Organisation de l'aviation civile internationale

**NOTE DE TRAVAIL**

AN-Conf/13-WP/270
28/9/18
**Français, anglais, arabe, chinois[1], espagnol et russe seulement[2]**

# TREIZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

**Montréal (Canada), 9 – 19 octobre 2018**

**COMITÉ A**

**Point 5 : Nouveaux enjeux**
**5.4 : Cyberrésilience**

## NOTION DE SYSTÈME DE SYSTÈMES DANS LA CYBERSÉCURITÉ EN AVIATION

[Présenté par le Canada, l'Autriche au nom de l'Union européenne et de ses États membres[3], et des autres États membres de la Conférence Européenne de l'aviation civile[4], par EUROCONTROL, par Singapour, et coparrainé par l'Australie et la Nouvelle-Zélande]

**RÉSUMÉ ANALYTIQUE**

Ce document de travail présentera brièvement le concept de système de systèmes, et établira pourquoi une telle approche serait appropriée dans le cadre de la réflexion sur la cybersécurité dans l'aviation civile. Ce document introduira également la notion de sécurité intégrée à la conception, et la façon dont l'intégration de cette notion dans le système de l'aviation pourra améliorer sa résilience.

**Suite à donner :**
La Conférence est invitée à adopter les recommandations présentées au paragraphe 3.

## 1. INTRODUCTION

1.1 La disponibilité d'informations exactes et le fonctionnement adéquat des systèmes essentiels à la sécurité sont des conditions préalables pour un système d'aviation civile sûr et sécuritaire, alors que ce secteur connaît une numérisation croissante. Le système d'aviation est fortement intégré et les

[1] La version chinoise est fournie par Singapour.
[2] Les versions française, anglaise, arabe, espagnole et russe sont fournies par le Canada.
[3] Autriche, Belgique, Bulgarie, Croatie, Chypre, République tchèque, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Espagne, Suède et Royaume-Uni.
[4] Albanie, Arménie, Azerbaïdjan, Bosnie-Herzégovine, Géorgie, Islande, République de Moldova, Monaco, Monténégro, Norvège, Saint-Marin, Serbie, Suisse, République de Macédoine, Turquie et Ukraine.

informations voyagent de par le monde. Conséquemment, les initiatives de cybersécurité dans le secteur aérien doivent adopter une approche globale et de bout en bout.

1.2 Une approche globale et de bout en bout ne peut réussir que si l'aviation est envisagée comme un « système de systèmes », pour lequel tous les membres de la communauté aéronautique assument une part de responsabilité. Le système de l'aviation est constitué d'une variété de réseaux et d'appareils qui sont de plus en plus connectés et interdépendants, en ce qui concerne l'échange de données et d'informations numériques, alors que les parties prenantes de l'aviation comme les États, les aéronefs et les exploitants d'aérodromes, les fournisseurs de services de navigation aérienne et autres s'appuient sur des systèmes de technologies de l'information et de la communication (TIC) interconnectés et interopérants pour leurs activités quotidiennes.

1.3 Les développements comme le programme de gestion de l'information à l'échelle du système (SWIM), l'introduction de systèmes d'aéronefs télépilotés (RPAS) et l'émergence de nouveaux utilisateurs de l'espace aérien et de parties prenantes qui ne sont pas encore opérationnelles renforcent encore davantage cette interdépendance. Le système de l'aviation de l'avenir devra donc être le fruit d'une conception plus concertée et d'une évolution moins individuelle, s'il veut maintenir sa résilience contre l'interférence informatique.

1.4 L'évolution vers des systèmes interconnectés et interopérants susmentionnée amène également son lot de nouvelles vulnérabilités. Les événements liés à l'informatique peuvent avoir une incidence sur l'aviation à plusieurs niveaux, nuire aux performances du système de navigation aérienne et mettre en danger la sécurité générale de l'ensemble du secteur. Ces événements peuvent influencer les échanges d'information entre les parties prenantes et avoir une incidence directe sur la sûreté, la sécurité, la capacité et l'efficacité pouvant avoir de graves répercussions.

## 2. ANALYSE

2.1 **L'aviation comme un système de systèmes** – Dans le secteur de l'aviation, plusieurs parties prenantes, directes comme indirectes, jouent un rôle dans le fonctionnement et l'entretien de sous-systèmes autonomes et du système dans son ensemble – étant entendu qu'un système peut être composé de produits, de personnes et de processus. Chacun de ces sous-systèmes est directement associé à d'autres sous-systèmes pour pouvoir fonctionner de façon harmonieuse et efficace ; inversement, chacun de ces sous-systèmes a également une incidence importante sur les autres, lorsqu'il n'est pas en mesure de fonctionner adéquatement.

2.2 Ces sous-systèmes que nous connaissons actuellement sont conçus, intégrés, exploités et gérés indépendamment les uns des autres, et ils évoluent à un rythme qui leur est propre, ce qui entraîne un processus d'évolution global qui est difficile à prévoir et à saisir de façon déterministe. Sachant que les parties prenantes de l'aviation assument une responsabilité pour l'ensemble du système pour le produit global, il est d'autant plus important de considérer l'aviation comme un système de systèmes. La responsabilité du bon fonctionnement du système de l'aviation inclut donc les parties prenantes directes, comme les propriétaires et les exploitants d'aéronefs et d'aérodromes, ainsi que les fournisseurs de SNA, de même que les parties prenantes indirectes, comme les États et les fabricants et les concepteurs d'équipement.

2.3 Étant donné que ces sous-systèmes servent des fonctions autonomes qui sont associées ensemble pour atteindre des objectifs communs (comme les communications entre le contrôle de la circulation aérienne et les pilotes, ou l'échange de données de localisation entre les centres de contrôle aérien et les aéronefs), le fait de compromettre l'un de ces sous-systèmes porterait atteinte à la fonctionnalité générale de toute la chaîne des sous-systèmes. Conséquemment, la gestion des risques liés à la cybersécurité devra être abordée à l'aide d'une approche holistique afin de réduire l'accessibilité des auteurs de menaces au fonctionnement global.

2.4 **La cybersécurité : Une considération constante et évolutive –** Étant donné la nature évolutive du système de systèmes décrit ci-dessus, la cybersécurité doit elle aussi être une considération constante chez les nombreuses parties prenantes du système de systèmes de l'aviation. Il est par ailleurs impératif que le système de systèmes de l'aviation maintienne les conditions nécessaires pour la cybersécurité en ayant une flexibilité et une adaptabilité suffisante, puisque ses composantes interagissent en permanence et de différentes façons les unes avec les autres (ainsi, les aéronefs interagissent avec différents prestataires de services de navigation aérienne alors qu'ils transitent par différentes régions d'information de vol).

2.5 En conséquence, le développement et l'entretien d'une pareille résilience informatique à travers le système de systèmes demandent une coordination permanente entre toutes les parties prenantes (voir le paragraphe 2.2), afin de maintenir le degré de flexibilité et d'adaptabilité nécessaires pour que le système de systèmes de l'aviation fonctionne correctement.

2.6 Le concept de « composabilité » – la capacité d'intégrer plusieurs éléments (les composantes, pour les systèmes ou les sous-systèmes pour le système de systèmes dans de plus grandes entités), de façon sécuritaire – représente un défi important à relever dans la poursuite de cet objectif. Le principal défi, ici, sera de quitter le paradigme de la sécurité dans lequel l'intégration des éléments mettait principalement l'accent sur leur fonctionnalité et sur les interactions à travers différentes interfaces. D'une perspective de cybersécurité, l'intégration d'éléments autonomes exige également une réflexion approfondie sur la façon dont la position de chaque élément par rapport à la cybersécurité contribue à l'état général de la cybersécurité. L'une des principales questions qui seront soulevées dans cette optique sera la façon de soutenir les États et les régions (et les autres parties prenantes individuelles) dans leur démarche de développement, pour que le système de systèmes puisse être protégé efficacement contre les attaques de cybersécurité, en dépit des variations inévitables qui existeront entre les sous-systèmes.

2.7 Pour atteindre l'objectif susmentionné, l'intégration des différents sous-systèmes demandera un examen sérieux, ainsi qu'une intégration des environnements de sécurité natifs pour chaque sous-système, de manière à permettre l'émergence d'un environnement holistique et cyberrésilient. Les approches non coordonnées de la cybersécurité pourraient mener à des failles non détectées dans la protection ; les chevauchements dans les systèmes de défense perçus sont tout aussi dangereux, puisque ce scénario pourrait offrir la possibilité d'une attaque viable du système de systèmes de l'aviation.

2.8 En conséquence, une approche globale et coordonnée de la gestion des interactions entre les systèmes est essentielle. Cet objectif repose sur l'adoption d'une vision commune par rapport à la façon dont ces systèmes et ces sous-systèmes interagissent.

2.9 **Introduire la sécurité intégrée à la conception dans les systèmes d'aviation –** Pour que le système de systèmes de l'aviation puisse atteindre le niveau souhaité de cyberrésilience, il est important que les considérations de cybersécurité soient incorporées dès le début du développement des systèmes, plutôt que d'être le fruit d'une réflexion rétroactive. Cela permettrait par ailleurs de tenir compte des considérations d'interface entre les sous-systèmes, puisque ces interactions se produiraient également de façon sécuritaire et efficace.

2.10 La plupart des normes de sécurité actuelles mettent l'accent sur les mesures d'atténuation prises et mises en œuvre *dans* le contexte organisationnel – il est urgent de recentrer nos objectifs pour qu'ils incluent et tiennent également compte des mesures qui doivent être prises dans une perspective interorganisationnelle. Cela permet d'avoir l'assurance d'une sécurité pour l'ensemble du système des systèmes, en plus de la sécurité provenant du regroupement de sous-systèmes qui sont sécurisés de façon autonome.

2.11 Sans gestion appropriée, les approches non coordonnées de la cybersécurité dans les sous-systèmes de l'aviation peuvent présenter un risque pour le système dans son ensemble. Cette absence de coordination découle peut-être aussi d'une communication insuffisante entre les gestionnaires des sous-

systèmes et des autres parties prenantes concernées lors du développement et de la conception des approches de cybersécurité.

2.12 Par différentes couches de coordination (par exemple entre les États en tant que gestionnaires de systèmes d'aviation domestiques, gestionnaires de sous-systèmes à l'intérieur des systèmes d'aviation domestiques, etc.) à travers différents niveaux de sous-systèmes, de même qu'en s'assurant que les sous-systèmes autonomes soient protégés de façon efficace en soi, les États pourront contribuer à un système de systèmes de l'aviation qui maintiendrait le principe de défense en profondeur comme le résultat naturel d'un tel travail.

2.13 **Travail futur** – Ces travaux constituant à introduire la sécurité intégrée à la conception dans le cadre de la conception initiale des systèmes ne devraient pas remplacer les meilleures pratiques développées par la communauté de l'aviation au fil de plusieurs décennies d'expérience dans le développement de systèmes d'aviation et de travail sur les défis posés par la cybersécurité. En incorporant de tels principes aux côtés et en complémentarité à l'accent qui a traditionnellement été mis sur la redondance des systèmes et sur l'importance accordée à l'accessibilité aux données et aux systèmes d'exploitation, les parties prenantes vont renforcer davantage le système de systèmes de l'aviation dans ses politiques de cyberrésilience, tout en maintenant une efficacité opérationnelle.

2.14 Parmi l'ensemble des concepts et des solutions opérationnelles qui sont abordées dans les différents forums sur l'aviation aujourd'hui, il est important que les États et l'industrie tiennent compte des considérations susmentionnées dans le processus de conception et de développement. Par extension, la communauté pourra également faire évoluer ses travaux collectifs pour mieux déterminer les sous-systèmes représentatifs et pour faire des recherches permettant de savoir dans quelle mesure ses résultats – en fonction des mesures prises et des pratiques employées – peuvent être transférés à d'autres sous-systèmes afin d'améliorer la cyberrésilience de façon universelle.

2.15 De même, à la suite de la réussite obtenue dans ce domaine, la communauté de l'aviation pourra envisager de collaborer pour amorcer le développement de sous-systèmes de plus en plus vastes, qui tiennent compte de la sécurité des informations dès leur phase de conception initiale. Alors que de tels travaux progressent et se développent, les parties prenantes pourront commencer à se questionner collectivement pour savoir si des candidats aptes et dignes de confiance pourraient se voir confier la responsabilité de développer et d'entretenir de pareils systèmes, qui sont sécuritaires de par leur conception, et étudier la faisabilité de pareils processus dans les systèmes de l'aviation de l'avenir.

2.16 Par un investissement continu et des efforts soutenus dans le domaine de la cyberrésilience des systèmes, la communauté de l'aviation contribuera véritablement aux opérations sécuritaires et efficaces de l'écosystème de l'aviation (le « système de systèmes ») pour un bon nombre d'années.

## 3. CONCLUSION

3.1 La Conférence est invitée à adopter les recommandations suivantes :

Que la Conférence :

a) exhorte l'OACI et les États à reconnaître que la cyberrésilience du système de l'aviation dépend d'une coordination continue entre l'ensemble des parties prenantes ;

b) demande à l'OACI de reconnaître le concept de système de systèmes, qui exige une collaboration et une coordination entre les gestionnaires de sous-systèmes particulièrement au moment de développer, d'intégrer, d'exploiter et d'entretenir des sous-systèmes qui sont « sécuritaires de par leur conception » ;

c) exhorte l'OACI à élaborer un cadre qui demandera aux États de mettre en œuvre des mesures pour atténuer les menaces informatiques et les risques envers les systèmes d'aviation civile, et qui les guidera dans ces mesures. Cela pourrait mener à l'élaboration de SARPS pour plusieurs annexes de l'OACI concernées ;

d) reconnaît les concepts exposés dans le document de travail « *Considérations relatives à la cybersécurité dans l'aviation* ».

— FIN —