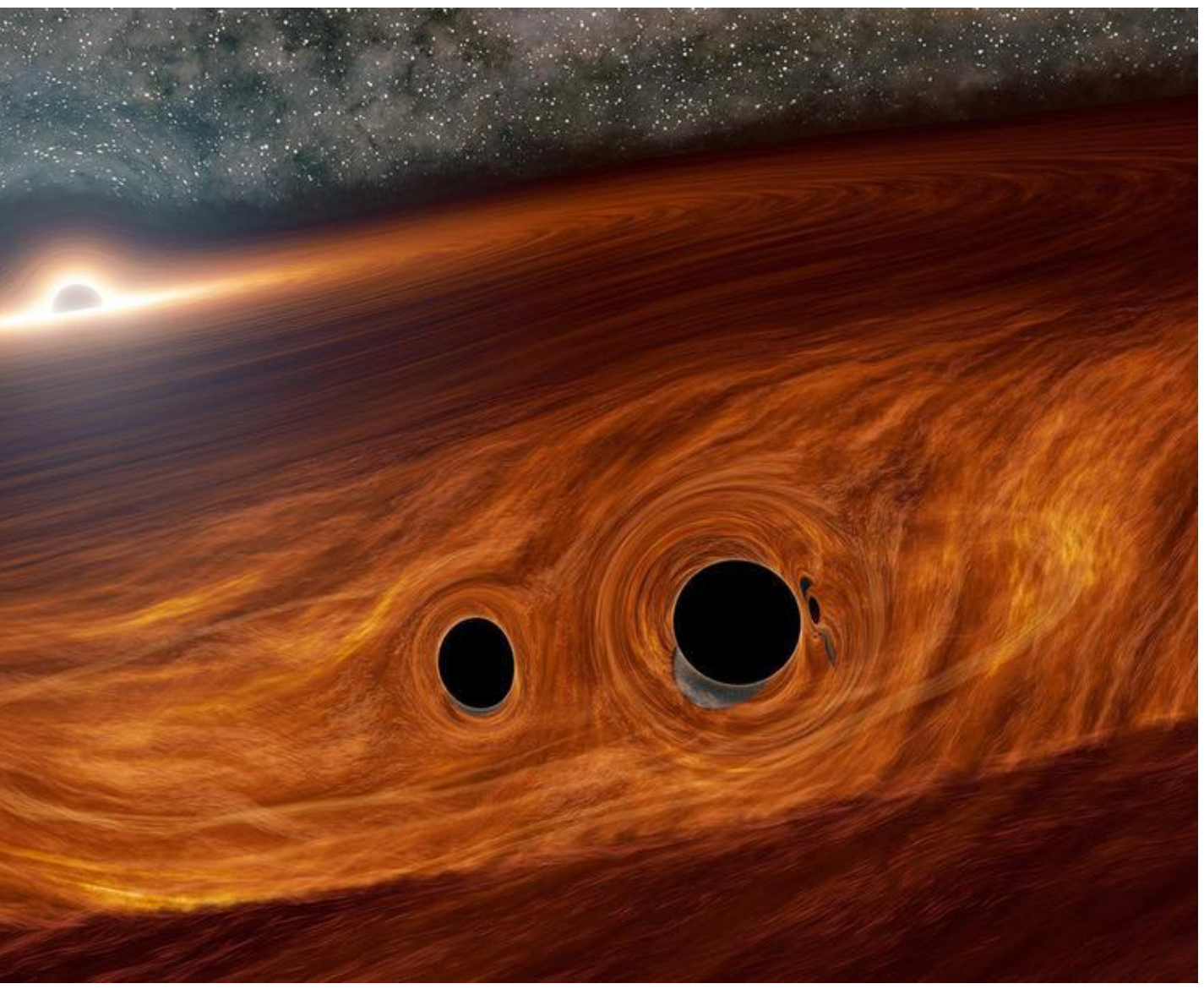
s de **trous noirs :** rs remise en question



La formation des trous noirs dans l'univers est l'un des problèmes majeurs auxquels doivent répondre les recherches modernes

Un des chercheurs de l'Université de Trieste

Il existe plus de trous noirs dans l'univers que d'habitants sur notre Terre.

© CALTECH/NASA

à l'intérieur de galaxies ou au-dehors, dans des amas globulaires.

C'est l'évolution de ce taux de formation que l'équipe d'astrophysiciens a réussi à modéliser. Suite à ces calculs, les chercheurs estiment qu'environ 1 % des protons et neutrons issus du big-bang se retrouvent aujourd'hui sous la forme de trous noirs stellaires. Ils ont même obtenu une fonction de distribution de ces trous noirs par galaxie. Au terme de ce décompte, le nombre dément de 40 milliards de milliards fait ainsi son apparition. C'est-à-dire 4 suivi de 19 zéros. Et cela sans compter les trous noirs supermassifs.

La détection d'une telle quantité de trous noirs – qui ont fréquemment une masse 25 fois supérieure à celle du Soleil – marque une avancée majeure dans l'étude de ces objets célestes. « La formation des trous noirs dans l'univers est l'un des problèmes majeurs auxquels doivent répondre les recherches modernes », précise l'un des chercheurs. Car tout cela signifie aussi qu'une bonne partie de ce qui nous entoure serait abrité dans ces trous noirs sans matière ni lumière. Quant à leur formation, on n'en sait guère plus sinon qu'ils proviennent d'implosions d'étoiles en fin de vie, étoiles qui peuvent être isolées, dans un système binaire ou au centre d'un amas d'autres astres.

Cette trouvaille démographique s'inscrit dans un programme qui s'appelle « Big Data Application for Black Hole Evolution Studies » et ouvre désormais la voie à des dizaines de trouvailles similaires. Elle fait aussi le point sur ces trous noirs intermédiaires appelés parfois « graines ». Vertigineux !

pays n'est pas compliqué »

mais, *a fortiori* après deux années de pandémie durant lesquelles nous nous sommes tournés vers le numérique. Les usines et des services essentiels tels que l'eau ou l'électricité, notamment, tout est connecté et contrôlé par l'internet. A partir d'un ordinateur distant, il est possible de paralyser des hôpitaux, d'aiguiller des rails de chemin de fer ou de fermer les tuyauteries d'adduction d'eau d'une ville. Et, bien sûr, d'accéder à nos données personnelles : où l'on se rend, avec qui, nos antécédents médicaux, nos finances, etc. Notre vie tout entière se heurte à un danger permanent, c'est un fait. De plus, contrairement au monde physique, le numérique rend pratiquement impossible la localisation de délinquants : un individu peut attaquer une infrastructure n'importe où à partir d'Israël par le biais de serveurs installés ailleurs dans le monde.

A partir d'un ordinateur distant, il est possible de paralyser des hôpitaux, d'aiguiller des rails de chemin de fer ou de fermer les tuyauteries d'adduction d'eau d'une ville

Accorde-t-on suffisamment d'attention à ces défis ?

Il faut mener plus d'actions. A notre niveau, nous développons des outils pour lutter contre la cinquième génération de cyberattaques. La plupart des organisations continuent de se prémunir de la quatrième, à tel point notamment qu'en Allemagne, au cœur de la pandémie, les systèmes d'un hôpital ont été séquestrés et que pour assurer son fonctionnement, l'institution a dû revenir intégralement au mode analogique.

En quoi consiste la cinquième génération de cyberattaques ?

Nous avons identifié une série de schémas propres aux attaques de nouvelle génération. Premièrement, elles sont polymorphes : même si, souvent, elles peuvent présenter quelques similarités, il n'y en a jamais deux qui sont identiques. Deuxièmement, elles sont multifactorielles. Dans le passé, vous faisiez l'objet d'une attaque sur le web, et c'était tout. Aujourd'hui, l'opération peut commencer par une app de jeu que l'on télécharge sur son portable et qui véhicule un *malware*. Ce logiciel malveillant vise votre identifiant du journal que vous consultez également sur votre ordinateur portable, auquel il va accéder pour subtiliser des données spécifiques sur cet appareil. Cette observation nous mène à leur troisième caractéristique : elles sont très difficiles à détecter et extrêmement sophistiquées. Nous avons observé la manière dont un *malware* modifie les caractéristiques chimiques de l'eau dans une usine de traitement de l'eau. Empoisonner tout un pays n'est pas compliqué.

Selon vous, comment peut-on se prémunir de ce type d'attaques ?

Nous devons nous protéger contre les dernières attaques détectées aujourd'hui, contre celles qui se sont produites il y a vingt ans et qui sont encore susceptibles de nous affecter, tout comme face à celles que nous n'avons pas encore connues. L'internet, les portables, les serveurs d'entreprise, le nuage et tous les appareils connectés à l'internet des objets doivent être protégés. Il faut une approche multivectorielle, qui s'appuie sur des technologies automatisées fondées sur l'intelligence artificielle. En fin de compte, c'est une question de prévention, et non de dissuasion. La plupart du temps, la police n'empêche pas le délit ; elle entre en scène au moment des faits. Une action à l'effet dissuasif, qui est toutefois inopérante dans le cyberespace.

La pandémie a-t-elle contribué au boom de la cybercriminalité ?

Enormément. L'année dernière, dans le monde, le nombre d'attaques a augmenté de 60 % par rapport à la précédente. Et de mon point de vue, ces chiffres vont continuer leur progression. Deux raisons expliquent cette croissance. Premièrement, le monde est désormais beaucoup plus connecté et encore plus dépendant de l'internet. Au cours de la pandémie, les gens ont consacré entre 70 et 90 % de leur temps à des activités en ligne. De même, cela signifie que beaucoup d'éléments jadis protégés de l'internet ne le sont plus. Dans de nombreuses usines, les machines étaient contrôlées et entretenues manuellement. Avec la pandémie, elles ont été progressivement connectées pour permettre le travail à distance. Dans les hôpitaux, les banques, les bureaux… tous ont permis à leur personnel d'accéder à des fonctionnalités à distance, ce qui, à son tour, démultiplie les vecteurs d'attaque. En effet, la personne qui s'immisce dans mon ordinateur peut, le cas échéant, pénétrer aussi dans les systèmes de l'entreprise qui m'emploie. Par ailleurs, les hackers ont également été confinés chez eux et ont pu consacrer plus de temps à leur travail. Leurs méthodes se sont perfectionnées.

Pendant ce temps, avez-vous aidé l'une ou l'autre entreprise à éviter sa destruction ?

Très souvent. En revanche, je ne peux pas donner de noms. Par exemple, une grande société publique qui fournit de nombreux services dans son pays nous a appelés à l'aide. Notre équipe a étudié et détecté deux *malwares* distincts qui la surveillaient et étaient présents dans ses systèmes depuis plusieurs mois. Nous avons stoppé près de 90.000 tentatives d'intrusion au cours des heures suivantes, installé des serveurs critiques comme système de messagerie et nettoyé 8.000 ordinateurs de cette organisation. Nous ignorons le nombre de données que ces pirates informatiques lui ont subtilisées avant notre intervention. Cependant, le fait est que ces hackers auraient pu mener cette société à sa destruction.

Certaines entreprises, dont la société israélienne NSO Group, développent des logiciels espions utilisés contre des particuliers. A l'instar des cyberdélinquants, ils exploitent les vulnérabilités pour s'immiscer dans d'autres systèmes. Opérez-vous également contre des sociétés de droit ?

Je tiens à souligner sans ambiguïté que nous n'avons rien à voir avec cette industrie. Lorsque nos enquêteurs découvrent une faille, ils ne l'exploitent pas pour gagner de l'argent ; ils ne la vendent pas à des tiers. Nous voulons clairement nous positionner du côté de la sécurité. Notre intervention commence par une notification de la faille à son propriétaire, à qui nous fournissons toutes les données que nous avons recueillies. Nous l'aidons à résoudre le problème puis, en bout de parcours, nous publions des informations sur cette faille.

« De nombreuses cryptomonnaies sont des arnaques »

Ces dernières années, l'utilisation et la popularité des cryptomonnaies se sont envolées. A quel point sont-elles sûres ?

« Je ne suis pas spécialisé dans ce domaine », nuance Gil Shwed, « mais il faut garder à l'esprit qu'en soi, de nombreuses cryptomonnaies sont des arnaques. Cela dit, malgré la grande robustesse des algorithmes de chiffrement, la faiblesse des monnaies électroniques vient des porte-monnaie électroniques, où se concentrent les actions des cyberdélinquants. De plus, elles constituent l'une des raisons à l'origine d'une telle expansion de la cybercriminalité au cours de ces derniers temps car elles permettent de monétiser les attaques. Il est désormais très facile de payer pour se libérer d'un *ransomware* », ces programmes qui paralysent les systèmes informatiques et les libèrent moyennant le versement d'une somme d'argent.

M.G.P.