

# Renseignor

le Renseignement ouvert par la radio

N°1309 le 3 décembre 2023

Dans ce numéro

**Au moins quarante civils tués lors d'une attaque d'envergure menée par des membres présumés du GSIM dans le nord du Burkina Faso...**

(Page 2)

**Aux États-Unis, un ressortissant indien accusé d'avoir participé à un complot visant à assassiner un Américain...**

(Page 3)

**Dans l'Extrême-Orient russe, le sabotage de deux trains transportant du carburant revendiqué par l'Ukraine...**

(Page 4)

**L'Iran serait en passe d'acquérir des avions de combat et des hélicoptères d'attaque russes...**

(Page 6)

**Des hackers auraient accédé au système informatique de l'Agence japonaise d'exploration aérospatiale...**

(Page 7)

## FORMULATION DES ARTICLES

Les textes sont des relevés d'écoute radio ; la formulation est donc celle du média cité.

Nous ne corrigeons que quelques fautes mineures de langue française. Les titres, par contre, sont de la rédaction.

## Intensification notable des cyberattaques chinoises visant Taïwan...

Kate Morgan, ingénieure du Groupe d'analyse des menaces de *Google*, vient d'indiquer au journal *Bloomberg* que la Chine avait considérablement intensifié ses cyberattaques visant Taïwan au cours des six derniers mois. Selon ce groupe chargé de surveiller les activités des hackers financés par le gouvernement, ces attaques visent aussi bien le secteur public que le secteur privé de Taïwan, comprenant les organismes relevant de la défense. *Google* a précisé que les hackers chinois déployaient des tactiques difficilement traçables comme le fait de s'introduire dans les routeurs internet des particuliers et des bureaux pour les réutiliser en menant des attaques tout en masquant leur véritable origine. Kate Morgan a dévoilé cette information lors d'une intervention à Malaga et a ajouté que *Google* avait tracé plus d'une centaine d'organisations en Chine tentant de pirater des entreprises technologiques ou des clients sur le *Cloud*.

(*Radio Taïwan international*, le 01-12-2023)

## En 2023, au moins trente personnes auraient été tuées lors d'attaques terroristes au Togo...

Le Togo a enregistré plus de trente morts, vingt-neuf blessés et trois disparus lors d'attaques qualifiées de terroristes en 2023, a déclaré hier soir à la télévision d'État Yawa Kouigan, ministre de la Communication et porte-parole du gouvernement. Les régions septentrionales du Bénin, du Togo et du Ghana font face à des attaques et des incursions de groupes djihadistes venant du Sahel et cherchant à étendre leur influence vers le sud.

(*La voix de l'Amérique*, le 28-11-2023)

## Tentative d'arraisonnement d'un pétrolier libérien en mer Rouge...

Selon des informations recueillies par la *NHK*, les Forces maritimes d'autodéfense du Japon (MSDF) ont réagi au détournement d'un pétrolier au large du Yémen, dimanche dernier. Des sources proches du ministère de la Défense indiquent que le destroyer *Akebono* et un avion de patrouille P3C des MSDF se sont rendus sur les lieux de l'incident dans le golfe d'Aden pour recueillir et transmettre des informations à l'armée américaine notamment. Le pétrolier *Central Park*, battant pavillon libérien et géré par une société britannique, a été saisi par des assaillants dimanche, puis relâché. Selon les mêmes sources, aucun membre des Forces maritimes d'autodéfense n'a été blessé. Elles ont également indiqué qu'aucune arme n'avait été utilisée. En vertu de la loi japonaise contre la piraterie, les membres des MSDF sont autorisés à tirer des coups de semonce. Le ministère japonais de la Défense est en état d'alerte dans le golfe d'Aden depuis qu'un groupe de rebelles houthis du Yémen s'est emparé d'un cargo exploité par une entreprise japonaise en mer Rouge, le 19 novembre dernier.

(*Radio Japon international*, le 27-11-2023)

## ... TERRORISME ...

### **Une cinquantaine de djihadistes présumés tués par l'explosion d'une mine dans le nord-est du Nigeria...**

Une cinquantaine de djihadistes affiliés à l'État islamique ont été tués dans l'explosion d'une mine anti-véhicule dans la région du lac Tchad dans le nord-est du Nigeria selon des chefs de milices antidjihadistes soutenant l'armée nigériane dans la lutte contre les terroristes. Les combattants planifiaient une attaque lorsque l'incident s'est produit, a déclaré un autre milicien, confirmant le même bilan.

*(La voix de l'Amérique, le 28-11-2023)*

### **Au moins quarante civils tués lors d'une attaque d'envergure menée par des membres présumés du GSIM dans le nord du Burkina Faso...**

Une attaque djihadiste massive contre une base militaire, dimanche, à Djibo, dans le nord du Burkina Faso, a coûté la vie à au moins quarante civils selon l'armée. Un habitant de Djibo a fait état sur *VOA Afrique* d'assaillants venus massivement à bord de motos et véhicules pickups. Ils ont effectué des tirs sur les civils, ont égorgé des personnes, incendié des maisons et des magasins. Le Haut commissariat de l'ONU aux droits de l'Homme se dit atterré. Selon l'ONU, un grand nombre de combattants du Groupe de soutien à l'islam et aux musulmans a attaqué une base militaire, des maisons et des camps de déplacés dans la ville de Djibo, tuant au moins quarante civils et faisant plus de quarante-deux blessés. Selon une source sécuritaire, l'attaque a débuté vers 15 heures dimanche et a été menée par plusieurs centaines d'hommes armés qui ont tenté en vain de pénétrer dans la base. L'attaque a été menée par plusieurs vagues pendant plus de trois heures. Selon l'agence d'information du Burkina Faso, plus de 400 terroristes ont été décimés dans la contre-offensive de l'armée contre près de 3 000 criminels qui ont tenté de s'emparer de Djibo.

*(La voix de l'Amérique, le 29-11-2023)*

### **En Allemagne, le risque d'attentat islamiste n'a jamais été aussi élevé selon les services de renseignement...**

En Allemagne, le conflit entre Israël et le Hamas continue d'avoir des conséquences sur la société, notamment la sécurité. Le service de renseignement intérieur allemand a assuré que le risque d'attentat islamiste dans le pays, en raison de la guerre entre Israël et le Hamas, était réel et qu'il n'avait pas été aussi élevé depuis longtemps. Cette mise en garde publique démontre l'inquiétude des autorités qui craignent des projets d'attaques potentiels contre la sécurité des juifs, des institutions israéliennes, mais aussi des grands événements publics dans le pays.

*(Deutsche Welle, le 30-11-2023)*

## ... ACTIVITÉS DES SERVICES DE RENSEIGNEMENT ...

### **Dix militaires taïwanais inculpés pour divulgation à la Chine d'informations classifiées...**

Le bureau du procureur général de la haute cour de justice a terminé aujourd'hui l'enquête sur une affaire de sécurité nationale et a inculpé dix militaires en service ou retraités impliqués dans la réalisation d'une vidéo de guerre psychologique et dans la divulgation des secrets de défense. Le bureau avait ordonné d'enquêter sur des personnes soupçonnées d'avoir été recrutées par les services de renseignement chinois depuis 2021, puis soudoyé des militaires en fonction et retraités. Fin juillet, les enquêteurs ont mené un certain nombre de perquisitions, y compris à la 601e brigade d'aviation de Longtan (Taoyuan) où un lieutenant-colonel est soupçonné d'avoir divulgué des secrets de défense nationale à des forces chinoises. Le parquet supérieur de Taïwan a souligné que deux militaires en service avaient été incités à accepter des pots-de-vin pour réaliser une vidéo de guerre psychologique intitulée « Je suis prêt à me rendre à l'Armée populaire de libération », qui a été remise au Parti communiste chinois, en échange d'un paiement. Cela représente une violation grave de l'obligation de loyauté envers l'armée nationale, et le bureau du procureur a recommandé la peine la plus lourde, à savoir l'emprisonnement à perpétuité.

*(Radio Taïwan international, le 27-11-2023)*

### **Le Mossad se serait engagé à ne pas commettre d'assassinats ciblés au Qatar...**

Le fait qu'aucun des acteurs de ce conflit n'ait opposé de réserves à la prolongation de la trêve pose question. La réponse pourrait se trouver dans les garanties récemment apportées par le Mossad au

négociateur qatari. Les services secrets israéliens, dont la traque des leaders exilés du Hamas risque d'entraîner des éliminations ciblées en Turquie, en Syrie et en Iran, auraient fait pression sur les autorités du Qatar où résident deux des plus éminents gazaouis, Khaled Mechaal et Ismaïl Haniyeh. En échange d'une attitude qatarie plus dure avec le Hamas, Israël s'est engagé à prolonger la trêve et à ne pas commettre d'assassinats sur le sol de la pétromonarchie, épargnant à celle-ci des sérieux troubles qui en résulteraient. Des accords arrachés à la force du poignet donc, et qui peuvent à terme mettre en danger les civils palestiniens et les 180 otages restant à Gaza.

*(Radio Vatican, le 28-11-2023)*

### **Le directeur du Mossad au Qatar pour discuter de la libération d'otages...**

Pour la troisième fois depuis le début de la guerre le 7 octobre, le chef du Mossad David Barnea, s'est envolé mardi pour le Qatar afin de discuter de la libération d'otages supplémentaires. 166 otages dont 9 enfants sont encore détenus à Gaza depuis maintenant 53 jours. Depuis 4 jours, grâce à un accord de trêve entre Israël et le Hamas, une cinquantaine d'otages ont pu être libérés en échange de prisonniers palestiniens et d'un cessez-le-feu des combats à Gaza. David Barnea est attendu à Doha pour une réunion tripartite avec le chef de la CIA, Bill Burns, et le Premier ministre du Qatar, Mohammed bin Abdulrahman bin Jassim Al Thani, concernant la guerre à Gaza, ont indiqué des sources à Washington. Cette visite intervient un jour après qu'Israël et le Hamas sont parvenus à un accord négocié par le Qatar et l'Égypte pour prolonger la trêve de deux jours et permettre la libération de 20 otages supplémentaires. Ces dernières semaines, le chef de la CIA, Bill Burns, a joué un rôle crucial dans les négociations, aux côtés du chef du Mossad David Barnea et du Premier ministre qatari. Les responsables israéliens ont déclaré que Burns était également en contact étroit avec le chef des services de renseignement égyptiens Abbas Kamel, en particulier samedi, lorsque l'on craignait que l'accord sur les otages ne soit annulé après que le Hamas a annoncé qu'il retardait la libération des otages au motif qu'Israël n'avait pas respecté ses engagements.

*(I24News, le 28-11-2023)*

### **Aux États-Unis, un ressortissant indien accusé d'avoir participé à un complot visant à assassiner un Américain...**

Le département de la Justice des États-Unis (DOJ) a dévoilé mercredi un acte d'accusation contre Nikhil Gupta, un ressortissant indien, pour sa participation présumée à un complot déjoué visant à assassiner un citoyen américain à New York qui a publiquement plaidé en faveur de la création d'un État souverain pour les sikhs. L'acte révèle plusieurs informations selon lesquelles des assassinats étaient aussi prévus en sol canadien. Dans un communiqué, le DOJ affirme qu'en mai 2023 ou aux alentours de cette date, un employé du gouvernement indien, qui n'est pas nommé, aurait recruté Nikhil Gupta pour orchestrer l'assassinat de la personne visée aux États-Unis. Sur les instructions de l'employé gouvernemental, Nikhil Gupta aurait contacté un individu qu'il croyait être un criminel afin d'obtenir de l'aide pour engager un tueur à gages pour assassiner la victime à New York. L'individu était en fait une source confidentielle travaillant avec l'Agence antidrogue américaine (DEA) selon le DOJ. Après avoir fourni des informations personnelles et des photographies de surveillance de la personne visée à l'agent infiltré, Nikhil Gupta lui aurait demandé de commettre le meurtre dès que possible, poursuit le DOJ. Il lui aurait toutefois donné pour instruction spécifique de ne pas commettre le meurtre à l'époque où des rencontres étaient prévues entre des représentants des gouvernements américain et indien. Cette période semble coïncider avec la visite du Premier ministre indien, Narendra Modi, à Washington en juin 2023. Le 18 juin, Hardeep Singh Nijjar, le président d'un temple sikh de Surrey, en banlieue de Vancouver, en Colombie-Britannique, a été tué par balles dans le parking du bâtiment.

*(Radio Canada international, le 30-11-2023)*

### **Sanctions américaines à l'encontre d'un groupe de hackers affilié aux services de renseignement nord-coréens...**

Aux États-Unis, le département du Trésor a annoncé hier qu'il avait ajouté l'organisation de hackers *Kimsuky* et huit ressortissants nord-coréens sur la liste des personnes et institutions faisant l'objet de sanctions. Il a indiqué qu'il s'agissait d'une réponse au lancement par Pyongyang d'un satellite militaire le 21 novembre dernier. *Kimsuky* est une organisation de hackers affiliée à la troisième direction du Bureau général nord-coréen de reconnaissance. En avril, le comité des sanctions du Conseil de sécurité des Nations unies avait affirmé dans un rapport que cet organisme ciblait les secteurs militaire, énergétique et des infrastructures, notamment dans le but de pirater des informations classées

confidentielles. En Corée du Sud, *Kimsuky* avait tenté de voler des informations en attaquant les boîtes mail de près de 400 citoyens, dont un ancien ministre et une cinquantaine d'experts des secteurs public et privé. Cependant, la police a précisé qu'aucune information confidentielle n'avait été divulguée. Séoul l'avait déjà désigné comme cible des sanctions unilatérales en juin dernier. En plus de cet organisme nord-coréen, huit individus inscrits sur la liste des personnes sanctionnées par Washington sont liés à des entreprises d'exportation d'armes et des sociétés écran nord-coréennes. Hier, le secrétaire d'État américain, Antony Blinken, a annoncé que les États-Unis, la Corée du Sud, le Japon et l'Australie imposeraient des sanctions à l'encontre de personnes en relation avec le royaume ermite, en réponse à son dernier lancement de satellite de reconnaissance militaire. D'après lui, c'est la première fois que ces quatre pays se coordonnent et rendent publiques des mesures de sanctions collectives contre le régime de Kim Jong-un. Les USA ont également maintenu, selon leur rapport annuel 2022, leur classement de la Corée du Nord dans la catégorie soutenant le terrorisme.  
(KBS World Radio, le 01-12-2023)

### **Dans l'Extrême-Orient russe, le sabotage de deux trains transportant du carburant revendiqué par l'Ukraine...**

Jamais l'armée ukrainienne n'a revendiqué une attaque en Russie aussi loin de sa frontière. Les services secrets ukrainiens auraient mené deux opérations de sabotage sur des trains transportant du carburant en Bouriatie, dans l'Extrême-Orient russe, à des milliers de kilomètres du front. Des engins explosifs auraient détonné au passage de ces trains. C'est une source au sein des forces de l'ordre ukrainiennes qui l'affirme, la Russie, elle, évoque simplement des incendies.  
(Deutsche Welle, le 01-12-2023)

## **... MILITAIRE ...**

### **Les affrontements en cours dans le nord du Myanmar inquiètent la Chine...**

L'armée du Myanmar semble perdre du terrain un mois après qu'elle a été la cible d'attaques de militants de minorités ethniques. Les attaques ont débuté le 27 octobre dans l'État shan, dans l'est du pays. Les militants ont pris le contrôle de plusieurs villes et postes militaires près de la frontière entre le Myanmar et la Chine. L'armée du Myanmar a pris le pouvoir lors d'un coup d'État en 2021. Selon les médias officiels, 120 camions transportant des marchandises en provenance de Chine auraient été vus en feu jeudi après avoir été attaqués par des drones du groupe de militants. Deux jours plus tard, Pékin a annoncé avoir entamé des exercices basés en partie sur un scénario de fermeture de la frontière entre les deux pays. Les forces pro-démocratie prêtent actuellement main forte aux militants ethniques dans l'espoir de prolonger les combats. Des centaines de militaires se sont rendus. Nakanishi Yoshihiro, professeur agrégé à l'université de Kyoto, affirme qu'il a souvent été difficile pour les minorités ethniques et les forces pro-démocratie de coordonner leurs opérations. Cependant, cette fois, elles ont uni leurs forces pour lancer des offensives contre l'armée. Selon lui, l'armée se trouve dans une situation difficile et peine à riposter. Elle semble perdre petit à petit ses zones de contrôle.  
(Radio Japon international, le 27-11-2023)

### **Premières patrouilles conjointes australo-philippines en mer de Chine méridionale...**

L'armée philippine a annoncé ses premières opérations conjointes de patrouille maritime et aérienne avec l'Australie, en mer de Chine méridionale. Cette initiative est considérée comme une tentative visant à maintenir Pékin sous contrôle, la Chine s'affirmant de plus en plus dans le domaine maritime. Les forces armées philippines ont annoncé dimanche que la première activité de coopération maritime avait débuté dans la zone économique exclusive du pays. Les exercices se poursuivront pendant trois jours jusqu'à lundi. Quatre navires et cinq avions philippins y participent, ainsi qu'une frégate et un avion de reconnaissance australiens. Selon un haut responsable militaire philippin, ils ont été suivis par un navire chinois lors d'une patrouille maritime samedi. Il a également indiqué que deux avions de chasse chinois avaient volé à proximité d'un avion philippin participant à l'exercice dimanche matin. Il a ajouté qu'il n'y avait pas eu d'approche dangereuse ni d'avertissement radio de la part de Pékin. Les Philippines et l'Australie ont signé un partenariat stratégique en septembre. Actuellement, Manille et Canberra renforcent leur coopération en matière de sécurité. L'armée philippine a effectué la semaine dernière des manœuvres conjointes de trois jours avec l'armée américaine, notamment en mer de Chine méridionale.  
(Radio Japon international, le 27-11-2023)

### **Remise en service des postes de garde nord-coréens dans la zone démilitarisée...**

La Corée du Nord restaure actuellement des postes de garde (GP) dans la zone démilitarisée, la DMZ, après avoir annoncé la rupture de l'accord militaire du 19 septembre 2018. Les quatre images rendues aujourd'hui publiques par les autorités militaires sud-coréennes montrent des soldats nord-coréens transporter des équipements et monter la garde. Rappelons que Pyongyang avait détruit onze GP selon le texte signé en 2018. Séoul a également révélé que le régime nord-coréen réinstallait des batteries d'artillerie côtière, alors qu'il n'en avait jusqu'aujourd'hui laissé qu'une ou deux ouvertes dans une région. L'armée sud-coréenne a déclaré qu'elle se concentrerait sur les mouvements des soldats nord-coréens dans les zones frontalières.

*(KBS World Radio, le 27-11-2023)*

### **Nouvelles manœuvres navales conjointes entre les marines sud-coréenne, japonaise et américaine...**

Séoul, Washington et Tokyo ont effectué hier un entraînement maritime au sud-est de l'île de Jeju. L'armée navale sud-coréenne a mobilisé le navire *Sejong le Grand*. La marine américaine a dépêché, de son côté, le porte-avions *Carl Vinson*, le destroyer lance-missiles *Sterett* et un de classe *Fletcher Kidd*. Quant au Japon, le *Kirisame*, le quatrième des destroyers de classe *Murasame*, a participé à l'exercice. Kim Seong-pil, le capitaine du navire sud-coréen, a déclaré que, si les trois nations établissaient des plans d'entraînement tripartite et les élargissaient, elles pourraient mieux réagir aux menaces nord-coréennes.

*(KBS World Radio, le 27-11-2023)*

### **En 2024, la République tchèque va poursuivre la formation de militaires ukrainiens...**

Les députés ont voté mardi pour la poursuite de la formation des soldats ukrainiens en Tchéquie l'année prochaine. Les députés de la coalition gouvernementale et ceux du parti d'opposition ANO ont validé le texte. La Chambre basse a également accepté de prolonger la plupart des missions des soldats tchèques à l'étranger, comme le proposait le gouvernement. Le Sénat a déjà donné son accord il y a trois semaines. Selon la ministre tchèque de la Défense, Jana Cernochova, quelque 3 500 soldats ukrainiens ont déjà été formés sur le territoire tchèque à ce jour et 500 autres ont été formés par des instructeurs tchèques en Pologne. S'adressant aux membres de la Chambre des députés, la ministre a déclaré que ces missions renforceraient la position de la Tchéquie en tant qu'allié et partenaire responsable.

*(Radio Prague international, le 29-11-2023)*

### **Plus de deux millions d'euros versés par la République tchèque au fonds d'affectation spéciale de l'OTAN...**

La Tchéquie va verser jusqu'à 2,5 millions d'euros au fonds d'affectation spéciale de l'OTAN destiné à l'assistance non militaire à l'Ukraine. Une décision approuvée mercredi par le gouvernement. Selon le ministère des Affaires étrangères, celle-ci reflète la nécessité de redoubler d'efforts pour maintenir le soutien à l'Ukraine parmi les priorités de la communauté euro-atlantique. Ce fonds d'affectation spéciale de l'OTAN fonctionne depuis 2016 et est un instrument d'assistance non militaire à l'Ukraine. Il couvre des éléments tels que le carburant, le matériel médical, la nourriture, les vêtements d'hiver et les systèmes de défense par drone, a encore précisé la diplomatie tchèque.

*(Radio Prague international, le 30-11-2023)*

### **En Roumanie, déploiement de quatre F-16 turcs en vue de renforcer la surveillance aérienne au profit de l'OTAN...**

Quatre avions F-16 de l'armée de l'air turque ont atterri en Roumanie pour effectuer des missions de surveillance aérienne renforcée sous le commandement de l'OTAN a annoncé jeudi le ministère roumain de la Défense. Les missions de police aérienne réalisées conjointement contribuent au développement de la capacité de réaction et de dissuasion, ainsi qu'à la consolidation de l'interopérabilité entre l'armée de l'air roumaine et l'armée de l'air turque, a indiqué la source citée.

*(Radio Roumanie international, le 30-11-2023)*

### **Participation bulgare à l'exercice de l'OTAN Cyber coalition 2023...**

La Bulgarie prend part à la 15e édition de l'exercice de l'OTAN en matière de cybersécurité *Cyber Coalition 2023*. 1 000 agents de trente structures de l'OTAN, l'UE et des pays membres prennent part à

cette opération. « Ce genre d'exercice est très utile pour renforcer l'interaction et permettre de réagir de manière rapide et plus adéquate aux défis de la cybercriminalité. Nous comptons sur nos partenaires, grâce à la mise en place de mécanismes efficaces d'échange et de coopération » a indiqué le ministre de la Défense, Todor Tagarev, qui a salué les participants bulgares à l'exercice *Cyber Coalition 2023*, qui travaillent à l'Institut de défense Tsvétan Lazarov. La Bulgarie participe pour la onzième fois à cet exercice.

(Radio Bulgarie, le 01-12-2023)

### **Mise en orbite réussie du premier satellite de reconnaissance militaire sud-coréen...**

La Corée du Sud célèbre aujourd'hui le lancement réussi de son tout premier satellite de reconnaissance militaire, marquant une avancée significative dans ses capacités de surveillance et de reconnaissance. Le satellite a été propulsé dans l'espace par le lanceur *Falcon 9* de SpaceX, décollant de la base spatiale de Vandenberg aux États-Unis à 3h19, heure de Séoul, le 2 décembre. Le ministère de la Défense et la société aérospatiale américaine ont confirmé le succès du lancement, soulignant que le satellite sud-coréen a établi avec succès sa première communication avec une station au sol étrangère à 4h37. Cette étape cruciale a eu lieu 78 minutes après son décollage ; 2 minutes 22 après le lancement, la première partie du propulseur a été détachée et 20 secondes plus tard la couverture de protection a été enlevée. Le premier satellite de reconnaissance sud-coréen se trouve actuellement en orbite basse autour de la Terre, à une altitude de 400 à 600 km. Il est équipé de caméras d'imagerie électro-optique (EO) et infrarouge (IR), offrant une résolution vidéo exceptionnelle de 0,3 m. Cette précision permet au satellite d'identifier des objets mesurant jusqu'à 30 cm au-dessus du sol. Les autorités militaires sud-coréennes prévoient de procéder à des tests d'essai approfondis et à une évaluation minutieuse au cours des quatre à six prochains mois avant de rendre l'engin opérationnel au premier semestre de l'année prochaine. Ces tests incluront la vérification de l'état de fonctionnement, des travaux de focalisation des images et une évaluation de la qualité des images capturées par le satellite. Le ministère de la Défense a souligné la résolution et le bon fonctionnement simultané de l'EO et de l'IR de ces satellites de reconnaissance, positionnant la Corée du Sud parmi les cinq meilleures nations au monde en termes de performances. Les capacités de surveillance spatiale nouvellement renforcées joueront un rôle central dans le système à trois axes de la Corée du Sud, composé de *Kill Chain*, de défense antimissile (KAMD) et de sanctions et représailles massives (KMPPR). Quant à l'avenir, la Corée du Sud a le plan ambitieux de lancer de manière séquentielle quatre satellites de reconnaissance supplémentaires d'ici 2025, en totalisant ainsi cinq en tout. Ces lancements sont prévus à bord du *Falcon 9* de SpaceX, en raison de son coût relativement bas et de son taux de réussite impressionnant de 99,2%. L'objectif ultime de cette initiative est de permettre une surveillance et une reconnaissance régulières de points spécifiques en Corée du Nord toutes les deux heures, renforçant ainsi les capacités de détection rapide des signes de provocations nucléaires et balistiques de cette dernière. Ce développement souligne l'engagement continu de la Corée du Sud à renforcer ses capacités de sécurité nationale dans une région géopolitique complexe.

(KBS World Radio, le 02-12-2023)

## **... L'ACTUALITÉ DES MARCHANDS D'ARMES ...**

### **L'Iran serait en passe d'acquérir des avions de combat et des hélicoptères d'attaque russes...**

Les forces armées iraniennes ont finalisé les arrangements pour la livraison d'un certain nombre d'avions avancés de fabrication russe, notamment les avions de combat Sukhoï Su-35, alors que Téhéran et Moscou forment des relations militaires plus étroites. Lors d'une interview accordée à l'agence de presse iranienne *Tasnim*, le vice-ministre iranien de la Défense, le général de brigade Mahdi Farahi, a confirmé la livraison prochaine des avions de combat russes Sukhoï Su-35, des hélicoptères d'attaque Mil Mi-28 et des avions d'entraînement Yak-130 aux forces armées du pays. « L'entrée des avions dans le pays est devenue certaine et le processus de réception est en cours » a précisé le général de brigade Farahi. Il a souligné que la République islamique possède la flotte d'hélicoptères militaires la plus puissante de la région en termes de quantité et qu'elle a amélioré les capacités de ses hélicoptères après plusieurs projets. L'avion de combat Su-35, propulsé par une paire de turboréacteurs à double flux Saturn AL-41F1S, est capable de détecter une cible aérienne jusqu'à 400 km de distance et il peut suivre 30 cibles aéroportées et en engager huit simultanément. L'hélicoptère d'attaque Mil Mi-28, connu sous le nom de *Night Hunter*, a une vitesse d'environ 320 km/h et est équipé de deux turbomoteurs produisant chacun 2 500 chevaux. Le Yak-130 est un avion d'entraînement à réaction avancé subsonique biplace et un avion de combat léger développé à l'origine

par le concepteur et constructeur d'avions russe Yakovlev. Il peut effectuer des tâches d'attaque légère et de reconnaissance, transportant une charge de combat de 3 000 kg.  
(*Press TV, le 29-11-2023*)

## ... CYBERESPACE ...

### **En Corée du Sud, la messagerie *Line* victime d'une cyberattaque...**

L'opérateur de l'application de messagerie *Line* signale une violation massive de données personnelles. *Line Yahoo*, ou LY Corporation, estime qu'environ 440 000 données pourraient avoir été divulguées en raison d'une cyberattaque ayant vraisemblablement ciblé le système informatique d'une filiale. L'entreprise affirme qu'un sous-traitant de sa filiale sud-coréenne Naver a été visé. Les dégâts se sont apparemment étendus à LY, dans la mesure où les deux sociétés partagent une partie de leurs systèmes informatiques. Naver est un actionnaire majeur de LY. Cette dernière affirme que les données divulguées, ou potentiellement divulguées, incluent le groupe d'âge et le sexe des utilisateurs, bien que ces informations ne permettent pas d'identifier les individus. La société répertorie également l'historique des achats d'autocollants *Line*, ainsi que les noms, fonctions et adresses e-mail des entreprises utilisatrices. LY affirme jusqu'à présent n'avoir pas confirmé la fuite du contenu de la messagerie des utilisateurs, des informations bancaires ou de cartes de crédit. La société assure qu'aucun dégât n'a été signalé lundi. Elle va toutefois contacter chacun des utilisateurs susceptibles d'avoir subi des dommages secondaires.

(*Radio Japon international, le 28-11-2023*)

### **L'ensemble du territoire chinois couvert par un réseau Internet par satellites en orbite haute...**

La Chine a achevé l'établissement initial de son premier réseau Internet par satellites en orbite haute a annoncé l'Agence chinoise des vols spatiaux habités. À la suite du lancement d'un groupe de satellites de communication à haut débit, l'Internet par satellite en orbite haute couvre pleinement tout le territoire de la Chine et les zones clés des pays participant à l'initiative *La ceinture et la route*. Les satellites à haut débit disposent d'une large bande passante et de vitesses de transmission rapides, facilitant les téléchargements et les appels vidéo. À la fin de la période du 14<sup>e</sup> plan quinquennal (2021-2025), la capacité totale des satellites à haut débit de la Chine dépassera 500 Gb/s. À ce moment-là, les satellites à haut débit du pays fourniront une communication en réseau à grande vitesse et des services d'accès à Internet par satellite aux industries telles que l'aviation, la navigation, les situations d'urgence, l'énergie, et l'exploitation des forêts et prairies.

(*Radio Chine internationale, le 28-11-2023*)

### **Des hackers auraient accédé au système informatique de l'Agence japonaise d'exploration aérospatiale...**

L'Agence japonaise d'exploration aérospatiale, ou JAXA, indique que des pirates ont eu accès à son système informatique. Elle précise que les informations confidentielles du personnel notamment pourraient avoir été divulguées. La JAXA et le ministère japonais des Sciences et des Technologies affirment que le serveur compromis est distinct du réseau qui contrôle les opérations des fusées et des satellites. Selon eux, il est peu probable que des renseignements confidentiels, tels que des données sur les opérations de fusées, aient été détournés. Les responsables de la JAXA expliquent avoir été informés de la cyberattaque par une organisation extérieure et que les pirates pourraient avoir eu accès à certaines données. Des sources proches de l'affaire indiquent que le serveur piraté contenait des informations personnelles sur plus de 5 000 fichiers, notamment des dirigeants, du personnel et des employés temporaires de la JAXA. La JAXA et les organisations associées enquêtent sur l'étendue des dégâts et sur les méthodes employées dans les attaques. La JAXA a refusé de commenter les détails de l'attaque, invoquant des questions de sécurité. L'agence affirme qu'elle continuera d'enquêter et de mettre en œuvre des mesures contre de nouvelles attaques.

(*Radio Japon international, le 29-11-2023*)

### **Sanction américaine à l'encontre de *Sinbad* accusé d'avoir facilité le blanchiment d'argent de la Corée du Nord...**

Les États-Unis ont sanctionné mercredi le « mixeur » de cryptomonnaies *Sinbad*. Le département du Trésor américain a fait cette annonce en publiant une série de nouvelles sanctions contre les cyberactivités illicites de la Corée du Nord. *Sinbad* est accusé d'avoir facilité les activités de blanchiment d'argent de Pyongyang grâce à sa technologie de mélange des transactions qui

deviennent ainsi anonymes. Selon les autorités américaines, *Lazarus*, un groupe de pirates informatiques parrainé par le régime nord-coréen, a dérobé plusieurs millions de dollars de monnaies virtuelles et les a blanchis par l'intermédiaire de cette entreprise. Dans le cadre de ses sanctions, l'administration américaine a interdit à cette dernière l'accès à Internet et a gelé ses avoirs aux États-Unis. Dans un rapport publié le mois dernier, le groupe d'experts du comité des sanctions contre la Corée du Nord du Conseil de sécurité de l'ONU avait déjà indiqué que *Lazarus* avait blanchi l'équivalent de 100 millions de dollars en bitcoins à l'aide des technologies de *Sinbad*. Pour rappel, lors de leur sommet en août, les dirigeants sud-coréens, américains et japonais s'étaient d'ailleurs engagés à réagir activement au blanchiment de cryptomonnaies pratiqué par Pyongyang pour financer ses programmes illégaux d'armes nucléaires et de missiles balistiques. Dans son communiqué, le département du Trésor américain a déclaré que les États-Unis n'hésiteraient pas à utiliser tous les outils à leur disposition pour empêcher les activités illicites de la Corée du Nord.  
(KBS World Radio, le 30-11-2023)

### **Mise en garde tchèque relative à l'utilisation de l'application chinoise WeChat...**

Alors que la Tchéquie compte environ 40 000 utilisateurs de *WeChat*, le Bureau national de la cybersécurité et de la sécurité de l'information (NUKIB) a émis ce jeudi un avertissement contre l'installation et l'utilisation de cette application de la société chinoise Tencent. Selon le NUKIB, l'application collecte un grand nombre de données qui pourraient être utilisées pour organiser des cyberattaques ou des tentatives d'extorsion. La société Tencent entretient des liens étroits avec le gouvernement chinois et le parti communiste, précise l'autorité tchèque. Au printemps dernier déjà, le NUKIB avait estimé que l'application chinoise *TikTok* représentait une menace pour la sécurité et avait mis en garde contre son installation et son utilisation.  
(Radio Prague international, le 30-11-2023)



Renseignor est une lettre hebdomadaire publiée par Isabel Intelligence

[www.isabel-intelligence.org](http://www.isabel-intelligence.org)

en partenariat avec le Centre Français de Recherche sur le Renseignement (CF2R)

[www.cf2r.org](http://www.cf2r.org)

Directeur de la publication, directeur de la rédaction : Alain Charret – [direction@renseignor.com](mailto:direction@renseignor.com)

Comité de rédaction : Julia Charret, Eric Denécé, Yves-Marie Peyry – [redaction@renseignor.com](mailto:redaction@renseignor.com)



Créé en 2000, le Centre Français de Recherche sur le Renseignement (CF2R) est un Think Tank indépendant qui a pour objectifs :

- Le développement de la recherche académique et des publications consacrées au renseignement et à la sécurité internationale.
- L'apport d'expertise aux parties prenantes, aux politiques (décideurs, administration, parlementaires, médias, etc.).
- La démystification du renseignement et l'explication de son rôle auprès du grand public.

Centre Français de Recherche sur le Renseignement (CF2R)

**[12/14 rond-point des Champs Elysées - 75008 Paris - 01 53 53 15 30](https://www.cf2r.org)**

**Toutes les informations de Renseignor et plus encore  
sur notre canal Telegram <https://t.me/renseignor>**

