Renseignor
le Renseignement ouvert par la radio
N°1275 le 9 avril 2023

Dans ce numéro

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.

P'yongyang annonce avoir procédé à un nouvel essai de son drone d'attaque sous-marine à capacité nucléaire...
La Corée du Nord affirme avoir procédé cette semaine à un nouvel essai de drone d'attaque sous-marine à capacité nucléaire. L'édition de samedi du journal du Parti des travailleurs au pouvoir indique qu'un institut de recherche scientifique de la défense nationale a effectué le test pendant quatre jours jusqu'à vendredi. Le rapport indique que le drone submersible *Haeil-2* est entré dans la zone d'essai mardi au large de la province orientale du Hamgyong du Sud. Il précise que le drone a passé environ 71 heures à parcourir une distance virtuelle de 1 000 kilomètres avant d'atteindre une cible simulée et de faire exploser avec précision une ogive d'essai. C'est la deuxième fois que la Corée du Nord annonce un essai de sa nouvelle arme, appelée *Haeil*, qui signifie tsunami en coréen. Le pays a déclaré avoir testé ce drone pour la première fois le mois dernier et a affirmé qu'il pouvait déclencher un tsunami radioactif capable de détruire les navires et les ports maritimes de l'ennemi.
(Radio Japon international, le 08-04-2023)

La CIA aurait été surprise par le rétablissement des relations diplomatiques entre l'Iran et l'Arabie saoudite...
Le directeur de la CIA, William Burns, a exprimé sa frustration face à la décision de Riyad de rétablir ses relations avec Téhéran et Damas, alors que les observateurs soulignent le déclin de l'influence américaine au Moyen-Orient. Selon le *Wall Street Journal*, le directeur de la CIA, William Burns a effectué une visite inopinée cette semaine à Riyad pour discuter avec les responsables saoudiens de la coopération en matière de renseignement. Lors d'une rencontre avec le prince héritier saoudien Mohammed ben Salmane, Burns s'est plaint que Washington se sentait pris au dépourvu par les mesures prises par Riyad pour rétablir les liens avec l'Iran et la Syrie, faisant l'objet des sanctions de l'Occident. Il a exprimé la frustration des États-Unis d'être exclus des évolutions de la région.
(Press TV, le 07-04-2023)

Le premier hélicoptère de combat *Viper AH-1Z* en passe d'être livré à l'armée tchèque...
Produit aux États-Unis, le premier hélicoptère de combat *Viper AH-1Z* devrait bientôt être livré à l'armée tchèque. L'hélicoptère doit d'abord être transféré par le fabricant au gouvernement américain, puis à l'armée tchèque. Les premières machines devraient arriver en République tchèque au plus tard en mai, a fait savoir le ministère tchèque de la Défense. Au total, la Tchéquie achète aux États-Unis huit hélicoptères *Venom UH-1Y* et quatre hélicoptères de combat *Viper AH-1Z*. L'armée tchèque recevra également six autres *Viper* plus anciens et deux *Venom* américains en échange de l'aide apportée à l'Ukraine. Ils doivent remplacer les Mi-24V/35 soviétiques utilisés jusqu'à maintenant.
(Radio Prague international, le 03-04-2023)

… TERRORISME …

Un blogueur pro-Poutine tué lors d'un attentat à la bombe dans un café de Saint-Pétersbourg...
« Aujourd'hui, un engin de nature inconnue a explosé dans un café du centre de Saint-Pétersbourg » a annoncé dans un communiqué le Comité d'enquête russe, chargé des principales investigations en Russie. « Une personne est morte et vingt-cinq ont été blessées dont dix-neuf sont hospitalisées » a précisé sur *Telegram* le gouverneur de Saint-Pétersbourg, Alexandre Beglov. Selon les enquêteurs, qui ont ouvert une enquête pénale pour « meurtre à l'aide d'un moyen dangereux », la victime est le blogueur militaire connu sous le pseudonyme de Vladlen Tatarski. Les abords du bâtiment étaient bouclés, avec une vingtaine de voitures de policiers, six ambulances et des camions de pompiers, a constaté un journaliste de l'*AFP*. Une fille a vraisemblablement apporté l'engin explosif, selon une source citée par l'agence de presse *Ria Novosti*. « Il y avait une figurine dans la boîte : un cadeau destiné à M. Tatarski » a ajouté cette source. « Elle lui a donné, puis plus tard, d'un coup, il y a eu une explosion » a raconté à l'*AFP* Alissa Smotrova, une femme présente. Une autre source, également citée par *Ria Novosti*, a précisé que la personne en question était connue du blogueur et qu'ils s'étaient croisés lors d'événements, sans donner plus de détails. Selon le ministère russe de l'Intérieur, à 18h13 (15h13 GMT), la police du quartier de Vasileostrovski a reçu des informations selon lesquelles une explosion s'était produite dans un café sur le quai Universitetskaïa, au numéro 25. La déflagration a eu lieu dans le café Street Food Bar No. 1 situé le long de la Neva, non loin du centre historique de Saint-Pétersbourg. « Toutes les mesures nécessaires sont prises pour identifier les personnes impliquées » a ajouté le Comité d'enquête russe.
(La voix de la Turquie, le 03-04-2023)

Un responsable du groupe État islamique tué lors d'une frappe américaine en Syrie...
Khaled Aydd Ahmad Al-Jabouri un chef du groupe djihadiste État islamique responsable d'attaques perpétrées en Europe a été tué lors d'une frappe américaine en Syrie ce mardi, a annonce CENTCOM, le Commandement militaire américain pour le Moyen-Orient soulignant que sa mort allait temporairement perturber la capacité de l'organisation à fomenter des attaques à l'étranger.
(La voix de l'Amérique, le 04-04-2023)

Au moins trente morts après de nouvelles attaques des ADF dans le nord-est de la République démocratique du Congo...
De nouvelles attaques des ADF auraient fait plus de trente morts en RDC selon l'ONU. Ces tueries ont eu lieu en Ituri dans le nord-est du pays les 2 et 3 avril derniers. Les ADF sont des rebelles affiliés au groupe État islamique qui les présente comme sa branche en Afrique centrale.
(Radio Vatican, le 07-04-2023)

… ACTIVITÉS DES SERVICES DE RENSEIGNEMENT …

Les États-Unis utiliseraient le logiciel espion israélien *Pegasus* pour surveiller des téléphones au Mexique...
Washington aurait conclu un contrat secret avec la firme israélienne NSO Group quelques jours seulement après avoir annoncé la mise en place de mesures de rétorsion contre celle-ci, selon une enquête parue lundi dans le *New York Times*. Dans le cadre de cet accord, NSO Group aurait donné au gouvernement américain l'accès à son logiciel *Pegasus*, un outil de géolocalisation capable de suivre secrètement les téléphones portables à l'insu de leurs utilisateurs. Selon le journal américain, le contrat a été finalisé le 8 novembre 2021 via une société fictive ayant servi de façade au gouvernement des États-Unis et la filiale américaine d'une société de piratage israélienne notoire. Une dissimulation qui s'explique par le fait que cinq jours plus tôt, l'administration Biden avait annoncé des mesures contre NSO, dont les outils de piratage ont été utilisés pendant des années par des gouvernements du monde entier pour espionner des dissidents politiques, des militants des droits de l'Homme et des journalistes. Le 3 novembre, la Maison-Blanche avait ainsi placé NSO sur une liste noire du département du Commerce, déclarant la société israélienne comme une menace pour la Sécurité nationale et incitant les entreprises américaines à cesser de traiter avec elle. Le contrat secret, qui viole la politique publique de l'administration Biden, semble toujours actif. D'après le *New York Times* qui a pu examiner l'accord, celui-ci a spécifiquement permis au gouvernement de tester, d'évaluer et même de déployer le logiciel espion contre des cibles de son choix au Mexique. Interrogés à propos de ce

contrat, les responsables de la Maison-Blanche ont déclaré ne pas en avoir entendu parler. « Nous ne sommes pas au courant de ce contrat, et toute utilisation de ce produit serait très préoccupante » a déclaré un haut responsable de l'administration Biden sous couvert d'anonymat.
(I24News, le 03-04-2023)

Plusieurs documents militaires américains classifiés diffusés sur les réseaux sociaux...
La Russie ou des éléments prorusses sont probablement à l'origine de la fuite de plusieurs documents militaires américains classifiés sur la guerre en Ukraine, datant d'un mois, publiés ,vendredi, sur les réseaux sociaux, ont déclaré trois responsables américains à l'agence *Reuters* vendredi, tandis que le ministère de la Justice a déclaré qu'il enquêtait sur la fuite. Les documents semblent avoir été modifiés pour réduire le nombre de pertes subies par les forces russes, ont déclaré les responsables américains, ajoutant que leurs évaluations étaient informelles et distinctes de l'enquête sur la fuite elle-même. Les responsables américains ont parlé sous le couvert de l'anonymat en raison du caractère sensible de l'affaire et ont refusé de discuter des documents en détail. Un premier lot de documents, datés du 1er mars et portant les mentions « Secret » et « Top Secret » a circulé vendredi sur *Twitter* et *Telegram*, avant qu'un nouveau lot de documents semblant détailler des secrets de sécurité nationale américains concernant notamment l'Ukraine, le Moyen-Orient et la Chine a fait surface sur les réseaux sociaux, a rapporté le *New York Times*. Le ministère américain de la Justice a déclaré qu'il était en contact avec le ministère de la Défense et qu'il avait ouvert une enquête sur cette fuite. Il s'est refusé à tout autre commentaire. « Nous sommes au courant des rapports sur les publications sur les réseaux sociaux et le département de la Défense examine la question », a déclaré Sabrina Singh, porte-parole du Pentagone. Un des documents qui a fuité indique qu'entre 16 000 et 17 500 membres des forces russes ont été tués depuis l'invasion de l'Ukraine par la Russie le 24 février 2022, ce qui est très loin des estimations officielles des États-Unis qui ont compté environ 200 000 Russes tués et blessés. À Kiev, un responsable de la présidence ukrainienne a déclaré que la fuite contenait une très grande quantité d'informations fausses et ressemblait à une opération de désinformation russe visant à semer le doute sur la contre-offensive prévue par l'Ukraine.
(I24News, le 08-04-2023)

… MILITAIRE …

Nouvelle intrusion de navires chinois dans les eaux territoriales japonaises...
Les garde-côtes japonais affirment que des navires du gouvernement chinois ont pénétré dans les eaux territoriales japonaises près des îles Senkaku, en mer de Chine orientale. Ils y sont restés pendant 80 heures et 36 minutes. Il s'agit de la plus longue intrusion de ces navires dans les eaux territoriales japonaises depuis que le gouvernement nippon a acheté certaines des îles à un propriétaire privé japonais en 2012. Les garde-côtes indiquent que quatre navires du gouvernement chinois ont commencé à pénétrer dans les eaux près des îles de Minamikojima et Uotsurijima peu après 11 heures jeudi. Ils semblaient suivre trois bateaux de pêche japonais. Selon les garde-côtes, un des navires chinois a quitté la zone samedi soir après qu'un des bateaux de pêche a fait de même. Ils ajoutent que les autres navires chinois ont également quitté la zone à 19h44 dimanche. Les garde-côtes restent en état d'alerte et avertissent les navires chinois de ne pas pénétrer à nouveau dans les eaux territoriales. Le Japon contrôle les îles. La Chine et Taïwan les revendiquent. Le gouvernement nippon maintient qu'il n'y a aucune question de souveraineté.
(Radio Japon international, le 03-04-2023)

Détection d'une forte activité au sein du site nucléaire nord-coréen de Yonbyon...
Au nord du 38e parallèle, un haut niveau d'activité a été détecté au sein du site nucléaire de Yonbyon. *38 North* a fait cette annonce samedi dernier, en s'appuyant sur des images satellites prises le 3 et le 17 mars. Selon le site américain spécialisé dans les dossiers nord-coréens, un réacteur expérimental à eau légère (ELWR) semble être en voie d'achèvement et s'apprête à être opérationnel. En rendant publiques des photos qui révèlent l'activation du réacteur et la construction d'un nouveau bâtiment qui a commencé à proximité, il a également affirmé que des rejets d'eau avaient été observés dans le système de refroidissement de l'ELWR. Il a aussi fait savoir que de nouveaux travaux susceptibles d'étendre les capacités de l'usine d'enrichissement d'uranium ont été lancés. Toujours selon *38 North*, ces mouvements semblent suivre l'ordre du dirigeant nord-coréen Kim Jong-un, qui a souligné, le 27 mars dernier, l'importance d'augmenter la production de matières nucléaires pour le développement

de l'arsenal du pays.
(KBS World Radio, le 03-04-2023)

P'yongyang continuerait de produire du matériel nucléaire militaire...
La Corée du Nord n'ose pas encore procéder à un nouvel essai atomique, mais semble continuer de produire du matériel nucléaire militaire. C'est une analyse du comité de suivi de l'ONU des sanctions imposées au pays communiste. Il en a fait part dans un nouveau rapport publié par son groupe d'experts. Celui-ci y précise qu'en 2022, le régime de Kim Jong-un a lancé ses missiles balistiques à un total de 73 reprises, dont huit ICBM. Ces spécialistes évoquent également le fait que le Nord a testé un moteur de fusée de grande poussée en vue de mettre au point un nouvel ICBM à combustible solide et qu'il a menacé d'une attaque nucléaire préemptive. Sur le principal financement du développement des armes atomiques, le document le lie au vol des cryptomonnaies. Concrètement, l'an dernier, les groupes de hackers associés au régime communiste en ont dérobé quelque 1 000 milliards de wons, soit quasiment 700 millions d'euros. Un record. Toujours selon le panel d'experts, P'yongyang continue de contourner les sanctions onusiennes, par la voie maritime. Effectivement, il importe illégalement des produits pétroliers raffinés ou du charbon à bord de bateaux. À noter que le rapport porte majoritairement sur les violations survenues au second semestre de l'année dernière. La plupart d'entre elles sont donc déjà connues. *(KBS World Radio, le 06-04-2023)*

Exercices militaires conjoints des marines américaine, japonaise et sud-coréenne...
La Corée du Sud, les États-Unis et le Japon ont lancé ce matin leur exercice maritime conjoint dans les eaux internationales au sud de l'île méridionale de Jeju, et ce pour deux jours. Selon le ministère sud-coréen de la Défense, le porte-avions à propulsion nucléaire américain, l'*USS Nimitz*, qui est arrivé à la base navale de Busan, y prendra part. Pour la marine sud-coréenne, des destroyers, tels que le *Yulgok Yi Yi*, le *Choe Yeong* et le *Daejoyeong*, ont été déployés. L'entraînement portera sur la lutte anti-sous-marine aujourd'hui, et sur la recherche et le secours pour les accidents en mer demain. Cette manœuvre intervient seulement six mois après la dernière, laissant penser que les trois partenaires ont partagé l'idée que la provocation nord-coréenne a atteint un niveau alarmant. Le ministère sud-coréen a déclaré qu'elle vise à augmenter la capacité de réponse des trois nations contre les menaces croissantes du régime de Kim Jong-un liées aux missiles mer-sol balistiques stratégiques (MSBS). Tout au long de cet événement, Séoul, Washington et Tokyo se méfieront des activités des pays voisins, d'autant qu'un navire collecteur de renseignements chinois a été détecté dans la mer à proximité, lors de l'exercice qui s'est tenu en automne dernier. Face à cette mobilisation, il est fort probable que P'yongyang effectue une nouvelle bravade. La *KCNA*, l'agence de presse nord-coréenne, a déjà fustigé hier cet entraînement maritime, en indiquant que si les trois nations mènent une telle activité hostile, le régime nord-coréen fera un choix qui y correspond. Le scénario le plus plausible est que la Corée du Nord procède à un tir de missile longue portée en prétextant un test d'un satellite artificiel. Après avoir lancé deux missiles balistiques de portée intermédiaire le 18 décembre 2022, elle a déclaré achever la préparation de son premier satellite de reconnaissance militaire d'ici ce mois-ci.
(KBS World Radio, le 03-04-2023)

Aux Philippines, quatre nouvelles bases militaires pourront être utilisées par l'armée américaine...
La guerre d'influence entre les États-Unis et la Chine se joue en partie dans l'archipel des Philippines. Manille annonce hier la localisation de quatre nouvelles bases militaires pouvant être utilisées par les États-Unis : l'une très proche de la disputée mer de Chine méridionale et une autre non loin de Taïwan. Les quatre sites ont été sélectionnés avec précision et pourront servir au déploiement de troupes américaines dans la région. Début février les deux pays avaient dévoilé un accord pour permettre aux soldats américains d'accéder à des bases supplémentaires situées dans l'archipel. Washington et Manille sont alliés depuis plusieurs décennies en matière de sécurité, notamment liées par un traité de défense et un accord de coopération renforcée signés en 2014 qui permet aux soldats américains d'accéder à des bases philippines, mais aussi d'y stocker des équipements et du matériel militaire. Au total, les États-Unis pourraient occuper dix bases aux Philippines, dont la base navale de Santa Ana qui est située à 400 kilomètres seulement de Taïwan. Le nouveau gouvernement philippin de Ferdinand Marcos Junior souhaite renforcer son partenariat avec Washington poussé par les revendications de Pékin à l'égard de Taïwan et la construction de bases chinoises en mer de Chine méridionale.
(Radio Vatican, le 04-04-2023)

Un porte-avions chinois aurait été déployé dans l'océan pacifique...
Le ministère japonais de la Défense déclare avoir confirmé mercredi la présence de trois navires de guerre chinois, dont le porte-avions *Shandong*, dans l'océan Pacifique, au sud du département d'Okinawa. Le premier porte-avions chinois construit dans le pays a été déployé en décembre 2019. C'est la première fois que le navire est repéré dans l'océan Pacifique. Jeudi, le ministère a fait savoir que les Forces maritimes d'autodéfense avaient aperçu le *Shandong*, une frégate et un autre navire mercredi soir, alors qu'ils se dirigeaient vers l'est dans des eaux situées à environ 300 kilomètres au sud de l'île de Hateruma. Une photo rendue publique par le ministère montre plusieurs avions de chasse et hélicoptères stationnés sur le pont du *Shandong*. Mercredi, le ministère taïwanais de la Défense a ajouté que le même porte-avions a franchi le canal de Bashi, situé entre Taïwan et les Philippines. Actuellement, deux porte-avions sont exploités par la marine chinoise : le *Shandong* et le *Liaoning*. Le *Liaoning* a effectué des exercices de décollage et d'atterrissage dans l'océan Pacifique en décembre et en janvier derniers. Pour les responsables du ministère japonais de la Défense, la Chine cherche à améliorer les capacités opérationnelles de ses deux porte-avions. Le *Shandong* a été aperçu avant la rencontre entre la présidente taïwanaise Tsai Ing-wen et le président de la Chambre des représentants des États-Unis, Kevin McCarthy. Le ministère japonais a fait savoir qu'il se tiendra en état d'alerte et surveillera de près la situation.
(Radio Japon international, le 06-04-2023)

Exercices militaires chinois autour de Taïwan...
La Chine a lancé samedi trois jours de patrouilles de préparation au combat et d'exercices militaires autour de Taïwan. L'armée chinoise a déclaré que la priorité absolue était de tester sa capacité à contrôler les voies maritimes et aériennes. Selon le commandement du théâtre oriental de l'Armée populaire de libération, les exercices se déroulent dans le détroit de Taïwan et dans les zones situées au nord, au sud et à l'est de l'île. Ces exercices sont considérés comme une réponse à la récente rencontre entre la présidente de Taïwan, Tsai Ing-wen, et le président de la Chambre des représentants des États-Unis, Kevin McCarthy. Le commandement a indiqué que l'armée de terre, la marine et l'armée de l'air, entre autres, se sont rapidement déployées dans les zones d'exercice désignées après en avoir reçu l'ordre. Il a précisé que les exercices de samedi visaient à tester les capacités de l'armée à prendre le contrôle des voies aériennes et maritimes. Le commandement a ajouté qu'un autre objectif était de tester la capacité de l'armée à positionner des troupes pour encercler et se rapprocher de Taïwan. Par ailleurs, le ministère de la Défense taïwanais a déclaré avoir repéré 71 avions militaires chinois, dont des avions de chasse, autour de Taïwan entre 7 heures et 17 heures samedi, heure locale. Il a précisé que 45 d'entre eux avaient franchi la ligne médiane du détroit ou pénétré dans la Zone d'identification de la défense aérienne du sud-ouest de Taïwan.
(Radio Japon international, le 09-04-2023)

… L'ACTUALITÉ DES MARCHANDS D'ARMES …

La Tchéquie serait encore en mesure de fournir du matériel militaire à l'Ukraine...
La République tchèque possède encore des réserves de matériel militaire qu'elle pourrait envoyer en Ukraine pour aider celle-ci dans les combats contre la Russie. C'est ce qu'a indiqué la ministre de la Défense, Jana Cernochova, à la télévision tchèque, ce dimanche. Dans les prochains jours, Jana Cernochova et le chef d'état-major de l'armée, Karel Rehka, rencontreront le président de la République, Petr Pavel, qui a déclaré la semaine dernière que la République tchèque ne disposait plus de beaucoup d'options pour soutenir l'Ukraine en matière d'armement. La ministre entend remettre au chef de l'État une liste du matériel qui pourrait être mis à disposition de l'Ukraine. Jana Cernochova a précisé qu'avec Karel Rehka, un calendrier et une liste de l'aide qui pourrait encore être fournie à Kiev avaient été établis. « Il y a encore des choses dans nos entrepôts dont nous avons la garantie qu'elles ne seront jamais utilisées par notre armée et que nous pouvons hypothétiquement envoyer en Ukraine si celle-ci est intéressée » a-t-elle déclaré.
(Radio Prague international, le 03-04-2023)

L'augmentation de la production de munitions sud-coréennes saluée par le secrétaire général de l'OTAN...
Le secrétaire général de l'Organisation du traité de l'Atlantique Nord (OTAN) a accueilli chaleureusement l'augmentation de la production de munitions par la Corée du Sud. Il a d'ailleurs salué cette fourniture militaire indirecte sud-coréenne à l'Ukraine. C'est ce qu'a fait savoir hier Jens

Stoltenberg lors d'une conférence de presse donnée à l'issue de la réunion ministérielle de l'Alliance atlantique tenue à Bruxelles avec quatre pays partenaires de l'Asie-Pacifique, à savoir la Corée du Sud, l'Australie, la Nouvelle-Zélande et le Japon. À la question de savoir si l'éventuelle fourniture d'armes par Séoul à Kiev a été évoquée lors du rassemblement, le secrétaire général a répondu que le Pays du matin clair, grand producteur de munitions, accentuait sa fabrication, ce qui permettrait de remplir les stocks des nations membres de l'OTAN. Cependant, Stoltenberg a annoncé ne pas pouvoir détailler la manière d'approvisionnement et le destinataire des munitions sud-coréennes, avant de souligner que l'Ukraine sera le pays le plus aidé et de manière régulière via l'arsenal que dispose l'organisation internationale. De son côté, un membre de la délégation sud-coréenne a confirmé lui aussi qu'aucun soutien militaire direct du Pays du matin clair n'avait été évoqué lors de la réunion. Suite aux propos favorables de l'OTAN, après ceux des États-Unis, sur l'accroissement de la production des munitions sud-coréennes, les observateurs misent sur la possible demande explosive de ces produits *made in Korea*.
(KBS World Radio, le 06-04-2023)

La Finlande en passe d'acheter le système de défense aérienne israélien *Fronde de David*...
Le ministère finlandais de la Défense a annoncé mercredi que son pays va acheter le système de défense aérienne *Fronde de David* à Israël pour un montant de 316 millions d'euros. Dans un communiqué, le ministère a indiqué que le système améliorera considérablement les capacités de défense de la Finlande et permettra aux forces d'intercepter des cibles à haute altitude. « Dans le même temps, nous poursuivons le développement ambitieux et à long terme de la capacité de défense de la Finlande dans un nouvel environnement de sécurité » a déclaré le ministre de la Défense Antti Kaikkonen. Le système *Fronde de David*, fabriqué par l'entreprise israélienne Rafael Advanced Defense Systems, est capable d'intercepter des fusées et des missiles à une distance de 40 à 300 kilomètres. Le communiqué précise que l'altitude de vol minimale requise par la Finlande pour le système a été fixée à 15 000 mètres. Le ministère de la Défense du pays a également déclaré que l'accord prévoit par ailleurs la possibilité de futurs achats supplémentaires d'un montant de 216 millions d'euros. L'annonce de la Finlande intervient au lendemain de l'adhésion d'Helsinki à l'alliance militaire de l'OTAN, ce qui a porté un coup dur au président russe Vladimir Poutine. La Finlande avait adopté la neutralité après sa défaite face aux Soviétiques lors de la Seconde Guerre mondiale, mais ses dirigeants ont formulé le souhait de rejoindre l'OTAN après l'invasion de l'Ukraine par la Russie. « L'ère du non-alignement dans notre histoire est arrivée à son terme, une nouvelle ère commence » a déclaré le président Sauli Niinistö avant que le drapeau bleu et blanc de son pays ne soit hissé à l'extérieur du siège de l'OTAN.
(I24News, le 06-04-2023)

… CYBERESPACE …

Vague de cyberattaques contre Israël revendiquée par *Anonymous Sudan*...
Les sites web de plusieurs grandes universités israéliennes ont été attaqués mardi par un groupe de pirates informatiques se faisant appeler *Anonymous Sudan*. Les sites de l'université de Tel Aviv, de l'université hébraïque de Jérusalem, de l'université Ben-Gourion du Néguev, de l'université de Haïfa, de l'institut Weizmann des sciences, de l'université ouverte d'Israël et de l'université Reichman figuraient parmi les sites inaccessibles à la navigation. Le groupe a publié un communiqué sur son compte *Telegram*, énumérant les sites attaqués. « Infrastructure : Universités - le secteur de l'éducation israélien a été abandonné à cause de ce qu'ils ont fait en Palestine » peut-on lire dans le communiqué. Le groupe a également ajouté qu'il ne s'agissait pas de son attaque principale, qui aura lieu le 7 avril. La société de cybersécurité Radware a déclaré que des cyberattaques de grande ampleur contre Israël se produisaient chaque année le 7 avril depuis dix ans. Mardi, l'entreprise a également identifié des attaques contre des sites web d'hôpitaux, des journaux, ou encore des raffineries. En février dernier, le site du Technion a été piraté, des informations lui ont été volées et les hackers ont exigé une rançon de plusieurs millions de shekels. Suite à l'incident, les systèmes informatiques de l'institut ont été déconnectés et la date de plusieurs examens a été reportée. Le National Cyber Array avait déclaré que l'Iran était à l'origine de la cyberattaque.
(I24News, le 04-04-2023)

Le groupe de hackers *Anonymous Sudan* a attaqué mercredi matin les sites de plusieurs médias

israéliens, dont celui d'*I24NEWS* pendant près de deux heures. Les autres médias attaqués étaient *Kan*, *Jerusalem Post* ou encore *Channel 12*. Cette cyberattaque survient au lendemain d'un piratage qui a visé plusieurs universités du pays, dont celle de Tel Aviv, de Jérusalem, de Beer Sheva, de Haïfa, l'institut Weizmann, l'université ouverte d'Israël et l'université Reichman (IDC). *Anonymous Sudan* est également parvenu à pirater la société israélienne de cybersécurité Checkpoint, ainsi que l'organisation United Hatzalah. Ces cyberattaques s'inscrivent dans le cadre de l'opération annuelle *OPIsrael*, une opération de piratage informatique propalestinienne qui vise les institutions israéliennes pendant une semaine afin de punir l'État hébreu pour ses actions en Cisjordanie. Le groupe a laissé entendre que ces attaques se poursuivraient vendredi sans donner de détails.
(I24News, le 05-04-2023)

Plus d'une centaine d'arrestations après une opération de police contre la plus grande plateforme de hackers au monde...
Elle s'appelle *Genesis Market* et est la plus grande plateforme de hackers au monde. Cette plateforme a vendu les données et identifiants de millions de personnes sur internet. Plus d'une centaine de personnes ont été arrêtées, 200 propriétés ont été perquisitionnées. Les enquêteurs de plus d'une vingtaine de pays ont été impliqués dans cette opération. Des actions ont notamment eu lieu en Australie, au Canada, aux États-Unis et dans une dizaine de pays européens.
(Deutsche Welle, le 05-04-2023)

La police européenne a annoncé mercredi la fermeture de l'une des plus grandes plateformes de piratage informatique du monde, qui vendait des identifiants de comptes volés, notamment au Canada. Une opération policière sans précédent impliquant 17 pays a entraîné le démantèlement de *Genesis Market*, l'un des marchés les plus dangereux du monde, a déclaré l'agence Europol dans un communiqué. Des actions coordonnées ont également été menées à travers le monde contre les utilisateurs de cette plateforme. Elles ont mené à 119 arrestations et à 208 perquisitions, dont 4 ont eu lieu au Canada. Ce coup de filet international a été mené par le Federal Bureau of Investigation (FBI) aux États-Unis, Politie (police nationale des Pays-Bas) et Europol, qui a coordonné le travail des agents impliqués partout dans le monde. Au Canada, le Service des enquêtes sur la cybercriminalité de la Sûreté du Québec (SQ) y a travaillé en collaboration avec le FBI, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) ainsi que la Gendarmerie royale du Canada (GRC). Au total, 28 services de police d'un océan à l'autre ont été impliqués dans cette journée mondiale d'action séquentielle, a expliqué la GRC. L'enquête a eu des répercussions au Québec, où 6 personnes ont été arrêtées, mardi, en lien avec cette affaire de portée internationale. Les suspects, 4 hommes et 2 femmes âgés de 21 à 37 ans, pourraient être accusés, entre autres, d'utilisation non autorisée d'un ordinateur et de possession de dispositif permettant l'utilisation non autorisée d'un ordinateur. Les perquisitions ont permis de saisir du matériel informatique et de l'équipement servant à produire de faux documents. Dans cette opération, la SQ a pris en charge l'enquête visant les utilisateurs québécois les plus actifs de *Genesis Market*. Le corps policier provincial a assuré la coordination avec 11 services de police québécois ainsi que la rencontre d'environ 59 sujets d'intérêt, tous des utilisateurs de *Genesis Market*, a-t-on expliqué dans un communiqué. La majorité des suspects identifiés au Canada lors de l'opération habitent le Québec. La principale marchandise de *Genesis Market* était les identités numériques. Ce marché vendait des bots (robots) qui avaient déjà infecté les appareils des victimes par le biais de logiciels malveillants ou d'attaques de prise de contrôle de compte, a expliqué l'agence dans un communiqué. *Genesis Market* avait 1,5 million de robots en sa possession au moment de l'action internationale concertée. À la suite de l'achat d'un robot, les criminels avaient accès à toutes les données qu'il avait collectées, telles que les empreintes digitales, les témoins de connexion (cookies), les connexions enregistrées et les informations de remplissage automatique (formulaires électroniques, par exemple). Ces informations étaient collectées en temps réel, c'est-à-dire que les acheteurs étaient avertis de tout changement de mot de passe, par exemple.
(Radio Canada international, le 06-04-2023)

Augmentation considérable des vols de cryptomonnaies effectués par des hackers nord-coréens présumés...
Un rapport des Nations unies indique qu'en 2022, la Corée du Nord a dérobé des avoirs en cryptomonnaie d'une valeur plus élevée que toute autre année, et ce en utilisant des techniques de plus en plus avancées. L'ONU recommande une sanction contre le chef de l'agence nord-coréenne

responsable. Le Conseil de sécurité de l'ONU qui définit les sanctions contre P'yongyang a publié un rapport mercredi couvrant la période de fin juillet à fin janvier. D'après le document, une firme de cybersécurité a estimé que la cybercriminalité nord-coréenne a amassé de la cryptomonnaie d'une valeur de plus d'un milliard de dollars en 2022. Les cryptoactifs volés par la Corée du Nord serviraient à financer ses programmes nucléaires et de missiles. Le rapport ajoute que le pays a utilisé des cybertechniques de plus en plus sophistiquées, et qu'il est donc difficile de retracer l'origine des actifs. Les auteurs du rapport affirment que les pirates informatiques responsables de la plupart des attaques sont des membres du Bureau général de reconnaissance. La commission recommande d'ajouter le chef du bureau, le général Ri Chang Ho, sur la liste des individus ciblés par des sanctions. Elle exhorte de nouveau les États membres à renforcer leurs mesures de sécurité.
(Radio Japon international, le 06-04-2023)

P'yongyang diversifierait ses moyens afin de dérober des cryptomonnaies...
La Corée du Nord semble diversifier les moyens de voler les cryptomonnaies pour financer son programme d'armement de destruction massive. Il a été révélé cette fois qu'elle a aussi recours à la finance décentralisée, abrégée en DeFi. Dans son premier rapport sur l'évaluation mondiale des risques de financement illicite DeFi, publié hier, le Trésor américain estime que les hackers nord-coréens transfèrent et blanchissent l'argent dérobé en utilisant ce système développé dans le sillage du marché des cryptoactifs, grâce aux fonctionnalités de la *blockchain*. Selon le ministère américain, le régime de Kim Jong-un, sous le coup de sanctions américaines et onusiennes, multiplie les récoltes illégales de fonds à l'aide du système en question et du VASP, fournisseur de services d'actifs virtuels. Le fameux groupe *Lazarus*, soutenu par le Nord, s'est par exemple emparé d'actifs numériques d'une valeur totale de 720 millions de dollars, en attaquant le jeu vidéo en ligne *Axie Infinity* en 2022 et la société de cryptomonnaie Harmony en 2020. Toujours selon le Trésor américain, des hackers liés au royaume ermite sont aussi impliqués dans les attaques de rançongiciels. Et plusieurs milliers de travailleurs nord-coréens des technologies de l'information, présents dans le monde entier, sont eux aussi derrière les cyberactivités illicites.
(KBS World Radio, le 07-04-2023)

Renseignor
le Renseignement ouvert par la radio

Renseignor est une lettre hebdomadaire publiée par Isabel Intelligence
www.isabel-intelligence.org

en partenariat avec le Centre Français de Recherche sur le Renseignement (CF2R)
www.cf2r.org

Directeur de la publication, directeur de la rédaction : Alain Charret – direction@renseignor.com

Comité de rédaction : Julia Charret, Eric Denécé, Yves-Marie Peyry – redaction@renseignor.com

Cf2R

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