DOSSIER 1

SANTÉ-SÉCURITÉ MONDIALE : CONFUSION OU PRÉVISION ?

https://doi.org/10.54695/secug.244.0007

Le renseignement médical, vigie sécuritaire mondiale

Julien MARX[1]

A l'origine soignant issu d'un parcours hybride Sécurité-Santé, je consacre ma thèse à un sujet qui, bien qu'existant officiellement depuis plus de 20 ans, reste mal connu de la culture française ; alors que, comme nous l'explorerons dans cet article, il possède un vaste potentiel d'outils défensifs.

Le renseignement médical est à l'origine une discipline militaire[2]. Il nous vient de la Guerre Froide, période trouble synonyme de secrets, tensions permanentes, programmes d'armes de destruction massive[3] et d'horloge de l'Apocalypse[4].

Conçu pour évaluer la dangerosité d'un champ de bataille et déterminer les moyens adaptés pour protéger les troupes avant leur projection, il faut attendre le séisme géopolitique du 11 septembre 2001[5], pour que quelques médecins de culture civilo-militaire envisagent une diffusion vers le champ civil, en lien avec la médecine de catastrophe[6]. Il reste cependant très discret, sous le contrôle du NCMI[7], basé à l'USAMRIID, le cœur du dispositif de défense médicale de l'armée américaine. On trouve quelques traces de son existence en Europe, notamment dans un document d'instruction de l'OTAN[8].

C'est finalement au cours de la pandémie de COVID-19 que le NCMI devient un peu plus visible, comme membre de la Communauté américaine du Renseignement, envoyée à l'assaut du microbe pour comprendre son origine[9].

Comme je tenterai de le présenter dans mon propos, le renseignement médical se veut une symbiose entre deux mondes professionnels :

- La communauté du Renseignement, conçue pour l'identification précoce du criminel et l'anticipation des menaces ;
- La communauté médicale, conçue pour la prise en charge des victimes des menaces, et l'atténuation de leurs conséquences en cas de nouvelle utilisation.

Cette symbiose, qui implique le partage des connaissances et moyens communs, a pour objectif global de renforcer la vigie sécuritaire mondiale, tant sur le plan anti-criminel que sanitaire.

Cette symbiose peut œuvrer sur trois axes :

- Le renseignement pour la protection de la santé publique ;
- Le renseignement pour la protection de l'infrastructure sanitaire ;
- Le renseignement pour la sécurité publique.

Défense biologique

Dans le domaine de la cybersécurité, un test de pénétration est une attaque simulée des défenses d'un système informatique qui utilise les outils et les techniques qu'un adversaire emploierait. Ces tests sont utilisés par toutes sortes de gouvernements et d'entreprises. Les banques, par exemple, engagent régulièrement des experts en informatique pour s'introduire dans leurs systèmes et transférer de l'argent à des personnes non autorisées.

Les banques, par exemple, engagent régulièrement des experts en informatique pour pénétrer dans leurs systèmes et transférer de l'argent sur des comptes non autorisés, souvent en hameçonnant des employés pour obtenir leurs identifiants de connexion. Une fois que les testeurs ont réussi, ils présentent leurs conclusions aux institutions et formulent des recommandations sur la manière d'améliorer la sécurité[10].

À la fin de la dernière décennie et au début de celle-ci, la société humaine elle-même a été soumise à une sorte de test de pénétration : le COVID-19. Le virus, un adversaire irréfléchi, a sondé la capacité du monde à se défendre contre de nouveaux agents pathogènes. À la fin du test, il était clair que l'humanité avait échoué. Le COVID-19 est allé partout, des stations de recherche éloignées de l'Antarctique aux tribus isolées d'Amazonie. Il a fait rage dans les maisons de retraite et sur les porte-avions. Au fur et à mesure qu'il se propageait, il s'attaquait aux personnes vulnérables et aux puissants, qu'il s'agisse de travailleurs de première ligne ou de chefs d'État. Les mesures draconiennes de confinement imposées par les autocraties et les vaccins miraculeux mis au point par les démocraties ont ralenti, mais pas stoppé, la propagation du virus.

Fin 2022, trois Américains sur quatre avaient été infectés au moins une fois. Au cours des six semaines qui ont suivi la fin des restrictions « zéro COVID » imposées par la Chine en décembre, plus d'un milliard d'habitants du pays ont été infectés. La raison principale du nombre relativement modeste de décès dus à la pandémie n'est pas que la société a maitrisé la maladie. C'est le fait que l'infection virale ne s'est avérée que modestement mortelle. En fin de compte, le COVID-19 s'est en grande partie éteint de lui-même.

L'échec de l'humanité face au COVID-19 donne à réfléchir, car le monde est confronté à un nombre croissant de menaces biologiques. Certaines d'entre elles, comme la grippe aviaire, proviennent de la nature. Mais beaucoup d'entre elles sont le fruit des progrès scientifiques. Au cours des 60 dernières années, les chercheurs ont acquis une connaissance approfondie de la biologie moléculaire et humaine, ce qui leur a permis de mettre au point des agents pathogènes remarquablement mortels et efficaces. Ils ont compris comment créer des virus capables d'échapper à l'immunité. Ils ont appris à faire évoluer les virus existants pour qu'ils se propagent plus facilement dans l'air et à les modifier pour les rendre plus dangereux.

On ne sait toujours pas si le COVID-19 est né de ces activités ou s'il est entré dans la population humaine par le biais d'une interaction avec des animaux sauvages. Quoi qu'il en soit, il est clair que la technologie biologique, aujourd'hui renforcée par l'intelligence artificielle, a rendu la production de maladies plus simple que jamais.

Si un agent pathogène fabriqué ou amélioré par l'homme s'échappe ou est libéré d'un laboratoire, les conséquences pourraient être catastrophiques. Certains agents pathogènes

synthétiques pourraient être capables de tuer beaucoup plus de personnes et de causer une dévastation économique beaucoup plus importante que le coronavirus. Dans le pire des cas, le nombre de morts dans le monde pourrait dépasser celui de la peste noire, qui a tué une personne sur trois en Europe[11] [...]. Les risques augmentent en partie grâce à une deuxième révolution technologique : l'essor de l'intelligence artificielle.

Les grands modèles linguistiques, tels que ceux de ChatGPT et de Claude, deviennent de plus en plus sophistiqués et puissants à chaque nouvelle itération. Aujourd'hui, les versions les plus récentes sont utilisées. Aujourd'hui, les versions les plus récentes sont utilisées chaque jour par des milliers d'employés de laboratoire pour accélérer leur travail, notamment en leur fournissant une multitude de conseils utiles sur des questions techniques.

En 2020, des chercheurs en IA ont créé un système, AlphaFold, qui a effectivement résolu un problème du Graal en biologie : prédire la structure tridimensionnelle d'une protéine à partir de la séquence de ses acides aminés. Mais pour les bioterroristes en puissance, ces systèmes pourraient faciliter la voie vers le chaos. Les plus grands modèles d'IA semblent avoir été formés à partir de l'ensemble des connaissances publiées dans le domaine des sciences de la vie. La plupart de ces connaissances étaient bien sûr déjà disponibles sur l'internet, mais aucun être humain ne pourrait les consommer, les traiter et les synthétiser toutes.

Les systèmes d'IA actuels peuvent également concevoir de nouvelles protéines (ce qui permet de concevoir des agents pathogènes dangereux) et exécuter des opérations de laboratoire. Certains informaticiens travaillent même à la réalisation de systèmes automatisés capables d'effectuer des tâches de laboratoire. Si ces efforts aboutissent, un acteur malveillant pourrait créer un nouvel agent pathogène mortel en détournant simplement ces installations automatisées. Et il sera très difficile pour les autorités de les arrêter.

Les pirates informatiques se sont révélés capables de s'introduire dans des systèmes de sécurité extrêmement complexes, et les matériaux nécessaires à la création de nouveaux agents pathogènes sont très rares. Les matériaux nécessaires à la création de nouveaux agents pathogènes comprennent des réactifs et des équipements qui sont largement disponibles.

Les régulateurs pourraient essayer de cibler les douzaines de fournisseurs qui passeront des commandes pour des composants clés.

Mais il existe des moyens de contourner ces fournisseurs, et leur fermeture pourrait ralentir la recherche et le développement biomédical de grande valeur.

Si des acteurs malveillants finissent par produire et diffuser un agent pathogène viral, celui-ci pourrait infecter de vastes pans de la population humaine en bien moins de temps qu'il faudrait aux autorités pour détecter et identifier la menace et commencer à riposter. Après tout, il est moins couteux de produire des agents pathogènes que de se défendre contre eux.

Les couts d'investissement des installations et des matériaux nécessaires à la fabrication d'une nouvelle maladie sont faibles, mais la réponse à une épidémie implique un ensemble de mesures complexe et d'un cout stupéfiant : des réseaux étendus de tests et de détection,

de vastes quantités d'équipements de protection individuelle, des fermetures socialement perturbatrices et un appareil capable de développer, de fabriquer et de distribuer des traitements et des vaccins, de développer, de fabriquer et de distribuer des traitements et des vaccins[12] [...].

Pendant la guerre froide, les puissances nucléaires du monde ont évité la catastrophe en grande partie grâce au concept de destruction mutuelle assurée (Mutually Assured Destruction, MAD) ; les responsables politiques ont reconnu qu'une seule attaque nucléaire pouvait déclencher des représailles planétaires, ou, comme l'ont déclaré le président américain Ronald Reagan et le dirigeant soviétique Mikhaïl Gorbatchev en 1985, « une guerre nucléaire ne peut être gagnée et ne doit jamais être menée ». Les États nucléaires ont produit des doctrines élaborées pour régir leur technologie et dissuader l'utilisation des armes.

Mais lorsqu'il s'agit d'armes biologiques, la formule de dissuasion de la guerre froide ne fonctionne pas. La destruction mutuelle assurée repose sur la peur, qui était très répandue à l'époque nucléaire, mais ne l'est plus autant dans le cas de la guerre biologique. La menace actuelle dépend de la poursuite de progrès technologiques fulgurants et d'inventions sans précédent, ce qui fait que les gens ont des difficultés à saisir pleinement les risques. Contrairement aux bombardements nucléaires d'Hiroshima et de Nagasaki, aucune attaque biologique n'a été un évènement historique mondial attirant durablement l'attention.

La destruction mutuelle assurée dépend aussi de la capacité d'un État à identifier l'attaquant. Avec les armes nucléaires, il est relativement de le faire. Mais les États pourraient disséminer des armes biologiques et échapper à la détection et, par conséquent, aux représailles. Un gouvernement pourrait secrètement diffuser un virus dangereux et l'imputer à un certain nombre d'autres États, voire à des acteurs non étatiques. Ou des acteurs non étatiques pourraient réellement libérer des agents pathogènes mortels, ce qui rend la destruction mutuelle assurée encore moins efficace. L'interception récente d'un courrier destiné au Ministre de l'Intérieur[13], contenant une légère trace de peste[14], démontre que cette menace n'est pas impossible sur notre territoire.

Aucun gouvernement ne veut risquer l'anéantissement de son pays, mais de nombreux terroristes ne se soucient guère de leur survie, et ils ont désormais accès au matériel, à l'équipement, aux connaissances et aux capacités techniques nécessaires pour fabriquer des armes biologiques.

Si les outils de régulation internationale et de surveillance officiels s'avèrent désormais obsolètes ou inadaptés face aux capacités du monde criminel, la solution se trouve peut-être dans le monde de l'invisible et du clandestin : le renseignement, mais dans une nouvelle dimension, plus développée et synergique avec la communauté médicale : le renseignement médical [15].

Le Renseignement Extérieur est déjà responsable de la lutte contre la prolifération des armes de destruction massive ; mais comme cela a été présenté plus haut, nous faisons désormais face à un monde criminel plus complexe, qui dépasse les surveillances basées sur la MAD. Il faut donc développer un appareil de renseignement au même niveau de complexité, basé sur les connaissances de la communauté scientifique, et actualisé sur la cinétique du progrès technique.

Cet appareil de renseignement se baserait sur des moyens déjà bien connus (humain, signal, imagerie satellite…) et plus récents (veille cyber, simulation de phénomène infectieux[16]…). Un partenariat plus étroit avec le monde de la recherche (technologique, fondamentale, médicale, sociale…) est tout aussi indispensable pour être « à jour » de la menace.

Enfin, on observe ces dernières années, des recrudescences ou déplacements de certains phénomènes infectieux (Mpox[17], encéphalite[18]…) susceptibles d'avoir de sérieuses conséquences. Les évolutions de répartition et comportement animales, et les risques de vectorisation infectieuse qui en résultent, cette communication Renseignement-Recherche devrait s'ouvrir à d'autres disciplines (vétérinaire, climatique…), pour se préparer aux conséquences sanitaires de Demain.

Par ailleurs, comme nous l'avons observé pendant la pandémie COVID-19, il est difficile pour un pays d'appréhender une menace émergente, et d'ajuster sa stratégie sanitaire sans faire d'erreurs, avec des conséquences sanitaires parfois non négligeables.

Or, comme l'a démontré la communauté hospitalo-universitaire[19] et les sociétés savantes médicales (SFMC, SFMU, SPILF…), le retour d'expérience (Retex) est un outil précieux, que ce soit « à chaud » pour avancer dans l'incertitude, ou « à froid » pour corriger ses erreurs. On pourrait donc envisager, dans l'appareil de renseignement proposé, un observatoire du Retex international, qui observerait en temps réel les difficultés des autres pays impactés par la menace, afin d'ajuster sa stratégie sanitaire au plus près des données disponibles.

Renseignement chirurgical

Dans un ouvrage de référence sur le Retex des attentats de 2015[20], un chapitre se focalise sur un service spécialisé en accueil de traumatologie lourde (SSPIAP)[21], qui a reçu le plus grand nombre de victimes lors de l'attentat multi-sites du 13 novembre. Une fois l'alerte d'un attentat en cours transmise par le SAMU, un certain nombre d'actions a été mis en place dans l'objectif de faciliter au plus vite l'accueil des victimes :

- Les médecins et chirurgiens de garde ont été invités à renforcer l'effectif présent ;
- Les personnels médicaux et non médicaux à domicile ont reçu pour consigne de se rendre à l'hôpital ;
- Les patients de Salle de Surveillance Post-Interventionnelle (SSPI) présentant les critères de sortie ont été transférés ;
- Les autres ont été transférés vers d'autres SSPI ou des réanimations ;
- Les chirurgies non urgentes ont été reportées ;
- Les soignants présents ont préparé l'unité dédiée à l'accueil des victimes conformément au plan AMAVI[22] ;
- Des manipulateurs en électro-radiologie et médecins radiologues ont été affectés dans l'unité ;
- Le service local de l'Établissement Français du Sang a délivré des produits sanguins pour renforcer le stock initial ;
- Les blocs opératoires ont été réouverts et armés en personnel et matériel ;
- L'équipe de stérilisation du matériel chirurgical a été renforcée, pour permettre le reconditionnement rapide des boites de matériel (obligatoire entre chaque opération) ;
- Le Service d'Accueil des Urgences a été divisé en deux, une pour la gestion de l'évènement, une pour la gestion du quotidien.

Le rapide passage en revue de ces actions expose l'organisation massive à mettre en place, dans un délai en asymétrie avec la cinétique rapide d'arrivée des victimes. D'autant que ce contexte d'effervescence facilite l'introduction du sur-attentat par ambulance piégée, point qui sera évoqué plus loin. À ce jour, et bien que les stratégies d'entrainement hospitalier aient nettement évolué depuis 2015, le système de réponse sanitaire est toujours conçu selon un modèle ou il attend l'afflux de victimes, au lieu de l'anticiper.

Le plan Vigipirate[23] est un dispositif global de vigilance, de prévention et de protection qui concerne l'ensemble des secteurs d'activité du pays ; la posture « urgence attentat » marque un nouveau durcissement de la posture Vigipirate en raison de l'évolution des menaces terroristes et cyber, et fait porter un effort plus particulier sur la sécurité. Ces mesures Vigipirate traduisent la volonté du Gouvernement en termes de préparation, de vigilance et de réaction face à la menace terroriste. Bien que ces mesures aient un impact fort sur la sécurisation des lieux publics et la posture de vigilance de la population (qui reste encore nettement à améliorer) l'institution hospitalière n'a pas encore su utiliser ce modèle pour améliorer sa stratégie d'anticipation de la menace, en concevant un système de mise en alerte précoce.

Comme nous l'avons vu plus haut, le plan AMAVI est conçu pour accueillir beaucoup de blessés, mais présente une contrainte temporelle majeure ; d'autant que l'exemple présenté ici est celui d'un hôpital rompu aux entrainements ; la situation serait probablement plus complexe dans un centre moins formé, voire pas identifié comme référent. Mais on peut difficilement demander aux terroristes « prière de taper à tel endroit, ce sera plus facile pour nous à gérer ».

Il serait donc plus stratégique de concevoir un dispositif de mise en alerte précoce hospitalier, dans une stratégie globale de Renseignement Chirurgical, en partenariat avec les services de Renseignement de la Sécurité Intérieure. Il pourrait prendre la forme d'un plan Vigipirate intra-hospitalier[24], avec un niveau supplémentaire (niveau noir - attentat imminent) un délai d'activation déterminé (quelques heures, levée automatique en l'absence d'attentat) voire une localisation d'activation (départementale, locale…) sous la coordination du SAMU territorialement concerné. Il engendrerait la même activation logistique que décrite plus haut, mais dans une temporalité précoce, pour limiter le stress des équipes et les tensions sur un système sanitaire qui souffre déjà d'une crise en ressources humaines. Une stratégie de Retex serait bien entendu à mettre en place en parallèle de son activation, qu'il y ait ou non l'occurrence d'un attentat.

Défense hospitalière physique

L'Hôpital, de par son héritage historique d'accueil des malades et des pauvres, s'est toujours considéré comme un environnement sanctuarisé, que la criminalité organisée ou le terrorisme n'oseraient pas toucher ; cette vision est désormais obsolète. L'attaque sur le site ou les personnels, quelle que soit sa forme, est une menace de plus en plus fréquente et polymorphe[25]. On observe d'ailleurs un changement de vision stratégique dans les établissements, que, d'après l'enquête doctorale en cours, l'on peut répartir en 3 catégories :

- Catégorie 1 : ceux ayant déjà vécu un ou plusieurs actes malveillants ou attentats, et qui ont déjà commencé leur mutation, pour se mieux se protéger et sensibiliser leur personnel (généralement des CHU et trauma-centers[26]).

- Catégorie 2 : ceux pour lesquels l'attentat ou l'intrusion restent théoriques, et qui sont encore dans une position d'hésitation ou de déni (en nombre décroissant, probablement proportionnel à la fréquence des attaques sur le territoire).
- Catégorie 3 : ceux qui viennent de subir une attaque, et qui ont commencé leur mutation, sans toutefois savoir comment ils vont évoluer ; ils savent seulement qu'il y aura « un avant et un après ».

Dans ce contexte fragilisant et allant vers l'aggravation, il apparait indispensable d'insuffler un changement intellectuel, pour aller vers une culture de sécurité et d'auto-protection.

Ce changement pourrait s'opérer en deux étapes, pour favoriser son assimilation par les professionnels : d'abord une sensibilisation à la menace dès l'école (médicale et paramédicale) et dans les services de soins par un enseignement spécifique, puis des simulations d'attaques, d'abord organisées puis inopinées, pour créer une « culture de défense ». Ces enseignements et exercices devraient être conçus avec la guidance des services de Renseignement, pour assurer une cohérence entre préparation et actualité des menaces. Cette approche peut aussi être appliquée face à la menace de la désinformation sanitaire, que nous aborderons plus loin.

Enfin en cas de sur-attentat hospitalier ou d'intrusion armée, avec identification des auteurs, il peut être intéressant d'envisager une transmission de ces informations aux services de Renseignement Extérieur des pays de la Communauté Européenne, pour anticiper une autre attaque sur leur territoire.

Défense sanitaire informationnelle

Alors que la guerre biologique a toujours été considérée comme une menace exigeant la présence d'un agent biologique [...] à la lumière de l'essor des campagnes de désinformation en ligne soutenues par les États, nous approchons d'une cinquième phase de la guerre biologique, avec un cadre « cyber-bio ».[27]

L'observation de plusieurs évènements (augmentation des cas de rougeole suite aux campagnes de désinformation liées aux élections présidentielles Américaines de 2016, montée de la désinformation dans la pandémie du COVID-19, impact de la désinformation sur les interventions de santé publique pendant les épidémies d'Ebola en Afrique entre 2014 et 2020...) pose la question de l'impact potentiel de ces campagnes (ébranlement des systèmes sociopolitiques, délégitimation des organismes scientifiques et de santé publique, détournement de la réponse de santé publique) qui peut être visualisée comme analogue aux impacts des conceptions plus traditionnelles de la guerre biologique. Nous pouvons alors anticiper l'avènement d'une guerre biologique et cybernétique combinée[28].

Pour reprendre la réflexion évoquée plus haut, les professionnels de santé n'ont généralement aucune culture défensive ; de plus, la culture de la Recherche, sur laquelle est basé le progrès médical, fonctionne sur le principe de la transmission libre et claire de l'information ; elle n'envisage pas le mensonge et la manipulation, encore moins dans une perspective offensive.

De plus, les étudiants sont souvent jeunes, inconscients du potentiel malveillant des médias et réseaux sociaux ; il est donc nécessaire de leur insuffler un esprit critique, pour

mieux percevoir la dimension offensive de ces vecteurs. Cela peut être effectué parallèlement à l'introduction à la recherche, qui nécessite également un esprit critique et une lecture « entre les lignes ».

Enfin, si l'on considère que la santé publique peut désormais être un champ de bataille, aux multiples théâtres (physique, cyber…) il semble indispensable de concevoir un nouvel appareil défensif (à l'image de la DRSD[29] pour les Armées) qui aurait pour responsabilité de lutter contre la désinformation à l'encontre des Autorités sanitaires et de l'infrastructure hospitalière, et ses conséquences sur la santé publique ; cette stratégie pourrait être construite sur le modèle du contre-espionnage ou de la contre-ingérence[30].

Médecine de Sécurité Intérieure

La fréquence des attaques à l'arme blanche à multiples victimes, est en constante augmentation ; dans un certain nombre de cas, l'enquête expose que l'auteur présentait des troubles du comportement, et était suivi en psychiatrie. Il existe un débat sur le lien entre radicalisation djihadiste et troubles psychiatriques, que nous n'aborderons pas ici ; la finalité du propos n'étant pas l'origine mentale de l'acte, mais la communication entre les services de santé publique et la Sécurité Intérieure, pour anticiper l'acte.

En raison du secret médical, cette information n'est généralement pas transmise aux forces de l'ordre, qui ne peuvent donc pas intercepter l'individu avant son passage à l'acte. Il existe des clauses de dérogation au secret médical[31], mais qui n'incluent *a priori* pas la notion de risque offensif, avec menace imminente pour autrui, à l'image de la menace terroriste.

Ainsi, les situations d'attaque à l'arme blanche, à multiples victimes, semblent être un éternel recommencement :

- Un individu armé d'un couteau, en libre circulation, s'en prend sans raison apparente à des passants ; la gravité de l'incident dépend alors de plusieurs facteurs (qualité et quantité des coups infligés, volume de personnes dans l'environnement immédiat, capacité du public à neutraliser l'agresseur, présence de forces de l'ordre à proximité…) et peut engendrer un certain nombre de morts et blessés graves.
- Une fois l'individu neutralisé et les victimes prises en charge, commence alors une enquête qui, dans la majorité des cas, montrera rapidement que l'agresseur était connu pour des troubles psychiatriques graves, mais était inconnu des services de police ; le désastre était donc évitable… désastre qui laissera néanmoins des vies brisées.
- Une fois le choc passé, la vie reprend son cours, jusqu'au prochain épisode.

La solution à cette histoire sans fin se trouve peut-être dans l'instauration d'une relation d'échange entre la psychiatrie (hospitalière et libérale) et la Sécurité Intérieure.

Si l'évaluation par le psychiatre démontre une gravité de l'état pathologique, associé à un fort risque de passage à l'acte offensif sur autrui, cette évaluation pourrait faire l'objet d'une dérogation au secret médical, avec déclaration aux services de renseignements intérieurs (DGSI, DNRT). Cette déclaration serait limitée, car elle ne concernerait que l'identité et la localisation de l'individu ; un score de dangerosité (à définir par des spécialistes) pourrait être envisagé, mais la délivrance complète du dossier médical ne semble pas présenter d'intérêt. La finalité étant d'identifier l'individu, afin de surveiller sa

localisation, notamment à proximité de lieux à risque (musées, spectacles, gares…) et d'anticiper un acte violent sur la foule.

Signalement qui pourrait être élargi à la Communauté Européenne, *via* Europol ou la coopération du Renseignement Extérieur, pour repérer plus d'agresseurs potentiels, et protéger un plus grand espace. Le couplage de ce signalement à la reconnaissance faciale par caméra, dans les zones à risque, présenterait probablement une plus-value supplémentaire.

Il est probablement impossible d'anticiper tout comportement violent, surtout vis-à-vis d'un esprit affecté par la maladie ; on peut de donner une chance de limiter le risque, grâce aux technologies disponibles, et à une meilleure communication entre les mondes de la Santé et de la Sécurité.

Notes

1. Master criminologie et NRBCE ; analyste au centre de veille & alerte du Ministère des Transports ; doctorant en renseignement médical et défense sanitaire, ESDR3C (CNAM) et SAMU-Paris,
2. Jonathan D. Clemente, « Medical Intelligence », *Journal of U.S. Intelligence Studies* 20, nº 2 (2013).
3. Claude Lefebvre et Guillaume Weiszberg, *Les armes de destruction massive et leur interdiction* (L'Harmattan, 2019).
4. Juha A. Vuori, « A Timely Prophet? The Doomsday Clock as a Visualization of Securitization Moves with a Global Referent Object », *Sage Journals* 41, nº 3 (7 juin 2010), https://doi.org/10.1177/0967010610370225.
5. Erik Dahl, *Intelligence and Surprise Attack : Failure and Success from Pearl Harbor to 9/11 and Beyond*, 2013.
6. Gregory Ciottone *et al.*, *Ciottone's Disaster Medicine*, Elsevier, 2015.
7. Joshua Michaud, « National Center for Medical Intelligence », in *Encyclopedia of Bioterrorism Defense* (John Wiley & Sons, Ltd, 2011), 1-3, https://doi.org/10.1002/0471686786.ebd0175.
8. « Guide to Medical Intelligence Handbook », Standards Related Document (OTAN, janvier 2018).
9. « Declassified Intelligence Community assessment on COVID-19 origins » (Office of the Director of National Intelligence, 29 octobre 2021), https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2021/3583-declassified-assessment-on-covid-19-origins.
10. Roger Brent, T.Greg jr McKelvey, et Jason Matheny, « The new bioweapons: how synthetic biology could destabilize the world », *Foreign Affairs*, 20 août 2024, https://www.foreignaffairs.com/world/new-bioweapons-covid-biology.
11. Brent, McKelvey, et Matheny.
12. Brent, McKelvey, et Matheny.
13. « Gérald Darmanin destinataire d'un courrier où des traces de peste ont été retrouvées », Huffington Post, 28 juillet 2024, https://www.huffingtonpost.fr/faits-divers/article/gerald-darmanin-destinataire-d-un-courrier-ou-des-traces-de-peste-ont-ete-retrouvees_237553.html.
14. « fiche médicale : peste », Institut Pasteur, s. d., https://www.pasteur.fr/fr/centre-medical/fiches-maladies/pestehttps://www.pasteur.fr/fr/centre-medical/fiches-maladies/peste.
15. Erik Dahl, *The COVID-19 intelligence failure : why warning was not enough.* (Georgetown University Press, 2023).
16. « Tabletop exercise: Dark Winter », Johns Hopkins Center for Health Security, s. d., https://centerforhealthsecurity.org/our-work/tabletop-exercises/dark-winter-a-training-tabletop-exercise.
17. « Pourquoi l'OMS a classé l'épidémie de mpox en Afrique comme "urgence de santé publique de portée internationale" », *Le Monde*, 15 août 2024, https://www.lemonde.fr/planete/article/2024/08/15/pourquoi-l-oms-a-classe-l-epidemie-de-mpox-en-afrique-urgence-de-sante-publique-de-portee-internationale_6281426_3244.html.

18. Lionel Cavicchioli, « Virus de l'encéphalite équine de l'Est aux États-Unis : quel niveau de menace ? », *The Conversation*, 2 septembre 2024, https://theconversation.com/virus-de-lencephalite-equine-de-lest-aux-etats-unis-quel-niveau-de-menace-237891.
19. « Le rôle des CHU dans l'enseignement supérieur et la recherche médicale » (Cour des comptes, 1 décembre 2017), https://www.vie-publique.fr/rapport/267827-role-chu-dans-lenseignement-superieur-et-la-recherche-medicale.
20. Pierre Pasquier, Stéphane Mérat, et Marie-Dominique Colas, *Le blessé par attentat terroriste*, Arnette, 2017.
21. APHP, « SSPI - Accueil des polytraumatisés », Département d'anesthésie-réanimation - CHU Pitié Salpêtrière, s. d., https://pitiesalpetriere.aphp.fr/anesthesie-reanimation/#1487529159476-8de83a1e-dfe0.
22. « Le dispositif ORSAN : cadre intégré de préparation et de réponse du système de santé aux situations sanitaires exceptionnelles », Ministère de la Santé, 6 août 2024, https://sante.gouv.fr/prevention-en-sante/securite-sanitaire/article/le-dispositif-orsan-cadre-integre-de-preparation-et-de-reponse-du-systeme-de.
23. « Le plan Vigipirate », SGDSN, s. d., https://www.sgdsn.gouv.fr/vigipirate/le-plan-vigipirate-faire-face-ensemble.
24. *Entretien de recherche doctorale, renseignement chirurgical* (CHUs Pitié Salpêtrière et Bichat, 2024).
25. Julien Marx *et al.*, « L'hôpital attaqué », *La Presse Médicale Formation* 5, nº 3 (juin 2024) : 225-31, https://doi.org/10.1016/j.lpmfor.2024.04.003.
26. C Broux, F-X Ageron, et C Jacquot, « Filières de soins en traumatologie, une organisation indispensable », *Société de Réanimation de Langue Française*, 15 septembre 2010, https://doi.org/10.1016/j.reaurg.2010.08.004.
27. Rose Bernard *et al.*, « Disinformation and epidemics: anticipating the next phase of biowarfare », *Health Security* 19, nº 1 (2021), https://doi.org/10.1089/hs.2020.0038.
28. Bernard *et al.*
29. « Direction du Renseignement et de la Sécurité de la Défense », s. d., https://www.drsd.defense.gouv.fr/nos-missions.
30. « The foreign malign influence center », Office of the Director of National Intelligence, s. d., https://www.odni.gov/index.php/fmic-home.
31. « Secret médical : respect, partage, dérogation et violation », santé.fr, 12 août 2019, https://www.sante.fr/secret-medical-respect-partage-derogation-et-violation#p-4.