Des milliers de cyberpirates anonymes agissent pour le compte de la Chine.

GETTY IMAGES/ISTOCKPHOTO

LA GRANDE OFFENSIVE DES ESPIONS CHINOIS

Engagés secrètement depuis des années dans un espionnage économique et technologique à grande échelle, les services secrets chinois multiplient les piratages et les cyberattaques contre les pays occidentaux. Ils se sont lancés plus récemment dans une guerre froide idéologique, utilisant la désinformation et l'intox, que la crise du Covid-19 n'a fait qu'amplifier.

Par Vincent Nouzille

« Je ne peux pas nommer l'attaquant. Cela relève d'un acteur étatique qui a des capacités techniques importantes. Et il n'y en a pas beaucoup qui ont de telles capacités… » Le 19 juin, le premier ministre australien, le conservateur Scott Morrison, a usé de son sens de la litote diplomatique pour ne pas accuser frontalement l'État chinois d'être l'origine de la vague sans précédent de cyberattaques « malveillantes » ayant frappé récemment les institutions de son pays. Durant quelques jours, des sites gouvernementaux, des hôpitaux, des écoles, des entreprises ont été la cible de virus informatiques « sophistiqués », laissant peu de doutes aux services de renseignement et aux experts sur leur origine. *« Les investigations techniques permettent de déduire, avec un haut degré de confiance, que la République populaire de Chine est le probable responsable de ces attaques »*, confie Jacob Wallis, spécialiste du cyber à l'Institut australien de stratégie politique (Aspi, en anglais). La tension n'a cessé de monter entre la Chine et l'Australie ces derniers mois. Mi-2018, suivant l'exemple de son allié américain, le gouvernement de Canberra a proscrit les équipementiers chinois Huawei et ZTE des futurs réseaux de télécom 5G, au nom de la « sécurité nationale », autrement dit des risques d'espionnage. En février 2019, des cyberattaques, attribuées officieusement à la Chine, ont visé le Parlement australien et plusieurs partis politiques, juste avant les élections générales. Durant la crise du coronavirus, l'Australie a été le premier pays à réclamer une enquête internationale sur la genèse de la pandémie à Wuhan. Des représailles chinoises ont suivi, avec des hausses des tarifs douaniers sur des produits australiens et une nouvelle vague de cyberattaques, auxquelles Pékin s'est dit étranger. D'autres raids numériques ont visé des pays européens, qui demandent également que la Chine s'explique sur le virus et stoppe ces campagnes de *« désinformation »*. →

Le président Xi Jinping (au centre) a fait adopter une stratégie internationale plus offensive lors du XIXe congrès du Parti communiste chinois, le 18 octobre 2017.

La reconnaissance faciale, l'un des nouveaux outils de contrôle de la population, est actuellement en cours de tests dans certaines villes, comme ici à Nankin.

LA CHINE DE XI JINPING MET AU POINT UNE SURVEIL LANCE NUMÉRIQUE INTÉGRALE, DIGNE DE BIG BROTHER

L'empire du Milieu, en vérité, n'a plus de complexes. Il déploie à l'étranger une armada d'agents, manipule les réseaux sociaux et utilise des groupes de hackers pour déstabiliser ses « ennemis » occidentaux et poursuivre, en dépit de la tourmente actuelle, son ascension mondiale. *« L'idée selon laquelle la Chine allait s'adoucir avec le développement des échanges économiques était une illusion. Elle devient plus agressive »,* commente Paul Charon, directeur du domaine renseignement, anticipation et menaces hybrides à l'Institut de recherche stratégique de l'École militaire (Irsem), à Paris.

UN MINISTÈRE DE LA SÉCURITÉ D'ÉTAT

Arrivé au pouvoir en 2012, le tout-puissant président, Xi Jinping, secrétaire général du Parti communiste chinois (PCC), règne d'une main de fer sur son 1,4 milliard d'habitants. Depuis le XIXe congrès du PCC, en octobre 2017, celui que l'on nomme « l'empereur Xi » assume aussi une stratégie internationale conquérante afin de détrôner les États-Unis. Son objectif : conduire son pays vers un leadership mondial incontesté à l'horizon 2049, année du centenaire de la fondation de la République populaire. Pour gagner cette course à l'hyperpuissance, le régime chinois emploie tous les moyens possibles, allant du rachat d'entreprises au soft power, des grands projets comme les nouvelles routes de la soie aux manœuvres les plus secrètes. Deux ex-agents de la DGSE à la retraite ont ainsi été condamnés, le 10 juillet, à des peines de prison respectivement de 12 et 8 ans par la cour d'assises spéciale de Paris pour avoir « livré » à la Chine des renseignements sensibles pendant plusieurs années. Ils peuvent faire appel de ce jugement.

Dans le domaine de l'espionnage, la Chine n'a de leçons à recevoir de personne. Au VIe siècle avant J.-C., le stratège militaire Sun Tzu, dans son essai *L'Art de la guerre,* vantait déjà l'utilisation des espions afin de supplanter l'ennemi. L'avènement du régime communiste en 1949, avec Mao Zedong, a conduit à l'instauration d'un système de renseignement tentaculaire, sous l'œil inquisiteur du parti unique. Il est réparti principalement entre le ministère de la Sécurité publique, appelé Gonganbu, qui gère la police, et, surtout, le ministère de la Sécurité d'État (MSE), nommé Guoanbu, avec ses quelque 200 000 agents, dirigé depuis 2016 par le ministre Chen Wenqing, un fidèle du Président. Créé en 1983, le MSE est chargé du renseignement intérieur et extérieur, à l'image du KGB de l'ère soviétique en URSS. Censure des médias, police de l'internet domestique, répression des dissidents et des minorités, gestion de camps de détention : rien n'échappe aux services de sécurité. Transformés en Big Brother orwellien, ils testent des outils technologiques (reconnaissance faciale, intelligence artificielle, big data, notation de la « fiabilité » citoyenne) pour contrôler les habitants. *« La Chine œuvre à mettre au point l'état de surveillance numérique parfait et ses ingénieurs de l'âme ont rouvert l'atelier de fabrication de "l'homme nouveau" dont rêvaient déjà Lénine, Staline et Mao »,* explique le journaliste allemand Kai Strittmatter dans son essai *Dictature 2.0,* à paraître fin août chez Tallandier. Ce système est tenu au sommet par Xi Jinping, via la Commission centrale de sécurité nationale et la Commission centrale militaire, les organes du PCC et du gouvernement chargés de superviser ce dispositif, ainsi que de contrôler l'Armée populaire de libération (APL).

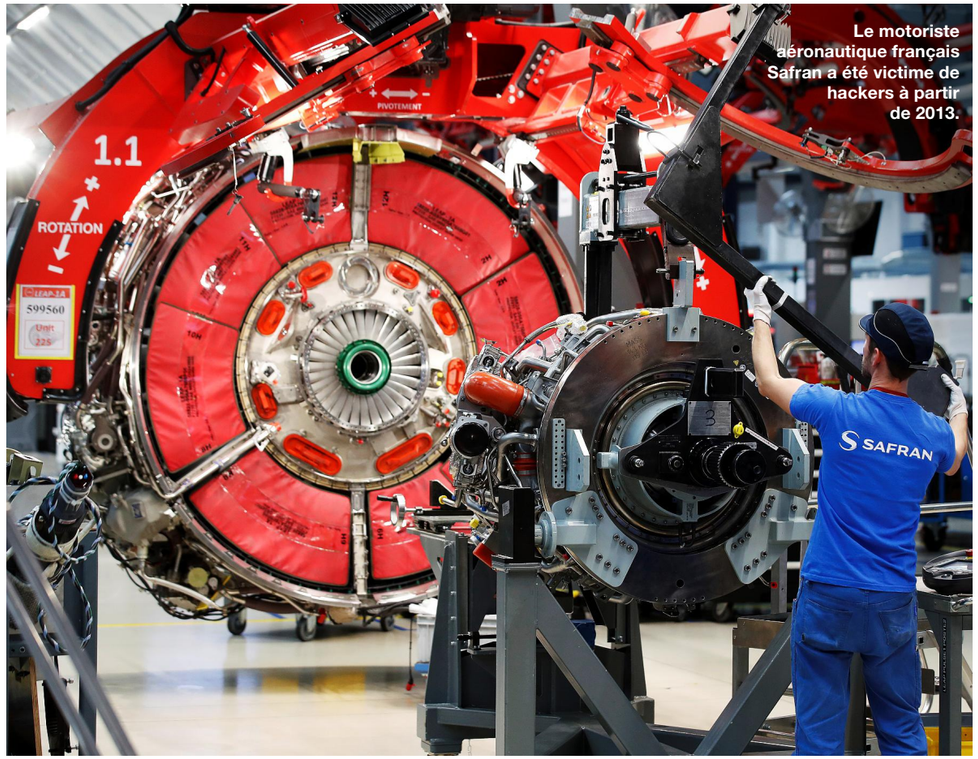
Les plans économiques chinois, très ambitieux, ont également poussé les services de renseignement – principalement le Guoanbu, mais aussi plusieurs départements spécialisés de l'APL – à organiser des opérations d'espionnage à l'étranger. *« Le pillage technologique fait partie des moyens autorisés pour rattraper le retard dans certains secteurs »,* explique un ancien responsable du renseignement français. Au début des années 2000, l'équipementier français de télécom Alcatel et l'américain Cisco ont constaté des similitudes entre les codes sources de leurs routeurs avec ceux de leur concurrent Huawei, fondé en 1987 par Ren Zhengfei, un ancien colonel de l'armée chinoise. Poursuivi par la justice aux États-Unis, Huawei a reconnu avoir usé du code source de Cisco *« par inadvertance »*. Alcatel a reçu un dédommagement de son rival chinois. Devenu depuis lors l'un des leaders mondiaux des télécoms, mais banni aux États-Unis, Huawei veut à tout prix installer ses réseaux 5G en Europe, ce qui soulève des questions sur leur sécurité, une loi de 2017 imposant aux entreprises chinoises de soutenir *« le travail national des services secrets ».*

PIRATAGE DANS L'AÉRONAUTIQUE

Le gouvernement français, lui, s'est alarmé dès 2010 que la Chine soit le pays menant le plus de cyberattaques contre les entreprises françaises. Fin 2013, Airbus a été victime de pirates informatiques, qui ont dérobé des documents sur l'avion de transport militaire A400M. Cette cyberoffensive *« aurait notamment permis à Pékin d'accélérer la certification de son avion de transport militaire Xian Y-20, entré en service en juillet 2016 »*, estime Antoine Izambard, dans son livre *France-Chine, les liaisons dangereuses* (Stock).

D'autres cyberpirates ont volé des données sur l'avion militaire C-17 de Boeing, sur le chasseur F-35 de Lockheed Martin et espionné des sous-traitants de l'aéronautique. Une opération sensible a, par exemple, visé à partir de 2013 le français Safran, fabricant de moteurs →

Annonce de poursuites par le FBI contre des agents de l'armée chinoise, pour vol de données, le 10 février 2020.



Le motoriste aéronautique français Safran a été victime de hackers à partir de 2013.

LE FBI MULTIPLIE LES ENQUÊTES CONTRE DES CYBERESPIONS CHINOIS

d'avions avec l'américain General Electric. Deux présumés agents chinois, liés au ministère de la Sécurité d'État, se sont infiltrés parmi les employés d'une filiale de Safran à Suzhou, à l'ouest de Shanghaï. L'un d'eux, Tian Xi, recruté comme chef de produit, a introduit un malware dans un ordinateur de Safran. *« Le cheval [de Troie] a été installé ce matin »*, a textoté Tian Xi le 25 janvier 2014 à un officier traitant. Les espions ont pu pénétrer des serveurs de Safran et y piocher des renseignements sur son futur turboréacteur. Aux États-Unis, le FBI, qui a détecté plusieurs intrusions, a prévenu les services français. Une enquête conjointe a été initiée. Interpellé à l'aéroport de Los Angeles le 21 août 2017, l'un des hackers suspectés a plaidé coupable. Il a permis aux policiers d'identifier d'autres pirates, dont les deux « infiltrés » chez Safran, ainsi qu'un officier du Guoanbu, Yanjun Xu, arrêté à Bruxelles le 1er avril 2018 puis extradé aux États-Unis. Élargissant son enquête, le département de la Justice a fini, le 30 octobre 2018, par inculper dix présumés agents chinois pour cyberespionnage. *« C'est un exemple des efforts criminels déployés par le ministère de la Sécurité d'État pour faciliter le vol des données afin de fournir à la Chine des avantages commerciaux »*, a dénoncé le procureur des États-Unis, Adam Braverman. Pékin a réagi en qualifiant les charges de *« pure fabrication »*.

Le lancement par la Chine, en 2015, de son vaste plan Made in China 2025, qui a pour objectif d'atteindre l'autonomie dans les hautes technologies, a redonné un coup d'accélérateur à la chasse secrète. *« Le dispositif a été rationalisé, les objectifs déclinés en lien avec le gouvernement, l'armée, les services et les grands groupes publics et privés, ce qui n'exclut pas des compétitions entre eux »*, juge Candice Tran Dai, vice-présidente du Centre Asie à Paris et experte à la Global Foundation for Cyber Studies and Research, à Washington.

RECRUTEMENTS SUR LINKEDIN

Résultat : après une pause décrétée suite à un accord de non-agression cyber négocié entre le président Barack Obama et Xi Jinping en 2015, la liste des affaires de piratage et d'espionnage chinois s'est à nouveau allongée. En France, un rapport confidentiel du Secrétariat général à la défense et à la sécurité nationale (SGDSN) évoquait, mi-2018, de nouvelles cyberattaques chinoises ayant touché le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) ainsi que des grands groupes comme Airbus, Safran, Dassault, Thalès ou Sanofi. Trois mois plus tard, *Le Figaro* révélait que les services chinois avaient lancé une campagne d'harponnage de jeunes cadres français, en les approchant surtout via le réseau LinkedIn, grâce à des faux profils de recruteurs qui proposaient des invitations en Chine. Plus de 4 000 personnes ont ainsi été démarchées, soit une *« ampleur sans précédent »*, selon une note des services français (DGSE et DGSI), appelant à la fin *« d'une période de naïveté coupable »* et à des répliques systématiques. Leurs homologues allemands ont détecté des opérations similaires en 2017, visant 10 000 personnes sur LinkedIn. Interrogée fin 2019 par Antoine Izambard sur tous ces soupçons d'espionnage, l'ambassade de Chine en France a répondu qu'il s'agissait *« d'allégations dépourvues de fondement »* et elle a accusé, en retour, la France de mener des cyberattaques qui auraient atteint 220 000 ordinateurs en Chine.

Outre-Atlantique, les Chinois sont aussi suspectés d'avoir, ces dernières années, piraté des données précieuses, tels que les fichiers du personnel de l'administration fédérale (dont des milliers d'agents du renseignement américain…) ou ceux du site de rencontres extramaritales Ashley Madison, avec ses 30 millions de clients, dont des célébrités et des hommes politiques. De quoi connaître leurs petits secrets et en faire chanter quelques-uns… En 2017, ce sont les serveurs de la société de crédit Equifax, basée à Atlanta, qui ont été piratés. *« Ils ont volé les données personnelles et sensibles de 145 millions d'Américains »*, dénoncent les procureurs dans leur acte d'accusation, rédigé le 10 février 2020, qui cite →

SARAH SILBIGER/ GETTY IMAGES/AFP ; JC MARMARA / LE FIGARO

Immeuble du secteur de Pudong, à Shanghaï, susceptible d'abriter des hackers de l'unité 61 398 de l'armée chinoise.

CARLOS BARRIA/REUTERS

DES GROUPES DE HACKERS, DITS APT, MÊLENT LA CYBER-CRIMINALITÉ, LE PILLAGE ET LE CYBERESPIONNAGE

nommément les suspects, en l'occurrence quatre agents de l'Institut de recherche N° 54 de l'armée chinoise.

Les cyberattaquants ne sont pas toujours faciles à identifier. La plupart du temps, ils avancent masqués, ce qui permet aux officiels chinois de nier toute responsabilité. En 2013, la société américaine de cybersécurité Mandiant a révélé pour la première fois qu'un groupe de hackers chinois très actifs surnommé APT1 – *« Advanced permanent threat N° 1 »,* ou menace permanente avancée N° 1 – était probablement le faux nez de l'Unité 61 398, une branche secrète du Département N° 3 de l'armée chinoise, composée de plusieurs centaines de cybersoldats, basés dans un immeuble du quartier de Pudong, à Shanghaï. Selon Mandiant, *« APT1 a systématiquement volé des centaines de téraoctets de données »* d'au moins 140 entreprises de 2006 à 2013, grâce à des e-mails piégés. Leurs cibles, situées aux États-Unis, au Canada et au Royaume-Uni, correspondaient aux ambitions de la Chine dans le secteur des télécoms, de l'espace, de l'énergie ou de l'ingénierie.

Depuis, les groupes de hackers dits « APT » liés à la Chine n'ont cessé de proliférer. Les experts du cyber, qui tentent de tenir à jour un « Who's Who » des pirates, établissent leurs connexions grâce à des indices concordants : horaires d'intervention calés sur les fuseaux de Pékin, cibles visées, méthodes utilisées, géolocalisation des noms des domaines et des adresses IP, codes des logiciels écrits en mandarin. Ils ont ainsi recensé au moins une soixantaine d'APT reliés à la Chine. Les équipes de cybersécurité de CrowdStrike en ont baptisé certains de noms de pandas : l'APT2, qui cache sans doute l'Unité militaire 61 486, spécialisée dans le renseignement spatial, est surnommé « Putter Panda » ; l'APT3, « Gothic Panda » ; l'APT10, « Stone Panda ». *« Ils mêlent souvent des activités de cybercriminalité pour gagner de l'argent, de pillage technologique et de cyberespionnage, pour le compte de l'armée ou du ministère de la Sécurité d'État. Tout cela constitue une vaste nébuleuse de cyberacteurs, qu'il est difficile de cerner »*, explique Paul Charon.

MI-ESCROCS, MI-ESPIONS

Des hackers du groupe APT10 sont, par exemple, soupçonnés par la justice américaine d'avoir pillé, entre 2006 et 2018, plus de 45 entreprises dans une douzaine de pays, ainsi que les données de 100 000 marins de l'US Navy. Selon la société de cybersécurité FireEye, le groupe APT40 multiplie, pour sa part, les opérations visant à *« accélérer la modernisation »* de la flotte militaire chinoise, tout en espionnant les pays d'Asie du Sud-Est. Le groupe APT41, sans doute lié au Guoanbu, serait, →

Policiers contre des opposants à la nouvelle loi sur la sécurité, défilant à Hongkong le 1er juillet 2020.

SOPA IMAGES/LIGHTROCKET VIA GETTYIMAGES

DES OPÉRATIONS SUR LES RÉSEAUX SOCIAUX ONT DÉBUTÉ EN 2017 CONTRE LES MANIFESTANTS À HONGKONG

quant à lui, composé de « mi-escrocs, mi-espions », qui exploitent des logiciels de rançonnage dans le secteur des jeux vidéo et surveillent des dissidents. Il aurait été à l'origine d'attaques en série, entre janvier et mars 2020, touchant notamment les routeurs de Cisco et 75 entreprises et organisations dans le monde.

Les espions chinois peuvent aussi employer des profils plus variés. Dans une note récente, datée du 22 juin, le département de la Justice américaine détaille une liste des 46 affaires, en cours depuis 2018, ayant pu profiter à l'État chinois, lesquelles représentent 80 % des dossiers d'espionnage économique recensés par ce ministère. Les poursuites judiciaires concernent notamment le géant Huwaei, ainsi que des hackers de divers APT. Elles visent aussi des employés malveillants de sociétés américaines, des anciens officiers de la CIA retournés, des chercheurs de prestigieuses universités suspectés d'avoir caché leurs liens avec des Chinois, des stagiaires travaillant pour le Guoanbu pris en flagrant délit ou des militaires chinois déguisés en faux étudiants.

En complément de ces actes d'espionnage, la Chine s'est également lancée plus récemment, à l'instar des Russes, dans des opérations de désinformation sur internet, voire d'ingérence dans les pays considérés comme hostiles. *« Le régime chinois veut occuper une place centrale sur l'échiquier mondial et exporter son modèle politique, jugé supérieur aux valeurs démocratiques occidentales. C'est pourquoi il est devenu plus offensif sur le terrain de la communication »*, estime Jean-Pierre Cabestan, professeur à l'Université baptiste de Hongkong, auteur du livre *Demain la Chine : démocratie ou dictature ?* (Gallimard). Plusieurs organes du PCC, dont le département du Travail du Front uni et celui des Liaisons internationales, orchestrent cette propagande en faveur de la *« zhongguo fang'an »*, la « solution chinoise ». Elle est relayée par les médias officiels, des services de « guerre psychologique » de l'armée, des pirates « patriotes » et des « armées de trolls », autrement dit des agences digitales spécialisées.

FAUX COMPTES TWITTER

Les manipulations ont démarré avec l'apparition de faux comptes sur les réseaux sociaux. *« Nous avons pu identifier une opération ciblant les opposants à Hongkong et la diaspora chinoise qui a commencé en avril 2017 sur Twitter »*, relève Jacob Wallis, coauteur d'études de l'Aspi sur le sujet. Durant l'été 2019, Google bloque 210 chaînes de sa filiale YouTube soupçonnées d'intoxication depuis la Chine, tandis que Facebook et Twitter suspendent plus de 200 000 comptes suspects. Pékin dément toute implication. D'autres campagnes massives →

Des campagnes d'intox ont visé Taïwan avant l'élection présidentielle de Tsai Ing-wen, réélue le 11 janvier 2020.

ACCUSÉE DE MENSONGES SUR LE COVID-19, LA CHINE CONTRE-ATTAQUE PAR DES FAKE NEWS

se déroulent fin 2019, à Taïwan, pour déstabiliser le régime anticommuniste, juste avant l'élection présidentielle, qui voit pourtant la réélection de la nationaliste Tsai Ing-wen.

Ces déconvenues ne freinent pas les services chinois. Déstabilisé par l'apparition sur son sol du coronavirus en décembre 2019 et par les accusations de mensonges sur la genèse de la contamination à Wuhan et sur la gravité de la situation, Pékin organise une contre-attaque. *« La pandémie a provoqué une crise politique pour le Parti communiste chinois, laquelle menace son pouvoir, tant à l'intérieur qu'à l'étranger. Il y a répondu en lançant des vagues de désinformation visant à étouffer les critiques de la communauté internationale »*, explique Jacob Wallis. Les médias officiels chinois en anglais diffusent la version d'une épidémie vite enrayée grâce à des mesures strictes de confinement. *« L'objectif est de montrer l'exemplarité de la réponse chinoise et, à l'inverse, de discréditer les démocraties »,* estime Antoine Bondaz, chercheur à la Fondation pour la recherche stratégique et enseignant à Sciences-Po Paris. Des tweets relaient massivement des images montrant la propreté des rues chinoises ou l'envoi d'aide médicale à certains pays européens, →

COURSE AUX VACCINS : NOUVELLE GUERRE SECRÈTE

Alors que le Covid-19 continue ses ravages planétaires, une nouvelle bataille s'est ouverte : la course aux vaccins. Désireux de prendre de l'avance, les Chinois ont commencé à tester cinq prototypes, alors qu'une centaine de laboratoires dans le monde planchent concurremment sur le sujet. Dans cette rivalité, tous les coups sont permis. Depuis plusieurs années, la santé et la biologie font partie des priorités industrielles de la Chine, qui est déjà devenue première productrice mondiale des principes actifs nécessaires aux médicaments. Pour monter en gamme, elle accueille à bras ouverts les grandes firmes pharmaceutiques internationales. Elle a aussi noué des accords avec des grandes universités américaines, des centres de recherches et des start-up. *« Il y a des risques que des données sur les patients américains et les essais thérapeutiques puissent tomber entre les mains de groupes publics ou privés chinois et qu'ils en tirent avantage »,* ont dénoncé des *congressmen* dans un rapport en novembre 2019, appelant à une plus grande vigilance. Depuis deux ans, les signaux se sont aussi multipliés concernant des cyberattaques dans le monde de la recherche et des hôpitaux. Des hackers liés à la Chine sont suspectés d'avoir dérobé, en juillet 2018, les données de 1,5 million de malades au sein de l'établissement singapourien SingHealth. Un centre américain sur le cancer a été visé par des pirates liés à la Chine en avril 2019. Le laboratoire Gilead, basé en Californie, en pointe dans la lutte contre le Covid-19, a subi un raid numérique au printemps. Plusieurs autres organismes de santé ont aussi été ciblés aux États-Unis, en Thaïlande, en République tchèque, au Royaume-Uni, en Espagne et en France, où les serveurs de l'AP-HP ont été frappés le 22 mars. Début avril, Interpol a lancé un message sur le sujet, évoquant une « hausse significative » de cyberattaques contre les hôpitaux, surtout à des fins de criminalité financière. Mais les hackers peuvent avoir d'autres objectifs. Le 11 mai, le département de la Sécurité intérieure américaine et le Centre national de cybersécurité britannique ont émis une alerte conjointe pour protéger les travaux scientifiques autour du Covid-19. Quelques jours plus tard, le FBI et l'agence de cybersécurité et de sécurité des infrastructures (Cisa) américaine ont prévenu les hôpitaux, les centres de recherche et les firmes pharmaceutiques qu'ils étaient ciblés par la Chine. L'heure est à la prudence dans les labos !

V. J.

SAM YEH/AFP ; CHINE NOUVELLE/SIPA

L'ambassadeur de Chine en France, Lu Shaye (à droite), fait un don de masques à un étudiant chinois à Paris, le 2 avril 2020.

Le porte-parole du ministère chinois des Affaires étrangères a relayé sur Twitter, le 13 mars 2020, des théories complotistes antiaméricaines (voir ci-dessous).

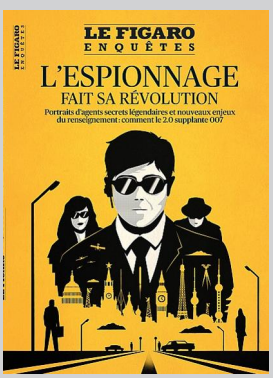
« Cet article est très important pour chacun d'entre nous. Veuillez le lire et le retweeter. COVID-19 : preuve supplémentaire que le virus est originaire des États-Unis. »

PÉKIN VEUT MONTRER L'EXEMPLARITÉ DU MODÈLE CHINOIS ET DISCRÉDITER LES DÉMOCRATIES

comme l'Italie. Problème : selon plusieurs experts de cybersécurité, nombre de ces tweets proviennent de faux comptes. Les diplomates diffusent également les « narratifs » chinois, parfois jusqu'au dérapage, notamment lorsque l'ambassadeur de Chine à Paris, Lu Shaye, fustige publiquement, en pleine épidémie, les soignants des maisons de retraite françaises qui auraient *« laissé mourir leurs pensionnaires de faim et de maladie »*.

Sous pression, Pékin affirme lutter contre la « désinformation » occidentale. Le régime tente surtout de détourner l'attention, en n'hésitant pas à propager des théories complotistes : le 13 mars, le porte-parole du ministère des Affaires étrangères, Zhao Lijian, évoque sur son compte Twitter une rumeur selon laquelle le Covid-19 serait issu d'un laboratoire militaire américain, en s'appuyant sur un article du site canadien GlobalResearch.ca. Curieusement, l'auteur de cet article, un certain Larry Romanoff, qui se présente comme un businessman à la retraite vivant à Shanghaï, est invisible. Il a commencé à écrire des analyses – plutôt prochinoises – en septembre 2019 et s'est interrompu le 10 avril 2020. *« Il s'agissait probablement d'un faux blogueur créé de toutes pièces par les Chinois pour faire écho à leurs messages »,* avance Antoine Blondaz. De nouvelles vagues de fake news continuent d'inonder les réseaux sociaux occidentaux, notamment pour créer une panique sanitaire aux États-Unis, conduisant Twitter à annoncer, le 12 juin, la fermeture de 23 750 comptes suspectés de « liens » avec l'État chinois.

Au risque de froisser temporairement les opinions publiques à l'étranger, la Chine veut reprendre la main à tout prix. Sur le terrain de l'image, comme sur le plan économique, par exemple en se lançant dans la course aux vaccins (voir encadré). *« La crise du Covid-19 n'est que la préfiguration de ce que les Chinois sont capables de faire. Ils vont vraisemblablement continuer à grande échelle »,* conclut Paul Charon. Cette guerre froide ne fait que commencer. ■ ***Vincent Nouzille***



"LE FIGARO ENQUÊTES"

Un nouveau numéro de la série « Le Figaro Enquêtes », consacré à l'espionnage, sera disponible en kiosque le 3 août prochain.

CARLOS GARCIA RAWLINS/REUTERS