

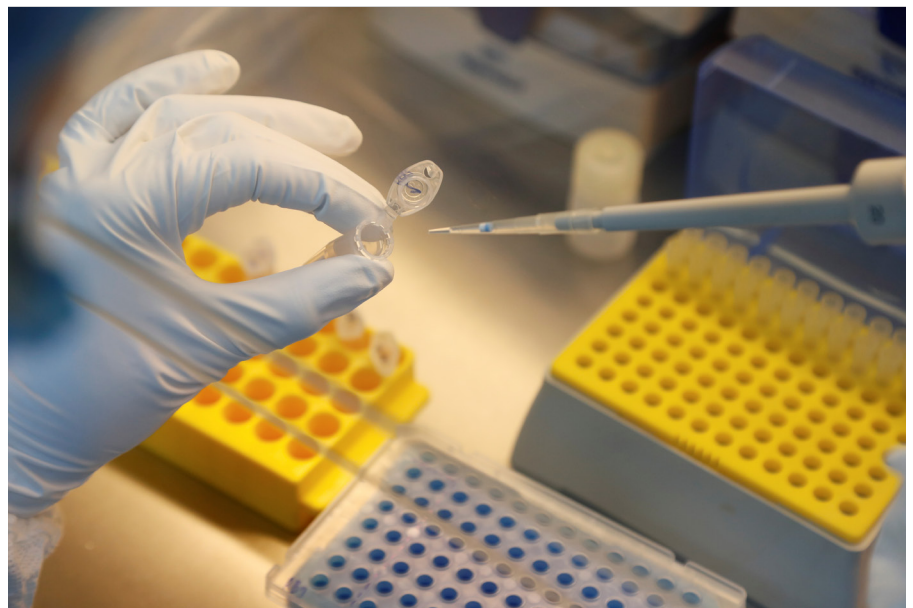
Les vaccins, champ de bataille de l'information

Le développement rapide d'un vaccin est devenu un nouveau critère de réussite dans la lutte contre le coronavirus. Plus que jamais, cette phase de la pandémie sera façonnée par l'information, avec des conséquences positives et d'autres plus néfastes. De fait, si cet élan élargit le champ des connaissances sur les vaccins, il s'accompagne de tentatives d'influence concernant leur sécurité et leur efficacité.

Par Jakob Bund et
Ann-Sophie Leonard

Après diverses mesures de confinement, les gouvernements du monde entier sont confrontés à de grandes attentes en matière de reprise économique et de retour à la vie sociale. Or, ces attentes dépendent fortement de la disponibilité d'un vaccin qui fonctionne contre les infections au COVID-19. Les questions concernant l'accès à un vaccin efficace en quantité suffisante ont intensifié la concurrence, les différents gouvernements cherchant à conclure des accords avec les organisations porteuses de projets de vaccin prometteurs.

Cette concurrence pourrait favoriser davantage la désinformation sur les efforts déployés par certains gouvernements dans le but de répondre aux attentes de la population, d'exploiter les sentiments de peur et d'incertitude, de prendre un avantage dans la recherche sur le vaccin et d'influencer positivement l'opinion publique en montrant qu'un État s'établit en partie prenante responsable. Dans ce contexte, le haut représentant de l'UE pour les affaires étrangères et la politique de sécurité Josep Borrell a mis en garde contre une «bataille mondiale des récits», certains gouvernements se livrant activement à la désinformation dans le but d'entacher la crédibilité d'autres États. La désinformation sur les origines de la pandémie de coronavirus, sa diffusion et les moyens de s'en protéger a également créé les conditions d'une «info-



Le développement, la production et la distribution de vaccins font de plus en plus l'objet de campagnes de désinformation et de concurrence géopolitique. Anton Vaganov / Reuters

démie» qui risque de discréditer les recommandations officielles en matière de santé.

Dans ce climat, la Russie a été le premier pays à autoriser un vaccin contre le coronavirus le 11 août. Pourtant, la troisième phase critique des essais cliniques, qui consiste à tester le vaccin sur un plus grand groupe de volontaires en intégrant un groupe témoin, ne devait commencer que le lendemain du jour où l'agrément a été

donné. Or cette troisième phase apporte des informations essentielles sur l'efficacité et la sécurité d'un candidat-vaccin. En recevant l'agrément des pouvoirs publics avant la fin des essais cliniques, le premier vaccin autorisé au monde a ouvert la porte au débat sur son efficacité.

Le PDG du Fonds russe d'investissement direct, qui a financé le développement du vaccin, a également déclaré avoir été la

cible d'«attaques informationnelles» et évoqué des pressions externes exercées sur des partenaires potentiels afin qu'ils ne participent pas. Ces dynamiques placent les questions relatives au développement, à la production et à la distribution d'un vaccin au cœur d'une mission d'une triple complexité: gérer la pandémie, relever le défi de l'information et intégrer les intérêts géopolitiques concurrents à plus vaste échelle.

Une infodémie autour de la pandémie

La pandémie venue de Chine a créé de nouvelles pressions, mais aussi de nouvelles opportunités. Depuis le début de la crise, les entreprises de la Chine sont motivées par ses ambitions de dissimuler l'étendue de l'épidémie initiale dans le pays, d'obtenir l'avantage du premier entrant sur le marché des équipements de protection et se présenter en partie prenante responsable. La Russie a également profité de l'occasion pour essayer de promouvoir la façon dont elle a géré la crise et apporté son aide à l'échelle internationale, de dénigrer les efforts déployés par d'autres pays pour répondre à la crise et de semer le doute sur l'origine de la pandémie de coronavirus.

Nombre de ces motivations, qui ont donné lieu à des tentatives de désinformation lors des différentes phases de la pandémie, convergent vers la question de la mise au point et de la distribution du vaccin. Les principaux objectifs de ces États sont de mettre en avant leurs efforts pour apporter

Le vaccin contre le coronavirus constitue un sujet facile à exploiter pour les campagnes d'information.

de l'aide, de dénigrer les actions des autres pays et de s'assurer l'accès aux moyens de protection – en particulier, à ce stade, aux candidats-vaccins prometteurs.

Le vaccin contre le coronavirus constitue un sujet facile à exploiter pour les campagnes d'information. Les découvertes scientifiques sur l'efficacité des candidats-vaccins restent pour l'instant limitées. Compte tenu de l'urgence de la situation, l'avancement des recherches est de plus en plus souvent communiqué à travers la presse, et non via les publications médicales traditionnelles, ce qui permet d'éviter les processus d'examen par des experts indépendants qui vérifient les informations avant leur diffusion à un public non averti. De par leur nature confidentielle, les ac-

L'infodémie: une maladie qui se propage en ligne

En Europe continentale, l'Italie compte parmi les pays les plus durement touchés par le coronavirus. La hausse rapide des infections sur son territoire a également créé des **défis dans l'espace informationnel**. La Chine a mené une campagne coordonnée de messages sur les réseaux sociaux et de diplomatie publique ciblant spécifiquement la population italienne. Les responsables et les médias d'État chinois ont mis en avant la fourniture de masques par la Chine en opposant ce soutien à l'aide européenne et américaine, initialement lente et discrète. L'un des objectifs était probablement de **modifier l'image** de la Chine dans **l'opinion publique** en remplaçant l'idée qu'elle était le point d'origine du virus par celle selon laquelle le pays serait un partenaire fiable en temps de crise. Les sondages réalisés par l'institut italien SWG montrent un **changement des attitudes**. En mars 2020, 52 pour cent des personnes interrogées considéraient la Chine comme «amicale», contre 10 pour cent seulement en janvier.

En mars, une déclaration de Bill Gates est devenue virale sur les réseaux sociaux. **D'authentiques propos** du milliardaire sur l'utilisation de «certificats numériques» pour les tests de dépistage du coronavirus ont été **délibérément détournés** pour évoquer un projet à grande échelle d'implantation de microprocesseurs traçables lors d'injections médicales ou dentaires. Un sondage réalisé par Yahoo News/YouGov révèle qu'aux États-Unis, 44 pour cent des républicains pensent que ce soi-disant projet de microprocesseurs est vrai. Des données recueillies par la société d'analyse des médias Signal indiquent que les fausses informations de ce type autour de Bill Gates et du coronavirus sont la théorie du complot la plus prolifique avec 1,2 million de mentions sur les réseaux sociaux et dans les émissions de télévision entre février et avril. En **amplifiant les convictions préexistantes** de militants antivaccins, de telles controverses qui tentent d'influencer les opinions sur les mesures de protection et les décisions médicales risquent d'avoir des conséquences sur la santé humaine. Profiter des positions polarisées sur la vaccination constitue, de fait, un **moyen peu coûteux de faire circuler la désinformation**.

cords d'achat anticipé et les échanges entre les gouvernements et les laboratoires pharmaceutiques sur cette question constituent également un aspect sensible.

Peu de moyens contre l'infodémie

Le scepticisme fondamental à l'égard des vaccins et les soupçons de collusion entre les gouvernements et les grands laboratoires pharmaceutiques, mobilisés par des groupes relativement restreints mais bien organisés, datent de bien avant le coronavirus. Ces groupes tentent de tirer parti des facteurs que nous venons d'évoquer pour élargir leur base, indépendamment des efforts que peuvent déployer certains acteurs étatiques pour les instrumentaliser à des fins ultérieures.

La concurrence entre les États autour du développement, de l'acquisition et de la distribution du vaccin agit comme un accélérateur des initiatives de désinformation déjà observées. Ils sont étroitement liés aux facteurs stratégiques qui ont alimenté les campagnes de désinformation dans le contexte de la pandémie. L'arrivée de différents vaccins renforcera ces facteurs et aiguïsera encore les tentatives d'influence. Les discours s'inscriront certainement dans la perspective d'améliorer l'accès des gouvernements à des vaccins efficaces et de promouvoir les efforts pour lutter contre la pandémie et fournir une assistance interna-

tionale, même si cette assistance peut présenter des risques pour la santé, comme ce fut le cas avec les équipements de protection déficients donnés ou vendus par certains fournisseurs chinois.

De telles dynamiques risquent d'accentuer les tensions géopolitiques, ce qui pourrait lever les obstacles aux tactiques de désinformation plus pernicieuses ayant pour but de discréditer les efforts d'autres pays pour mettre au point un vaccin, ainsi que leurs accords de réservation. Tant que ces conditions perdureront, tout vaccin susceptible de contenir dans une certaine mesure la pandémie ne sera guère efficace pour endiguer les campagnes d'information qui prétendent le contraire.

Des vaccins à tout prix

Les gouvernements du monde entier ont mobilisé des moyens financiers impressionnants pour soutenir la mise au point d'un vaccin. Les institutions destinataires de ces fonds sont devenues la cible privilégiée de tentatives illicites pour acquérir les informations et le savoir-faire qu'elles ont développés. Un certain nombre d'opérations de cyberespionnage ont déjà été observées. En mai 2020, l'Agence de cybersécurité et de sécurité des infrastructures des États-Unis et le Centre national de cybersécurité du Royaume-Uni ont lancé une alerte commune contre les agissements d'acteurs de pointe, soutenus par certains États, ciblant les organismes de santé, les

laboratoires pharmaceutiques, les instituts universitaires et les centres de recherche médicale qui participent à la recherche sur le coronavirus. Au cours du même mois, les réseaux soutenant les superordinateurs de la Suisse et du Royaume-Uni utilisés pour la recherche sur le coronavirus ont été temporairement mis à l'arrêt pour lutter contre des intrusions.

Un rapport interne présenté en avril au ministère chinois de la Sécurité d'État a indiqué que l'hostilité internationale envers la Chine atteignait un niveau inégalé depuis la répression des manifestations de la place Tiananmen en 1989. À noter que cette étude a été réalisée avant la promulgation de la loi sur la sécurité nationale de Hong Kong. Cette lecture de la réputation de la Chine dans le monde montre à quel point le développement et la distribution d'un vaccin pourraient lui offrir une chance de redorer son blason.

D'après les conclusions de la police fédérale américaine (FBI), ces enjeux croissants ont poussé la Chine à entreprendre des actions visant à compromettre les organismes de santé, les laboratoires pharmaceutiques et les instituts universitaires des États-Unis qui mènent des recherches essentielles sur le coronavirus. Le ministère de la Justice des États-Unis a étayé ces affirmations en dévoilant en juillet l'inculpation de deux entrepreneurs chinois qui se sont avérés travailler pour le ministère de la Sécurité d'État de leur pays. Parmi d'autres accusations de cyberespionnage économique contre des cibles industrielles à forte valeur dans onze pays, l'acte évoque des préparatifs pour pénétrer dans les réseaux informatiques d'entreprises participant à la mise au point d'un vaccin, de technologies de dépistage et de traitements contre le coronavirus.

Outre des informations sur les recherches menées, ces intrusions peuvent également

Les campagnes de désinformation peuvent chercher à renforcer délibérément des idées préconçues.

avoir pour but de recueillir des éléments compromettants susceptibles d'être exploités dans le cadre de campagnes de désinformation. Il peut notamment s'agir d'interactions entre les entités qui développent les vaccins et les États, lorsque ces interactions sont contraires aux engagements publics pris par certains gouvernements. Les

La place de la Suisse dans les enchères au vaccin

Les efforts de la Suisse pour mettre au point et acquérir un vaccin s'articulent autour de la *task force* de santé publique sur le vaccin contre le Covid-19. L'Office fédéral de la santé publique a annoncé des accords avec l'entreprise américaine de biotechnologies Moderna et la société suisse Molecular Partners concernant des options sur les futurs stocks de vaccin contre le coronavirus à hauteur de 4,5 millions et 3,2 millions de doses, respectivement. Ce dernier accord **assure à la Suisse le premier accès** aux doses du programme anti-COVID-19 DARPin(R), une technologie développée à l'Université de Zurich. Selon les dernières informations, Moderna prévoit de fabriquer les principes pharmaceutiques actifs de son vaccin en Suisse. Cela pourrait élargir les vulnérabilités à de **possibles opérations de *hack and leak* en Suisse**, avec les **campagnes de désinformation** qui en découlent. Les organisations qui ne sont pas seulement impliquées dans la recherche de candidats-vaccins, mais également dans leur production, pourraient devenir des cibles intéressantes pour les tentatives d'acquisition illicite d'informations et de savoir-faire développés dans ces institutions, ainsi que de détails confidentiels sur leurs interactions avec les gouvernements. La Suisse a la chance d'abriter des sociétés de biotechnologies de premier plan et d'excellentes infrastructures de recherche et d'innovation scientifiques. Par conséquent, il est d'autant plus **important de sécuriser l'épine dorsale électronique et numérique** de ces institutions et activités critiques. La menace d'opérations de *hack and leak* démontre la nécessité d'intégrer dans cette préparation des mesures efficaces d'atténuation de la désinformation.

preuves de ces contradictions apparentes pourraient également être contrefaites et intégrées dans la fuite d'un plus grand ensemble de documents authentiques.

Comprendre les vulnérabilités

Les défis croissants liés à l'information viennent s'ajouter à la difficile gestion de la pandémie. L'impact des campagnes de désinformation reste particulièrement difficile à évaluer. Un aspect mérite d'être exploré dans ce contexte: l'utilisation de conversations à forte charge émotionnelle ou politique, ou «discours amorcés», via des tactiques de piratage informatique suivi de fuites (*hack and leak*).

Dans l'une des rares études d'impact empiriques existantes, les chercheurs du Annenberg Public Policy Center de l'Université de Pennsylvanie ont montré les effets isolés d'opérations de *hack and leak* visant à tirer parti de certains sujets de controverse connus lors de la campagne présidentielle américaine de 2016. D'après leurs conclusions, la publication stratégique d'extraits de discours prononcés à huis clos par Hillary Clinton, obtenus illégalement, a influé sur la façon dont les animateurs ont formulé leurs questions lors des débats suivants de la présidentielle et, par conséquent, sur les préférences des électeurs qui ont regardé les débats.

Si ces fuites ont pris une telle importance, c'est parce que, sans contexte complet, les passages sélectionnés semblaient valider les préoccupations qui avaient dominé les débats avec Bernie Sanders, opposant de

Clinton lors des primaires du parti démocrate, cherchant ainsi à saper sa base démocrate. Les chercheurs du Centre Annenberg décrivent ces extraits diffusés comme des «discours amorcés» car ils sont marqués par des positions polarisées et offrent ainsi des moyens peu coûteux d'exploiter des sentiments préexistants à des fins de désinformation. En mettant en avant des faits ciblés (présupposés ou sélectifs) qui concordent avec ces discours, les campagnes de désinformation peuvent chercher à renforcer délibérément des idées préconçues en vue d'atteindre leurs fins.

Les débats autour des vaccins sont depuis longtemps marqués par de profondes divisions (voir encadré p.2). Les discours offrent une multitude de sources de désinformation qui peuvent être exploitées par des acteurs étatiques, y compris en introduisant des informations authentiques dans des échanges déjà polarisés – soit en diffusant de façon sélective des informations obtenues illégalement, soit en exploitant le sentiment que ces informations ont été volontairement gardées confidentielles pour dissimuler de prétendus méfaits.

La fuite de documents internes, même s'ils ont été acquis par des moyens illicites, tend à créer l'idée que le public a un intérêt légitime à connaître les informations qu'ils révèlent et donc que les médias doivent relayer ces fuites afin d'informer le public. Cependant, tous les auteurs de fuites n'ont pas le profil du lanceur d'alerte. Dans le cas des discours piratés d'Hillary Clinton, l'objectif final de l'opération (influencer les opinions et les décisions en vue d'atteindre un certain résultat) n'est pas du tout en

accord avec l'ambition générale des médias de fournir au public une information impartiale. En outre, l'authenticité présumée de documents internes ou d'échanges privilégiés peut servir de couverture pour introduire de subtiles contrefaçons dans une précieuse collection de documents ayant fait l'objet de fuites.

Or les opérations actuelles d'espionnage dans le cadre du vaccin contre le coronavirus posent des problèmes qui vont au-delà de la possible interruption d'expériences sensibles ou de la perte de précieux actifs de propriété intellectuelle. Les évolutions possibles dans ce sens soulignent le rôle des intérêts géopolitiques dans l'espionnage des activités de recherche d'un vaccin, ces intérêts étant en eux-mêmes susceptibles d'alimenter les tensions.

La Suisse abrite plusieurs centres de pointe en matière de recherche sur les vaccins et un certain nombre d'initiatives internationales qui appuient ces efforts, notamment l'alliance du vaccin Gavi mise en place avec l'aide financière de la Fondation Gates (voir encadré p. 3). Sans être forcément la cible directe d'éventuelles opérations de *hack and leak*, la Suisse et d'autres pays neutres pourraient se trouver impliqués dans de telles actions du fait de leur rôle de médiateurs.

Tempête dans une poupée gigogne

Il est important de noter que, à ce jour, aucune opération de *hack and leak* n'a été publiquement observée dans le contexte du vaccin contre le coronavirus. Toute évolution marquerait toutefois une escalade significative. Un rapport d'enquête de juillet 2020 a révélé que l'Agence centrale du renseignement (CIA) des États-Unis s'était

vu attribuer en 2018 des pouvoirs supplémentaires pour entreprendre des opérations de *hack and leak* sans autorisation présidentielle préalable. S'écartant des pratiques antérieures, le décret présidentiel accordant ces pouvoirs mettait l'accent sur le développement des capacités en tant que telles, et non sur un objectif stratégique global à atteindre.

Le décret présidentiel désigne en particulier l'Iran, la Russie, la Chine et la Corée du Nord comme les cibles potentielles des

Cette pandémie s'accompagne d'une infodémie nourrie par la concurrence géopolitique.

opérations menées en vertu de ces nouveaux pouvoirs. La Russie et la Chine ont été mises en cause pour avoir tenté de pirater des activités de recherche sur les vaccins, ce qui leur aurait également permis de recueillir des éléments compromettants.

La mise au pilori des acteurs engagés dans des opérations de cyberespionnage et de vol de propriété intellectuelle peut cependant avoir pour effet secondaire involontaire de conférer une certaine crédibilité aux futures opérations d'influence. Des acteurs pourraient profiter du fait que des violations précédentes de ces organisations aient été rendues publiques pour divulguer des informations (soi-disant) authentiques qui proviendraient de ces organisations.

La révélation du mandat accordé à la CIA pour réaliser des activités de *hack and leak* coïncide avec une phase cruciale. Toute normalisation perçue de telles opérations pourrait réduire les inquiétudes quant à leurs conséquences – inquiétudes qui contribueraient normalement à modérer ce type d'activités malveillantes.

En ce qui concerne l'adoption plus large de tactiques de *hack and leak*, il est utile de rappeler que les efforts présumés de la Russie pour interférer dans la période préélectorale de 2016 aux États-Unis trouvent leur contrepartie dans des accusations précédemment portées par la Russie à l'encontre des États-Unis. L'atmosphère polarisée qui entoure les prochaines élections de 2020 pourrait ajouter une couche aux efforts de désinformation axés sur des récits concurrents. Si les mesures pour atténuer efficacement la pandémie actuelle restent contestées, l'aide apportée par un vaccin pourrait également entraîner des dommages collatéraux.

Dans ce contexte, toute tentative de lutte contre des campagnes coordonnées de désinformation sur le vaccin doit intégrer le fait que cette pandémie s'accompagne d'une infodémie nourrie par la concurrence géopolitique. Pour désamorcer les tentatives de désinformation, il faudra en acquérir une solide compréhension sur trois tableaux, à savoir la gestion de la pandémie, les défis croissants liés à l'information et la concurrence géopolitique, ainsi que leurs interactions.

Voir le [site thématique du CSS](#) pour en savoir plus sur les implications du coronavirus sur la politique de sécurité.

Jakob Bund est responsable de projet pour la cyberdéfense au sein de l'équipe «Risk and Resilience» au Center for Security Studies (CSS) à l'ETH de Zurich.

Ann-Sophie Leonard est chercheuse invitée au Center for Security Studies (CSS) à l'ETH de Zurich dans le cadre d'un «Mercator Fellowship» sur les affaires internationales.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'EPF de Zurich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Éditeurs: Julian Kamasa
Révision linguistique: Henrik Larsen, Névine Schepers
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

Le dilemme de l'OMS dans la lutte contre les épidémies No 268
Coronavirus: une arme à double tranchant pour la Chine No 267
Virus dans le système russe No 266
Intelligence artificielle et cybersécurité No 265
Technologies numériques et la crise du coronavirus No 264
Les Balkans occidentaux entre nouvelles dépendances No 263

© 2020 Center for Security Studies (CSS), ETH Zurich
ISSN: 2296-0228; DOI: 10.3929/ethz-b-000432875