REE REVUE DE L'ELECTRICITÉ ET DE L'ELECTRONIQUE

La Direction d'analyse de la menace cyber de Thales a présenté le bilan 2022 d'un an d'attaques cyber à l'échelle du continent européen.

L'agression militaire de la Russie contre l'Ukraine a remodelé le panorama des menaces cyber en Europe en 2022. Le conflit a mobilisé de nombreux « hacktivistes », des cybercriminels et des groupes instrumentalisés par des États.

Une nouvelle géographie des attaques en Europe

La fin de 2022 marque un tournant dans la cyberguerre liée au conflit en Ukraine avec une transition très nette d'une cyberguerre centrée sur l'Ukraine et la Russie vers une cyberguerre hybride de haute intensité s'étendant à l'Europe [1].

Une nouvelle géographie des attaques se dessine après douze mois de conflit. Si la majorité des incidents dans le monde était concentrée sur l'Ukraine au moment de l'invasion (50,4 % au premier trimestre 2022 contre 28,6 % au troisième trimestre), les pays membres de l'Union européenne ont vu le nombre d'incidents liés au conflit augmenter de façon spectaculaire sur les 6 derniers mois, passant de 9,8 % à 46,5 % des attaques mondiales.

A l'été, on dénombrait autant d'incidents liés au conflit dans les pays de l'UE qu'en Ukraine (85 contre 86). Le début de l'année 2023 confirme cette tendance avec une écrasante majorité des incidents concentrée dans les pays européens (80,9 %).

L'Europe de l'Est et l'Europe du Nord en première ligne de la cyberguerre

La cyberguerre cible en particulier la Pologne, les pays baltes et les pays nordiques, et de manière croissante dans les secteurs des infrastructures nationales critiques, notamment dans les domaines de l'aviation, l'énergie, la santé, les banques et l'administration publique.

Les pays candidats à l'intégration européenne tels que le Monténégro et la Moldavie sont de plus en plus ciblés (de 0,7 % des attaques au premier trimestre 2022 à 2,7 % en fin d'année 2022), la Pologne est constamment harcelée avec le nombre record de 114 incidents liés au conflit en un an et les « hacktivistes » de guerre se concentrent particulièrement sur les pays baltes (157 incidents en Estonie, Lettonie, Lituanie) et les pays du Nord (95 incidents en Suède, Norvège, Danemark, Finlande). Hormis l'Allemagne avec 58 incidents en un an, les pays comme la France (14), le Royaume-Uni (18), l'Italie (14) ou encore l'Espagne (4) sont davantage préservés (figure 1).

Une augmentation générale des cyberattaques au niveau mondial

L'Amérique du Nord (+52 %), l'Amérique latine (+29 %) et l'Europe (+26 %) ont enregistré les plus fortes augmentations du nombre de cyberattaques en 2022, par rapport à 2021 (figure 2).

En Europe, la France se situe en deçà du niveau moyen européen (+26 %) avec une augmentation de 19 % du nombre moyen hebdomadaire de cyberattaques observée par organisation en 2022 (soit 826 attaques hebdomadaires en moyenne), l'Espagne une augmentation de 11 % (soit 1260 attaques en une semaine par organisation en moyenne), l'Italie 23 % (soit 1225 attaques en une semaine par organisation en moyenne), l'Allemagne et la Grèce respectivement + 27 % et + 40 % (864 et 801 attaques hebdomadaires observées en moyenne par organisation).

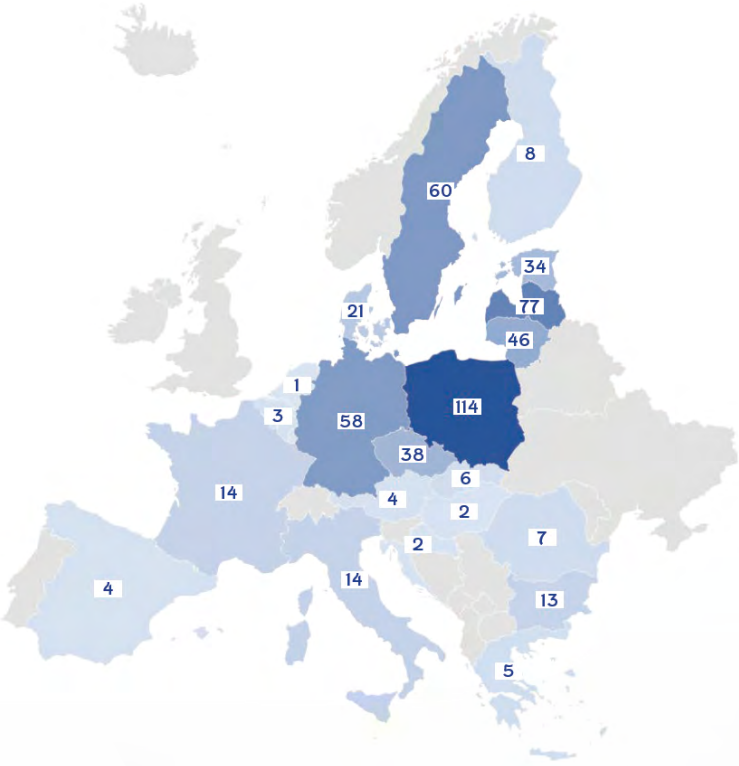

Figure 1 : Distribution des attaques dans les pays européens (Source Thales).

1 Source : Thales Presse Release 23 mars 2023.

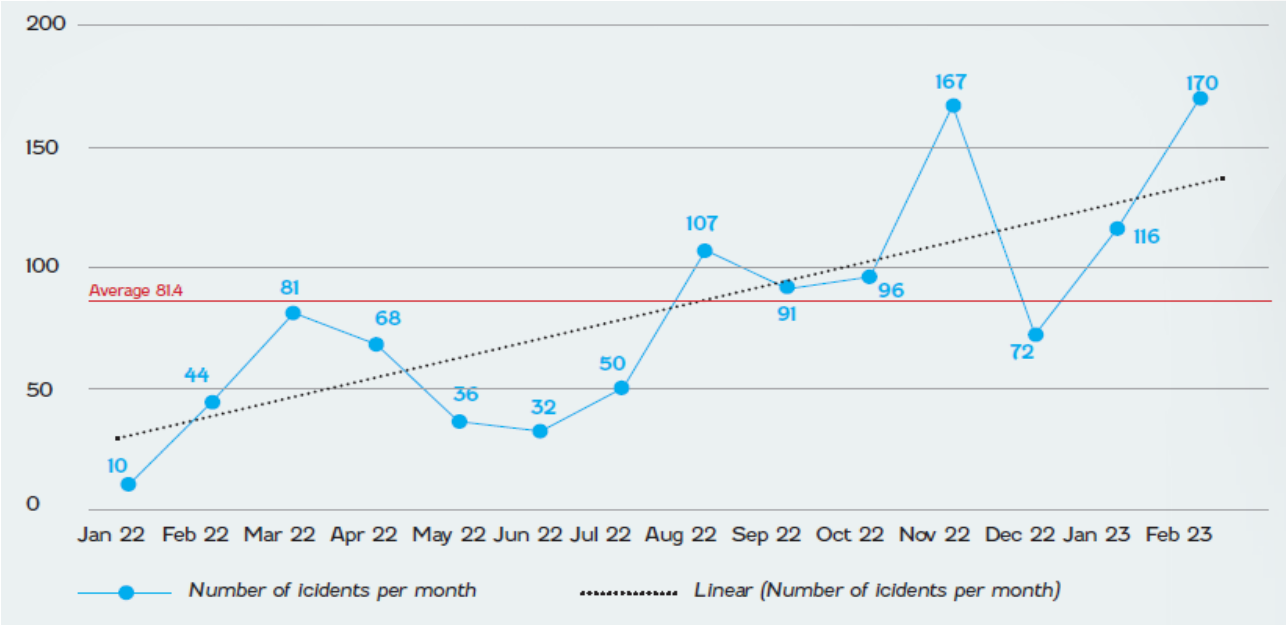

Figure 2 : Accélération du nombre d'attaques en Europe en seconde moitié de 2022 (Source Thales).

Des attaques massives en déni de service (DDoS)

Le troisième trimestre 2022 marque un tournant avec une vague de dénis de service alors que le premier trimestre faisait état d'un panorama des modes d'attaques très variés, à part quasi égale entre vols et fuites de données, DDoS, espionnage, influence, intrusion, rançongiciel [2] *phishing* [3], *wiper* [4] et *infostealer* [5].

Les cyberattaquants agissent à travers des attaques massives par déni de service (à 75 %) à l'encontre des entreprises et des administrations, déployant ainsi des techniques de harcèlement systématique, souvent à faible impact opérationnel, mais mettant sous tension les équipes de sécurité et les décideurs (figure 3). L'objectif n'est pas d'obtenir des impacts significatifs, mais de harceler et décourager tout soutien à l'Ukraine.

Les attaques par « *wiper* » peuvent détruire les systèmes de l'adversaire et l'espionnage à long terme peut compromettre l'intégrité de sa sécurité mais ces attaques doivent faire l'objet d'une préparation beaucoup plus longue dans le temps, et nécessitent plus de ressources. Les opérations cyber-militaires destructrices ne représentent que 2 % du volume total des incidents tout comme les techniques d'espionnage et sont principalement concentrées sur les organisations publiques ukrainiennes.

Figure 3 : Motivations des attaquants (Source Thales).

2 Les *ransomwares* ou ransongiciels sont des logiciels d'extorsion qui peuvent verrouiller votre ordinateur et demander une rançon en échange du déverrouillage de celui-ci.

3 Le *phishing* est une technique d'hameçonnage destinée à leurrer l'utilisateur pour l'inciter à communiquer des données.

4 Un *wiper* est un type de malware dont l'objectif est d'effacer les données du système infecté.

5 Un *infostealer* est un logiciel espion utilisé pour récupérer des informations dans un système.

Des « hacktivistes » de guerre aux techniques de cyberharcèlement

Sur l'ensemble des cyberattaques enregistrées dans le monde sur la période du conflit, 61 % sont issues de groupes d' « hacktivistes » pro-russes, aux premiers rangs desquels : Anonymous Russia, KillNet et Russian Hackers Teams. Ces groupes, apparus au cours du conflit, se sont organisés en miroir des efforts des « hacktivistes » ukrainiens de l'IT Army au début du conflit. Plus structurés, utilisant des ressources de la cybercriminalité organisée de type « *botnet-as-a-service* » [6] comme Passion Botnet, ils ont pour objectif de cyberharceler les pays occidentaux apportant leur soutien à l'Ukraine. Les « hacktivistes » sont donc la nouvelle composante du conflit. Ce sont des groupes civils indépendants, pouvant être assimilés à un groupe cybercriminel agissant selon des objectifs et des intérêts politiques précis, sans être directement sponsorisés par un Etat mais agissant en soutien par conviction. De toutes origines et de tous niveaux techniques, ils proviennent également d'horizons très variés.

L'écosystème des rancongiciels continue également d'évoluer et de croître avec des groupes criminels plus petits et plus agiles qui se forment pour échapper aux forces de l'ordre. De plus, les pirates élargissent leurs objectifs pour cibler les outils de collaboration d'entreprise tels que Slack, Teams, OneDrive et Google Drive en exploitant le *phishing*. Ces outils constituent une source importante de données sensibles, car la plupart des employés des entreprises continuent de télétravailler.

Malheureusement, on s'attend à ce que l'augmentation des cyberattaques ne fasse que croître. Avec des technologies d'IA telles que ChatGPT facilement accessibles au public, il est possible pour les pirates de générer des codes et des e-mails malveillants à un rythme plus rapide et plus automatisé.

Protéger les infrastructures critiques

Si les actes de cyberguerre ont encore lieu en Ukraine comme nous l'avons vu avec l'attaque ATK256 [7] contre plusieurs organismes publics ukrainiens à l'occasion de l'anniversaire du conflit (23 février 2023), ils sont noyés, aux yeux des Occidentaux, par un cyberharcèlement constant.

Les menaces à la cybersécurité dans l'Union européenne affectent des secteurs vitaux. Car à la lumière de cette latéralisation du conflit de l'Ukraine à l'Europe dans sa globalité, les attaques à court terme contre les infrastructures critiques doivent être considérées avec attention en Europe occidentale dans l'hypothèse d'une nouvelle accélération du conflit. Les trois secteurs les plus attaqués en 2022 sont l'éducation et la recherche, les administrations publiques et la santé (figure 4).

Les établissements d'enseignement sont devenus un terrain de prédilection pour les cybercriminels suite à la numérisation rapide qu'ils ont entreprise en réponse à la pandémie de COVID-19. En fait, le secteur de l'éducation et de la recherche est le premier secteur le plus attaqué au monde, avec une augmentation de 43 % en 2022 par rapport à 2021, et une moyenne de 2 314 attaques par entreprise chaque semaine.

En 2022, les entreprises du secteur de la santé en France ont subi en moyenne 644 cyberattaques hebdomadaires par entreprise, soit une augmentation de 191 % par rapport à 2021 (contre + 74 % dans le monde sur la même période pour une moyenne de 1463 attaques). C'est le 7ème secteur français le plus fréquemment attaqué et la plus forte augmentation de tous les secteurs observés en France, devant l'industrie manufacturière (+ 113 %) et les vendeurs de logiciels (+ 106 %).

Pour se protéger, il est impératif de penser d'abord à la prévention, et non à la détection. Il existe plusieurs bonnes pratiques

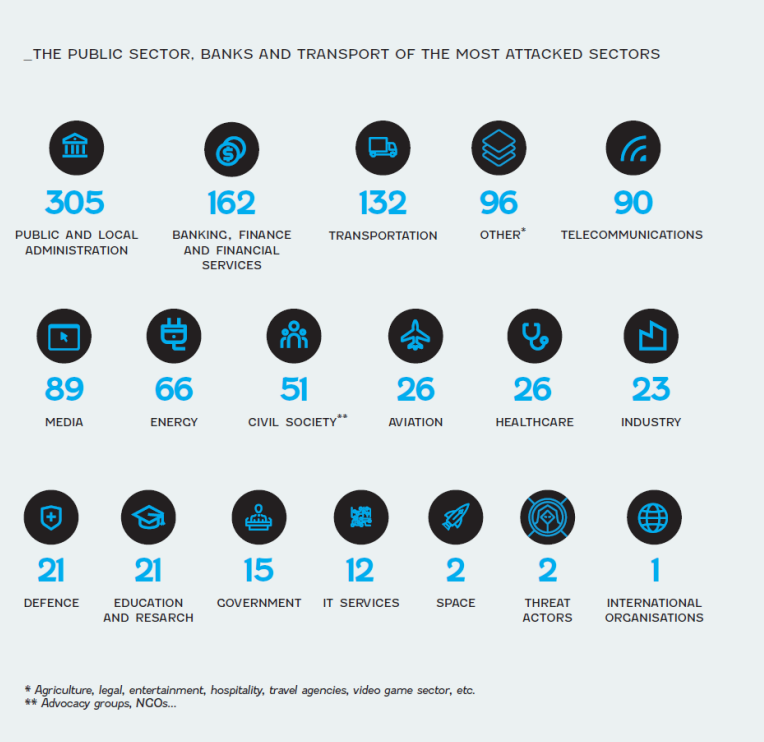

Figure 4 : Distribution des attaques 2022 par secteur d'activité (Source Thales).

6 *botnet-as-a-service* : Un *botnet* est un ensemble d'appareils connectés au Web, qu'il s'agisse de serveurs, PC, appareils mobiles ou de l'Internet des objets, tous infectés et contrôlés par un même programme malveillant.. En général, une machine intègre un *botnet* totalement à l'insu de son utilisateur. Ces appareils piratés peuvent être utilisés pour lancer des attaques par déni de service distribué, pour voler des données ou envoyer du spam, ou encore pour accéder à distance au réseau local de l'appareil.

7 ATK256 est une série d'attaques cyber qui a ciblé l'Ukraine et qui s'articule autour d'un binaire compilé en Python qui se fait passer pour un logiciel de traduction en ukrainien.

et mesures qu'une entreprise peut prendre pour minimiser son exposition à une nouvelle attaque ou brèche, telles que la formation à la cybersécurité, le maintien à jour des correctifs et la mise en œuvre d'une technologie anti-ransongiciel.

Vers une cyberguerre hybride de haute intensité s'étendant à toute l'Europe

La cyberguerre fait dorénavant partie de l'arsenal indispensable aux nouvelles techniques de guerre, c'est-à-dire la désinformation, la manipulation de l'opinion publique, la guerre économique, le sabotage, ou encore la guérilla.

La Russie considère l'information comme un espace de conflits à exploiter, et donc la cyberguerre constitue un outil idéal pour harceler ses ennemis. Certains observateurs ont affirmé que les « hacktivistes » étaient directement contrôlés par la Défense russe. Même s'il est difficile de le prouver, leurs actions créent un climat de suspicion et d'insécurité auprès des décideurs européens en déployant le conflit au-delà des frontières entre la Russie et l'Ukraine. Elles contribuent aux procédés russes de guerre informationnelle ayant pour but d'épuiser les organisations privées comme publiques dans les pays alliés de l'Ukraine. ■ **SD**

Nouvelle étude de la problématique de l'énergie des ordinateurs quantiques

Comme pour les ordinateurs classiques, le développement des ordinateurs quantiques va poser à terme des problèmes aigus de dissipation thermique ; il n'est pas trop tôt pour s'en préoccuper et de tenter de les quantifier.

Depuis les premiers ordinateurs les concepteurs et les utilisateurs de l'informatique en particulier les supercalculateurs sont de gros consommateurs d'énergie dont une partie importante est purement thermique. La chaleur est une conséquence inévitable du fonctionnement d'un processeur, une chaleur excessive risque d'entraver les performances des composants et limite les vitesses de calcul ce qui implique l'utilisation de systèmes de climatisation également consommateurs d'énergie.

Ce problème se pose aussi pour l'informatique quantique qui demeure encore au stade expérimental mais se développe rapidement si l'on en juge par le nombre croissant des qubits qui devrait atteindre le millier dans quelques années. La plupart des technologies de qubits des ordinateurs quantiques sont basées sur des qubits supraconducteurs or ce problème sera d'autant plus vif que ces appareils fonctionnent à des températures proches du zéro absolu (-273,14°C), avec des unités de calcul de

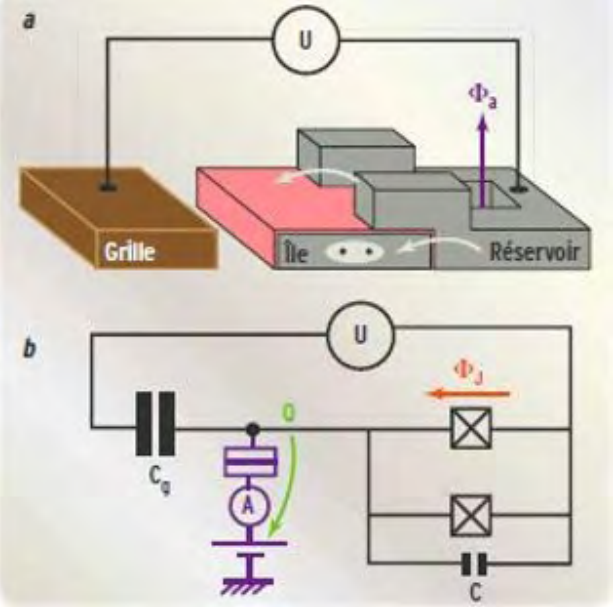

Figure 1 : Jonction Josephson et son schéma.

très petite taille, et qu'ils seront donc d'autant plus sensibles à la chaleur. Cet aspect souvent négligé par les recherches, a été étudié par Clemens Winkelmann, maître de conférences à Grenoble INP Phelma, UGA, et chercheur à l'Institut Néel, dans un article publié dans *Nature Physics*.

La supraconductivité est un état de la matière qui apparaît à des températures proches du zéro absolu et fait disparaître toute résistance. Les qubits supraconducteurs sont maintenus dans des jonctions Josephson (figure 1) qui réalisent un contact entre deux matériaux supraconducteurs. Lorsqu'un courant passe à l'intérieur d'un supraconducteur, il n'y a aucune perte, aucune dissipation d'énergie et dans cet état de la matière, les électrons ne se comportent plus comme des particules individuelles, mais comme un tout qui peut être décrit par une fonction d'onde unique dont la phase tourne quand un courant passe. Dans une jonction Josephson, il existe une différence de phase entre les deux supraconducteurs, laquelle est l'équivalent d'une tension en électronique classique. A la base du calcul quantique, il faut maintenir dans une superposition d'état les électrons tant que n'intervient pas de phénomène de décohérence. La manipulation du vecteur d'état superposé permet d'effectuer des calculs. La décohérence est un phénomène contextuel qui perturbe l'évolution de la phase du vecteur d'état. Clemens Winkelmann s'est demandé ce qui se passait quand intervient le phénomène de décohérence qui fausse le calcul quantique. Lorsque la cohérence est brisée, la dissipation apparaît, explique le chercheur qui s'est penché dans un article sur la mesure de la chaleur dégagée par un saut de phase dans une jonction Josephson. Le but de cet article est d'attirer l'attention de la communauté scientifique sur le fait que les ordinateurs quantiques vont dissiper de la chaleur, et que c'est un problème qu'il faut prendre en compte et évaluer . Avec son équipe, Clemens Winkelmann a ainsi réussi à quantifier ●●●

la chaleur dégagée lors d'une brève perte de cohérence au cours de laquelle le système est revenu à son état initiale Cette expérience a permis de quantifier au niveau élémentaire la dissipation d'énergie produit par une décohérence connue et devrait ainsi permettre de prévoir la perte d'énergie au niveau macroscopique des futurs ordinateurs quantiques.

La problématique de l'énergie nécessaire à l'exécution d'un algorithme quantique n'a pas fait l'objet de beaucoup d'études car les ordinateurs quantiques expérimentaux actuels traitent un nombre relativement faible de qubits. Face aux prévisions des constructeurs qui planifient à l'horizon 2030 des milliers de qubits ce problème devrait devenir crucial au regard des efforts actuels autour de la consommation numérique.

Gümüş, E., et al. «Calorimetry of a phase slip in a Josephson junction» Nature Physics (2023): 1-5. ■ **ML**

Le béryllium, un matériau stratégique méconnu

Le béryllium est un métal incontournable pour certaines applications. Même s'il représente un marché mondial de faible tonnage, il intervient dans la fabrication de nombreux dispositifs ce qui lui vaut de figurer dans la liste des matériaux stratégiques de nombreux Etats.

Figure 1 : Bloc de béryllium.

Le béryllium est un métal de la famille des alcalino-terreux, voisin du magnésium qui présente des propriétés physiques et chimiques très particulières. De masse atomique 4, il est très léger, possède une résistance mécanique élevée (6 fois plus résistant que l'aluminium), une bonne conductivité électrique et thermique, un faible coefficient d'absorption des rayons X et des neutrons ainsi qu'une bonne résistance à la corrosion.

Revers de la médaille c'est un produit toxique ainsi que tous les composés qui en sont dérivés, notamment son oxyde, le béryl, excellent isolant électrique, ce qui amène parfois à rechercher des produits de substitution. Une exposition à plus de 100 microgrammes de Be par m^3 peut en effet provoquer des pneumopathies graves, voire, à doses plus faibles mais répétées, des troubles pulmonaires chroniques (bérylliose).

Autre inconvénient, le prix de revient du béryllium qui est très élevé, il se négocie actuellement à plus de 500 $ le kilo.

Sans béryllium, pas de télescope James Web

Le lancement du télescope James Webb par la NASA qui a permis d'étendre considérablement le champ d'exploration de l'univers et les moyens d'investigation des astronomes et astrophysiciens du monde entier, a été l'occasion de focaliser l'attention sur le béryllium, un métal dont on parle peu bien qu'il soit classé dans les matériaux stratégiques. Dans le cas du télescope spatial, ce métal a été choisi pour confectionner les miroirs qui le composent car Il est à la fois extrêmement solide tout en étant très léger et surtout il conserve sa forme initiale même aux températures très basses rencontrées dans l'espace lointain. C'est une caractéristique essentielle car la sensibilité d'un télescope spatial tel que le James Webb est fortement dépendante de la surface réfléchissante de ses miroirs, et la stabilité en température du béryllium permet de capter la lumière des galaxies lointaines sans déformation sensible des miroirs. De l'avis des spécialistes de la NASA, sans le béryllium, le projet James Webb n'aurait pas pu voir le jour. [1]

Applications nucléaires

Une autre propriété du béryllium mise à profit est la grande section efficace de diffusion des neutrons de haute énergie (> 10 keV). Celui-ci peut agir comme un réflecteur ou un modérateur de neutrons dans les réacteurs nucléaires, ralen-

1 Le ministère américain de la défense qui utilise le béryllium dans ses systèmes d'armement et les satellites de surveillance a fait en sorte que la NASA puisse se procurer la quantité de béryllium nécessaire à la fabrication des miroirs. Ceci a été facilité par le fait que 65 % du béryllium mondial est originaire des Etats-Unis (Utah et Alaska).

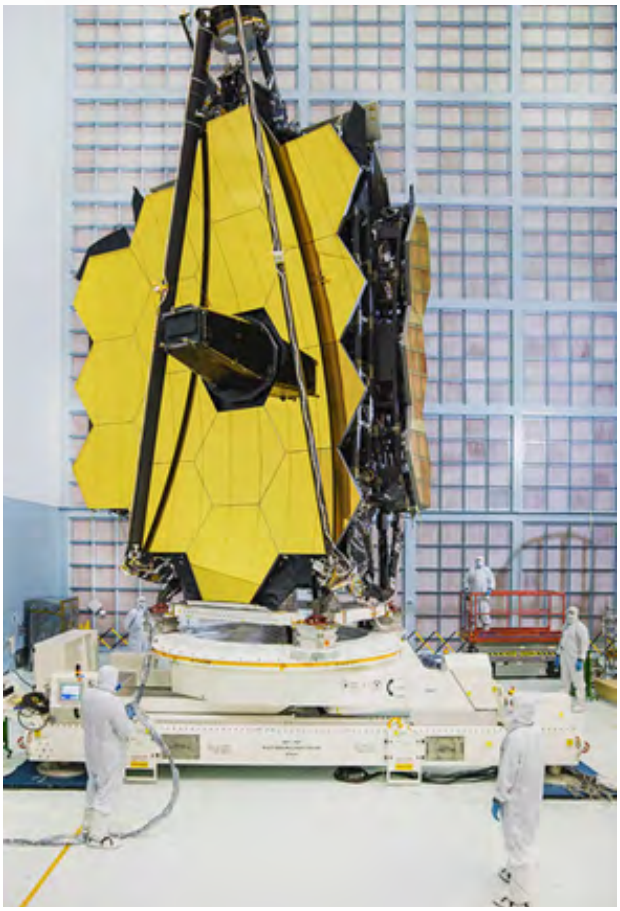

Figure 2 : Miroir primaire du télescope spatial James Webb de 6,5 m de diamètre (source NASA).

tissant efficacement les neutrons jusqu'à l'énergie thermique. C'est ainsi que les parois du réacteur ITER sont protégées par plusieurs tonnes de béryllium. Il sert également pour le gainage des combustibles nucléaires.

D'autre part, étant donné que le béryllium possède une énergie de seuil très faible pour l'émission de neutrons, il peut être utilisé comme source de neutrons dans les réacteurs nucléaires. Mélangé à un émetteur alpha, comme l'américium, il est utilisé comme source de neutrons à longue durée de vie (en fait celle de l'émetteur α utilisé) en exploitant la réaction :

$$^{4}_{2}\alpha + {}^{9}_{4}\mathrm{Be} \rightarrow n + {}^{12}_{6}\mathrm{C}$$

Le mélange doit être intime car les particules alpha électriquement chargées sont rapidement arrêtées dans la matière. Il est également possible de déclencher une source de neutrons à partir de rayons gamma de forte énergie selon la réaction suivante :

$$\gamma + {}^{9}_{4}\mathrm{Be} \rightarrow n + 2 * {}^{4}_{2}\alpha - 2,0\mathrm{MeV}$$

Comme la réaction est endothermique, l'énergie des neutrons produits est assez faible.

Autres applications

• Dans l'industrie spatiale ou de défense, en plus de son utilisation pour les miroirs de télescope spatial, déjà citée, le béryllium entre dans la composition des structures légères et rigides des étages supérieurs de lanceurs, de gyroscopes et de systèmes de guidage. Il s'avère souvent indispensable dans la conception de composants légers et résistants pour des éléments tels que satellites, missiles, avions, radars, etc.

• Dans l'instrumentation scientifique et technique, on l'emploie dans le secteur de la radiographie et de l'imagerie médicale, pour les fenêtres transparentes aux rayons X dans les tubes à rayons X et les instruments de spectroscopie.

• Dans le domaine médical, la création d'implants médicaux biocompatibles et amagnétiques pour l'orthopédie et la dentisterie où le béryllium est utilisé pour la fabrique d'alliages pour prothèses dentaires.

Dans les applications industrielles plus traditionnelles, on notera la fabrication d'alliages à base de le cuivre ou d'aluminium à faible teneur en béryllium (quelques %) pour améliorer de nombreuses propriétés comme la coulabilité, la capacité d'absorption calorifique, la dureté, l'élasticité et la résistance à la fatigue. Ces alliages sont utilisés pour réaliser des pièces de frottement, des ressorts, des outils anti-étincelles pour les poudreries, des moules pour matières plastiques, etc. Enfin, le cupro-béryllium notamment (à 2,6 % Be) est un alliage de choix pour la connectique utilisé dans les contacteurs et connecteurs électroniques. ■ **AB**

Vers les lunes glacées de Jupiter

Le dernier lancement par Ariane 5

Le 14 avril 2023 le tir réussi du dernier lanceur Ariane 5 emportait la mission européenne Juice (*JUpiter ICy moons Explorer*) vers Jupiter et ses satellites. Dans le futur, c'est la série des lanceurs Ariane 6 qui prendra la relève.

La mission JUICE sera la première mission spatiale à utiliser, au cours de son voyage vers Jupiter, une assistance gravitationnelle du couple Terre-Lune entier et à se placer en orbite autour d'une autre lune que celle de la Terre. Notons qu'ici le terme « lune » désigne un satellite naturel pour le différencier d'un satellite artificiel.

Juice présente de nombreux objectifs scientifiques clés, allant de l'exploration des trois grandes lunes océaniques de Jupiter à l'exploration de l'atmosphère complexe et de l'environnement magnétique de la planète. Juice contribuera à explorer l'histoire de notre voisine planétaire, révélant ses modes de formation, son évolution et la possibilité d'apparition de la vie quelque part dans le système de Jupiter. ●●●

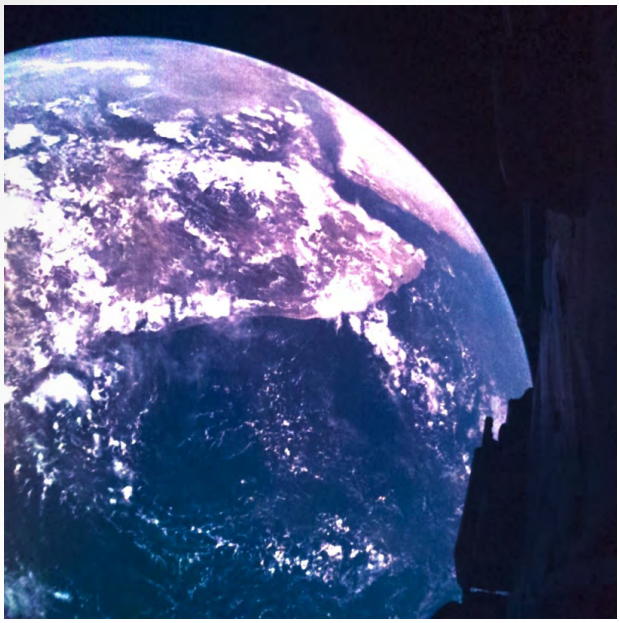

Figure 1 : Image de la terre prise par la plateforme Juice après son lancement. Crédits : ASA.

Une mission scientifique ambitieuse

L'objectif principal de Juice est la caractérisation des lunes de Jupiter à la fois comme des corps célestes et des habitats possibles pour la vie passée ou présente.

Au cours de son périple, Juice survolera Callisto, une lune composée à 50 % de glace. Elle survolera aussi Europa pour étudier les zones les plus actives de sa croûte glacée et identifier un site adapté à une future exploration *in situ*. Mais la mission principale reste Ganymède, une lune de 2 600 km de rayon. C'est la première fois qu'une sonde se mettra en orbite autour d'une lune de glace pour l'étudier en détails. Ganymède possède un océan qui est pris en sandwich entre 2 couches de glaces, tout comme Callisto, Titan, et vraisemblablement les planètes océans. De plus, elle est la seule lune glacée à posséder un champ magnétique propre. Juice étudiera leurs réservoirs océaniques cachés, cartographiera leurs coquilles glacées et étudiera leurs sous-sol. Bien que leurs océans soient d'un intérêt clé pour Juice, chaque lune est également intéressante individuellement : Callisto est un monde ancien représentatif du système Jupiter primitif, Europe semble avoir une surface jeune et active qui évacue l'eau dans l'espace, et Ganymède, la plus grande lune du système solaire, présente des caractéristiques uniques. Ganymède, principale cible scientifique de Juice, présente un large éventail d'âges et de caractéristiques de surface, fournissant une caractéristique géologique recouvrant plusieurs milliards d'années. Ce satellite entretient une relation complexe et unique avec l'environnement spatial autour de sa planète mère et présente à la fois un océan souterrain et une dynamo magnétique active. Seuls deux autres corps solides du système solaire engendrent un champ magnétique comme celui de Ganymède et tous deux sont des planètes : Mercure et la Terre dont l'une abrite la vie.

De nombreuses géantes gazeuses sont connues pour orbiter autour d'autres étoiles. Jupiter est la plus grande des géantes gazeuses du système solaire et est bien placée pour agir comme modèle pour d'autres systèmes de ce type dans l'Univers. Jupiter a un environnement spatial extrêmement complexe, avec l'atmosphère de la planète, le magnétisme, les lunes et les anneaux poussiéreux qui interagissent tous les uns avec les autres. En caractérisant et en explorant comment tous ces composants fonctionnent ensemble, Juice nous aidera à comprendre non seulement à quoi ressemblent les systèmes géants gazeux, mais aussi comment des lieux habitables pourraient apparaître ailleurs dans des systèmes semblables à Jupiter.

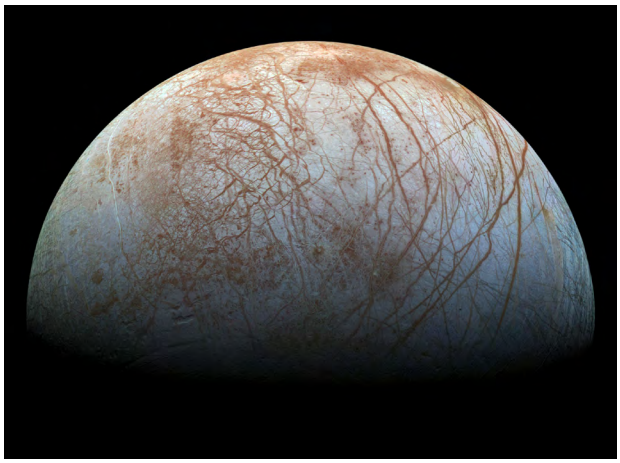

Figure 2 : Image de Europa montrant les traces d'eau glacée. Crédits : NASA.

Des instruments scientifiques en nombre

Juice transporte le plus puissant système de télédétection géophysique jamais transporté vers le système solaire externe. Il comprend dix instruments scientifiques dédiés, un moniteur de rayonnement et un interféromètre radio planétaire.

3GM (*Gravity & Geophysics of Jupiter and Galilean Moons*) étudiera le champ de gravité de Ganymède, l'étendue des océans internes sur les lunes glacées et la structure des atmosphères de Jupiter et de ses lunes.

GALA, l'altimètre laser étudiera la déformation des marées de Ganymède et la topographie des surfaces des lunes glacées.

JANUS, un système de caméras optiques, étudiera les caractéristiques sur les lunes, ainsi que les nuages de Jupiter.

J-MAG est un magnétomètre. Il est équipé de capteurs pour caractériser le champ magnétique jovien et son interaction avec celui de Ganymède. Il mesurera les océans souterrains des lunes glacées.

MAJIS est un spectromètre imageur. Il observera les caractéristiques des nuages et les constituants atmosphériques sur Jupiter, il caractérisera les glaces et les minéraux sur les surfaces glacées des lunes.

PEP et RPWI comprend un ensemble de capteurs pour caractériser le plasma du système Jupiter et les lunes glacées.

RIME est un radar capable de pénétrer dans la glace pour étudier la structure souterraine des lunes glacées jusqu'à une profondeur d'environ neuf kilomètres.

SWI étudiera la structure, la composition et la dynamique des températures, ainsi que les exosphères et les surfaces des lunes glacées.

UVS est un spectrographe imageur UV pour caractériser la composition et la dynamique des exosphères des lunes glacées, étudier les aurores boréales joviennes et étudier la composition et la structure de la haute atmosphère de la planète.

RADEM est un moniteur de rayonnement qui mesurera la quantité de rayonnement à laquelle Juice est exposé, tout en étant utilisé pour la science.

PRIDE utilisera le système de télécommunication standard de Juice, ainsi que des radiotélescopes sur Terre pour effectuer des mesures précises de la position et de la vitesse de l'engin spatial afin d'étudier les champs de gravité de Jupiter et des lunes glacées.

Une ultime manœuvre avant de quitter la terre

Deux semaines après le lancement de sa mission d'exploration l'ESA annonçait que l'antenne radar RIME n'était pas encore déployée comme prévu. Cet instrument, l'un des 10 embarqués sur le satellite, a été conçu pour étudier la structure de la surface et du sous-sol jusqu'à 9 km de profondeur des lunes glacées de Jupiter. Son déploiement était une condition indispensable au bon déroulement de la mission. Pour tenter de déplacer la goupille qui empêchait le déploiement du bras, les équipes de l'ESA au centre de contrôle de la mission à Darmstadt ont décidé d'impulser une secousse à la plateforme en mettant en marche ses propulseurs. Une seconde manœuvre a consisté à réchauffer cette partie en la plaçant face vers le soleil par une série de rotations. C'est au bout de 2 semaines que le bras de RIME a finalement été réveillé en sursaut lorsque l'équipe de contrôle du vol a actionné un dispositif mécanique, appelé « actionneur non explosif », situé dans le support bloqué. Ce dispositif a produit un choc qui a déplacé la goupille de quelques millimètres et a permis à l'antenne de se déployer. Cet épisode démontre la possibilité de traiter quelques dysfonctionnements par des manœuvres adaptées.

Figure 3 : La sonde Juice avec ses panneaux solaires déployés. Crédits : ESA.

Une forte participation française

Décidée en 2012, Juice est la mission phare du programme Cosmic Vision de l'ESA, avec un budget de plus d'un milliard d'euros. Cette mission réunit une quinzaine de pays européens, en plus des Etats-Unis, du Japon et d'Israël. La France a contribué au développement de six instruments de pointe parmi les dix à bord de la sonde. Cette contribution, pilotée par le CNES, a impliqué neuf laboratoires français du CNRS. De la même manière, six autres laboratoires les ont rejoints pour, dès à présent, anticiper et participer aux prochaines étapes de la mission : la calibration en vol des instruments et l'exploitation des données scientifiques.

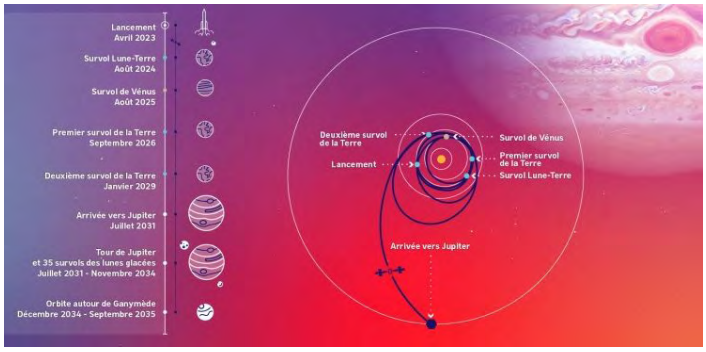

Figure 4 : Déroulement du voyage de la sonde Juice vers Jupiter. Crédits : CNES.

Une assistance gravitationnelle pour un long voyage

Après de multiples assistances gravitationnelles de Vénus et de la Terre, Juice arrivera vers Jupiter en juillet 2031. L'insertion en orbite autour de Jupiter sera le début d'une phase d'étude du système jovien comportant la planète Jupiter, sa magnétosphère et deux satellites Europe et Callisto. Cette investigation durera deux années et demie. Suivra une phase de huit mois en orbite autour de Ganymède, où des phases en orbites elliptiques et circulaires d'observations scientifiques sont programmées afin de répondre à tous les objectifs de la mission.

Rendez-vous en 2031. ■ **AD**