partagé avec tout une communauté pour garantir qu'il soit porté à la connaissance d'un large public et suivi d'effet.

- **IoC** : TLP:GREEN

- **TTP** : TLP:GREEN

- **Vulnérabilités** :
  - Vulnérabilité exploitée : TLP:RED
  - Vulnérabilité confirmée (avec ou sans correctif) : TLP:AMBER
  - Vulnérabilité potentielle sans correctif : TLP:AMBER
  - Vulnérabilité potentielle avec correctif : TLP:GREEN

RAPPORT DE CYBERINCIDENT

- Pas de recommandation, car tout dépend de la nature, du contexte et du déroulement de l'incident (c'est-à-dire du temps écoulé entre le cyberincident et le partage d'informations). TLP:CLEAR peut être exclu dans les premières phases, bien que ce marquage puisse devenir applicable après un certain temps.

3.4 Évaluation et analyse des informations en tant que destinataire

Le destinataire doit analyser les informations reçues pour s'assurer qu'elles sont :

1. **Fiables/garanties/de qualité** : le niveau de confiance[11] dans les cyberinformations peut ne pas être suffisant pour considérer qu'elles doivent déclencher certaines actions de la part du destinataire.
2. **Pertinentes** : à titre d'illustration, le destinataire peut ne pas être en position d'agir sur la base des informations (p. ex. : parce qu'il n'a pas besoin d'en connaître) alors que celles-ci sont pertinentes pour un autre membre du personnel de l'organisation. Cela peut être gênant si les informations reçues sont de type TLP:RED. Dans ce cas, le destinataire doit prendre contact avec l'émetteur afin de lui demander son accord pour les transmettre au(x) destinataire(s) concerné(s), après en avoir reçu une version satisfaisant à un marquage moins sélectif, ou de lui indiquer un autre point de contact à qui adresser la version TLP:RED au sein de l'organisation.
3. **Exploitables** : le marquage TLP peut empêcher le destinataire d'agir sur la base des informations reçues, obligeant à une discussion plus approfondie entre l'émetteur et le destinataire pour y remédier. Par exemple :
   - Si les informations sont marquées TLP:RED et que le destinataire doit collaborer avec d'autres membres de l'organisation pour y donner suite, mais que les personnes concernées n'ont pas reçu les mêmes informations.
   - Si les informations sont marquées TLP:AMBER+STRICT et que le destinataire doit collaborer avec une autre organisation pour agir en fonction de leur teneur.

[11] Voir 3.3.1.1, 3.3.1.2 et appendices B, C et D.

L'analyse passe aussi par les activités suivantes :

- Le destinataire combine les cyberinformations reçues avec les éléments de renseignement disponibles (p. ex. : en les corrélant et/ou en les complétant avec d'autres informations), ce qui a pour effet d'accroître ou de réduire la confiance accordée à ces informations.
- Le destinataire contextualise les informations par rapport à ses fonctions, ce qui permet de répondre à la question du sens de l'information pour le destinataire dans un contexte politique, stratégique, opérationnel, technique et/ou de cybersécurité.

3.5 Relation de confiance entre les parties

La confiance est un concept dynamique et multiforme qui revêt une importance cruciale pour le partage et l'échange d'informations sensibles dans de bonnes conditions de sûreté. Elle ne vaut pas de manière absolue, mais varie plutôt en fonction du contexte, des relations et des comportements.

L'instauration de relations de confiance entre les parties émettrices et destinataires est essentielle à l'efficacité du partage de cyberinformations.

Des relations de confiance peuvent également s'imposer avec des partenaires ou acteurs inhabituels. Il importe de déterminer quelles sont les principales parties concernées par le partage de cyberinformations à titre préventif et/ou en réaction à un fait nouveau, de manière à garantir une diffusion opportune et pertinente.

Des relations de confiance peuvent être nouées avec des partenaires et des acteurs divers, par exemple :

- Dans l'aviation :
  - Entre les institutions publiques (au niveau national et/ou international)
  - Des institutions publiques aux organisations de l'aviation et vice-versa
  - Entre les organisations du secteur
  - Des institutions publiques ou des organisations de l'aviation aux organisations internationales (p. ex. : l'OACI) et vice-versa
- Avec des partenaires et acteurs extérieurs au secteur de l'aviation :
  - Organisations non gouvernementales
  - Organisations à but non lucratif
  - Organisations internationales (p. ex. : les organismes compétents des Nations Unies)
  - Organisation internationale de police criminelle (OIPC–INTERPOL)

Bâtir la confiance prend généralement du temps. Les États et les parties prenantes peuvent établir, entretenir et favoriser des relations de confiance par les moyens suivants :

- Alliances avec des partenaires aux vues similaires
- Activités régulières : participation à des réunions ou conférences périodiques
- Accords : les deux sections à suivre fournissent des orientations sur les types d'accords qui peuvent être élaborés pour le partage de cyberinformations

Les États et les parties prenantes doivent également examiner les avantages (voir section 1.1) et les coûts de l'établissement et du maintien de relations de confiance, afin de justifier et de déterminer les investissements nécessaires pour de telles entreprises. Les questions qu'il convient de se poser portent sur les points suivants :

- Temps : combien de temps faut-il consacrer à l'établissement et au développement d'une relation ?
- Ressources : quelles sont les ressources humaines et financières à prévoir ?
- Avantages : qu'est-ce que chaque partie obtient de la relation ?
- Risques : qu'est-ce que les parties ont à perdre en nouant une relation ?

- Entretien : quel est le coût du maintien d'une relation en termes de temps et de ressources ?

Le maintien d'une relation de confiance passe notamment par les activités suivantes :

- Réunions en présentiel et à distance : tenues à une fréquence convenue entre les parties, selon que nécessaire et de préférence au moins une fois par an pour les réunions en présentiel, compte tenu du niveau de responsabilité du personnel concerné (supérieur, intermédiaire ou technique)
- Partage de cyberinformations à titre préventif : de façon régulière en fonction des besoins et des priorités, notamment sur les sujets suivants :
    - Modifications de politiques et de procédures pouvant concerner le(s) destinataire(s)
    - Produits : comptes rendus immédiats, analyses stratégiques, etc.
    - Informations brutes : codes sources, journaux, etc.
- Partage de cyberinformations en réaction, par exemple sur la réponse opposée à un cyberincident :
    - Pendant le cyberincident : suivi en temps réel et en continu
    - Après le cyberincident : conclusions, causes profondes, enseignements tirés, etc.

Les relations fondées sur la confiance peuvent prendre fin si celle-ci est rompue à la suite d'un manquement, par exemple :

- Divulgation non autorisée d'informations classifiées : divulgation accidentelle ou délibérée à des personnes ou organisations non autorisées d'informations classifiées pouvant intéresser la sûreté nationale ou concerner des intérêts exclusifs
- Partage délibéré d'informations sensibles : communication intentionnelle d'informations sensibles touchant la sûreté ou de nature exclusive à des personnes ou des organisations dans le but d'exposer des vulnérabilités ou de nuire à la crédibilité d'un tiers, en particulier s'il y est procédé dans le domaine public

3.5.1 Accords formels

Le partage de cyberinformations entre parties peut être formalisé par des accords bilatéraux ou multilatéraux, contraignants ou non contraignants.

Ces accords impliquent différents types de parties. Il peut notamment s'en conclure entre États, entre organismes publics (p. ex. : entre une autorité de l'aviation civile et un organisme national de cybersécurité du même État), entre services gouvernementaux de différents États (p. ex. : entre les autorités de l'aviation civile de différents États), entre un organisme public et une ou plusieurs parties prenantes de l'aviation du même État, entre un organisme public et une ou plusieurs parties prenantes du secteur relevant d'un autre État, et/ou entre des parties prenantes de l'aviation.

À titre de recommandation, l'appendice E fournit une liste de sections à inclure dans un accord formel relatif au partage de cyberinformations afin d'indiquer clairement les rôles et les responsabilités des parties concernées, ce qui aura pour effet de renforcer la confiance entre les parties au fil du temps.

3.5.2 Accords informels

Il est souvent fait recours à des accords informels quand la confiance entre les parties à l'échange est déjà établie ou va sans dire. Les accords de ce type doivent être employés avec précaution, dans la mesure où ils sont sans incidence juridique sur les parties signataires. Il ne faut pas qu'ils constituent le principal ou seul mécanisme de partage de cyberinformations.

Ces accords comprennent des indications limitées qui sont nécessaires pour que les parties puissent échanger des informations, par exemple :

- les moyens techniques à utiliser pour communiquer les informations ;
- les points de contact respectifs (coordonnées de la personne et de l'équipe).

Une utilisation rigoureuse et cohérente du marquage TLP revêt d'autant plus d'importance lorsque des cyberinformations sont mises en commun dans le cadre d'accords informels, afin d'entretenir et de renforcer la confiance entre les parties.

4. STRUCTURATION, COMMUNICATION ET ARCHIVAGE DES CYBERINFORMATIONS PARTAGÉES

4.1 Structuration des cyberinformations à partager

Les cyberinformations doivent être structurées suivant des taxonomies définies ou à l'aide d'une structure définie afin de garantir une contextualisation adéquate et l'incorporation de détails utiles et exploitables.

Exemple de structuration des cyberinformations à partager :

- Titre : description générale des cyberinformations
- Numéro de référence : pour aider l'émetteur à suivre les informations
- Marquage TLP
- Principaux aspects, notamment :
    - Catégorie (p. ex. : cyberespionnage, cybercriminalité, opération d'information)
    - Type (p. ex. : vulnérabilité, botnet, surveillance, données personnelles, médias sociaux, fuite de données d'identification, hameçonnage, déni de service distribué, logiciel malveillant)
    - Niveau de cybermenace (p. ex. : critique, élevé, intermédiaire, faible)
    - Domaine/secteur
    - Fiabilité de la source d'informations (voir 3.3.1.1)
- Points clés : liste de puces expliquant les informations
- Résumé
- Attribution : acteur à l'origine de la menace identifié comme auteur potentiel ou avéré de l'infraction, le cas échéant (il peut y en avoir plusieurs)
- Évaluation des répercussions, des objectifs, des victimes, etc.
- Recommandations concernant les mesures à prendre pour le ou les destinataires
- Informations exploitables
    - Cyberactifs touchés
    - Déroulement
    - IoC
    - Règles de détection
    - TTP
- Stratégies d'atténuation
    - Génériques
    - Spécifiques
- Références

4.2 Communication des cyberinformations

La présente section contient des indications sur les avantages et les inconvénients de différents médias pour le partage de cyberinformations.

4.2.1 Téléphone

Ce mode de communication convient au marquage **TLP:RED** pour garantir une communication synchrone avec le destinataire des informations. Il permet également de communiquer des informations critiques demandant une réponse immédiate.

Pour le partage d'informations par téléphone, il est recommandé de prévoir des contrôles destinés à confirmer l'identité des deux parties (p. ex. : pour éviter les injections audio générées au moyen de l'intelligence artificielle).

De manière générale, ce support offre une utilisabilité limitée (il sert principalement à partager des cyberinformations très urgentes et/ou marquées **TLP:RED**) et doit donc être envisagé en parallèle avec d'autres supports pertinents.

4.2.2 Courriel ordinaire

Des cyberinformations peuvent être communiquées en texte clair dans un courriel.

Le recours à ce support implique ce qui suit :

- Le destinataire doit ouvrir le courriel et lire les informations.
- Un analyste CTI doit examiner le contenu afin d'évaluer sa pertinence pour le destinataire.
- Dans un premier temps, les informations seront traitées manuellement.

Le recours à des courriels en texte clair pour communiquer des cyberinformations présente certaines limites, dont les suivantes :

- Ce support convient aux contenus courts et textuels.
- Certains systèmes de messagerie électronique risquent de bloquer le courriel car celui-ci peut contenir des IoC, déclenchant alors des contrôles de sécurité informatique.
- Il est difficile de tenir à jour des listes de courriels, et donc recommandé d'utiliser des adresses électroniques individuelles et génériques.
- Les informations marquées **TLP:RED** ne peuvent pas être envoyées à des adresses génériques (p. ex. : groupmailbox@company.com), mais seulement à des adresses individuelles (p. ex. : someone@company.com).
- Certains types d'adresses électroniques peuvent ne pas être considérés comme des supports fiables (p. ex. : adresses électroniques non professionnelles hébergées sur des services commerciaux de courrier électronique tels que gmail/hotmail/yahoo/etc.).
- Il existe un risque d'usurpation d'identité par courrier électronique. Par conséquent, il est recommandé d'utiliser des méthodes d'authentification adéquates, telles que la signature électronique des courriels, pour tenir compte de ce risque.

4.2.3 Courriel avec pièce jointe

Des cyberinformations peuvent être communiquées sous forme de pièce jointe à un courriel. La pièce jointe peut être cryptée à l'aide d'un mot de passe envoyé au destinataire par un autre moyen fiable (p. ex. : SMS, application de messagerie sécurisée).

Le recours à ce support implique ce qui suit :

- Le destinataire doit ouvrir la pièce jointe et lire les informations.

- Un analyste CTI doit examiner le contenu afin d'en évaluer la pertinence pour le destinataire.
- Dans un premier temps, les informations seront traitées manuellement.

Le recours à des courriels avec pièce jointe pour communiquer des cyberinformations présente certaines limites, dont les suivantes :

- Il existe un risque de cliquer sur une pièce jointe piégée – l'innocuité de la pièce jointe doit donc être vérifiée au préalable.
- Certains systèmes de messagerie électronique bloquent certains types de pièce jointe (p. ex. : fichiers compressés en .zip, .rar et .7z).
- Certains systèmes de messagerie électronique risquent de bloquer l'accès au document car celui-ci peut contenir des IoC, déclenchant alors des contrôles de sécurité informatique.
- La taille de la pièce jointe peut empêcher sa transmission par courrier électronique.
- Il est difficile de tenir à jour des listes de courriels, et donc recommandé d'utiliser des adresses électroniques individuelles et génériques.
- Les informations marquées **TLP:RED** ne peuvent pas être envoyées à des adresses génériques (p. ex. : groupmailbox@company.com), mais seulement à des adresses individuelles (p. ex. : someone@company.com).

4.2.4 Registre privé

Des cyberinformations peuvent être partagées dans un registre privé.

Dans ce cas, il convient de mettre en place des méthodes de notification pour avertir le ou les destinataires que de nouvelles cyberinformations sont disponibles à la consultation.

Ces notifications peuvent être automatisées et s'effectuer par courrier électronique ou par d'autres moyens (p. ex. : SMS, application de messagerie sécurisée).

L'accès au registre doit être protégé et tenu à jour :

- Des contrôles de sûreté/dispositifs de protection doivent être déployés en fonction du caractère plus ou moins sensible des informations partagées dans le registre. Les contrôles peuvent porter sur : hébergement du registre (p. ex. : serveur privé/partagé, hébergement en nuage), contrôle/droits d'accès, méthodes d'authentification des utilisateurs (p. ex. : authentification unique (SSO), authentification à deux facteurs/multifactorielle (2FA/MFA)), etc.
- La liste des organisations/personnes autorisées à accéder au registre doit être tenue à jour en permanence afin d'en garantir l'actualité et l'authenticité.
- Les droits d'accès, tels que les privilèges de lecture et d'écriture, doivent être attribués à des comptes individuels, et tenus à jour.
- Tous les accès au registre et toutes les actions qui y sont effectuées doivent être enregistrés et analysés.
- Les cyberinformations publiées dans le registre doivent être soigneusement classées dans des dossiers, sachant que tous les participants n'y ont pas le même accès. En outre, il est nécessaire de déplacer les informations d'un dossier à un autre lorsque leur classification (p. ex. : marquage TLP) évolue (elles peuvent par exemple être accessibles à un public plus large si la classification/le marquage TLP descend à un niveau moins strict). Ce processus peut devenir complexe quand le nombre de membres de la communauté et le volume d'informations partagées sur le registre augmentent avec le temps.

4.2.5 Applications

Divers logiciels (libres ou commerciaux) peuvent être utilisés pour partager des cyberinformations (p. ex. : MISP, OpenCTI, CyWare, etc.).

Il n'est pas possible de dresser une liste générique d'aspects à prendre en considération pour les applications en général, car cela dépend de la nature de l'application (p. ex : libre ou commerciale), de qui est en charge du développement et de la mise à jour des contrôles de sûreté, des droits d'accès, du classement des informations (p. ex. : manuel ou automatique selon des règles), du stockage des informations sensibles (p. ex. : serveurs sécurisés/privés ou publics), etc. Il est donc recommandé d'évaluer tous ces aspects, et d'autres si nécessaire, au moment d'envisager le recours à des applications pour le partage de cyberinformations.

Parmi les applications existantes, l'appendice F contient des informations sur MISP - Plateforme de renseignement de sources ouvertes et de partage d'informations sur les menaces, car cette plateforme présente des caractéristiques intéressantes pour soutenir les efforts du secteur de l'aviation en matière de partage de cyberinformations.

4.3 Archivage des cyberinformations

Les cyberinformations partagées doivent être archivées à la fois par l'émetteur et par le destinataire aux fins de tenue des dossiers et de contrôle de la qualité.

Il convient de tenir compte des aspects ci-après pour l'archivage d'informations :

- Réglementation : il importe de prendre en considération les règles pouvant s'appliquer à l'archivage des informations (p. ex. : lois sur la protection de la vie privée et prescriptions connexes en matière d'archivage de certains types d'informations, durée maximale autorisée pour la conservation de ces informations dans les archives, etc.).
- Supports de stockage : le support de stockage utilisé dépend du type d'informations. Différents types de support peuvent être utilisés pour archiver des cyberinformations. Par exemple, les rapports de cyberincident peuvent être stockés dans une base de données autonome spécifique, les rapports de renseignements sur les cybermenaces peuvent être stockés sous la forme d'un fichier sur un disque informatique, etc.
- Contrôle et droits d'accès : l'accès aux cyberinformations archivées doit être défini dans une directive précisant qui peut accéder à quel type d'informations. Cela s'inscrit dans la logique du marquage TLP des informations (p. ex. : **TLP:AMBER+STRICT** ne veut pas dire tous les membres d'une organisation, mais seulement ceux qui ont besoin d'en connaître).
- Accessibilité locale ou à distance : l'accès à certaines cyberinformations peut ne pas être autorisé depuis l'extérieur de l'organisation (p. ex. : par des intranets), mais uniquement en interne. Il s'agit donc également de définir, en fonction des attributions des membres du personnel, les privilèges relatifs aux droits d'accès qui peuvent être utilisés aux fins d'audit/d'assurance.
- Contrôles de sûreté/protection : il convient d'établir différentes strates de contrôles de sûreté et différents niveaux de protection selon le type d'informations. Par exemple, les contrôles destinés à protéger les rapports de cyberincident doivent être plus stricts que ceux déployés pour surveiller les vulnérabilités déjà corrigées.
- Pertinence : certaines cyberinformations peuvent devenir obsolètes en raison de certains faits nouveaux (p. ex. : vulnérabilités de systèmes qui ne sont plus utilisés par l'organisation, éléments de renseignement stratégique sur des cybermenaces en lien avec des situations géopolitique qui n'ont plus cours, etc.).
- Utilisabilité : il importe de définir différentes catégories d'archives afin de garantir l'utilisabilité constante des informations. Par exemple :
    - « Brûlantes » : comprend les données récentes qui sont stockées sans compression dans les fichiers, ce qui permet d'obtenir des performances maximales pour l'extraction et le traitement ;
    - « Chaudes » : comprend les données stockées légèrement compressées, ce qui permet d'obtenir de très bonnes performances pour l'extraction et le traitement en cas de besoin ;

    - « Froides » : comprend les données qui ont été archivées et entièrement compressées, et qui nécessitent une extraction et une décompression manuelles pour être mises à disposition.
- Durée : la durée d'archivage des cyberinformations doit être déterminée en fonction du type d'informations. Par exemple, des règles d'archivage peuvent être définies pour conserver les IoC ne datant pas de plus de [X] ans. En outre, les actions liées à la suppression des informations obsolètes doivent s'effectuer dans le cadre des processus de gestion de l'archivage des cyberinformations.

5. PARTAGE ÉLARGI DE CYBERINFORMATIONS

5.1 Pourquoi relayer des cyberinformations ?

Il peut être nécessaire de partager plus avant les cyberinformations reçues d'une source externe afin de s'assurer qu'elles sont connues de tous ceux qui ont besoin d'en connaître. Toutefois, la prudence s'impose.

Par exemple, un organisme public reçoit des informations d'un émetteur qui n'autorise leur transmission ultérieure qu'à des entités auxquelles cet émetteur est lié par un accord formel. L'organisme public estime que d'autres organismes publics, qui n'ont pas conclu d'accord formel avec l'émetteur des informations, ont besoin de connaître les informations. Dans ce cas, le destinataire doit contacter l'émetteur afin d'obtenir son assentiment pour à son tour porter les informations à la connaissance des autres organismes qui ont besoin d'en connaître.

Pour déterminer s'il convient d'élargir le partage de cyberinformations et à qui, leur destinataire doit notamment prendre en considération les facteurs suivants :

- Limites : ces informations peuvent-elles ou doivent-elles être communiquées à d'autres ? En cas de doute (p. ex. : suspicion d'utilisation potentiellement abusive du marquage TLP), le destinataire peut demander à l'émetteur la permission de relayer les informations.
- Objectif de la transmission, et rôle des nouveaux destinataires envisagés.

L'objectif de la transmission à d'autres des cyberinformations reçues est lié à l'action attendue de la part des nouveaux destinataires :

- Information/sensibilisation : les destinataires envisagés ont besoin d'en connaître et les informations sont partagées à des fins d'information uniquement.
- Pour suite à donner : les destinataires envisagés ont besoin d'en connaître, et les cyberinformations leur sont transmises en vue d'une action précise de leur part, comme :
  - Allouer ou mobiliser des ressources pour remédier à un problème particulier.
  - Allouer ou mobiliser des ressources pour atténuer une cybermenace ou une vulnérabilité particulière.
  - Allouer ou mobiliser des ressources aux fins d'assistance.

Le rôle des destinataires envisagés peut être un facteur déterminant dans la décision de relayer les cyberinformations. Les rôles susceptibles d'impliquer un besoin d'en connaître peuvent être notamment les suivants :

- **Expert technique** : expert ou spécialiste qui supervise la protection de réseaux, de systèmes, de services, d'applications, d'infrastructures de technologie de l'information/technologie opérationnelle, entre autres, contre des accès non autorisés.
- **Responsable des politiques** : personne qui élabore des stratégies, politiques, procédures et/ou processus de cybersécurité dans le domaine de l'aviation ou dans d'autres domaines, applicables par les parties prenantes du secteur de l'aviation.
- **Décideur** : responsable de haut niveau qui approuve la mise en œuvre des stratégies, politiques, procédures et/ou processus de cybersécurité dans le domaine de l'aviation ou dans d'autres domaines.
- **Coordonnateur** : expert ou spécialiste en cybersécurité chargé de faire en sorte que les informations communiquées parviennent bien au personnel concerné.
- **Spécialiste de la sécurité de l'aviation** : expert de la sécurité de l'aviation qui peut déterminer plus précisément les répercussions possibles sur la sécurité de l'aviation, l'efficacité et/ou les capacités.
- **Spécialiste de la sûreté de l'aviation** : expert en sûreté de l'aviation qui peut déterminer plus précisément les répercussions possibles sur la sûreté de l'aviation.

5.2 Règles à respecter pour relayer des cyberinformations

Les règles à respecter pour relayer des cyberinformations couvrent de nombreux aspects qu'il importe d'examiner attentivement :

- L'organisation à laquelle les informations sont relayées (p. ex. : État/partie prenante du secteur/partie prenante extérieure à l'aviation, entité nationale/internationale).
- Le rôle des nouveaux destinataires des cyberinformations.
- Ce qui sera communiqué : les cyberinformations dans leur entier ou seulement un extrait (p. ex. : intégralité d'un document ou paragraphes pertinents uniquement).
- Les circonstances de la transmission des informations : à titre préventif ou en réaction.
- La fréquence de partage : régulière ou au besoin.
- La raison de la mise à disposition des cyberinformations (p. ex. : pour information ou suite à donner).
- Le traitement des cyberinformations : toutes les classifications et mises en garde initiales doivent rester sur les canaux de communication appropriés (à savoir : canaux de communication classifiés et non classifiés).
- Le marquage TLP des cyberinformations ne peut pas être modifié lorsqu'elles sont retransmises.

5.3 Méthode et support à utiliser pour relayer des cyberinformations

La méthode/le support dont il est fait usage pour relayer des cyberinformations doit se caractériser par sa sûreté et sa simplicité, selon qu'il convient.

Informations physiques : Informations fournies sur papier. Les informations doivent être correctement conditionnées (p. ex. : dans un dossier) et sécurisées (p. ex. : dans un folio fermé par un dispositif adapté) pendant le transport jusqu'au lieu de la réunion et avant la remise du ou des exemplaires papier. Les éventuels rappels ou avertissements concernant le traitement doivent être notés sur le support même ou sur une page de garde (p. ex. : les avertissements relatifs au traitement des informations sensibles de sûreté (SSI)[12] se trouvent généralement sur une page de garde contenant des instructions).

Informations électroniques : Les mêmes moyens indiqués pour le partage de cyberinformations dans la section 4.2 s'appliquent au partage élargi de ces informations. Toutefois, il faut avoir à l'esprit que les nouveaux destinataires envisagés pour la transmission des cyberinformations n'ont pas forcément accès à certains moyens électroniques auxquels l'émetteur a accès (p. ex. : adresse électronique sur liste blanche, portail/registre où les informations se trouvent).

Il existe des règles supplémentaires applicables au traitement des informations classifiées, qui varient selon les États ou les organisations. Ces règles doivent être strictement respectées, conformément aux normes et procédures en vigueur.

— — — — — — — —

[12] La section 2.3 du *Manuel de sûreté de l'aviation* de l'OACI (Doc 8973 – Diffusion restreinte), intitulée « Informations sensibles relatives à la sûreté de l'aviation », contient des orientations qui peuvent être utiles dans le cadre du partage de cyberinformations.

Appendice A

Cyberinformations qu'il est recommandé de partager dans le secteur de l'aviation, en fonction du type d'informations

CYBERRENSEIGNEMENT

- **Renseignement sur les cybermenaces (CTI)** :
  - **Stratégique :**
    - Des organismes publics (centre national de cybersécurité, AAC, etc.) aux parties prenantes de l'aviation d'un même État
    - Du centre national de cybersécurité aux CERT/ISAC de l'aviation
    - Des CERT/ISAC de l'aviation aux parties prenantes de l'aviation
    - Entre centres nationaux de cybersécurité de confiance
    - Entre États de confiance
  - **Opérationnel :**
    - Entre parties prenantes de l'aviation
    - Des CERT/ISAC de l'aviation aux parties prenantes de l'aviation
    - Des parties prenantes de l'aviation aux organismes publics (centre national de cybersécurité, AAC, etc.) d'un même État
  - **Tactique :**
    - Entre parties prenantes de l'aviation
    - Des CERT/ISAC de l'aviation aux parties prenantes de l'aviation
    - Du centre national de cybersécurité aux CERT/ISAC de l'aviation
    - Du centre national de cybersécurité aux parties prenantes de l'aviation d'un même État
    - Des parties prenantes de l'aviation aux organismes publics (centre national de cybersécurité, AAC, etc.)

- **Indicateurs de compromis (IoC) :**
  - Entre parties prenantes de l'aviation
  - Des CERT/ISAC de l'aviation aux parties prenantes de l'aviation
  - Du centre national de cybersécurité aux CERT/ISAC de l'aviation
  - Du centre national de cybersécurité aux parties prenantes de l'aviation d'un même État
  - Des parties prenantes de l'aviation au centre national de cybersécurité d'un même État

- **Tactiques, techniques et procédures (TTP) :**
  - Entre parties prenantes de l'aviation
  - Des CERT/ISAC de l'aviation aux parties prenantes de l'aviation
  - Du centre national de cybersécurité aux CERT/ISAC de l'aviation
  - Du centre national de cybersécurité aux parties prenantes de l'aviation d'un même État
  - Des parties prenantes de l'aviation au centre national de cybersécurité d'un même État

- **Vulnérabilités :**
  - Entre parties prenantes de l'aviation
  - Des parties prenantes de l'aviation aux fournisseurs de leur chaîne logistique
  - Des chercheurs aux CERT/ISAC de l'aviation
  - Des chercheurs aux organismes publics (centre national de cybersécurité, AAC, etc.)
  - Des chercheurs aux parties prenantes de l'aviation
  - Des chercheurs aux fournisseurs de la chaîne logistique
  - Des CERT/ISAC de l'aviation aux parties prenantes de l'aviation
  - Du centre national de cybersécurité aux CERT/ISAC de l'aviation
  - Du centre national de cybersécurité aux parties prenantes de l'aviation d'un même État
  - Des parties prenantes de l'aviation aux organismes publics compétents (centre national de cybersécurité, AAC, etc.) d'un même État

RAPPORT DE CYBERINCIDENT

- Rapports obligatoires sur les cyberincidents (en vertu des lois et/ou réglementations nationales applicables) :
  - Des parties prenantes de l'aviation aux organismes publics compétents (centre national de cybersécurité, AAC, etc.) d'un même État (pour les incidents intéressant la sécurité et/ou la sûreté de l'aviation)
  - Des parties prenantes de l'aviation aux autorités d'application de la loi (pour des incidents spécifiques liés à la cybercriminalité, comme la fraude, ou à des lois spécifiques, comme les lois sur la protection de la vie privée)
  - De l'État à l'OACI (pour les cyberincidents liés à des actes d'intervention illicite)

- Rapports facultatifs sur les cyberincidents :
  - Des parties prenantes de l'aviation au centre national de cybersécurité
  - Entre parties prenantes de l'aviation (surtout si elles interagissent)
  - Des parties prenantes de l'aviation aux CERT/ISAC de l'aviation

— — — — — — — —

Appendice B

Exemple de cadre pour l'évaluation d'une source de cyberinformations/cyberrenseignement et le calcul de son indice de confiance

1. Réputation et antécédents :
   - Évaluer l'historique de la source et sa réputation dans la communauté de la cybersécurité.
   - Rechercher ses réalisations passées, ses contributions et son implication dans les organisations du secteur.
   - Évaluer ses antécédents en matière de fourniture d'informations/d'éléments de renseignement précis et opportuns sur les cybermenaces.

2. Crédibilité et expertise :
   - Évaluer les qualifications, les certifications et l'expertise des personnes ou des équipes qui constituent la source.
   - Prendre en considération leur expérience spécifique dans le domaine des informations/du renseignement sur les cybermenaces.

3. Sources de données et méthodes de collecte :
   - Examiner les méthodes utilisées par la source pour recueillir des données et l'origine de ces données.
   - Déterminer si elle a accès à des flux de données diversifiés et fiables.
   - Évaluer la rigueur de ses procédures de collecte de données.

4. Partage de données et collaboration :
   - Déterminer si la source échange des informations/des éléments de renseignement sur les cybermenaces avec des organisations de confiance ou des pairs du secteur.
   - Tenir compte du fait que la collaboration avec d'autres entités spécialisées dans la cybersécurité peut renforcer la crédibilité.

5. Transparence :
   - Évaluer le niveau de transparence des comptes rendus et des méthodes de la source.
   - Déterminer si elle indique ses sources de données, ses techniques d'analyse et la fréquence de ses mises à jour.

6. Opportunité et précision :
   - Évaluer l'aptitude de la source à fournir des informations/des éléments de renseignement opportuns et précis sur les cybermenaces.
   - Prendre en considération son bilan en termes de prédiction et de détection des cybermenaces.

7. Analyse et contexte :
   - Analyser la profondeur et la qualité de l'analyse des cybermenaces par la source.
   - Évaluer l'aptitude de la source à contextualiser les cybermenaces, notamment en termes d'attribution et de répercussions possibles.

8. Conformité avec les normes du secteur :

- Déterminer si la source satisfait aux normes et s'inspire des meilleures pratiques du secteur en matière d'informations/de renseignement sur les cybermenaces, par exemple en utilisant des cadres tels que STIX/TAXII et des formats de données communs.

9. Respect de la législation et de l'éthique :
    - S'assurer que la source respecte les normes juridiques et éthiques concernant la collecte et le partage de données.

Pour mesurer le degré de fiabilité d'une source de cyberinformations/de cyberrenseignement, il est possible de recourir à un système de notation basé sur les critères susmentionnés.

On trouvera ci-dessous un exemple de dispositif d'évaluation.

1. Attribuer un coefficient de pondération à chaque critère en fonction de son importance par rapport aux besoins spécifiques et au profil de risque de l'organisation.
2. Noter la source sur une échelle (p. ex. : de 1 à 5) pour chaque critère – 5 étant alors le niveau de confiance le plus élevé.
3. Calculer une note de confiance globale en additionnant les notes pondérées pour chaque critère. Plus la note est élevée, plus la source est fiable.

Voici un exemple simplifié de calcul d'une note de confiance globale :

- Réputation et antécédents : 4/5
- Crédibilité et expertise : 5/5
- Sources de données et méthodes de collecte : 3/5
- Partage de données et collaboration : 4/5
- Transparence : 4/5
- Opportunité et précision : 4/5
- Analyse et contexte : 5/5
- Conformité avec les normes du secteur : 4/5
- Respect de la législation et de l'éthique : 5/5

La note de confiance globale de la source serait alors :

(4 x 0,1) + (5 x 0,15) + (3 x 0,1) + (4 x 0,1) + (4 x 0,1) + (4 x 0,1) + (5 x 0,15) + (4 x 0,1) + (5 x 0,1) = **4,30**

— — — — — — — —

Appendice C

Exemple de cadre pour l'évaluation de la plausibilité/crédibilité de cyberinformations/d'éléments de cyberrenseignement

1. Corroboration à partir de sources multiples :
   - Établir si les informations/éléments de renseignement sur la cybermenace sont corroborés par plusieurs sources indépendantes ; par exemple, le fait que plusieurs sources rapportent les mêmes informations peut accroître la plausibilité.

2. Cohérence par rapport aux menaces et tactiques connues :
   - Déterminer si les informations/éléments de renseignement sur la cybermenace rappellent des cybermenaces, techniques d'attaque et tactiques connues ; par exemple, des incohérences peuvent indiquer un degré de plausibilité plus faible.

3. Détails techniques et éléments de preuve :
   - Rechercher la présence de détails techniques et d'éléments de preuve à l'appui des informations/éléments de renseignement sur la cybermenace ; par exemple, des indications techniques solides augmentent la plausibilité.

4. Attribution et motivations :
   - Évaluer l'attribution de la cybermenace à des acteurs ou à des groupes spécifiques.
   - Étudier les motivations de ces acteurs et voir si elles correspondent à la cybermenace signalée.

5. Moment et contexte :
   - Analyser à quel moment la cybermenace survient et comment elle s'inscrit dans le paysage de la cybersécurité.
   - Établir si la cybermenace peut être en lien avec des événements en cours ou des tendances actuelles.

6. Fiabilité habituelle :
   - Évaluer la fiabilité habituelle de la source en matière de signalement des cybermenaces ; par exemple, des signalements régulièrement exacts augmentent la plausibilité.

7. Validation par des pairs et des groupes de confiance :
   - Déterminer si les informations/éléments de renseignement sur les cybermenaces ont été validés ou approuvés par des pairs ou des groupes du secteur qui sont dignes de confiance ; par exemple, la validation par des pairs peut renforcer la plausibilité.

8. Signaux d'alerte et anomalies :

- Rechercher des signaux d'alerte, des anomalies ou des éléments suspects dans les informations/éléments de renseignement sur les cybermenaces ; le fait d'en tenir compte et de les expliquer peut améliorer la plausibilité.

Pour mesurer le degré de plausibilité/crédibilité d'une source de cyberinformations/de cyberrenseignement, il est possible de recourir à un système de notation basé sur les critères susmentionnés.

On trouvera ci-dessous un exemple de dispositif d'évaluation.

1. Attribuer un coefficient de pondération à chaque critère en fonction de son importance et de sa pertinence par rapport à l'évaluation des cyberrisques concernant l'organisation.
2. Noter l'élément de renseignement relatif à la menace sur une échelle (p. ex. : de 1 à 5) pour chaque critère – 5 étant alors le niveau de plausibilité le plus élevé.
3. Calculer une note de plausibilité globale en additionnant les notes pondérées pour chaque critère. Plus la note est élevée, plus le rapport de renseignement sur la menace est plausible.

Voici un exemple simplifié de calcul d'une note de plausibilité/crédibilité globale :

- Corroboration à partir de sources multiples : 4/5
- Cohérence par rapport aux menaces et tactiques connues : 3/5
- Détails techniques et éléments de preuve : 5/5
- Attribution et motivations : 4/5
- Moment et contexte : 4/5
- Fiabilité habituelle : 4/5
- Validation par des pairs et des groupes de confiance : 4/5
- Signaux d'alerte et anomalies : 3/5

La note de plausibilité/crédibilité globale serait alors :

(4 x 0,15) + (3 x 0,15) + (5 x 0,15) + (4 x 0,1) + (4 x 0,15) + (4 x 0,1) + (4 x 0,1) + (3 x 0,1) = **3,90**

— — — — — — — —

Appendice D

Exemple de mécanisme d'évaluation pour les cyberinformations

Le présent appendice décrit le code de l'Amirauté[13], autre exemple de méthode d'évaluation des éléments de renseignement recueillis.

Cette échelle peut être utilisée pour le partage d'informations afin d'avoir une idée de la fiabilité de la source et de la crédibilité des informations. La méthode consiste en une notation à deux caractères (une lettre et un chiffre), la lettre évaluant la fiabilité de la source et le chiffre reflétant la confiance accordée aux informations.

Fiabilité de la source

La fiabilité d'une source est évaluée sur la base d'un examen technique de ses capacités ou, dans le cas du renseignement humain, de son historique. La notation repose sur un codage alphabétique de A à F pour évaluer la fiabilité de la source, comme suit.

Code de fiabilité	Fiabilité	Explication
A	Totalement fiable	Aucun doute sur l'authenticité, la confiance à accorder ou la compétence ; a toujours été d'une fiabilité à toute épreuve.
B	Généralement fiable	Doute mineur sur l'authenticité, la confiance à accorder ou la compétence ; a l'habitude de fournir des informations valables la plupart du temps.
C	Plutôt fiable	Doute sur l'authenticité, la confiance à accorder ou la compétence, mais a déjà fourni des informations valables par le passé.
D	Généralement pas fiable	Doute important sur l'authenticité, la confiance à accorder ou la compétence, mais a déjà fourni des informations valables par le passé.
E	Non fiable	Manque d'authenticité, indigne de confiance et compétence insuffisante ; communication d'informations non valables par le passé.
F	Fiabilité à déterminer	Il n'existe aucune base pour évaluer la fiabilité de la source.

[13] Les détails de la méthode figurent aux pages 59 et 60 de la publication de doctrine interarmées 2-00, *Intelligence, Counter-intelligence and Security Support to Joint Operations* (quatrième édition), disponible à l'adresse suivante : https://www.gov.uk/government/publications/jdp-2-00-understanding-and-intelligence-support-to-joint-operations.

Crédibilité des informations

La crédibilité est évaluée d'après la probabilité et le degré de corroboration par d'autres sources. La notation repose sur un codage numérique de 1 à 6 pour évaluer la crédibilité des informations, comme suit.

Note de crédibilité	Crédibilité	Explication
1	Confirmées par d'autres sources	Confirmées par d'autres sources indépendantes ; logiques en soi ; cohérentes par rapport à d'autres informations sur le sujet.
2	Probablement vraies	Non confirmées ; logiques en soi ; cohérentes par rapport à d'autres informations sur le sujet.
3	Peut-être vraies	Non confirmées ; raisonnablement logiques en soi ; en accord avec d'autres informations sur le sujet.
4	Douteuses	Non confirmées ; possibles mais pas logiques ; pas d'autres informations sur le sujet.
5	Improbables	Non confirmées ; pas logiques en soi ; contredites par d'autres informations sur le sujet.
6	Véracité à déterminer	Il n'existe aucune base pour évaluer la validité des informations.

Les tableaux ci-dessus peuvent être combinés pour former le tableau ci-dessous.

Fiabilité de la source		Crédibilité des cyberinformations	
A	Totalement fiable	1	Confirmées par d'autres sources
B	Généralement fiable	2	Probablement vraies
C	Plutôt fiable	3	Peut-être vraies
D	Généralement pas fiable	4	Douteuses
E	Non fiable	5	Improbables
F	Fiabilité à déterminer	6	Véracité à déterminer

Voici deux exemples de notation des cyberinformations partagées :

- *C4, signifiant : source plutôt fiable mais informations douteuses.*
- *A1, signifiant : source totalement fiable et informations confirmées par d'autres sources.*

Bien que l'évaluation soit subjective, la note constitue un outil utile pour que le destinataire des cyberinformations puisse faire sa propre estimation.

— — — — — — — —

Appendice E

Structure recommandée pour un accord formel relatif au partage de cyberinformations

Il est souhaitable qu'un accord formel relatif au partage de cyberinformations comprenne les sections suivantes :

- ✓ Préambule incluant les noms et la description des parties.
- ✓ Définitions et sigles.
- ✓ Champ d'application : description du champ d'application du document et référence à l'appendice 1 sur le type de cyberinformations à partager.
- ✓ Droits et obligations de la partie recevant les informations (destinataire).
- ✓ Sources des informations : pour savoir qui fournira quelles informations à qui et sur la base de quelles sources, et si la source des informations doit être divulguée.
- ✓ Limites concernant la nature des informations qui peuvent être communiquées et à qui, compte tenu des lois en vigueur, des droits de propriété intellectuelle, des informations commerciales confidentielles, de la définition des marquages TLP, etc.
- ✓ Format des informations échangées et fréquence des échanges.
- ✓ Moyens de transmission des informations (p. ex. : lettre, téléphone, SMS, courrier électronique, registre, etc.), y compris la protection et l'assurance de la confidentialité, de l'intégrité et de la disponibilité des informations transmises par voie numérique.
- ✓ Exigences de qualité : description des actions à effectuer par l'émetteur avant de transmettre les informations, ainsi que des moyens de garantir l'intégrité et la qualité des informations partagées, notamment leur anonymisation et/ou leur nettoyage.
- ✓ Stockage des informations et tenue des registres : description des politiques et procédures d'archivage des informations partagées, et indication de la durée minimale pendant laquelle les informations envoyées/reçues doivent être archivées aux fins de contrôle de la qualité en vertu de l'accord et de la relation entre les parties.
- ✓ Coût : indication de la partie prenant en charge le coût du partage des informations. Il est recommandé que chaque partie prenne en charge ses propres coûts liés à la mise en œuvre de l'accord.
- ✓ Procédures de gouvernance et de gestion du changement au titre de l'accord.
- ✓ Correspondance et avis relatifs à l'accord.
- ✓ Responsabilité : description des responsabilités des uns et des autres. Il est recommandé de dégager la partie émettrice de toute responsabilité liée aux informations partagées.
- ✓ Traitement des données à caractère personnel : description de la manière dont les données à caractère personnel doivent être traitées, y compris aux termes des lois et règlements applicables.
- ✓ Règlement des différends : comment et en vertu de quelles lois les différends liés à l'accord seront tranchés. Il est recommandé que les parties tentent d'abord de régler leurs différends à l'amiable, avant de s'en remettre si nécessaire à la médiation d'une juridiction convenue.
- ✓ Intégralité de l'accord et amendements : description de la primauté des différentes parties de l'accord.

- ✓ Date d'entrée en vigueur de l'accord, durée et procédures de renouvellement et de résiliation.
- ✓ Attribution : signatures des personnes autorisées pour chaque partie.
- ✓ Appendices :
  - Appendice 1 – Informations à fournir : description du type d'informations à partager, pour chaque partie.
  - Appendice 2 : définition des marquages TLP, y compris une référence à la norme TLP FIRST.

— — — — — — — —

Annexe F

MISP – Plateforme de renseignement de sources ouvertes et de partage d'informations sur les menaces

La plateforme MISP[14] est une plateforme de partage, de stockage et de corrélation d'indicateurs de compromis (IoC) concernant des cyberattaques ciblées, ainsi que d'éléments de renseignement sur les cybermenaces – informations sur des acteurs à l'origine de la menace, informations sur des fraudes financières, etc.

Il s'agit d'une plateforme gratuite de renseignement de sources ouvertes et de partage d'informations sur les cybermenaces qui permet aux organisations de créer des communautés afin de mettre en commun des informations telles que des éléments de renseignement sur les cybermenaces, des indicateurs, des informations sur des acteurs à l'origine de la menace ou toute autre sorte de donnée sur une cybermenace pouvant être intégrée dans le système.

Les utilisateurs de MISP bénéficient des connaissances obtenues par la collaboration sur les logiciels malveillants ou les cybermenaces en activité. Le fonctionnement repose sur la création de « communautés ». Le partage d'informations se fait au sein d'une communauté d'utilisateurs. Cette plateforme fondée sur la confiance a pour but de contribuer à l'amélioration des contre-mesures employées contre les cyberattaques ciblées et à la mise en œuvre d'actions de prévention et de dispositifs de détection.

Il est recommandé aux États et aux parties prenantes de l'aviation de considérer MISP, de même que toute plateforme équivalente, comme un moyen/une méthode de partage de cyberinformations, sachant que la plateforme :

- facilite l'exploitation automatisée des informations pour mettre à jour différents systèmes de sûreté, comme la gestion des événements et des informations de sécurité (SIEM) et les centres des opérations de sûreté (SOC), les pare-feu, les logiciels antivirus, ainsi que les systèmes de détection et de prévention des intrusions (IDPS) et les systèmes de prévention des intrusions (IPS) ;
- offre la possibilité de partager des cyberinformations rapidement, le temps pouvant être un facteur critique en cas de partage d'informations dans le cadre d'une intervention en cours face à un cyberincident ;
- permet d'actualiser les cyberinformations relatives à un cyberincident en y ajoutant des informations supplémentaires dès qu'elles sont disponibles ;
- se prête au partage de tous les types d'informations portant un marquage TLP. Cependant, les informations marquées **TLP:RED** ne sont partagées sur la plateforme MISP que si la communauté concernée est composée d'un nombre limité de personnes qui y consentent. En règle générale, les informations **TLP:RED** ne sont pas partagées sur la plateforme MISP, mais par d'autres moyens (p. ex. : téléphone, SMS, courrier électronique).

[14] Pour plus d'informations sur l'utilisation de la plateforme MISP : https://www.circl.lu/services/misp-malware-information-sharing-platform/.