POSITION: TRANSINNE
ORIGINE: BEL-N-225
VITESSE: 73
ÉQUIPAGE: 15
CARGO: 2963

Wallonie Relance

Les Talents du futur sont ici !

DOSSIER PÉDAGOGIQUE

DESTINÉ AUX ENSEIGNANT·ES

De la 5e PRIMAIRE À la 6e SECONDAIRE

Opération Cyber Espace

UNIVERSITÉ DE NAMUR

EURO SPACE CENTER

Nexova

AVANT-PROPOS

Chères, chers enseignant·es,

Ce dossier pédagogique a été conçu pour vous accompagner dans la sensibilisation de vos élèves à la cybersécurité. Il se veut à la fois une source d'inspiration, un outil pratique et un support concret pour enrichir vos pratiques pédagogiques.

Jusqu'à présent un animateur de l'Euro Space Center prenait en charge l'animation dans les classes. Désormais, il vous revient de prendre en charge seul·e cette animation.

Mais pas de stress, à travers ce dossier, nous allons vous aider :

- À **comprendre l'objectif** de l'animation et **identifier les savoirs et savoir-faire** qui pourront être développés chez vos élèves s'iels la vivent (page 3).
- À comprendre **pourquoi** il devient essentiel de **former les jeunes** à la cybersécurité (page 5).
- À découvrir **comment** vous pouvez **enseigner la cybersécurité** à travers des ressources existantes et bien pensées (page 9).

Ce dossier (V2, mars 2025) va évoluer grâce à vous. Nous vous encourageons vivement à nous partager vos retours, vos suggestions et vos expériences afin d'enrichir et de perfectionner ce projet. Que ce soient vos scénarios pédagogiques, les éléments que vous avez trouvé utiles, des photos et retours de vos interventions avec vos classes, ou encore toute ressource pédagogique complémentaire, chaque contribution est précieuse !

Pour nous faire part de vos commentaires,

- Vous pouvez nous écrire par email à : cyberatschool@eurospacecenter.be
- Ou remplir le formulaire en ligne via l'URL http://bit.ly/43TLPUI ou le QR code

Rapport de mission

Nous comptons sur votre collaboration pour faire évoluer ce projet ensemble.

Nous espérons que ce dossier vous inspira et vous aidera à susciter chez vos élèves une réflexion constructive sur la cybersécurité et les métiers associés.

Bonne découverte et bon travail !

OPÉRATION CYBER ESPACE

Vis ma vie d'expert·e pour apprendre

Le jeu *"Opération Cyber Espace"* sensibilise les jeunes au domaine de la cybersécurité en leur faisant découvrir ses métiers. Grâce à un scénario immersif, les participants acquièrent des connaissances et développent des savoir-faire propres à ce domaine.

Le jeu propose deux versions adaptées à l'âge des participants : une pour les 10-14 ans (P5-P6-S1-S2) et une pour les 15-18 ans (S4-S5-S6). Des carnets *"Journal de mission"*, conçus spécifiquement pour chaque tranche d'âge, sont disponibles sur demande à l'Euro Space Center ou téléchargeables gratuitement sur notre site web (https://www.eurospacecenter.be/fr/ecole/cyber-at-school).

Ce jeu permet d'acquérir des connaissances et des compétences pratiques en lien avec les attendus européens (voir pages 6, 7 et 8) et les attendus du tronc commun de l'enseignement obligatoire en Belgique francophone (voir pages 5 et 6). Les attendus communs aux deux versions sont présentés ci-dessous. Il est important de les adapter à l'âge des participants pour assurer une progression adaptée.

Savoirs	Attendus
Vocabulaire spécifique au domaine de la cybersécurité	**Connaitre** et **comprendre** les termes repris dans la section "Vocabulaire" du "*Journal de mission*"
	Distinguer cybermenace de cyberattaque, données importantes de données sensibles
	Connaître les différentes formes de cyberattaque et identifier des conséquences possibles de celles-ci
	Nommer les étapes-clé d'une cyberattaque
	Nommer et expliquer les actions-clé de cyberdéfense

Savoir-faire	Attendus
Utiliser adéquatement le vocabulaire spécifique au domaine de la cybersécurité	**Utiliser** adéquatement **les** termes repris dans la section "Vocabulaire" du "*Journal de mission*"
Réagir face à des situations de cybermenaces, de cyberattaques	**Reconnaître** une cybermenace et/ou une cyberattaque (sa forme, les failles utilisées, les données visées, etc.)
	Proposer des pistes d'action, parmi celles mises à dispositions ou non, pour faire face à une situation de cybermenace et/ou de cyberattaque

De plus, le jeu vise à faire découvrir les métiers liés à la cybersécurité dès le plus jeune âge. La version pour les 15-18 ans est plus avancée : elle explore notamment les parcours de formation permettant d'évoluer dans ce domaine.

En tant qu'enseignant·e, vous jouez un rôle essentiel dans l'orientation des jeunes, comme le confirment de nombreuses études. En leur permettant de découvrir les métiers de la cybersécurité et d'autres domaines techniques, vous élargissez leurs perspectives professionnelles et les aidez à envisager des parcours auxquels ils n'auraient peut-être jamais pensé.

Des outils comme *"Opération Cyber Espace"* offrent l'opportunité de faire découvrir des carrières innovantes, de lutter contre les stéréotypes et d'encourager les jeunes à explorer des secteurs encore méconnus. Comme le montrent les tableaux des savoirs et savoir-faire présentés précédemment, ce jeu constitue une véritable porte d'entrée vers le monde de la cybersécurité.

Pour les plus jeunes, il répond pleinement aux exigences du tronc commun de l'enseignement obligatoire belge francophone (voir pages 5 et 6) tout en les dépassant. Pour les plus âgé·es, grâce à la collaboration avec l'entreprise Nexova, le jeu propose des contenus réalistes et adaptés à différents niveaux de compétences, reflétant concrètement les métiers du secteur.

Enfin, *"Opération Cyber Espace"* se distingue par son caractère inclusif, un aspect crucial dans un domaine encore marqué par une faible représentation des femmes due à des stéréotypes persistants. Avec le soutien de l'Université de Namur, le jeu contribue à briser ces barrières et à encourager une plus grande diversité dans les carrières techniques.

LA CYBERSÉCURITÉ

Compétence-clé de la citoyenneté numérique

Pourquoi devriez-vous proposer cette animation dans votre classe ? Nous allons tenter de vous convaincre (si vous ne l'êtes pas déjà) à travers des référentiels de compétences reconnus et adoptés de tous·tes.

Commençons par le référentiel qui vous touche le plus : le référentiel "Formation Manuelle Technique, Technologique et Numérique" (FMTTN).

LA CYBERSÉCURITÉ DANS LES PROGRAMMES SCOLAIRES BELGES

La cybersécurité fait désormais partie du tronc commun de l'enseignement obligatoire en Belgique francophone. Elle est intégrée dans le volet numérique du référentiel FMTTN, avec des contenus répartis sur les années d'étude P6 (6e primaire) et S1 (1re secondaire). Vous trouverez ci-dessous des tableaux détaillant les connaissances, les compétences pratiques et les savoir-faire attendus pour chacun de ces niveaux.

P6

SÉCURITÉ

Savoirs	Attendus
Vocabulaire spécifique à la protection des personnes	Utiliser, adéquatement en contexte, les termes dont identité numérique*, cyberharcèlement*, cyberdépendance*.
Vocabulaire spécifique à la protection des données	Utiliser, adéquatement en contexte, les termes dont sauvegarde, mise à jour, cookie*, hameçonnage*, spam, piratage, cyberattaque*, antivirus, mot de passe, authentification.

Savoir-faire	Attendus
Créer un mot de passe respectant un niveau de sécurité élevé.	Créer un mot de passe respectant un niveau de sécurité élevé.
Effacer ses traces personnelles sur un équipement partagé.	Effacer ses fichiers personnels sur un équipement partagé.
Réagir face à des situations de cyberattaque*, de cyberharcèlement*, de cybermanipulation.	Proposer des pistes d'actions, parmi celles mises à disposition, pour faire face à des situations de cyberattaque*, de cyberharcèlement*, de cybermanipulation.
	Reconnaitre des situations de cyberattaque*, de cyberharcèlement*, de cybermanipulation.

Compétences	Attendus
Prévenir et limiter les risques relatifs à la protection des données.	Adopter un comportement responsable relatif à la protection des données.
Prévenir et limiter les risques de déséquilibre social et psychologique de la personne (cyberattaque*, cyberharcèlement*, cyberdépendance*).	Adopter un comportement responsable face à une situation de cyberattaque*, cyberharcèlement*, cyberdépendance*.

S1

SÉCURITÉ

Savoirs	Attendus
Vocabulaire spécifique à la protection des personnes	Utiliser, adéquatement en contexte, les termes dont profil, protection de la vie privée.
	Décoder une signalétique (PEGI…).
Vocabulaire spécifique à la navigation sécurisée	Distinguer HTTP et HTTPS.

Savoir-faire	Attendus
Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles.	Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles.
Paramétrer les options de confidentialité d'un compte.	Paramétrer les options de confidentialité d'un compte.
Effacer ses traces personnelles sur un équipement partagé.	Effacer toute trace de connexion sur un équipement partagé.
Réagir face à des situations de cyberattaque*, de cyberharcèlement*, de cybermanipulation.	Proposer et mettre en place des actions pertinentes pour faire face à des situations de cyberattaque*, de cyberharcèlement*, de cybermanipulation.

Compétences	Attendus
Gérer son identité numérique*, ses traces et ses données personnelles, pour protéger sa vie privée et celle des autres.	Gérer son identité numérique*, ses traces, ses données personnelles, de manière responsable.
Prévenir et limiter les risques de déséquilibre social et psychologique de la personne (cyberattaque*, cyberharcèlement*, cyberdépendance*).	Réagir, de manière responsable, face aux risques de cyberattaque*, de cyberharcèlement*, de cyberdépendance*.

Vous n'enseignez pas en P6 ou en S1 ? Peu importe ! Même s'il n'existe pas d'attentes officielles pour vos élèves, cela ne signifie pas que la cybersécurité ne doit pas être abordée. Le référentiel DigComp, reconnu comme la référence européenne pour l'éducation à la citoyenneté numérique, souligne depuis longtemps l'importance de sensibiliser chacun·e à la cybersécurité.

Avant d'explorer DigComp en détail, prenons un moment pour comprendre ce qu'implique l'éducation à la citoyenneté numérique.

L'ÉDUCATION À LA CITOYENNETÉ NUMÉRIQUE

> *"La citoyenneté numérique est la capacité à participer de manière active, continue et responsable à des communautés en ligne et hors ligne, grâce à un engagement compétent et positif avec les technologies numériques (en créant, travaillant, partageant, socialisant, enquêtant, jouant, communiquant et apprenant"*
>
> (https://www.coe.int/fr/web/education/digital-citizenship-education).

Le jeu "*Opération Cyber Espace*" répond aux besoins d'éducation à la citoyenneté numérique définis par le Conseil de l'Europe en raison de son approche innovante et de ses trois objectifs clés : développer des

compétences numériques fondamentales, promouvoir une culture de la sécurité et encourager la pensée critique.

1. **Compétences numériques fondamentales** : La citoyenneté numérique repose sur la capacité à interagir de manière responsable avec les technologies numériques. "*Opération Cyber Espace*" répond à cet impératif en enseignant la cybersécurité dès le plus jeune âge. En apprenant à utiliser les appareils en toute sécurité, à gérer les mots de passe et à protéger leur vie privée en ligne, les jeunes développent des compétences numériques essentielles pour participer activement et de manière responsable à la société numérique. Cette approche leur permet de naviguer dans un monde où la technologie est omniprésente tout en respectant des principes fondamentaux de sécurité.

2. **Citoyenneté numérique et culture de la sécurité** : Le jeu favorise l'établissement d'une culture de la sécurité en inculquant des habitudes responsables dès l'enfance. En apprenant à respecter la vie privée d'autrui et à comprendre les conséquences de leurs actions en ligne, les enfants deviennent non seulement des utilisateurs responsables, mais aussi des citoyen·nes numériques averti·es. Cela permet de construire une génération consciente des enjeux liés à la sécurité et au respect des données personnelles, essentiels pour une participation active et saine dans les communautés en ligne.

3. **Promotion de la pensée critique** : Enfin, "*Opération Cyber Espace*" encourage les jeunes à développer une pensée critique face aux informations qu'iels rencontrent en ligne. Le jeu incite les joueur·euses à évaluer la fiabilité des sources, à poser des questions sur le contenu numérique et à faire preuve de discernement avant de partager ou de croire ce qu'iels voient. En intégrant ces compétences dans leur réflexion quotidienne, les jeunes deviennent des acteur·rices critiques et informé·es dans leur environnement numérique, capables de participer activement à la création et à la diffusion d'informations de manière responsable.

En bref, "*Opération Cyber Espace*" offre une approche ludique et pédagogique pour développer des compétences numériques, une culture de la sécurité et une pensée critique, contribuant ainsi de manière significative à la formation de citoyen·nes numériques compétent·es et responsables.

LE RÉFÉRENTIEL DIGCOMP

Enfin, il est fort probable que la cybersécurité soit abordée de manière plus approfondie après le tronc commun, en raison de son importance croissante dans le référentiel DigComp. Ce référentiel définit les compétences numériques essentielles qui sont cruciales pour la formation, la certification, l'insertion sur le marché de l'emploi et la participation à la vie citoyenne dans le monde numérique. DigComp sert de

référence pour préparer les jeunes aux exigences du numérique. Parmi ces compétences, la protection des données et la sécurité en ligne occupent une place centrale. Dans cette optique, il est primordial de les intégrer de façon progressive et continue dans l'enseignement secondaire, afin de préparer les élèves à des défis numériques toujours plus complexes et omniprésents.

Le référentiel DigComp identifie la cybersécurité comme un domaine de compétence clé, structuré autour de quatre axes principaux :

1. **La protection des appareils numériques** : Il s'agit d'apprendre à sécuriser les appareils numériques ainsi que leurs contenus en comprenant les risques et les menaces qui peuvent les affecter.

2. **La protection des données personnelles et de la vie privée** : Cet axe consiste à comprendre comment protéger ses données numériques, en particulier en ce qui concerne le partage des informations personnelles, et à prendre conscience des enjeux de la vie privée en ligne.

3. **La protection de la santé et du bien-être** : Il est essentiel de prévenir les risques liés à l'utilisation excessive des technologies numériques, qu'ils soient physiques (problèmes de santé) ou psychologiques (bien-être). Cet axe sensibilise également aux dangers potentiels des environnements numériques pour soi-même et pour les autres.

4. **La protection de l'environnement** : Cet axe met l'accent sur l'impact environnemental des technologies numériques et de leurs usages, en encourageant une prise de conscience de leur effet sur la planète.

Ces compétences sont transversales et s'appliquent à tous les usages du numérique, quel que soit le type d'activité exercé à travers des moyens numériques. Ainsi, il est essentiel d'intégrer la cybersécurité de manière transversale dans l'ensemble des apprentissages numériques.

Pour accompagner les enseignants dans cette démarche, le site Comprendre DigComp (https://www.comprendredigcomp.com/) propose une approche pratique du référentiel. Vous y trouverez une description détaillée des compétences numériques à développer avec vos apprenants, ainsi que des exemples et des scénarios d'intégration.
La cybersécurité est abordée dans le « Domaine 4 : Protection et Sécurité ».

ENSEIGNER LA CYBERSÉCURITÉ

Ressources et approches

Comment enseigner la cybersécurité ?

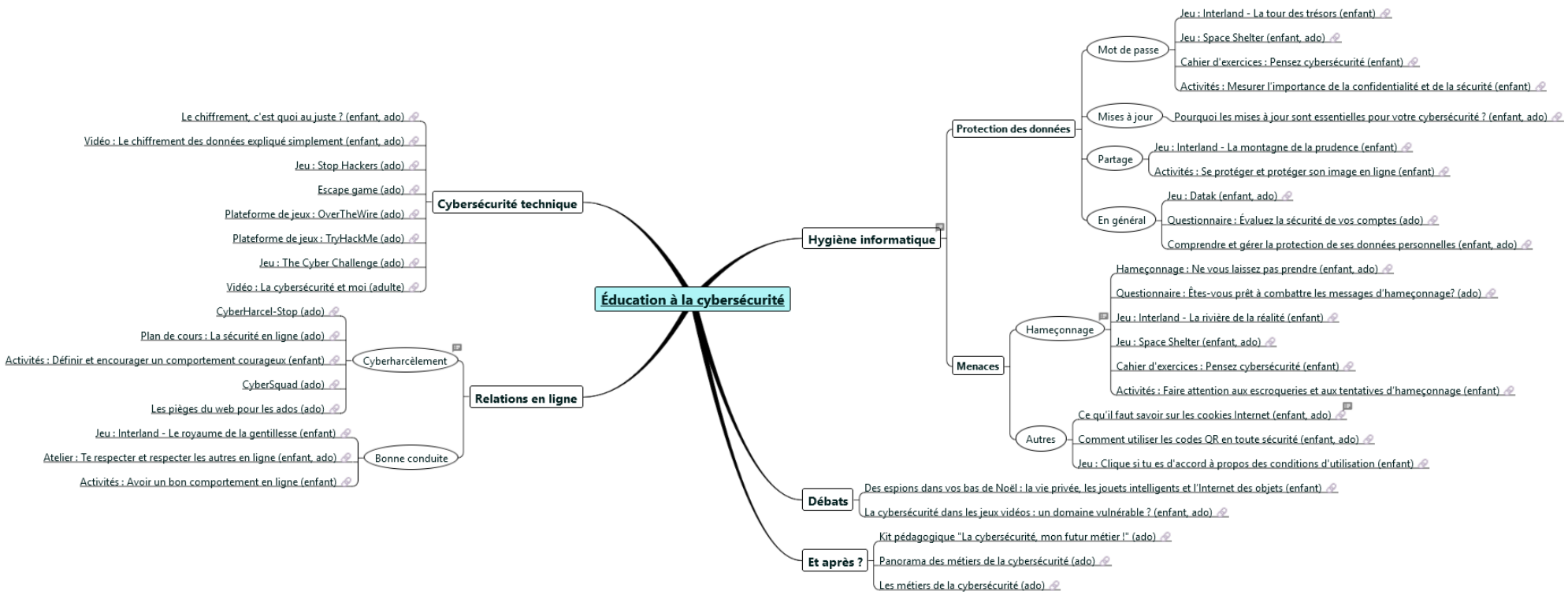
L'éducation à la cybersécurité peut couvrir divers aspects, tels que la dimension technique, l'hygiène informatique ou encore les relations interpersonnelles en ligne. Selon votre familiarité avec le numérique, vous pourriez être davantage attiré·e par l'un de ces aspects, ou peut-être ne vous sentir à l'aise avec aucun d'entre eux. Cela n'a pas d'importance : vous pouvez choisir d'adopter une posture plus passive, en devenant celle ou celui qui accompagne les élèves dans leur parcours personnel, tout en les responsabilisant.

Nous vous proposons une carte mentale regroupant des ressources validées par l'équipe ayant développé le jeu "Opération Cyber Espace" (cf. page suivante) : Éducation à la cybersécurité - Digimindmap by La Digitale ou via le QR code

Carte mentale

Ces ressources peuvent servir d'inspiration ou être directement utilisées dans vos séquences pédagogiques. Il n'est pas nécessaire de réinventer la roue : il est plus pertinent de réfléchir à la manière dont ces ressources peuvent s'articuler avec le jeu "*Opération Cyber Espace*" pour construire une séquence pédagogique riche et cohérente. Par exemple, après avoir utilisé le jeu, vous pourriez approfondir les thématiques liées au phishing, une attaque très courante, notamment chez les publics non avertis. Vous pourriez aussi explorer la manière dont les jeunes perçoivent la valeur de leurs données personnelles à travers des activités comme le jeu "Stop Hackers", développé dans le cadre du groupe de travail du Pacte d'Excellence.

Et si malgré tout vous ressentez le besoin de vous former sur les aspects techniques, nous vous invitons à découvrir l'ouvrage "*Éduquer au numérique. 12 clés pour comprendre l'informatique*" : https://bit.ly/4iE5EUn


Éducation à la cybersécurité
Cybersécurité technique
Le chiffrement, c'est quoi au juste ? (enfant, ado)
Vidéo : Le chiffrement des données expliqué simplement (enfant, ado)
Jeu : Stop Hackers (ado)
Escape game (ado)
Plateforme de jeux : OverTheWire (ado)
Plateforme de jeux : TryHackMe (ado)
Jeu : The Cyber Challenge (ado)
Vidéo : La cybersécurité et moi (adulte)
Relations en ligne
Cyberharcèlement
CyberHarcel-Stop (ado)
Plan de cours : La sécurité en ligne (ado)
Activités : Définir et encourager un comportement courageux (enfant)
CyberSquad (ado)
Les pièges du web pour les ados (ado)
Bonne conduite
Jeu : Interland - Le royaume de la gentillesse (enfant)
Atelier : Te respecter et respecter les autres en ligne (enfant, ado)
Activités : Avoir un bon comportement en ligne (enfant)
Hygiène informatique
Protection des données
Mot de passe
Jeu : Interland - La tour des trésors (enfant)
Jeu : Space Shelter (enfant, ado)
Cahier d'exercices : Pensez cybersécurité (enfant)
Activités : Mesurer l'importance de la confidentialité et de la sécurité (enfant)
Mises à jour
Pourquoi les mises à jour sont essentielles pour votre cybersécurité ? (enfant, ado)
Partage
Jeu : Interland - La montagne de la prudence (enfant)
Activités : Se protéger et protéger son image en ligne (enfant)
En général
Jeu : Datak (enfant, ado)
Questionnaire : Évaluez la sécurité de vos comptes (ado)
Comprendre et gérer la protection de ses données personnelles (enfant, ado)
Menaces
Hameçonnage
Hameçonnage : Ne vous laissez pas prendre (enfant, ado)
Questionnaire : Êtes-vous prêt à combattre les messages d'hameçonnage? (ado)
Jeu : Interland - La rivière de la réalité (enfant)
Jeu : Space Shelter (enfant, ado)
Cahier d'exercices : Pensez cybersécurité (enfant)
Activités : Faire attention aux escroqueries et aux tentatives d'hameçonnage (enfant)
Autres
Ce qu'il faut savoir sur les cookies Internet (enfant, ado)
Comment utiliser les codes QR en toute sécurité (enfant, ado)
Jeu : Clique si tu es d'accord à propos des conditions d'utilisation (enfant)
Débats
Des espions dans vos bas de Noël : la vie privée, les jouets intelligents et l'Internet des objets (enfant)
La cybersécurité dans les jeux vidéos : un domaine vulnérable ? (enfant, ado)
Et après ?
Kit pédagogique "La cybersécurité, mon futur métier !" (ado)
Panorama des métiers de la cybersécurité (ado)
Les métiers de la cybersécurité (ado)


EURO
SPACE
CENTER
CRÉATEUR DE HÉROS SPATIAUX
1, rue devant les Hêtres | B-6890 Transinne, Belgique
Tel. : + 32.61/ 65 64 65 | Fax : + 32.61/ 65 64 61
Mail : info@eurospacecenter.be
www.eurospacecenter.be