Note sur la Space Policy Directive 5 (SPD-5) – Cybersecurity Principles for Space Systems

Le 4 septembre 2020, le Président des États-Unis Donald Trump a promulgué la ***Space Policy Directive 5*** (SPD-5) dite « *Cybersecurity Principles for Space Systems* » **relative à la cybersécurité des systèmes spatiaux et de leurs infrastructures de support**. Il s'agit de la 5ème SPD promulguée par Donald Trump sur la base des travaux du *National Space Council* (NSpC) après les :

- SPD-1 (2017) qui fait de l'exploration spatiale humaine une priorité, avec un retour des astronautes sur la Lune en 2024
- SPD-2 (2018) qui vise une révision de la réglementation relative aux applications spatiales commerciales
- SPD-3 (2018) qui traite de la gestion du trafic spatial commercial
- SPD-4 (2019) qui met sur pied l'*U.S. Space Force* (USSF)

A titre d'information, une 6ème SPD a été promulguée le 16 décembre 2020 sur le recours à l'énergie et la propulsion nucléaires dans le domaine spatial (voir note dédiée).

1. Contexte

L'adoption de la SPD-5 était attendue compte tenu de l'**attention portée par le Président Donald Trump aux enjeux de cybersécurité** – attention qui ne devrait pas s'estomper sous la prochaine présidence (dernier exemple en date : Joe Biden a annoncé que la cybersécurité serait l'une des priorités de son gouvernement suite à la cyberattaque de grande ampleur qu'ont connu les États-Unis fin 2020). La SDP-5 a par ailleurs vocation à s'inscrire dans le sillage de la stratégie américaine de cybersécurité développée par l'administration Trump depuis quelques années à travers la *National Cyber Strategy* (2018) et, plus largement la *National Security Strategy* (2017).

La promulgation de ce nouveau décret s'explique également par les **risques accrus de cyber-attaques qui pèsent sur les systèmes spatiaux**. En effet, le nouveau paysage de l'industrie spatiale, porté par les sociétés du *New Space*, a ouvert la voie à une **démocratisation de l'accès à l'Espace et à une multiplication des acteurs sur l'ensemble des chaînes de valeur**. Bien que cette diversification ait permis une baisse des coûts de production, celle-ci a eu pour contrepartie de **rendre les chaînes d'approvisionnement plus larges et plus diffuses, ayant pour conséquence d'accroître la vulnérabilité des infrastructures spatiales**.

En outre, **le nombre croissant de données transitant *via* les réseaux satellitaires constitue une cible de prédilection pour les cyber-attaquants**. Ceux-ci peuvent profiter de l'**ancienneté de certains satellites** conçus il y a plusieurs décennies et dont la modernisation ou la défense face à une cyberattaque se révèle difficile, **ou du manque de prise en considération par certains acteurs publics ou privés des problématiques de cybersécurité.**

Enfin, **les situations de crise** comme la pandémie de Covid-19, pendant lesquelles les sociétés de l'industrie spatiale ont dû adapter leurs opérations et travailler à distance, **créent des environnements instables propices aux attaques**.

Le nombre de cyberattaques contre les systèmes spatiaux s'est d'ailleurs accru depuis le début de la crise mondiale.

2. Objectifs et contenu de la SPD-5

A travers la SPD-5, l'Exécutif a donc souhaité :

- **Souligner l'urgence à se saisir des problématiques de cybersécurité dans le secteur spatial.** La SPD-5 mentionne à ce titre que les principes et mesures de cybersécurité applicables aux systèmes terrestres le sont également aux systèmes spatiaux
- **Faire des enjeux de cybersécurité une priorité pour les acteurs du Spatial** (plus que la rapidité de mise en service et le coût des systèmes) et les inciter à les prendre en compte dès la conception de leurs systèmes (dans la mesure où les satellites peuvent difficilement être dépannés une fois lancés)
- **Offrir aux acteurs du spatial une référence commune en matière de cybersécurité des systèmes spatiaux.** En effet, les politiques du gouvernement américain en la matière étaient jusqu'alors fragmentées voire parfois absentes, de sorte que les acteurs spatiaux – y compris les agences fédérales – ne partageaient pas systématiquement la même perception des menaces

Pour ce faire, la SPD-5 a vocation à **définir des principes haut niveau et non contraignants** permettant aux entités gouvernementales et privées américaines de maximiser la protection de leurs systèmes spatiaux et des données qui y transitent. Parmi ces principes, la SPD-5 insiste sur :

- **La prise en compte des menaces cyber tout au long du cycle de vie des systèmes spatiaux**. Elle insiste sur l'importance de développer des systèmes qui puissent continuellement anticiper et répondre à d'éventuelles attaques
- **La mise en place de mesures de cybersécurité par les propriétaires et les opérateurs de systèmes spatiaux** afin de garantir l'intégrité, la confidentialité et la disponibilité des services et des données fournis par les systèmes spatiaux. Ces mesures incluent, entre autres, la protection contre les accès non autorisés, contre le brouillage et l'usurpation des communications (notamment *via* le recours au cryptage et à

l'authentification), la protection des infrastructures au sol, la gestion des risques liés aux chaînes d'approvisionnement (en encourageant la surveillance et la sensibilisation des fournisseurs), etc.

- **La nécessité de mettre en œuvre des mesures de protection équilibrées,** c'est-à-dire qui soient efficaces sans constituer une charge injustifiée pour les propriétaires ou opérateurs de systèmes spatiaux
- **La coopération et le partage d'informations** concernant les menaces, les alertes ou les incidents en s'appuyant sur le *Space Information Sharing and Analysis Center* (Space ISAC) créé en 2019

La SPD-5 encourage également la **mise en application des principes qu'elle contient à travers l'adoption de normes de comportement, de bonnes pratiques, de règles voire de véritables réglementations**. Elle ne donne toutefois aucune directive aux agences fédérales sur la façon de retranscrire ces principes au sein de réglementations contraignantes (ce qui aurait pu être le cas par exemple en demandant l'adoption de nouvelles exigences de cybersécurité dans le cadre du processus de demande licence pour lancer ou opérer un satellite). La SPD-5, qui ne constitue pas un texte contraignant, n'a, à dessein, pas vocation à être prescriptif. De ce fait, **d'importants défis se posent quant à sa mise en œuvre effective**.

3. Défis de mise en œuvre et réactions

Non contraignante, la SPD-5 **nécessitera une volonté politique forte et une bonne gouvernance pour la mettre en application**. Ce volontarisme politique sera d'autant plus nécessaire que les mesures encouragées par la SPD-5 pourraient **affecter la compétitivité des entreprises américaines qui subissent déjà les contraintes liées à d'autres normes de conformité** comme l'*International Traffic in Arms Regulations* (ITAR), l'*Export Administration Regulations* (EAR), le *National Institute of Standards and Technology* (NIST), etc. En effet, en demandant de leur part des efforts importants pour garantir l'intégrité de leurs systèmes, les entreprises américaines devront augmenter leurs coûts qui se répercuteront en fin de course sur le prix à l'international.

Malgré les difficultés qui s'annoncent dans sa mise en œuvre, la SPD-5 a été plutôt

bien reçue par la communauté de cybersécurité spatiale, qui se réjouit de la prise en compte des problématiques liées à la protection des réseaux satellitaires. Cette communauté estime d'ailleurs avoir joué un rôle majeur dans la publication de la SPD-5 en faisant prendre conscience de ces problématiques aux décideurs américains. Selon certains membres de cette communauté, la SPD-5 serait « *the best space cybersecurity policy we have ever had* », bien que celle-ci pourrait faire l'objet de diverses améliorations.

En effet, les acteurs du secteur ont mis en avant plusieurs failles affectant la SPD-5 et ont émis plusieurs recommandations :

- **La SPD-5 serait tout d'abord trop haut niveau** : des détails supplémentaires seraient nécessaires pour faire évoluer les systèmes afin de garantir leur sécurité et leur résilience face aux attaques
- **La SPD-5 ne serait pas suffisamment contraignante** : il serait nécessaire de mettre en place un système de surveillance afin de s'assurer que les agences fédérales s'y conforment
- **La SPD-5 aurait dû encourager l'adoption d'un *Risk Management Framework*** (RMF). Le RMF est une politique adopté en 2010 par le *National Institute of Standards and Technology* (NIST) qui définit un cadre commun pour assurer la sécurité des systèmes d'information du gouvernement et de ses contractants
- **La SPD-5 pourrait reconnaître et adopter les standards développés** au sein des *Cybersecurity Maturity Model Certification* (CMMC) et *Infrastructure Asset Pre-Assessment* (IA-Pre) qui s'appliquent déjà aux entreprises du spatial agissant pour le cadre de missions gouvernementales. Le CMMC définit des standards communs pour assurer la cybersécurité des systèmes d'information de la base industrielle de défense américaine. Le IA-Pre définit des exigences de cybersécurité pour les opérateurs commerciaux de satellites de télécommunications souhaitant intégrer le marché des communications militaires

Outre ces réactions, la publication de la SPD-5 a déjà été suivie d'actions concrètes. **En octobre dernier, l'USSF a annoncé qu'elle allait accueillir plus de mille opérateurs cybersécurité actuellement intégrés au sein de l'*U.S. Air Force* et**

qui détiennent une expertise dans les programmes spatiaux. Leur transfert pourrait avoir lieu dès l'année fiscale 2021.

En guise de synthèse, il est possible de dire que la SPD-5 établit des principes clés de cybersécurité pour guider et servir de base à la stratégie américaine de la cyber-protection des systèmes spatiaux, mais que ces principes devront, pour être véritablement efficaces, être approfondis et mis en œuvre de façon à ce que toutes les parties prenantes les respectent.

4. Sources

- *White House Factsheet*, 4 septembre 2020
- *SPD-5 text*, 4 septembre 2020
- *Department of Homeland Security release*, 4 septembre 2020
- *White House issues cybersecurity space policy*, Space News, 4 septembre 2020
- *President Trump Signs Space Policy Directive Establishing America's First Comprehensive Cybersecurity Policy For Space Systems*, Parabolic Arc, 4 septembre 2020
- *Donald Trump signe la Space Policy Directive 5 relative à la cybersecurité des systèmes spatiaux*, Bulletin d'actualité Espace n°20-15, 18 septembre 2020
- *More than 1,000 Air Force cyber security operators to transfer to Space Force*, Space News, 8 octobre 2020
- *Cybersecurity Influencers React to Space Policy Directive 5*, Satellite Today, 15 octobre 2020