



Le nano satellite *Moonlighter* : vers un renforcement de la cybersécurité spatiale américaine

Le 24 février 2022, des hackers liés à l'armée russe conduisent une cyberattaque contre le segment sol utilisateur de l'entreprise VIA-SAT et réussissent à interrompre les services de communication délivrés par le satellite KA-SAT à l'Ukraine¹. Dans un contexte de vulnérabilité croissante des satellites aux menaces cybernétiques, l'US Space Force (USSF) déploie en 2023 le cubesat expérimental *Moonlighter*, outil d'évaluation de la cybersécurité de ses satellites.

Le premier démonstrateur de cybersécurité spatiale en orbite

Une cyberattaque peut viser trois éléments d'un système spatial : le segment sol, les liaisons et les satellites. Développé par le *Space Systems Command* (SSC) et l'*Air Force Research Laboratory*, le *Moonlighter* est un nano satellite de type *CubeSat 3U*, doté d'une charge utile numérique de type « bac à sable »², conçue pour tester les failles de cybersécurité des satellites³.

Mis en orbite lors de la mission *SpaceX CRS-28* en juillet 2023, le *Moonlighter* est utilisé pour l'exercice *Hack-A-Sat 4*, organisé par l'*US Air Force* et l'*USSF* en août 2023⁴. Des spécialistes américains et européens de la cybersécurité s'affrontent dans cette compétition dont l'objet consiste à prendre le contrôle du nanosatellite, lui faire prendre une photo d'un objectif au sol et envoyer celle-ci à une station terrestre.

En novembre 2023, il est à nouveau mis à contribution lors de l'exercice *Moonlight Defender* organisé par l'*USSF*⁵. Le 527th *Space Aggressor Squadron Cyber Flight* simule des cyberattaques contre le *Moonlighter*, tandis que six escadrons cyber, appuyés par un détachement du *Space Delta 6* de l'*USSF* le défendent pour garantir l'intégrité de ses systèmes d'information.

Une réponse à l'essor des capacités ASAT cybernétiques russes et chinoises

Le déploiement du *Moonlighter* s'inscrit dans l'évolution de la doctrine spatiale américaine. Dès 2020, la *National Space Policy* fait de la cybersécurité une priorité dans le domaine spatial, réaffirmée par la *National Cybersecurity Strategy* de 2023⁷ puis consacrée dans la doctrine de l'*USSF* en avril 2025⁸. Elle place la guerre cybernétique au cœur de la supériorité spatiale. Le *Moonlighter* complète ainsi deux programmes initiés en 2023 par le SSC : le *Battle Management Command, Control and Communications*, qui vise à sécuriser les systèmes de commandement, de contrôle et de communication spatiaux et le *Space Domain Awareness and Combat Power*, destiné à renforcer les capacités de l'*USSF* face aux menaces spatiales, notamment d'ordre cyber.

Le *Moonlighter* fait face à l'essor des capacités anti-satellites (ASAT) cybernétiques russes et chinoises. Selon la CIA, Pékin développerait des moyens offensifs cyber capables de neutraliser, de prendre le contrôle de satellites adverses et de leur faire transmettre de fausses informations⁹. L'Armée populaire de libération (APL) dispose d'unités spécialisées dans ce type d'opérations¹⁰, regroupées au sein de la nouvelle *Aerospace Force*.

Des documents publiés en février 2024¹¹ montrent que l'APL externalise davantage ses opérations cyber dans le domaine spatial, ce qui semble constituer une stratégie pour gêner l'identification de l'origine des attaques.

Alors que les systèmes spatiaux deviennent toujours plus vulnérables, l'US Space Force met en œuvre le cubesat expérimental *Moonlighter*, outil innovant qui permet d'évaluer et renforcer la cyber sécurité des satellites. Il s'inscrit dans une stratégie plus large des États-Unis destinée à protéger ses systèmes contre les capacités anti-satellites cybernétiques. L'attaque dont a été victime l'Ukraine souligne la nécessité d'une adaptation constante face à l'évolution des menaces, sans doute dans le cadre de coopérations internationales.

Remerciements à Théo Siguier pour son travail de recherche

1 « [Ukraine suffered two cyberattacks in the lead-up to Russia's invasion](#) », *The Washington Post*, 03/2022.

2 De l'anglais « *sandbox* », il s'agit d'un environnement informatique isolé, conçu pour réaliser des tests sans risquer d'endommager le système principal.

3 « [Moonlighter](#) », *Aerospace*, 04/2023.

4 « [Hack-A-Sat's Moonlighter satellite...](#) », *AFRL*, 07/2023.

5 « [Space Force Guardians hone cyber defense skills using on-orbit satellite](#) », *USSF*, 12/2023.

6 La *Space Delta 6* est une unité de l'*USSF* chargée de sécuriser et de défendre les systèmes spatiaux militaires américains et de garantir aux forces un accès sécurisé à l'espace.

7 « [Space and Cyber Warfare as One](#) », *CSIS*, 10/2024.

8 « [Space Force Doctrine Document 1](#) », *USSF*, 04/2025.

9 « [China building cyber weapons to hijack enemy satellites, says US leak](#) », *Financial Times*, 04/2023.

10 « [China's Space Capability and What This Means for the West](#) », *CASI*, 06/2024.

11 « [Global Counterspace Capabilities](#) », *SWF*, 04/2025.