Organisation de l'aviation civile internationale

AN-Conf/14-WP/125[1]
29/6/24

NOTE DE TRAVAIL

QUATORZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal (Canada), 26 août – 6 septembre 2024

Point 4 : Hyperconnectivité du système de navigation aérienne
4.2 : Cybersécurité et résilience des systèmes d'information

LA CYBERSÉCURITÉ DANS LA FOURNITURE DE SERVICES DE LA CIRCULATION AÉRIENNE (ATS)

[Note présentée par l'Argentine avec l'appui de 19 États membres de la Commission latino-américaine de l'aviation civile (CLAC)][2]

RÉSUMÉ ANALYTIQUE

La présente note propose des réflexions sur la conception de mécanismes visant à aider les fournisseurs de services de la circulation aérienne (ATS) à gérer les cybermenaces et les cyberévénements, et à mettre au point des stratégies d'atténuation efficaces.

Suite à donner : La Conférence est invitée à :

a) élaborer des mécanismes d'orientation pour aider les fournisseurs de services de la circulation aérienne à gérer les cyberrisques qui compromettent la sécurité dans le cadre de leur système de gestion de la sécurité ;
b) élaborer et/ou mettre en œuvre des technologies, des procédures et des mesures qui permettent aux contrôleurs de fournir des services de la circulation aérienne (ATS) en toute sécurité et de reprendre rapidement les activités à la suite d'un cyberévénement ;
c) déterminer les compétences et les aptitudes dont les contrôleurs de la circulation aérienne ont besoin pour évaluer et traiter les cyberévénements et leurs incidences sur la fourniture de services de la circulation aérienne, et pour devenir cyberrésilients.

1. INTRODUCTION

1.1 Compte tenu de la hausse du nombre de cybermenaces et des cyberattaques dans le secteur de l'aviation, et étant donné que l'un des sept piliers de la *Stratégie de l'OACI pour la cybersécurité de l'aviation*, et de la *Politique de cybersécurité* sous-jacente, est l'intégration de la cybersécurité dans la gestion des risques aéronautiques, il est plus important que jamais de déterminer et de mesurer les effets

[1] Version espagnole fournie par l'Argentine.
[2] Aruba (Royaume des Pays-Bas), Belize, Chili, Colombie, Costa Rica, Cuba, El Salvador, Équateur, Guatemala, Honduras, Jamaïque, Mexique, Nicaragua, Panama, Paraguay, Pérou, République dominicaine, Uruguay, Venezuela (République bolivarienne du).

de tels événements sur la fourniture de services de la circulation aérienne (ATS), nonobstant le fait que des technologies émergentes en navigation aérienne évoluent pour mieux faire face aux cyberévénements.

1.2 Dans la mesure où les systèmes aéronautiques sont étroitement liés les uns aux autres ainsi qu'à d'autres systèmes externes, les cyberévénements ont gagné en portée et en impact, et peuvent créer des événements perturbateurs à l'échelle mondiale[3]. Il est donc important de les considérer comme des dangers pour la sécurité, ou du moins comme des précurseurs et des facteurs contributifs à la catégorie d'événements à risque élevé dans le monde (G-HRC), décrits dans le *Plan pour la sécurité de l'aviation dans le monde 2023-2025* (Doc 10004, GASP). De plus, le *Concept opérationnel d'ATM* (Doc 9854) attire l'attention sur le fait que les décisions sont souvent prises sur la base de critères variables, y compris en faveur de la sécurité. Cette situation appelle à agir pour obtenir l'un des avantages escomptés cités à l'appendice E du Doc 9854, à savoir l'élargissement de la définition des dangers, qui permettra des trajectoires plus stables pour les utilisateurs.

1.3 En raison de l'environnement plus automatisé, numérisé et interconnecté dans lequel ils sont fournis, les services de la circulation aérienne deviennent plus vulnérables aux cybermenaces et aux cyberattaques. L'utilisation des communications contrôleur-pilote par liaison de données (CPDLC), l'intégration d'aéronefs non habités dans l'espace aérien contrôlé, les tours numériques à distance et les services automatisés d'information de vol d'aérodrome (A-AFIS) ne sont que quelques exemples de technologies qui plaident en faveur d'une plus grande sensibilisation et de mesures renforcées pour faire face à l'incidence des cyberévénements dans la fourniture de services de la circulation aérienne.

1.4 Des progrès majeurs ont en effet été réalisés dans la prévention et/ou l'atténuation des cyberévénements. Cependant, par définition, de tels événements affectent directement la gestion du trafic aérien, les communications, la navigation et la surveillance (ATM/CNS) et les systèmes d'information, et il est donc nécessaire d'accroître les efforts pour s'attaquer d'urgence à l'incidence des cyberévénements sur la gestion de la circulation aérienne.

1.5 Si les organismes des services de la circulation aérienne n'ont pas mis en place de mesures de contrôle du risque ni de barrières défensives adéquates, ils peuvent subir une perturbation partielle des services, des conditions « Taux zéro » de contrôle de la circulation aérienne (ATC), ou même des incidents de sécurité comme la perte de l'espacement entre aéronefs pouvant provoquer une collision en vol (MAC), qui constitue l'une des cinq catégories d'événement à risque élevé dans le monde.

1.6 La section 4 — *Élaboration d'une politique de cybersécurité* du *Plan d'action pour la cybersécurité* (CyAP), préparé par le Groupe d'étude du Secrétariat de l'OACI sur la cybersécurité (SSGC), propose des mesures de gestion des cyberrisques. Sur cette base, il convient de repenser les approches en matière de gestion des risques dans le cadre de la fourniture de services de la circulation aérienne dans un contexte mondial décrit comme volatile, incertain, complexe et ambigu, et de plus en plus friable et non linéaire[4].

[3] Événement perturbateur : Événement inhabituel et grave à l'échelle nationale, régionale ou mondiale qui compromet gravement la sécurité aérienne. De tels événements ne découlent habituellement pas d'activités aéronautiques, mais peuvent néanmoins avoir une forte incidence sur l'exploitation.

[4] Cette description s'inspire des paradigmes connus dans les sciences sociales sous le nom de *VUCA* (volatile, incertain, complexe, ambigu) et *BANI* (friable, anxieux, non linéaire, incompréhensible), qui servent à décrire la situation dans le monde d'aujourd'hui et qui peuvent s'appliquer à tous les domaines d'étude.

2. ANALYSE

2.1 Au vu de ce qui précède, il est essentiel de recenser les possibilités d'amélioration des capacités prédictives et des mesures de promotion de la cybersécurité dans la fourniture de services de la circulation aérienne.

2.2 Tout d'abord, il est important de réexaminer la complexité croissante du contexte opérationnel dans lequel les services de la circulation aérienne sont fournis et de redéfinir le rôle et les fonctions des services de la circulation aérienne, en particulier à l'intersection de quatre grands systèmes de gestion où des mesures sont nécessaires : la gestion des cyberrisques, la gestion des risques de sécurité, la gestion du dispositif de sécurité et la gestion de la sécurité de l'information.

2.3 De plus, il y a trois aspects relatifs aux services de la circulation aérienne pour lesquels des mesures d'atténuation des cyberévénements doivent être conçues et mises en œuvre :

a) la gestion des risques de sécurité en relation à la fourniture de services de la circulation aérienne ;

b) les outils techniques/opérationnels[5] utilisés par les organismes des services de la circulation aérienne pour mener leurs activités ;

c) les aptitudes et les compétences dont les contrôleurs de la circulation aérienne (ATCO) ont besoin pour instaurer la cyberrésilience dans leur organisme des services de la circulation aérienne.

2.4 S'agissant de la gestion des risques de sécurité dans la fourniture de services de la circulation aérienne, les cybermenaces et les cyberattaques devraient être prises en compte dans le système de gestion de la sécurité (SGS) du fournisseur de services de la circulation aérienne (ATSP). La composante 2 d'un SGS revêt naturellement une importance particulière dans la mesure où les dangers doivent logiquement être recensés afin de gérer les risques qui y sont associés. Par conséquent, il est fondamental de comprendre que les cybermenaces et les cyberattaques doivent être reconnues comme telles avant de pouvoir enregistrer leur occurrence, mesurer les impacts qu'elles ont sur les services de la circulation aérienne et évaluer les risques qu'elles posent.

2.5 Cette approche ne devrait pas se limiter au recensement de dangers traditionnellement associés aux services de la circulation aérienne, mais devrait aussi prendre en compte ceux liés aux technologies de l'information, notamment le réseau prenant en charge les systèmes d'ATM et de CNS, les logiciels, le serveur et le matériel utilisés, ainsi que d'autres éléments pertinents d'un organisme des services de la circulation aérienne. Face à l'évolution fulgurante de la technologie, cette approche ne doit absolument pas être statique, mais plutôt dynamique et évolutive. Elle doit donc être révisée et adaptée en permanence pour suivre le rythme rapide des avancées technologiques dans le domaine opérationnel, mais aussi dans l'environnement global. Il faut donc comprendre qu'un cyberévénement ou un cyberincident peut devenir un événement de sécurité dans la fourniture de services de navigation aérienne et les opérations aériennes.

2.6 S'agissant des outils opérationnels utilisés par les organismes des services de la circulation aérienne, il s'agit ordinairement des technologies, des procédures et des dispositions dont les contrôleurs ont besoin pour fournir des services de la circulation aérienne en toute sécurité, et pour devenir cyberrésilients et reprendre rapidement les activités à la suite d'un cyberévénement. Pour cette raison, il est

[5] Il s'agit notamment des procédures opérationnelles, des systèmes informatiques et autres TIC, de la surveillance ATS, des communications, etc.

d’une importance vitale de mettre au point des mécanismes qui peuvent aider les contrôleurs à identifier rapidement des cybermenaces et à prendre des mesures appropriées.

2.7 Le rôle des contrôleurs de la circulation aérienne a changé, et leur mode d’interaction avec les éléments du modèle SHELL est en train de s’adapter à la nouvelle normalité. La symbiose entre les humains, le matériel et les logiciels s’est intensifiée et a accru l’exposition aux cyberévénements. Les compétences et les aptitudes nécessaires doivent donc être développées pour que les contrôleurs des organismes des services de la circulation aérienne puissent devenir cyberrésilients et être en mesure de gérer différents scénarios relatifs à des cyberévénements.

3. CONCLUSION

3.1 Compte tenu de ce qui précède et en gardant à l’esprit la nature transversale de la cybersécurité dans la fourniture de services de la circulation aérienne, il est nécessaire de mettre en place des mécanismes pour aider les fournisseurs de tels services à prendre en compte la gestion des cybermenaces et des cyberévénements dans leur SGS, et d’acquérir aussi les outils analytiques nécessaires à l’élaboration de stratégies d’atténuation et de procédures de détection précoce, ainsi que d’instruments pour aider les contrôleurs à prendre des décisions immédiates en réponse à des cyberincidents.

3.2 Il convient aussi de déterminer les compétences et les aptitudes que doivent avoir les contrôleurs de la circulation aérienne pour être en mesure d’évaluer et d’intervenir en cas d’événement de cybersécurité susceptible d’avoir une incidence sur la fourniture de services de la circulation aérienne, et de les aider à affiner leur appréciation de leurs conséquences possibles et des facteurs humains en jeu.

3.3 La Conférence est invitée à envisager :

a) d’élaborer des mécanismes d’orientation pour aider les fournisseurs de services de la circulation aérienne à gérer les cyberrisques dans le cadre de leur système de gestion de la sécurité ;

b) d’élaborer et/ou de mettre en œuvre des technologies, des procédures et des mesures qui permettent aux contrôleurs de fournir des services de la circulation aérienne (ATS) en toute sécurité et de reprendre rapidement leurs activités en cas de cyberévénement ;

c) de déterminer les compétences et les aptitudes dont les contrôleurs de la circulation aérienne ont besoin pour évaluer et traiter les cyberévénements et leurs incidences sur la fourniture de services de circulation aérienne, et pour devenir cyberrésilients.

— FIN —