Introduction

Le cyberespace est composé de plusieurs strates différentes et essentielles dans le fonctionnement d'un réseau interconnecté et fonctionnel. Les strates physiques, logicielles et informationnelles, bien que formant le corps fonctionnel, soulèvent peu l'intérêt du champ politique. C'est, au contraire, la strate sociale qui concerne et intéresse particulièrement les politiques et les politologues. Cette couche inclut l'ensemble des comportements individuels en interaction avec le cyberespace et une composante collective qui touchent les politiques, les institutions, les lois, les normes, régulant et encadrant les interactions et l'utilisation du cyberespace. Ainsi, bien que les cybercriminels puissent s'intéresser aux failles dans les logiciels ou dans les systèmes physiques pour commettre leurs crimes, le caractère social présente aussi de possibles failles qui peuvent être identifiées et utilisées par les cybercriminels. En effet, étant donné que chaque utilisateur est responsable de ses actions dans le cyberespace et que ses pratiques en matière de cybersécurité nsont e pas toujours appropriées ou suffisantes, il est à la fois une victime potentielle et une porte d'entrée vers les systèmes. Ces derniers sont donc plus vulnérables, à partir du moment où un utilisateur a un comportement non sécuritaire.

Le cyberespace, par son caractère supranational, est difficile à gouverner et à sécuriser. Compte tenu de la quantité d'informations qui transitent sur les réseaux à chaque instant, superviser et contrôler les informations et les transactions, vérifier la légitimité et la légalité des contenus, traiter dans des délais raisonnables les plaintes ou rapports d'incidents sont autant de défis pour les organes de surveillance gouvernementaux, industriels, publics ou privés. Les phases de détection et de rétablissement peuvent être affectées par ces limites capacitaires, rendant les systèmes non opérationnels, ou les exposant à des risques multiples.

Introduction rédigée par Daniel VENTRE et Hugo LOISEAU.

La sécurité et la protection des réseaux sont déterminées comme des responsabilités partagées entre les agences de sécurité et de police, les gouvernements, les entreprises, les organisations ainsi que les individus. Plusieurs changements sociaux se sont donc opérés dans les dernières années, avec l'augmentation de la dépendance et du recours au cyberespace, les politiques et la surveillance ne suivant pas toujours la vitesse des avancées de cet espace. Cela est d'autant plus vrai en cas de crise comme celle qu'ont connue tous les États du monde avec la pandémie du SARS-CoV-2 (ou Covid-19) en 2020.

Or, durant cette crise sanitaire, les cyberrisques et les cybermenaces ont, semble-t-il, augmenté. Le cyberrisque, c'est le produit du niveau de menace et du niveau de vulnérabilité. Alors que le cyberrisque détermine la probabilité de réussite d'une cyberattaque [SAN 22], la cybermenace représente un potentiel de violation de la sécurité qui existe lorsqu'il y a une circonstance, une capacité, une action ou un événement qui pourrait violer la sécurité et causer un préjudice [SAN 22]. Ces deux notions sont fondamentales, car la cybernétisation qu'ont vécue les sociétés durant les vingt dernières années a contribué largement à la complexification des enjeux de cybersécurité. Beck l'annonçait déjà en 2001, en affirmant que « la production sociale de richesses est systématiquement corrélée à la production sociale de risques » [BEC 01, p. 36]. La pandémie du SARS-CoV-2 en 2020 et la crise multidimensionnelle (sociale, économique, politique, etc.) qui s'en est suivie représentent une fenêtre contextuelle illustrant parfaitement la société du risque dont parle Beck, caractérisée par la multiplication et la diffusion de risques systémiques et transversaux issus des développements technologiques et industriels. La mondialisation et l'expansion du cyberespace accroissent ces risques [BEC 01]. Durant cette période, la cybercriminalité a évolué dans un contexte de mondialisation et de cybernétisation.

Les recherches sur la cybercriminalité s'intéressent principalement à deux grandes catégories de criminalité :

– le cybercrime organisé, les cyberattaques de grande ampleur, qui pourraient s'inscrire dans le cadre plus général de l'étude de la grande criminalité. Jean-François Gayraud propose quatre grandes caractéristiques « des grandes criminalités » :

- la grande criminalité se manifeste tout d'abord par la polycriminalité. Les grands groupes criminels sont opportunistes et pragmatiques dans les marchés criminels puisqu'ils ne développent pas nécessairement de spécialisation dans leurs pratiques criminelles ;

- ces groupes sont territorialisés, car enracinés dans un espace qui leur permet de créer leur propre biotope, c'est-à-dire des enclaves hermétiques aux pouvoirs publics. Cela favorise leur expansion territorialisée et immatérielle dans le cyberespace ;

- ces groupes et organisations sont qualifiés d'insubmersibles. Ils sont, en effet, adaptatifs aux changements socioéconomiques et résistants à la répression des pouvoirs publics ou à la concurrence des autres groupes criminels ;

- enfin, ces groupes ont des impacts macroéconomiques majeurs puisqu'ils gèrent des flux financiers massifs, mondialisés et interconnectés qui facilitent et favorisent la corruption et le blanchiment de leurs revenus illicites [GAY 21] ;

– la cybercriminalité et son étude ne concernent pas uniquement le crime organisé, mais comprend aussi des actes d'une criminalité quotidienne, voire ordinaire, comme la diffamation en ligne, l'extrémisme violent et les discours haineux proférés sur Internet et les médias sociaux [BEN 22], la radicalisation [ALA 21], la désinformation [PAR 20], etc., qui sont des formes courantes du cybercrime.

Les grands groupes criminels et la cybercriminalité ordinaire participent de façon importante à ce qui peut être nommé le « fond diffus criminologique », qui est omniprésent et constant dans le cyberespace et est à la base de nombreuses pratiques illicites qui intéressent la cybersécurité [BRE 10]. De ce fait, la cybercriminalité profite d'un marché immense composé de l'offre (logiciels, services, techniques qui sont disponibles dans le cyberespace) et d'une demande de la part des organisations criminelles ou non, des États et des particuliers dans le but d'échanger un bien (des données) au moyen d'une monnaie de plus en plus dématérialisée et fongible : la cryptomonnaie [BAD 20]. L'agrégation de ces caractéristiques a facilité la cybercriminalité, mais qu'en est-il du contexte de crise en 2020 ?

Le contexte

La pandémie, sa gestion, ses effets

L'épidémie de SARS-CoV-2 est apparue fin 2019, les premiers cas étant enregistrés en Chine, puis en Thaïlande. Rapidement, la Chine a mis en place des mesures pour tenter de contenir l'épidémie : confinement des populations à Wuhan, construction d'hôpitaux de campagne dont le monde entier pouvait suivre la progression en direct *via* des webcams connectées en permanence sur le chantier. Rapidement, de nombreux cas et victimes ont été identifiés en divers points du globe. L'OMS a annoncé officiellement l'apparition de cette nouvelle maladie le 30 janvier 2020 et l'a déclarée pandémie mondiale le 11 mars 2020. Dès lors, plusieurs États dans le monde ont décidé de la mise en œuvre de politiques de sécurité sanitaire d'urgence. Ces politiques n'ont pas été mises en œuvre partout au même moment, ni de la même manière, l'épidémie n'évoluant, d'une part, pas en tous points du globe au même rythme, et les gouvernements ayant parfois des approches distinctes de ce qu'il

convenait de faire (fermer les frontières ou non, confiner toute la population ou uniquement certaines tranches d'âges ou catégories professionnelles, etc.).

Ces mesures ont pris plusieurs formes.

Il y a eu celles qui visaient à lutter contre l'épidémie elle-même :

– des mesures d'interdiction ou de restriction des déplacements à l'intérieur des États et/ou internationaux, confinement des populations nationales ou locales (quartiers, villes, régions), mise en isolement des individus, distanciation sociale ;

– des mesures réduisant les activités sociales, économiques, professionnelles : fermetures des magasins, réduction des volumes du commerce international, fermeture des écoles, des entreprises.

Ces mesures ont été appliquées différemment selon les États, pas dans tous les États, à des moments distincts, et parfois différemment à l'intérieur même d'un État en fonction de calendriers propres à chaque région (ce fut le cas en France, c'est encore le cas en 2022 en Chine, où la population de Shanghai a par exemple été contrainte à un confinement strict, quand d'autres régions du pays ne l'ont pas été).

Certains États ont également décidé de la mise en œuvre de mesures permettant d'atténuer les effets négatifs produits sur la société par les contraintes sanitaires, en particulier l'impact sur l'économie. On rappellera :

– les mesures de sécurité économique : financements étatiques d'aide à l'activité économique des entreprises, prêts aux entreprises, prestations sociales d'urgence, etc. ;

– les mesures permettant d'assurer la continuité des activités : télétravail, enseignement à distance, mais aussi formules hybrides (*hybrid work*) alternant télétravail et présentiel en entreprise.

La pandémie de Covid-19, en raison de sa létalité et morbidité, de la perturbation du fonctionnement des sociétés qui en résulte, est considérée comme une « crise de santé publique sans précédent […] qui entraîne avec elle la troisième et plus grande crise économique, financière et le plus grand choc social du XXI^{e} siècle, après le 11 septembre et la crise financière globale de 2008 » [OEC 20]. Selon ce rapport de l'OCDE, le « choc » se produit à plusieurs niveaux :

– arrêt ou ralentissement de l'appareil de production dans les pays touchés par la pandémie et les phases de confinement ;

– perturbation de la logistique mondiale ;

– chute drastique de la consommation ;

– effondrement de la « confiance » (qui se traduit sur les fluctuations des marchés financiers confrontés à une situation de forte incertitude) ;

– pertes importantes en vies humaines ;

– mise en évidence de la fragilité des systèmes de soins dans le monde, y compris dans les pays les plus riches.

Mais nous pourrions ajouter à cette liste d'autres éléments, comme l'émergence de mouvements conspirationnistes et antivaccins.

Nous sommes donc en présence *a minima* de deux types de crises dont les effets se combinent : une crise sanitaire et une crise économique et financière.

Le concept de « crise »

Le terme « Covid-19 » a très rapidement été associé à celui de « crise ».

Les crises sont des moments de tension particuliers, qui exacerbent certains phénomènes ou processus. Les définitions de la « crise » en soulignent les caractéristiques : « L'accent est mis sur l'idée de manifestation brusque et intense de certains phénomènes, marquant une rupture » ; « manifestation brusque et intense, de durée limitée (d'un état ou d'un comportement), pouvant entraîner des conséquences néfastes » ; « situation de trouble, due à une rupture d'équilibre et dont l'issue est déterminante pour l'individu ou la société » ; « situation de trouble profond dans laquelle se trouve la société ou un groupe social et laissant craindre ou espérer un changement profond »[1]. La crise est une situation temporaire, un tournant, un moment d'instabilité et de stress. Mais cette approche suppose surtout la préexistence d'un état de normalité, qui est interrompu temporairement, et qu'il faut retrouver. Le retour à l'état antérieur sera considéré comme une résolution de la crise. La crise est donc un moment d'exception, mais qui peut être traité.

Pour Fearn-Banks [FEA 09], la crise est « un événement majeur dont l'issue peut être négative et qui affecte une organisation, une entreprise ou un secteur d'activité, ainsi que le public, les services ou la bonne réputation. Elle interrompt les transactions commerciales normales et peut parfois menacer l'existence de l'organisation »[2].

1. Voir : www.cnrtl.fr/definition/crise.

2. « A major occurrence with a potentially negative outcome affecting an organization, company, or industry, as well as publics, services or good name. It interrupts normal business transactions and can sometimes threaten the existence of the organization » [FEA 09, p. 2].

Mais on peut aussi considérer que la normalité soit la crise : l'histoire du monde serait ainsi faite de crises successives, superposées, emboîtées [CAR 18], qui seraient la normalité du monde, la signature structurelle du monde moderne [KOS 72].

Les crises sont des moments de tension, de désorganisation, qui atteignent des seuils inacceptables ou insupportables pour un individu, un groupe d'individus, une société. Le pic d'intensité ne saurait donc durer. Mais on constate aussi que des crises s'inscrivent dans la durée, ce qui peut paraître incompatible avec sa définition même (crises économiques, sécuritaires, climatiques, politiques, sociales, etc.) Or cette notion de durée reste très subjective. Ce n'est d'ailleurs peut-être pas tant la durée qui caractérise la crise, que le niveau de désorganisation, voire de destruction, ainsi que le seuil d'acceptabilité par l'individu ou la société de cet état exceptionnel. La crise marque un moment de tension insupportable. Ce que l'on nomme fin de crise, après crise, sortie ou résolution de crise, est le retour à un niveau d'acceptabilité, même si la perturbation demeure. Mais elle est simplement soit moins intense, soit perçue comme telle. Ce que l'on nomme sortie de crise n'est pas toujours la fin de l'événement lui-même, mais la capacité à vivre avec, à l'accepter partiellement. La *tolérance au risque* est donc une composante essentielle dans la définition de la crise. Elle peut être différente d'une société à l'autre. Or, c'est bien cette tolérance qui définit le seuil à partir duquel il y a crise ou non.

Enfin, nous ne considérons pas qu'il puisse y avoir, avec la résolution ou sortie de crise, retour à une normalité antérieure à la crise. Car la crise a nécessairement marqué la société qu'elle a traversée. On a ainsi un avant crise (A), la période de crise (B) et l'après-crise (C), où C diffère de A, car C = A + les effets de B.

La notion se décline en crise économique, financière, de la dette, sociale, démographique, systémique, politique (crise de l'État, crise de pouvoir, de confiance, crise de démocratie, etc.), humanitaire, migratoire, sanitaire, climatique, environnementale, nationale, internationale ou globale, crise du crime [ALT 07]. Les crises cyber, ou cybercrises, désignent les crises qui résultent d'une ou plusieurs cyberattaques. Ce sont des événements rares et qui ont un impact très fort, des situations où une ou plusieurs actions malveillantes contre un système d'information provoquent une perturbation majeure de l'entité, avec des impacts multiples et significatifs, et parfois des dommages irréversibles [ANS 21].

Des indices des crises ont été conçus pour tenter d'assurer un suivi des nombreuses crises qui surgissent dans le monde. Les « crises » recensées[3] trouvent leur origine dans des affrontements armés, des mouvements d'insurrection, des guerres civiles, des guerres proxy, des conflits infraétatiques, des conflits pour le contrôle de territoires

3. Voir : www.theowp.org/our-work/crisis-index/.

et de ressources, qui débouchent sur des crises humanitaires (en raison de la raréfaction des ressources et des déplacements massifs des populations), sanitaires, économiques. D'autres indices proposent une mesure quantitative du degré de gravité des crises humanitaires pour adapter les réponses à y apporter. L'*INFORM Severity Index*, produit par l'ACAPS[4], identifie 136 situations de crises dans le monde en 2022[5].

Les crises sont des moments de déstabilisation vécus par les sociétés, et de manière différente selon les groupes sociaux, dont peut se saisir le crime pour asseoir son emprise, sa présence, développer ses activités. Les cartels de la drogue mexicains ont ainsi profité de la crise de la Covid-19 pour s'implanter encore davantage dans des zones ou des domaines d'activités dans lesquels l'État s'est montré défaillant ou absent (théorie de la protection) [JAS 19, KLE 14] :

> « Avec un système de santé inaccessible à une grande partie de la population, ainsi que des programmes de protection sociale mis à rude épreuve, des organisations criminelles ont été observées en train de distribuer des ressources à certaines communautés locales. Bien que les efforts de lutte contre la drogue se poursuivent au niveau des États et au niveau fédéral, les responsables du gouvernement ont largement mis de côté la sécurité accordant la priorité à la réponse à la pandémie. »[6]

Face à la crise des masques [WAN 20], c'est-à-dire à la pénurie de masques et à l'incapacité d'en assurer une production industrielle suffisante, les acteurs du crime se sont engouffrés dans la brèche, espérant tirer profit des attentes des populations. Des cyberopérations criminelles sur le thème de la Covid, des masques, des médicaments ont été menées dans le monde entier [EUR 20a].

Le lien entre le crime et les crises a fait l'objet de nombreux travaux, tout particulièrement empruntant à la théorie économique du crime [DEF 11], mais s'intéressant aussi à d'autres catégories de crises telles que les guerres, les crises politiques, les catastrophes. Kontula [KON 97], par exemple, considère que le crime survenant dans des circonstances exceptionnelles est marqué par des comportements prédateurs, l'érosion des valeurs morales, et la diminution de la peur du châtiment, et par la perte de maîtrise de la situation par les acteurs de la sécurité. L'UNODC [UNO 12] affirme que les facteurs économiques sont importants dans l'évolution du crime. Mais les analyses

4. L'ACAPS est une initiative non gouvernementale soutenue par trois ONG : the Norwegian Refugee Council (NRC), Save the Children et Mercy Corps. Voir : www.data.humdata.org/organization/acaps.

5. Voir : www.acaps.org/sites/acaps/files/crisis/gcsi-download/2022-06/20220606_inform_severity_-_may_2022.xlsx.

6. Voir : www.theowp.org/crisis_index/mexican-drug-war-2/.

divergent : John Kurtz [KUR 15], traitant des effets de la crise financière internationale de 2008, conclut en l'absence de relation étroite entre les deux phénomènes. En Russie, au contraire, les périodes de turbulence économique auraient coïncidé avec un regain de l'activité criminelle, en 1998, puis en 2008-2010 (les crimes économiques et contre la propriété paraissant être les plus réactifs aux changements des conditions économiques) [IVA 12]. Des « pics » d'activité criminelle peuvent survenir lors des périodes de crise économique ou de « stress économique ».

Du rôle du cyber dans les crises

Le numérique fut rapidement considéré comme l'une des réponses à certains aspects de la crise de la Covid-19 : le télétravail était supposé garantir en partie la continuité d'activités dans plusieurs secteurs, le commerce électronique devait soutenir l'activité marchande et les diverses applications en ligne proposées par les gouvernements et/ou des initiatives du secteur privé devaient appuyer l'efficacité du système de santé, organiser la logistique des phases de vaccination à grande échelle, permettre de gérer les confinements et les restrictions des déplacements (grâce à des applications de traçage, notamment), assurer le respect de la distanciation sociale (contrôler la possession d'un laissez-passer sanitaire pour accéder aux lieux qui l'imposaient). Plus encore, le numérique devait être un outil créant du lien social à un moment où les individus étaient interdits de la moindre relation en présentiel, il devait sortir les citoyens de leur isolement, les aider à supporter des situations qui jusqu'alors n'auraient pu exister que dans des œuvres de fiction (nous avons tous en tête les images de ces villes désertées, et de ces millions d'individus à leur fenêtre, cloîtrés de force, attendant leur libération).

Mais si le numérique a contribué, à sa manière, à l'effort planétaire de lutte contre la propagation du virus, il a aussi exacerbé le degré de dépendance, déjà très élevé, dans lequel se trouvaient les sociétés vis-à-vis des technologies de communication, en particulier Internet, le cyberespace.

Le cybercrime s'est-il nourri de ce contexte particulier, a-t-il tiré parti de cette dépendance, de ces vulnérabilités, et de l'accroissement du recours au numérique ? Comme nous le rappellent les indices évoqués ci-dessus, les crises dans le monde sont multiples à un instant t, simultanées, réparties au sein de l'ensemble du système international. Ce sont autant de contextes dans lesquels le crime, et donc le cybercrime, peut évoluer. Ce point sera essentiel dans notre analyse : nous ne pouvons pas considérer la Covid-19 comme une crise unique, isolée. Il serait plus juste de parler « des crises » de la Covid-19, au pluriel, pour désigner les crises qui découlent de l'épidémie, de sa gestion, des effets qu'elle produit sur les sociétés. Ces crises seront de nature sanitaire, économique, sociale, politique peut-être aussi. Mais à ces crises

s'ajoutent toutes celles qui existaient avant l'épidémie de Covid-19 et pendant, événement qui a pris place dans un monde qui était animé de tensions, de conflits et de crises, et qui a continué de l'être. Les crises sont amenées à coexister, voire à s'enchâsser, crises nées de la pandémie, avant, pour d'autres mobiles, et qui peuvent également devenir interdépendantes, produire des effets les unes sur les autres : l'épidémie n'a pas épargné les populations qui étaient déjà confrontées aux guerres, à d'autres maladies, à des difficultés économiques ; les populations déplacées du fait de la crise du climat ou des guerres ou des crises économiques ou politiques ont été confrontées aux effets de la pandémie, etc. Le cybercrime prend place dans des sociétés qui sont à des degrés divers touchées par de multiples crises. Nous ne pouvons pas considérer les évolutions du cybercrime à la lumière des seules crises liées à la pandémie de Covid-19, mais devons plutôt les intégrer dans un contexte fait de crises multiples, dans lequel la pandémie est venue s'ajouter.

Revue de littérature : travaux sur le thème « cybercrime et Covid »

Principaux thèmes et hypothèses

Les effets de l'épidémie sur la société mondiale ont alimenté dès les premiers mois de l'année 2020 de multiples réflexions. Elles traitent des impacts de la pandémie sur :

– l'économie : où l'on souligne par exemple l'accroissement de la pauvreté, la crise sanitaire y ayant plongé des millions de travailleurs supplémentaires, et une augmentation du chômage car « quelque 205 millions de personnes devraient être sans emploi en 2022, soit bien plus que les 187 millions de 2019 » [ONU 21][7] ;

– la culture [YU 21], l'éducation [ONY 20], la science [GUP 21] ;

– la sécurité et la défense : l'épidémie a mis en exergue les faiblesses de la politique commune européenne de sécurité et de défense, mis en évidence les vulnérabilités des États membres en matière d'infrastructures, de chaînes logistiques, de sécurité des communications. La pandémie devrait accélérer le recul des États-Unis et de l'UE sur la scène internationale, au profit de la Chine, qui constitue un défi dans plusieurs domaines, notamment la sécurité IT et les capacités cyber. La pandémie est qualifiée d'accélérateur des tendances préexistantes et d'amplificateur des instabilités [MEY 21]. La protection contre les pandémies est affaire de sécurité nationale, car elles mettent en péril à la fois la vitalité économique d'une nation et ses modes de vie, mais aussi

7. Organisation internationale du travail [En ligne]. Disponible à l'adresse : https://www.msn.com/fr-fr/finance/other/coronavirus-la-pand%c3%a9mie-%c2%ab-quatre-fois-plus-grave-%c2%bb-que-la-crise-de-2008/ar-AAKNv6l?ocid=mailsignout&li=AAaCKnE [Consulté le 8 juin 2021].

l'ensemble des États, dont les destins sont plus étroitement liés qu'ils ne l'étaient au cours des siècles passés, en raison de la mondialisation. Les pandémies ont un caractère destructeur et disruptif, elles perturbent, voire paralysent les capacités de sécurité et de défense des États qui se trouvent dès lors exposés à plusieurs catégories de menaces ou de risques : criminalité, terrorisme, menaces étatiques étrangères. De manière plus générale, la pandémie de Covid-19 est considérée comme un événement qui aura des répercussions profondes et durables sur l'environnement de sécurité internationale [ORO 22]. La période de Covid a favorisé et dynamisé le développement de nouvelles activités criminelles [EUR 20b] (fraude, trafics internationaux, contrefaçon, etc.) qui se nourrissent de l'instabilité mondiale [KEN 21].

Très tôt, dès les premiers mois de l'année 2020, alors que la pandémie n'en est encore qu'à ses débuts, des articles abordent la question de l'évolution du cybercrime dans ce contexte de pandémie.

Quelques thèmes et hypothèses émergent de l'abondante littérature produite depuis lors, tant académique que non académique (organisations nationales et internationales, entreprises de cybersécurité, secteurs privé et public, etc.). Nous en retenons les suivants :

– la gestion de la crise de la Covid-19 (confinements, télétravail, distanciation sociale, applications de traçage, e-commerce, etc.), en renforçant le rôle essentiel de l'Internet, a créé des conditions bénéfiques pour le cybercrime, lequel a pu tirer parti de l'élargissement de la surface d'attaque, de la multiplication ou diversification des opportunités criminelles [TRI 20]. Les conditions créées ont ainsi fait office de catalyseur [BOU 21] de la cybercriminalité, et d'accélérateur ;

– la multiplication des vulnérabilités et donc des opportunités criminelles est centrale dans l'évolution de la cybercriminalité dès le début de la pandémie : les confinements transforment les usages de l'Internet, certaines pratiques en ligne comme le e-commerce sont propices au vol de données personnelles ; le télétravail [TAB 20] isole des salariés qui peuvent être la cible d'attaques d'ingénierie sociale [VEN 21]. Les changements induits par la pandémie dans la vie quotidienne, notamment en matière d'usages du « cyber », sont un élément central dans l'explication des évolutions du cybercrime ;

– les vecteurs d'attaque se sont diversifiés, impliquant la création de nouveaux scénarios d'attaque [GRY 21]. Si le cybercrime a prospéré au cours de cette période pandémique, il le doit à sa capacité d'adaptation, d'innovation, de renouvellement de ses modes opératoires [COR 20], de son modèle économique [LAA 21], voire à la reconfiguration de certains de ses groupes. L'ANSSI évoque la professionnalisation des groupes du cybercrime organisé, et le processus de spécialisation qui caractérise l'évolution du cybercrime au cours des dernières années [ANS 22]. Les usages de

l'Internet ont changé au cours des phases de confinement, déplaçant les vulnérabilités ou en créant de nouvelles : le cybercrime a ainsi dû s'adapter lui aussi à cette reconfiguration de la surface d'attaque afin de saisir les opportunités [LAZ 21], par exemple par le biais d'opérations « thématisées » (enregistrement de plusieurs dizaines de milliers de noms de domaine utilisant le terme « covid » et des termes associés) [NAI 20], ou en orientant ses actions vers les secteurs essentiels en période de crise sanitaire (industrie de la santé, centres de recherche sur le vaccin, hôpitaux, logistique, etc.) Ces attaques contre les acteurs du domaine de la santé sont au cœur du travail réalisé par Joel Chigada et Rujeko Madzinga [CHI 21]. Le crime demeure donc inchangé dans sa nature ou sa composition, il s'adapte simplement à la situation. Le cybercrime adapte ses méthodes, son ciblage, peut-être parfois aussi son organisation, aux contextes dans lesquels il est appelé à agir. Notons que les évolutions au sein du cybercrime organisé ont d'autres moteurs que la seule crise de la Covid au cours des deux dernières années. On pensera notamment à la nécessaire adaptation des modes opératoires, des outils d'attaque utilisés, des choix des cibles qu'imposent les évolutions techniques : la cybersécurité peut par exemple rendre certaines cibles trop résistantes, demander trop d'efforts aux attaquants, les rendre donc moins attractives. Certaines compétences aussi peuvent devenir nécessaires quand d'autres ne le sont plus, et ce toujours en raison des évolutions techniques, technologiques ;

– la raréfaction des opportunités criminelles dans le monde « offline » confiné aurait entraîné un glissement du crime « hors ligne » vers le crime « en ligne » [PLA 21]. Cette hypothèse a ses détracteurs [MIR 21], pour qui le glissement ne s'effectue pas du crime hors ligne (*offline*) vers le crime en ligne (*online*), mais à l'intérieur du crime *online* principalement.

Cadres théoriques

Insistant sur l'importance qu'ont pu avoir tout au long de cette période les transformations des modes de vie et des pratiques quotidiennes de centaines de millions d'individus de par le monde, offrant de nouvelles opportunités au crime, la théorie des activités routinières [COH 79] s'est imposée comme principal cadre explicatif [HAW 20, CHE 21, GOV 21, HOR 21, KEM 21, PLA 21, KOP 22, OLO 22, SMI 22].

Selon cette théorie, un crime pourrait être commis lorsque trois conditions sont remplies : la présence d'un délinquant motivé, la présence d'une cible accessible au délinquant/criminel et l'absence d'un gardien efficace. La vulnérabilité des cibles est accrue lorsque ces trois éléments sont présents. Hawdon *et al.* [HAW 20] avancent que les changements sociétaux forcés par les ordres de confinement augmentent quantitativement et qualitativement ces conditions. La vulnérabilité, ou plutôt le cyberrisque, a augmenté puisque la menace (l'acteur malveillant motivé) et la vulnérabilité

(la présence de cibles convenables) ont convergé vers un même lieu (le cyberespace) au même moment.

Pour Collier *et al.* [COL 20], les cybercrimes de bas niveaux (en termes de capacités techniques) auraient augmenté à cause d'une hausse du nombre d'adolescents et de jeunes adultes confinés qui semblaient lancer des attaques simples contre des réseaux peu protégés pour s'amuser et gagner un peu d'argent. Cette idée est reprise par Brian Payne [PAY 20] qui affirme également qu'une victimisation particulièrement importante des personnes de 50 ans et plus, souvent moins outillées pour se défendre et ayant une moins bonne cyberhygiène, a pu être constatée durant la première vague de confinement. Les cybercrimes tels que les fraudes ciblées sur le thème de la pandémie étaient particulièrement utilisées par les cybercriminels.

Ainsi, il semble y avoir à la fois augmentation du nombre de délinquants motivés par l'argent et la dimension ludique et présence de cibles conformes aux objectifs des cyberdélinquants, tout particulièrement celles n'ayant pas d'habitudes sécuritaires bien établies. À cela s'ajoute le fait que les domaines touchés par le confinement incluent aussi les acteurs de la cybersécurité dans les entreprises privées et les organismes gouvernementaux. Le télétravail imposé a contraint nombre d'employeurs à concentrer leur attention sur l'assistance au transfert du travail des salariés vers leur domicile plutôt qu'à la sécurisation des réseaux. La sécurité des réseaux n'est donc pas nécessairement assurée par les services de cybersécurité, déplaçant ainsi parfois vers les services policiers la responsabilité de la surveillance d'une plus grande partie des réseaux. Sur ce point, Dupont explique que les méthodes policières classiques ne sont pas nécessairement suffisantes dans le cas d'un confinement urgent : « Les méthodes policières classiques d'enquête et d'arrestation s'avèrent insuffisantes, car trop lentes à produire des résultats tangibles et à grande échelle. Elles sont plus efficaces lorsqu'elles sont combinées à des stratégies innovantes de prévention et d'atténuation des dommages » [DUP 20].

Toutefois, les impacts des consignes de confinement ont été très rapides, limitant les possibilités de faire de la prévention. Les campagnes publicitaires d'atténuation ont plutôt été lancées vers fin mars et début avril 2020 au Canada, par exemple. La diminution des capacités et des ressources en protection des réseaux est donc aussi un effet corollaire des premiers instants du confinement.

Plusieurs auteurs appuient leurs analyses sur la théorie des activités routinières, afin d'expliquer la structure d'opportunités particulières qui s'est constituée avec les règles de confinement dans les États fédérés des États-Unis et dans les provinces canadiennes. L'augmentation de la surface d'attaque, l'augmentation du nombre d'acteurs du cybercrime ayant des motivations et des ressources diverses ainsi que les

problèmes de surveillance des réseaux sont tous mentionnés comme étant des facteurs augmentant la vulnérabilité des utilisateurs et des réseaux. À cela s'ajoute la grande flexibilité adaptative des groupes criminels, décrite par Gayraud, ci-dessus, qui a facilité l'adaptation des activités de ces groupes au nouveau contexte pandémique mondial en s'appuyant sur le « fond diffus criminologique » du cyberespace.

Nos questions de recherche

Notre travail traite de la place du cybercrime dans le monde et de son évolution au cours de la période de pandémie qui prend forme aux premiers jours de l'année 2020, et qui n'est toujours pas terminée à l'heure où nous écrivons ces lignes. Les études de cas que nous proposons contribuent aux réflexions sur le lien entre cybercrime et crises et sur les variables explicatives du cybercrime.

Chapitre 1. Évolutions du cybercrime durant la crise de la Covid-19

Le récit dominant depuis les premiers mois de l'épidémie de Covid-19 affirme que celle-ci, par les effets qu'elle a produits sur les sociétés, s'est traduite par une augmentation, parfois spectaculaire, de l'activité cybercriminelle. La situation de crise sanitaire, mais aussi ses prolongements économiques, créerait un contexte favorisant l'activité cybercriminelle et accroissant les risques de victimisation en ligne.

Notre propos ici consiste, en consultant des séries statistiques produites dans plusieurs pays, à remettre en question ce postulat : les chiffres confirment-ils vraiment cette affirmation ? L'évolution de la tendance du cybercrime est-elle corrélée aux diverses phases de la crise sanitaire ?

Pour tenter de répondre à ces questions, nous exploitons comme principale source de données sur l'état de la cybercriminalité, les rapports des CERT (*Computer Emergency Response Teams*) et des données de police, que nous mettrons en miroir avec des données qui traduisent les modifications des styles de vie des citoyens. Les confinements, les restrictions à la mobilité des individus étant l'un des principaux marqueurs de ces modifications, nous exploitons des données sur la mobilité qui permettent de reconstituer la chronologie des périodes de restrictions.

Nous aborderons également la question centrale de l'évolution des tendances du cybercrime au cours de la crise sanitaire, en traitant des évolutions des cyberattaques sur la scène internationale.

Chapitre 2. La crise pandémique de SARS-CoV-2 et l'évolution de la cybercriminalité aux États-Unis et au Canada

À l'instar du reste du monde, la crise pandémique causée par le SARS-CoV-2 en 2020 a perturbé le fonctionnement normal des sociétés au Canada et aux États-Unis. Sur le plan de la cybersécurité, selon toute vraisemblance, les acteurs malveillants ont adapté leurs pratiques en fonction du contexte pandémique. Ainsi, la cybercriminalité a-t-elle évolué et s'est-elle ajustée à ce nouveau contexte. Ce chapitre expose ces changements à partir de rapports gouvernementaux et d'organisations privées sur la cybercriminalité en offrant un point de vue critique. La cybercriminalité aux États-Unis et au Canada pendant la crise pandémique y est analysée dans ses tendances diverses. La nécessité de la coopération internationale pour contrer la cybercriminalité et les enjeux méthodologiques associés à cette étude concluent ce chapitre.

Chapitre 3. Radicalisation en ligne et cybercriminalité : le militantisme américain pendant la Covid-19

Le 6 janvier 2021, l'attaque du Capitole à Washington fut le point culminant d'une période plus large de militantisme sociopolitique aux États-Unis. La trajectoire de cette période qui, à bien des égards, se prolonge encore, a suivi de près la propagation de la pandémie de SRAS-CoV-2. L'objectif de ce chapitre est de se demander dans quelle mesure le cadre analytique de base de la théorie de la cybercriminalité reste valable dans des conditions de pandémie. Notre argument est que la pression sans précédent de l'accélérationnisme que les États-Unis ont connue pendant la Covid-19 nous oblige à repenser la radicalisation en ligne comme forme de cybercriminalité. L'étendue, la vitesse et la dynamique globale extraordinaires de l'activité accélérationniste qui s'est confrontée aux institutions américaines séculaires ces dernières années sont les signes d'un nouveau type d'association symbiotique entre les éléments en ligne et hors ligne.

Chapitre 4. Cybercriminalité au Brésil : évaluation des politiques post-Covid de coopération internationale en matière d'enquêtes et de poursuites

La cybercriminalité n'est pas un sujet nouveau pour les autorités brésiliennes. En 2015, le Brésil était le deuxième pays le plus vulnérable à la cybercriminalité, la société brésilienne ayant perdu entre 4,1 et 4,7 milliards de dollars américains en vols de données et en fraudes financières. Comment le cybercrime a-t-il évolué au cours de la période de pandémie de Covid-19, et quelles réponses le gouvernement et la société brésilienne ont-ils apportées à ces enjeux ? En exploitant des données

quantitatives et des entretiens réalisés auprès de membres des forces de sécurité, le chapitre esquisse les grandes lignes des réformes en cours en matière de lutte contre la cybercriminalité au Brésil.

Chapitre 5. Impacts de la crise de Covid-19 sur la peur et la victimisation liées au vol d'identité en ligne au Portugal

Ce chapitre se concentrera sur le vol d'identité en ligne, désormais considéré comme l'un des crimes en ligne à la croissance la plus rapide, et qui entraîne des pertes financières importantes pour les victimes. Cette recherche, entreprise dans le contexte portugais (2017 et 2021), vise à : i) analyser les niveaux de victimisation, de peur et de perception du risque du vol d'identité en ligne, avant et après la crise pandémique de Covid-19 ; ii) analyser l'évolution des activités routinières en ligne, également avant et après la crise pandémique de Covid-19 ; iii) comprendre l'évolution d'autres formes de victimisation en ligne au cours des deux dernières années.

Chapitre 6. Une perspective sud-africaine sur la cybercriminalité pendant la pandémie

Ce chapitre examine l'activité cybercriminelle pendant la pandémie de Covid-19 du point de vue sud-africain. L'Afrique du Sud a-t-elle été victime d'une augmentation de la cybercriminalité ou bien les tactiques des cybercriminels ont-elles changé ? Les avis divergent sur ces questions. Ce chapitre propose une recherche exploratoire pour étudier les tendances de la cybercriminalité en Afrique du Sud et tente d'apporter des éléments de réponse aux deux questions. Les classements internationaux, les législations et réglementations nationales et les rapports d'incidents sont pris en compte pour analyser les tendances. L'absence de rapports officiels sur la cybercriminalité et les incidents de cybersécurité en Afrique du Sud constitue une limite. Les informations requises sont obtenues à partir de rapports d'incidents, de rapports industriels et de livres blancs illustrant les tendances.

Bibliographie

[ALA 21] Alava S., "Internet est-il un espace de radicalisation ?" in Morin D., Aoun S., Al Baba Douaihy S. (eds), *Le nouvel âge des extrêmes ? : Les démocraties occidentales, la radicalisation et l'extrémisme violent*, Les Presses de l'Université de Montréal, 2021.

Cette bibliographie est identique à celle de l'ouvrage correspondant en anglais publié par ISTE.

[ALT 07] ALTBEKER A., *A Country at War with Itself: South Africa's Crisis of Crime*, Jonathan Ball, Johannesburg and Cape Town, 2007.

[ANS 21] ANSSI, Organising a cyber crisis management exercise, available at : https://www.ssi.gouv.fr/en/guide/organising-a-cyber-crisis-management-exercise/, 2021.

[ANS 22] ANSSI, Panorama de la menace informatique 2021, Report 1.9.1, available at : https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf, 2022.

[BAD 20] BADAWI E., GUY-VINCENT J., Cryptocurrencies emerging threats and defensive mechanisms: a systematic literature review, Faculty of Engineering, University of Ottawa, available at: https://ieeexplore-ieee-org.ezproxy.usherbrooke.ca/stamp/stamp.jsp?tp=&arnumber=9243940, 2020.

[BEC 01] BECK U., *La société du risque. Sur la voie d'une autre modernité*, Aubier, Paris, 2001.

[BEN 22] BENCHERIF A., BELPORO L.C., MORIN D., Étude internationale sur les dispositifs de prévention de la radicalisation et de l'extrémisme violents dans l'espace francophone, Chaire UNESCO en prévention de la radicalisation et de l'extrémisme violents, 2022.

[BOU 21] BOU SLEIMAN M., GERDEMANN S., "Covid-19 : a catalyst for cybercrime?", *International Cybersecurity Law Review*, vol. 2, pp. 37–45, 2021.

[BRE 10] BRENNER S. W., *Cybercrime : Criminal Threats from Cyberspace*, Praeger, Santa Barbara, CA, 2010.

[CAR 18] CARASTATHIS A., SPATHOPOULOS A., TSILIMOUNIDI M., "Crisis, what crisis ? Immigrants, refugees, and invisible struggles", *Refuge, Canada's Journal on Refugees*, vol. 34, no. 1, 2018.

[CHE 21] CHEN P., KURLAND J. R., PIQUERO A. et al., "Measuring the impact of the Covid-19 lockdown on crime in a medium-sized city in China", *Journal of Experimental Criminology*, pp. 1–28, 2021.

[CHI 21] CHIGADA J. and Madzinga, R., "Cyberattacks and threats during Covid-19: a systematic literature review", *South African Journal of Information Management*, vol. 23, no. 1, pp. 1277, 2021.

[COL 20] COLLIER B., HORGAN S., JONES R. et al., "The implications of the Covid-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations", *The Scottish Institute for Policing Research*, nos 1 – 18, available at: https://www.researchgate.net/publication/341742472_Issue_No_1_The_implications_of_the_Covid-19_pandemic_for_cybercrime_policing_in_Scotland_A_rapid_review_of_the_evidence_and_future_considerations, 2020.

[COR 20] CORDEY S., *The Evolving Cyber Threat Landscape during the Coronavirus Crisis*, Cyberdefense Project (CDP), Center for Security Studies (CSS), ETH Zurich, 2020.

[DEF 11] DEFLEM M. (ed.), "Introduction : criminological perspectives of the crisis", *Economic Crisis and Crime*, Emerald, Bingley, 2011.

[DUP 20] DUPONT B., "La cybercriminalité au temps de la Covid-19", *Policy Options*, available at: https://policyoptions.irpp.org/magazines/july-2020/la-cybercriminalite-au-temps-de-la-covid-19/, 2020.

[EUR 20a] EUROPOL, Corona crimes : suspect behind €6 million face masks and hand sanitisers scam arrested thanks to international police cooperation, available at: https://www.europol.europa.eu/media-press/newsroom/news/corona-crimes-suspect-behind-%E2%82%AC6-million-face-masks-and-hand-sanitisers-scam-arrested-thanks-to-international-police-cooperation, 2020.

[EUR 20b] EUROPOL, How Covid-19-related crime infected Europe during 2020, European Union Agency for Law Enforcement Cooperation, available at: https://www.europol.europa.eu/sites/default/files/documents/how_covid-19-related_crime_infected_europe_during_2020.pdf, 2020.

[FEA 09] FEARN-BANKS K., *Crisis Communications : A Casebook Approach*, Routledge, New York, 2009.

[GAY 21] GAYRAUD J.-F., "Les grandes criminalités, entre réalité géopolitique et menace stratégique", *Revue Défense Nationale*, vol. 7, no. 842, pp. 28–33, 2021.

[GOV 21] GOVENDER I., WATSON B.W.W., AMRA J., "Global virus lockdown and cybercrime rate trends: a routine activity approach", *Journal of Physics: Conference Series*, vol. 1828, 2021.

[GRY 21] GRYSZCZYNSKA A., "The impact of the Covid-19 pandemic on cybercrime", *Bulletin of the Polish Academy of Sciences Technical Sciences*, vol. 69, no. 4, 2021.

[GUP 21] GUPTA R., PRASAD A., BABU S. et al., "Impact of coronavirus outbreaks on science and society: insights from temporal bibliometry of SARS and Covid-19", *Entropy*, vol. 23, pp. 626, 2021.

[HAW 20] HAWDON J., PARTI K., DEARDEN T., "Cybercrime in America amid Covid-19 : the initial results from a natural experiment", *American Journal of Criminal Justice*, vol. 45, pp. 546–562, 2020.

[HOR 21] HORGAN S., COLLIER B., JONES R. et al., "Re-territorialising the policing of cybercrime in the post-Covid-19 era: towards a new vision of local democratic cyber policing", *Journal of Criminal Psychology*, vol. 11, no. 3, pp. 222–239, 2021.

[IVA 12] IVASCHENKO O. et al., "The role of economic crisis and social spending in explaining crime in Russia", *Eastern European Economics*, vol. 50, no. 4, pp. 21–41, 2012.

[JAS 19] JASPERS J.D., "Business cartels and organised crime: exclusive and inclusive systems of collusion", *Trends in Organized Crime*, vol. 22, pp. 414–432, 2019.

[KEM 21] KEMP S., BUIL-GIL D., MONEVA A. et al., "Empty streets, busy internet: a time-series analysis of cybercrime and fraud trends during Covid-19", *Journal of Contemporary Criminal Justice*, 2021.

[KEN 21] KENNEDY L., SOUTHERN N.P., "The pandemic is putting gangsters in power, as states struggle, organized crime is rising to new prominence", *Foreign Policy*, 2021.

[KLE 14] KLEEMANS E.R., "Theoretical perspectives on organized crime", in PAOLI L. (ed.), *Oxford Handbook on Organized Crime*, Oxford University Press, Oxford, 2014.

[KON 97] KONTULA O., Crime in times of crisis, from research report summaries, Report, National Research Institute of Legal Policy, 1997.

[KOP 22] KOPPEL S., CAPELLAN J.A., SHARP J., "Disentangling the impact of Covid-19: an interrupted time series analysis of crime in New York City", *American Journal of Criminal Justice*, 2022.

[KOS 72] KOSELLECK R., "Krise", in BRUNNER O., KONZE W., KOSELLECK R. (eds), *Geschichtliche Grundbegriffe: Historisches Lexicon zur politisch-sozialen Sprache in Deutschland*, Klett-Cotta, Stuttgart, 1972.

[KUR 15] KURTZ J., Crisis and crime: examining the effect of macroeconomic conditions on criminal activity during the great recession, New York University, available at: https://as.nyu.edu/content/dam/nyu-as/politics/documents/Kurtz.pdf, 2015.

[LAA 21] LAAN J., The impact of the Corona-pandemic on the business model of cybercrime, Master's Thesis, University of Twente, 2021.

[LAZ 21] LAZAROV S., "The impact of Covid-19 on cybercrime trends", *Proceedings of the Sixth International Scientific Conference on Telecommunications, Informatics, Energy and Management,* TIEM 2021, pp. 62–65, 2021.

[MEY 21] MEYER C.O., BRICKNELL M., PACHECO P.R., How the Covid-19 crisis has affected security and defense-related aspects of the EU, European Parliament, Belgium, available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/653623/EXPO_IDA (2021) 653623_EN.pdf, 2021.

[MIR 21] MIRÓ-LLINARES F., "Crimen, cibercrimen y Covid-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", *Revista de los Estudios de Derecho y Ciencia Política*, IDP, no. 32, Marzo, Universitat Oberta de Catalunya, 2021.

[NAI 20] NAIDOO R., "A multi-level influence model of Covid-19 themed cybercrime", *European Journal of Information Systems*, vol. 29, no. 3, pp. 306–321, 2020.

[OEC 20] OECD, Coronavirus (Covid-19): joint actions to win the war, OECD Secretary General, available at: https://www.oecd.org/about/secretary-general/Coronavirus-Covid-19-Joint-actions-to-win-the-war.pdf, 2020.

[OLO 22] OLOFINBIYI S.A., "Cyber insecurity in the wake of Covid-19: a reappraisal of impacts and global experience within the context of routine activity theory", *Journal ScienceRise : Juridical Science*, vol. 1, no. 19, pp. 37–45, 2022.

[ONU 21] ONU INFO, La pandémie de Covid-19 a coûté 255 millions d'emplois en 2020 (OIT), available at : https://news.un.org/fr/story/2021/01/1087652, 2021.

[ONY 20] ONYEMA E.M., EUCHERIA N.C., OBAFEMI F.A. et al., "Impact of coronavirus pandemic on education", *Journal of Education and Practice*, vol. 11, no. 13, 2020.

[ORO 22] O'ROURKE R., *Covid-19 : Potential Implications for International Security Environment – Overview of Issues and Further Reading for Congress*, Congressional Research Service, Washington, DC, 2022.

[PAR 20] PARK A., MONTECCHI M., FENG C. et al., "Understanding 'fake news': A bibliographic perspective", *Defense Strategic Communications*, vol. 8, pp. 141–172, 2020.

[PAY 20] PAYNE B., "Criminals work from home during pandemics too: a public health approach to respond to fraud and crimes against those 50 and above", *American Journal of Criminal Justice*, vol. 45, pp. 563–577, 2020.

[PLA 21] PLACHKINOVA M., "Exploring the shift from physical to cybercrime at the onset of the Covid-19 pandemic", *Journal of Cyber Forensics and Advanced Threat Investigations*, vol. 2, no. 1, pp. 50–62, 2021.

[SAN 22] SANS INSTITUTE, Glossary of security terms, available at: https://www.sans.org/security-resources/glossary-of-terms/, 2022.

[SMI 22] SMITH T., "Assessing the effects of Covid-19 on online routine activities and cybercrime: a snapshot of the effect of sheltering in place", *Caribbean Journal of Multidisciplinary Studies*, vol. 1, no. 1, pp. 36–60, 2022.

[TAB 20] TABREZ A., Corona virus (Covid-19) pandemic and work from home: challenges of cybercrimes and cybersecurity, available at: http://dx.doi.org/10.2139/ssrn.3568830, 2020.

[TRI 20] TRIPATHI K., Cybercrime against older people during Covid19 pandemic, UCL JDI Special Series on Covid-19, issue 4, available at: https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/cybercrime_0.pdf, 2020.

[UNO 12] UNODC, Monitoring the impact of economic crisis on crime, Vienna, available at: https://www.unodc.org/documents/data-and-analysis/statistics/crime/GIVAS_Final_Report.pdf, 2012.

[VEN 21] VENKATESHA S., RAHUL R.K., CHANDAVARKAR B.R., "Social engineering attacks during the Covid-19 pandemic", *Springer Nature Computer Science*, vol. 2, no. 78, 2021.

[WAN 20] WANG M.W., ZHOU M.-Y., JI G.-H. et al., "Mask crisis during the Covid-19 outbreak", *European Review for Medical and Pharmacological Sciences*, vol. 24, pp. 3397–3399, 2020.

[YU 21] YU Y.J., PARK Y.S., KELLER A. et al., "A mixed methods systematic review of the impacts of coronavirus on society and culture", *International Journal of Environmental Research and Public Health*, vol. 18, pp. 491, 2021.