ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus
Biologies

Alain-Jacques Valleron

Biosécurité et surveillance épidémiologique

Volume 347 (2024), p. 181-186

En ligne depuis le 13 novembre 2024

https://doi.org/10.5802/crbiol.166

Les Comptes Rendus. Biologies *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org — e-ISSN : 1768-3238

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus. Biologies
2024, Vol. 347, p. 181-186
https://doi.org/10.5802/crbiol.166

Article de synthèse

Biosécurité et surveillance épidémiologique

Alain-Jacques Valleron [a]

[a] Académie des sciences, Paris, France
Courriel : alain-jacques.valleron@academie-sciences.fr

Résumé. La biosécurité concerne d'une part les mesures à mettre en œuvre dans les laboratoires pour éviter par exemple la dissémination accidentelle d'agents infectieux, et d'autre part la lutte contre des actes éventuels de bioterrorisme, ou de guerre utilisant des armes biologiques. La surveillance épidémiologique est souvent vue comme un outil indispensable pour renforcer la biosécurité. Cependant, la surveillance épidémiologique traditionnelle, qui vise à aider les choix de politiques de santé, n'a pas les qualités de sensibilité nécessaires aux tâches de sécurité sanitaire. Celles-ci nécessitent en effet avant tout un système d'alerte rapide. Dans les années récentes, il est apparu de nombreux outils biologiques prometteurs comme la surveillance des eaux usées, le développement grâce aux techniques CRISPR de nouveaux outils de détection des agents infectieux. Un défi à surmonter est de faire face aux risques que représentent les nouvelles techniques biologiques à cause de leur faible coût et de leur simplicité qui les rend accessibles à des personnes extérieures aux laboratoires établis. Enfin, l'enjeu principal n'est pas seulement la découverte rapide d'un défaut de sécurité, qui est facilitée par les outils informatiques actuels, mais la mise au point d'une articulation efficace entre cette découverte rapide, et l'identification et la connexion des bons professionnels biomédicaux et des moyens techniques capables d'y faire face.

Mots-clés. Surveillance, Alerte, Bioterrorisme.
Manuscrit reçu le 11 juillet 2024, accepté le 7 octobre 2024.

1. Qu'est-ce que la biosécurité ?

La définition de la « biosécurité » est compliquée. Celle du Conseil national consultatif pour la biosécurité (CNCB) concerne les risques créés par les armes biologiques et chimiques (voir : https://www.sgdsn.gouv.fr/nos-missions/anticiper-et-prevenir/lutter-contre-la-proliferation/le-conseil-national-consultatif). Mais une interrogation internet montre que cette définition est beaucoup plus large pour le grand public, et inclut par exemple les risques induits par les microbes pathogènes susceptibles de contaminer les élevages d'animaux domestiques, ou la faune sauvage.

Le mot « biosécurité » pose de plus un problème particulier, car il recouvre deux notions très différentes, exprimées en anglais par des mots (et une littérature) différents : « biosafety » et « biosecurity ». La « biosafety » concerne la dissémination accidentelle et non intentionnelle de toxines ou d'agents infectieux manipulés dans les laboratoires. La « biosecurity », elle, concerne une contamination causée volontairement, par exemple dans un acte bioterroriste. Un exemple simple de la distinction entre « biosafety » et « biosecurity » peut être trouvé en pensant au transport d'agents biologiques dangereux. Au nom de la « safety » il faudrait étiqueter des échantillons de variole. Mais au nom de la « security » cet étiquetage fait courir des risques car il rend les échantillons facilement repérables par des personnes mal intentionnées.

Nous utiliserons dans ce texte biosécurité selon l'usage français qui regroupe les deux sens du mot, mais en essayant de les identifier. Notons que, dans ses deux sens, la biosécurité concerne des actions individuelles (celle d'un chercheur laissant par négligence échapper de son laboratoire un agent infectieux, ou celle d'un terroriste disséminant volontairement un agent infectieux). La biosécurité ne concerne pas, en revanche, la lutte contre les risques

épidémiques « naturels », comme ceux concernant les maladies (ré)émergentes, ou ceux de nouvelles épidémies causées par la mauvaise observation des règles de vaccination obligatoire.

2. La surveillance épidémiologique

La nécessité d'une surveillance épidémiologique performante est classiquement immédiatement évoquée lorsqu'on cherche comment améliorer la biosécurité, dans les deux sens de ce mot. L'importance de la surveillance épidémiologique des maladies infectieuses est apparue au milieu du 20^{e} siècle. Alexander Langmuir, épidémiologiste aux « Centers for Disease Control and prevention » (actuels CDC), écrivit en 1963 l'article princeps [1] qui définit encore maintenant la surveillance : c'est « la collecte systématique et active des données pertinentes sur les maladies ciblées, les rapports analysant ces données, leur communication aux personnes et institutions ayant la responsabilité des actions à mettre en œuvre ». La qualité d'un système de surveillance épidémiologique ne s'apprécie donc pas seulement par le nombre et la qualité des données recueillies. Elle s'apprécie aussi en évaluant comment ses résultats sont communiqués non seulement aux responsables de la santé publique, mais à tous les acteurs concernés : médecins et grand public. Dans ses débuts, la surveillance épidémiologique avait pour but primordial de guider les politiques de santé publique, par exemple dans le domaine de la vaccination. Il était donc crucial d'avoir des données de qualité. Souvent la source de ces données était mal contrôlée : c'était par exemple des consultations de médecins généralistes, non formés à recueillir des données de façon standardisée, et sans moyens efficaces de communication. Aussi, beaucoup de temps s'écoulait entre l'observation d'un événement d'intérêt par un professionnel de santé, sa notification (rare) dans un système de surveillance, sa validation (longue) par les autorités de santé, sa publication, et les actes qu'elle impliquait éventuellement. Dans les années 80, la téléinformatique a permis de renouveler la surveillance épidémiologique, en facilitant le recueil de données dans de multiples sources, et — surtout — en permettant la communication immédiate de ses résultats, analysés en détail, à tous ses acteurs, notamment à ceux qui en étaient à la source [2]. Puis Internet a diffusé massivement les outils de la téléinformatique à l'ensemble du grand public, facilitant des retours d'information détaillés et généralisés, ainsi que la communication en temps réel entre tous les acteurs impliqués, changeant ainsi la dimension et la portée des systèmes de surveillance. En permettant l'exploitation immédiate des données de surveillance, la téléinformatique (« le web ») a permis d'envisager de passer à des applications d'« alerte » où le signal d'un événement intéressant peut être immédiatement transmis à tous ceux qui sont en charge des actions correspondantes. Or, c'est précisément d'un système d'alerte efficace que le domaine de la sécurité sanitaire a besoin.

Un cadre administratif précis existe pour guider la politique de surveillance : depuis 2005, le Règlement sanitaire international (*International Health Regulations*, abrégé par IHR 2005), précise les mesures que les 194 états membres doivent prendre pour prévenir la diffusion de maladies. Ceci concerne en particulier la surveillance épidémiologique de l'ensemble des maladies, et notamment les Urgences de santé publique de portée internationale (*Public Health Emergency of International Concern*, PHEIC). La définition de ces urgences est faite par le Directeur Général de l'OMS. Elle inclut les maladies émergentes, et d'éventuels actes bioterroristes. Les problèmes pouvant limiter la mise en œuvre de ce traité, qu'ils soient techniques, liés au manque de ressources idoines dans beaucoup de pays, ou juridiques (s'ils contredisent des législations en place) sont nombreux et ont été discutés en détail par Baker et Fidler [3].

3. Le bioterrorisme

Ce sujet relève de la composante « biosecurity », et la lutte contre le bioterrorisme est placée au premier rang des priorités. Une première question est cependant de savoir si le bioterrorisme est un risque important, ou en croissance. Les bases de données existantes permettent de répondre à cette question.

Le CDC lança en 2003 le programme Biosense [4] destiné à la détection rapide des affections possiblement générées par une tentative bioterroriste ; ce programme mettait en application le *Public Health Security and Bioterrorism Preparedness and Response Act* de 2002. En 2014, le CDC lança ensuite la *Biosense Enhancement Initiative* qui avait pour but, dans sa stratégie de surveillance épidémiologique, d'améliorer les procédures de communication et d'analyse

des données. C'est dans ce contexte que l'Université du Maryland a constitué une base de données (*Global Terrorism Database*, GTD) [5] qui décrit les plus de 200 000 événements terroristes « internationaux » de toute sorte survenus dans la période 1970–2020. Ce travail énorme fut financé par diverses agences des gouvernements américain, anglais et allemand. La base de données est d'accès libre et documente facilement les méthodes employées, le nombre des victimes, le lieu des attentats, etc.) (consulter : https://www.start.umd.edu/gtd/). Dans cette base de données, il est possible de retrouver, en tout, 38 attentats de nature biologique (en sélectionnant grâce au moteur de recherche les actes terroristes ayant utilisé une « biological weapon »). C'est donc une infime minorité, par conséquent, de l'ensemble des attaques terroristes. Il n'y a pas d'attaque fichée en France ; il y a 24 attaques listées aux USA, dont cinq avec un ou deux décès. Cinq de ces attaques sont postérieures à 2010. Faut-il se rassurer de ces petits chiffres ? Le bioterrorisme n'a pas été le danger majeur parfois imaginé. Qu'en sera-t-il dans l'avenir ? La prédiction qui fonde la prévention est un art difficile !

La surveillance épidémiologique pourrait-elle renforcer sa vigilance pour permettre la détection rapide de maladies causées par un acte bioterroriste ? Une revue systématique de la littérature publiée en 2004 [6] a analysé 115 systèmes mondiaux de surveillance capables de détecter des événements bioterroristes. Elle a identifié deux catégories de systèmes : ceux qui effectuent de la surveillance « syndromique » (fondée sur la collection de cas atteints d'un certain syndrome, en général celui des symptômes grippaux) et ceux reposant sur la collecte de données environnementales, comme c'est le cas de l'*Integrated Biological Detection System* (IBDS) développé par l'armée britannique. La conclusion de cette revue est mitigée sur l'utilité pratique de ces systèmes, faute d'évaluation fiable de leur sensibilité et rapidité de détection. Une étude détaillée de la surveillance syndromique a été faite à l'occasion des attentats à l'Anthrax effectués aux États Unis en 2001 (un des rares exemples de bioterrorisme, dont l'auteur très probable était un biologiste qui se suicida). Les cas des 11 personnes contaminées ont été examinés et l'évaluation de l'utilité qu'aurait pu avoir une approche de surveillance syndromique, comparée à la simple détection fournie par les cliniciens, a été jugée négative. Ces réserves semblent s'appliquer aussi à la peste, au botulisme, à la variole et aux fièvres hémorragiques lorsque les mêmes évaluations ont été réalisées [7]. Remarquons cependant que, s'ils ne paraissent pas aptes à détecter efficacement des événements très rares comme le serait une attaque terroriste biologique ou chimique, les systèmes sentinelles sont de coût faible et ont un grand intérêt pour décrire rapidement les épidémies « habituelles » : un exemple en est le système PROMED [8] développé aux USA depuis 1994, avec des correspondants dans le monde entier et qui alerte journellement sur de nouvelles épidémies. D'autre part, la surveillance syndromique, couplée à une exploitation des données des réseaux sociaux, pourrait être utile en cas de rassemblements de masse localisés [9], comme ceux des jeux olympiques de Paris [10]. Un évènement infectieux soudain du type syndrome grippal, qui survient dans nombre d'infections causées par une attaque terroriste, pourrait facilement être ainsi identifié.

4. Les armes biologiques de destruction massive

En principe, les armes biologiques de destruction massives sont interdites par la convention de Genève de 1925. Mais ces armes ont néanmoins été développées, et utilisées, dans l'histoire moderne, notamment pendant la seconde guerre mondiale par le Japon qui y consacra des unités spécialisées, avec comme résultat des milliers de morts, par exemple de la peste en Chine [11]. La possibilité d'actions de guerre biologique à l'initiative de groupes terroristes ou d'états « voyous » existe toujours ; il est donc nécessaire de disposer d'outils sensibles et surtout très rapides d'alerte analysant toutes les sources possibles d'information, très variées, qui sont disponibles. La variété de ces sources mène à des « big data » pour lesquelles des méthodes de plus en plus puissantes d'analyse existent [12]. Celles-ci peuvent aider à identifier plus rapidement une maladie émergente, une action de guerre biologique, ou une attaque terroriste, précisément parce qu'elles sont capables de traiter de grandes quantités d'information de natures différentes. On peut aussi en sens inverse arriver à déterminer, à partir de l'analyse de « big data », en particulier en utilisant de puissantes méthodes de visualisation de l'information comme l'a étudié un meeting de l'OTAN [13], ce qui peut être

utilisé dans les ressources actuelles pour développer de nouvelles armes biologiques.

5. La biosécurité

La biosécurité dans les laboratoires implique une action sur des domaines très différents, incluant les méthodes de stockage, de transport des agents et les innombrables étapes de leur manipulation. De nombreux accidents liés à un défaut de biosécurité ont été signalés, causés par le manque de respect d'une préconisation existante.

L'énorme développement ces dernières années de la biologie synthétique, utilisant des outils informatiques complexes et l'automatisation de nombreuses pratiques de laboratoire, mène à de nombreuses applications remarquables, mais parallèlement à de nouveaux risques dans les laboratoires.

Elle pose de nouveaux et importants problèmes de biosécurité, par exemple de cybersécurité à cause de l'utilisation, qui peut être mal contrôlée, des banques de données génomiques et cliniques [14]. La difficulté de contrôler ces risques tient en particulier au fait que beaucoup d'équipes pratiquant la biologie synthétique sont de statut privé, de petite taille, et travaillent en dehors du monde universitaire. Elles sont — par conséquent — peu soumises à la discipline de la biosécurité telle qu'elle est diffusée dans le milieu universitaire public. La surveillance épidémiologique traditionnelle ne semble pas être un moyen de lutte possible contre les défauts de biosécurité qu'ils soient traditionnels, ou concernent la biologie synthétique. Il faut plutôt promouvoir des approches d'assurance qualité, et rechercher la déclaration volontaire exhaustive des multiples défaillances de sécurité, et leur analyse, sans l'associer à des sanctions, de sorte d'amener les biologistes à eux-mêmes construire un environnement évitant ces risques.

6. Nouvelles techniques biologiques appliquées à la surveillance épidémiologique

La surveillance de la présence de nombreux pathogènes dans une communauté peut être effectuée à partir des eaux usées, et ceci s'applique à la découverte de la présence d'agents bioterroristes éventuels [15]. Dans les années récentes, l'avancée des techniques biochimiques et génomiques a permis des réussites remarquables dans ce domaine de la surveillance épidémiologique. Grâce à elle, les prélèvements effectués dans des stations d'épuration de 101 pays a permis par exemple de documenter une géographie mondiale des gènes de résistance aux antibiotiques [16]. La pandémie de COVID-19 a aussi illustré la puissance de ces méthodes, en identifiant grâce à l'analyse des eaux usées, des variants qui n'avaient pas été détectés auparavant. La métagénomique est une approche puissante, dont la limitation est la difficulté de travailler en temps réel à la collecte des données [17].

De leur côté, les techniques CRISPR d'édition de gènes permettent de développer des outils nouveaux de reconnaissance et de caractérisation des agents infectieux. Leur succès a été reconnu lors de la pandémie de COVID19 où ils permirent de développer des outils diagnostiques très rapides [18]. Cependant, bien entendu, ces outils font aussi apparaître de nouveaux risques. Ils sont en effet facilement accessibles, de coût assez faible, et pourraient être (sont) utilisés en dehors des laboratoires de recherche pour créer de nouveaux agents infectieux. Ainsi, on a montré que de l'ADN sur commande pouvait être utilisé pour créer *de novo* un virus de la variole équine [19].

7. Conclusion : surveillance et alerte doivent être pensées pour l'action

Si, pour l'instant, les actes de bioterrorisme restent rarissimes, on sait que les outils biologiques pour en créer sont là, et même qu'il y en a de nouveaux. Les moyens pour créer des armes biologiques de masse existent aussi. L'acquisition de beaucoup des techniques « utiles » à cet égard est facile et est « ouverte » , ce qui signifie qu'elle est disponible pour des « non professionnels » de la biologie. Là est le risque principal. On doit, de plus, aussi considérer le risque inverse de celui de bioterroristes devenant biologistes, à savoir celui de biologistes professionnels entrant dans une démarche terroriste. Tous ces risques sont -on peut l'espérer- très faibles. Mais ils ne sont pas nuls.

La surveillance épidémiologique est souvent imaginée pouvoir être une des réponses à tous ces risques. En fait, elle ne dispose pas de techniques révolutionnaires, et la plus grande force des méthodes de surveillance modernes est la capacité que

nous avons, maintenant, à recevoir et communiquer à grande échelle, en temps réel, les informations épidémiologiques. Cependant, la surveillance épidémiologique est destinée avant tout à guider la politique de santé publique au cours du temps. Par exemple, la surveillance de la rougeole, lorsqu'elle fit apparaître dans les années 2000 une recrudescence des cas, a été particulièrement utile pour se rendre compte de l'urgence qu'il y avait à revitaliser la politique de vaccination [20]. Dans le domaine de la surveillance épidémiologique, le délai entre l'arrivée de l'information et les actions correspondantes — variées et complexes — qui devraient en découler peut être long, contrairement à ce dont on a besoin dans un système d'alerte. La surveillance épidémiologique n'est donc pas l'outil garantissant un système d'alerte fort en cas d'attaque bioterroriste, ou d'un événement nocif causé par un défaut de sécurité sanitaire, comme par exemple l'échappement non contrôlé d'agents infectieux depuis un laboratoire de recherche. « Surveillance » et « alerte » ne doivent pas être confondus.

Dans le domaine du bioterrorisme, et de la sécurité sanitaire en général, le mot clé doit être plutôt « alerte » que « surveillance ». On veut au service de la biosécurité un système d'alerte efficace, c'est-à-dire un système qui avertisse très rapidement si un des événements redoutés survient. Alors qu'on attend d'un système de surveillance qu'il ait une bonne spécificité, car on veut éviter que des cas notifiés pour une maladie soient en fait des cas d'une autre maladie, la qualité principale recherchée pour un système d'alerte est la sensibilité (c'est-à-dire sa probabilité forte d'émettre un signal lorsqu'il est face à un des événements redoutés). On comprend donc que les critères permettant de juger la qualité d'un système d'alerte ne sont pas simplement ceux de la qualité d'un système de surveillance.

Enfin, la raison d'être d'un système d'alerte épidémiologique ne doit pas être… l'alerte, mais l'efficacité de l'action prise en cas d'alerte. Ce qui compte n'est pas le délai entre le moment où un défaut de sécurité sanitaire apparaît et son signalement. C'est le délai entre le moment où ce défaut de sécurité sanitaire apparaît et le moment où son contrôle efficace est mis en place qui compte. Or ce paramètre est d'une grande complexité : selon l'événement de sécurité sanitaire en cause, les spécialistes à contacter, les traitements à donner, les lieux de traitement seront différents. Un exemple de cette complexité a été bien illustré par la présentation de l'ensemble des mesures à prendre en analysant finement la découverte de cas d'anthrax d'origine bioterroriste [21].

La surveillance et l'alerte ne doivent pas être pensées sans que leur articulation avec la « préparation à l'action » ne soit prévue. L'organisation de cette préparation à l'action (en anglais : « preparedness ») est un chapitre différent de celui de la surveillance et de l'alerte ; il doit recevoir le niveau maximum de priorité.

Déclaration d'intérêts

Les auteurs ne travaillent pas, ne conseillent pas, ne possèdent pas de parts, ne reçoivent pas de fonds d'une organisation qui pourrait tirer profit de cet article, et n'ont déclaré aucune autre affiliation que leurs organismes de recherche.

Références

[1] A. D. Langmuir, « The surveillance of communicable diseases of national importance », *N. Engl. J. Med.* **268** (1963), p. 182-192.

[2] A. J. Valleron, E. Bouvet, P. Garnerin *et al.*, « A computer network for the surveillance of communicable diseases: the French experiment », *Am. J. Public Health* **76** (1986), p. 1289-1292.

[3] M. G. Baker, D. P. Fidler, « Global public health surveillance under new international health regulations », *Emerg. Infect. Dis.* **12** (2006), p. 1058-1065.

[4] D. W. Gould, D. Walker, P. W. Yoon, « The evolution of biosense: lessons learned and future directions », *Public Health Rep.* **132** (2017), p. 7S-11S.

[5] J. Wigle, « Introducing the worldwide incidents tracking system (WITS) », *Perspect. Terrorism* **4** (2021), p. 3-23.

[6] D. M. Bravata, K. M. McDonald, H. Szeto, W. M. Smith, C. Rydzak, D. K. Owens, « A conceptual framework for evaluating information technologies and decision support systems for bioterrorism preparedness and response », *Med. Decis. Making* **24** (2004), p. 192-206.

[7] J. W. Buehler, R. L. Berkelman, D. M. Hartley, C. J. Peters, « Syndromic surveillance and bioterrorism-related epidemics », *Emerg. Infect. Dis.* **9** (2003), p. 1197-1204.

[8] M. Carrion, L. C. Madoff, « ProMED-mail: 22 years of digital surveillance of emerging infectious diseases », *Int. Health* **9** (2017), p. 177-183.

[9] T. Hanslik, P. Y. Boelle, A. Flahault, « Setting up a specific surveillance system of community health during mass gatherings », *J. Epidemiol. Community Health* **55** (2001), p. 683-684.

[10] A. C. Berry, « Syndromic surveillance and its utilisation for mass gatherings », *Epidemiol. Infect.* **147** (2018), article no. e2.

[11] V. Barras, G. Greub, « History of biological warfare and bioterrorism », *Clin. Microbiol. Infect.* **20** (2014), p. 497-502.

[12] K. M. Vogel, « Big data and biodefense: prospects and pitfalls », in *Defense Against Biological Attacks*, Springer, Cham, 2019, p. 297-315.

[13] NATO, *Distributed Data Analytics for Combating Weapons of Mass Destruction*, STO, MP-IST-1312017, ISBN: 978-92-837-2089-8.

[14] D. DiEuliis, C. D. Lute, J. Giordano, « Biodatarisks and synthetic biology: a critical juncture », *J. Bioterror. Biodef.* **9** (2018), p. 159-171.

[15] R. G. Sinclair, C. Y. Choi, M. R. Riley, C. P. Gerba, « Pathogen surveillance through monitoring of sewer systems », *Adv. Appl. Microbiol.* **65** (2008), p. 249-269.

[16] P. Munk, C. Brinch, F. D. Moller *et al.*, « Genomic analysis of sewage from 101 countries reveals global landscape of antimicrobial resistance », *Nat. Commun.* **13** (2022), article no. 7251.

[17] M. B. Diamond, A. Keshaviah, A. I. Bento *et al.*, « Wastewater surveillance of pathogens can inform public health responses », *Nat. Med.* **28** (2022), p. 1992-1995.

[18] K. E. Watters, J. Kirkpatrick, M. J. Palmer, G. D. Koblentz, « The CRISPR revolution and its potential impact on global health security », *Pathog. Glob. Health* **115** (2021), p. 80-92.

[19] A. S. Khan, P. S. Amara, S. A. Morse, « Forensic public health: epidemiological and microbiological investigations for biosecurity », in *Microbial Forensics*, Elsevier, 2020, chapter 8, p. 105-122.

[20] I. Parent du Chatelet, D. Floret, D. Antona, D. Levy-Bruhl, « Measles resurgence in France in 2008, a preliminary report », *Euro. Surveill.* **14** (2009), nº 6, p. 5-7.

[21] M. A. Honein, A. R. Hoffmaster, « Responding to the threat posed by anthrax: Updated evidence to improve preparedness », *Clin. Infect. Dis.* **75** (2022), p. S339-S340.