Médecine de Catastrophe - Urgences Collectives 2020;4(4):295–300

La gestion de crise intra-hospitalière face à la menace terroriste

Hospital intra-crisis management facing terrorist attack

Matthieu Langlois [a,b]
Mathieu Raux [b,c]

[a] *Service médical du RAID, RAID — Police nationale, France*
[b] *Département d'anesthésie-réanimation, groupe hospitalier universitaire AP–HP, Sorbonne université, AP–HP, site Pitié-Salpêtrière, 75013 Paris, France*
[c] *Inserm, UMRS1158, neurophysiologie respiratoire expérimentale et clinique, Sorbonne université, Paris, France*

RÉSUMÉ

Les hôpitaux représentent, de toute évidence, une cible sensible pour une agression collective à caractère terroriste. Le fonctionnement très particulier associant une activité de soins permanents, milieu par définition ouvert, et une capacité à accueillir, à tout moment, un afflux de blessés va déterminer la réponse stratégique en cas d'intrusion. Cette réponse doit impérativement être coordonnée entre, d'une part, la direction de l'hôpital, l'équipe de soins et, d'autre part, les acteurs publics de la sécurité intérieure et du secours. Cela demande une préparation spécifique impliquant, en premier lieu, la cellule de crise, mais aussi l'ensemble du personnel hospitalier. L'élaboration d'un plan, régulièrement remis à jour et connu de tous, sera indispensable pour réduire au mieux la phase initiale de chaos. Il est urgent d'introduire une culture de l'exercice dans les hôpitaux. Sans monopoliser inutilement le personnel, mais en cherchant avant tout à évaluer sa capacité pour répondre à une intrusion. La coordination des équipes soignantes avec la police et les secours (pompiers et samu) est essentielle. Elle est la clé de la réussite. Elle doit donc être travaillée, sans relâche, par les acteurs qui occuperont une place de décideur dans les différents postes de commandement ou cellule de crise. En outre, il faut impérativement se préparer à être surpris et mis sous forte tension. La déstabilisation de l'hôpital agressé est logique, mais la poursuite de l'activité est un enjeu majeur. Les mouvements de foule spontanée, dans et autour de l'hôpital, impacteront fortement la stratégie de réponse. Ils sont, certes, difficiles à modéliser, mais ne pas les anticiper serait une erreur. Enfin, il est primordial d'anticiper un point de rupture pour garder un peu d'avance dans l'organisation de la réponse, même s'il ne fait aucun doute qu'une acceptation de l'imprévu est obligatoire. Cela aussi doit s'appréhender.

MOTS CLÉS

Attaque terroriste
Hôpital
Management de crise

KEYWORDS

Terrorist attack
Hospital
Crisis management

SUMMARY

Hospitals are clearly a sensitive target for a collective terrorist attack. The very particular way in which they operate, combining a permanent care activity, an open environment by definition, and a capacity to receive an influx of wounded at any time, will determine the strategic response in the event of an intrusion. This response must be coordinated between the hospital management, the care team and the public internal security and rescue services. This requires specific preparation involving, in the first instance, the crisis unit but also all hospital staff. The development of a plan, regularly updated and known to all, will be essential to reduce the initial phase of chaos as much as possible. There is an urgent need to introduce a culture of exercise in hospitals. Without unnecessarily monopolizing staff, but above all seeking to assess their capacity to respond to an intrusion. The coordination of health care teams with the Police and the emergency services (fire brigade and samu) is essential. It is the key to success. It must therefore be worked on relentlessly by the players who will occupy a decision-making position in the various command posts or crisis units. Furthermore, it is imperative to prepare to be surprised and put under high tension. The destabilisation of the hospital under attack is logical, but the continuation of the activity is a major challenge. Spontaneous crowd movements in and around the hospital will have

Auteur correspondant.
M. Langlois,
Service médical du RAID,
Domaine du Bel air
91570 Bièvres, France.
Adresse e-mail :
matthieu.langlois@aphp.fr

doi:10.1016/j.pxur.2020.06.008

M. Langlois, M. Raux

a strong impact on the take not to anticipate them. Finally, it is essential to anticipate a breaking point in order to stay a little ahead in the organization of the response, even if there is no doubt that an acceptance of the unexpected is mandatory. This too must be understood.

Les centres hospitaliers constituent par nature une cible intéressante à toutes formes d'agression perpétrée par des organisations terroristes [1]. Ils sont facilement accessibles, accueillent massivement du public et sont pour le moment moins sécurisés que d'autres catégories d'établissements (écoles, gares, salles de concerts, stades, etc.). De plus, ils sont fréquentés par un public sensible, d'une part, des personnes malades, blessées ou dépendantes et, d'autre part, du personnel soignant, dont la blessure ou la mort créerait inévitablement un fort retentissement sur l'opinion publique. Or, on sait que cette caractéristique est fondamentale dans la motivation de l'acte terroriste. . .

Bien qu'aucune attaque n'ait visé des hôpitaux en France, la récente intervention du « Recherche-assistance-intervention-dissuasion » (RAID) aux CHU de Caen en mars et de Dunkerque en octobre 2018 pour une suspicion d'intrusion terroriste dans les locaux a démontré qu'une réponse spécifique devait absolument être développée et anticipée par les acteurs de la gestion de crise. Le RAID dispose non seulement d'une expérience unique en la matière, mais la présence de médecins hospitaliers intégrés au sein du service permet un partage de culture entre monde de la sécurité intérieure et monde hospitalier à l'origine de ce travail.

Un établissement de soins doit pouvoir, en cas d'agression, y répondre et éviter au maximum l'interruption d'activité, voire la perte de capacité opérationnelle. Il doit pour cela non seulement assurer la continuité des soins, mais également proposer un circuit interne et rapide pour soigner les blessés les plus graves. Le centre hospitalier constitue simultanément la cible qui doit se défendre et l'un des acteurs majeurs de la réponse à la crise. Cette dualité est particulièrement complexe motivant en grande partie notre réflexion de par notre savoir-faire et notre expérience de terrain.

On peut raisonnablement se montrer optimiste sur la capacité d'un centre hospitalier à affronter une crise terroriste, dans la mesure où il dispose « ab initio » d'atout majeurs dans la gestion d'un tel événement : bâtiments adaptés aux grands flux de personnes et de véhicules, matériel dédié et personnel formé à la prise en charge de blessés sur place, responsables entretenant des relations habituelles avec le samu, l'Agence régionale de santé et les acteurs locaux du secours et de la sécurité.

Toutefois, la capacité d'une structure n'emporte pas de facto sa compétence. La survenance d'une attaque terroriste est par nature déstructurante et seuls des professionnels avertis (à défaut d'être aguerris) seront en capacité d'apporter une réponse efficace au chaos ambiant. La réponse opérationnelle des services de sécurité intérieure (police, gendarmerie) et de secours (sapeurs-pompiers et samu) à une attaque terroriste sera d'autant plus efficace qu'elle s'appuiera sur le ou les responsables du site attaqué. En tant que gestionnaire de centre hospitalier ou directeur médical de crise, il convient de bien intégrer ce paradigme.

COMMENT PRÉPARER SON ÉTABLISSEMENT ?

La principale clef de la gestion de crise dans un hôpital confronté à une attaque terroriste, c'est la préparation [2]. Cette préparation peut se décliner en trois points concrets : la constitution d'un plan de réponse [3], l'entraînement à la crise et l'identification d'un point de rupture.

Un plan de réponse

La constitution d'une planification en cas d'intrusion est la première pierre à l'édifice de la sécurité des établissements hospitaliers. Dans ce plan figurent un certain nombre d'items destinés à anticiper les risques physiques, qu'ils soient de nature terroriste ou non [4]. Le plan porte à la fois sur des solutions techniques et organisationnelles. Car il ne suffit pas d'acquérir des portiques détecteurs de métaux ou des barrières anti-intrusions, encore faut-il du personnel opérationnel qui sache les utiliser ! L'identification claire des personnes ressources en capacité de décision est cruciale, car le moment venu ils seront au cœur de la gestion de crise. Leur rôle primordial est de conseiller et d'informer les forces de sécurité et de secours. Dans cette perspective, deux acteurs au minimum doivent être impliqués : le directeur d'établissement et des soins et le directeur médical de crise.

Le détenteur de l'autorité est le chef d'établissement, directeur du centre hospitalier. La responsabilité générale de la sûreté et de la sécurité sur le site lui revient, que ce soit au quotidien ou en cas de crise. Il s'appuie lui-même sur un ou des collaborateurs compétents en la matière (responsable sécurité incendie par exemple), qui connaissent les lieux et pourront mettre en œuvre les moyens techniques nécessaires à la gestion de la crise (coupure des flux, ouverture et fermeture des accès, etc.).

Le directeur médical de crise quant à lui est un médecin expérimenté, interne à la structure, dont le rôle est d'aider le directeur et la cellule de crise à piloter l'organisation médicale de l'hôpital en cas d'évènement grave et déstructurant [5].

Une préparation à la crise

L'entraînement à la crise constitue naturellement la deuxième pierre à l'édifice de la sécurisation des établissements hospitaliers [6]. Cet entraînement s'entend classiquement comme la répétition des gestes et des procédures à mettre en œuvre en cas de crise [7].

Cependant, deux problèmes apparaissent immédiatement : la disponibilité du personnel d'une part, et l'inconstance du public, d'autre part. En effet, organiser une simulation dans un lieu ouvert 24 h/24, 7 jours/7, 365 jours par an relève du tour de force. C'est pourquoi il faut s'aventurer avec précaution dans la répétition d'exercices dimensionnant (tels que la

simulation à grande échelle d'une tuerie de masse) et préférer de petits exercices tournés vers un service ou un étage de l'établissement. Par ailleurs, le fait que les patients soient par nature de passage enlève de l'intérêt à la sensibilisation par l'exercice. En réalité, il faut voir cette caractéristique comme un atout, qui va simplifier les simulations. Ainsi, lors des exercices, seul le personnel travaillant dans le centre hospitalier sera évalué et accompagné vers une acquisition des compétences et une amélioration des pratiques.
Les patients (joués par des volontaires, élèves infirmiers par exemple), quant à eux, ne seront pas jugés pour la pertinence de leur réaction, car elle sera toujours, par nature, spontanée. Par voie de conséquence, comme pour d'autres établissements recevant du public, comme les salles de spectacle, le personnel hospitalier sera exercé à sa capacité à réagir pour lui-même et pour les autres. Il est, par ailleurs, peut être préférable de séquencer l'entraînement en l'acquisition de deux thématiques de compétences distinctes : réponse à l'agression et accueil d'un afflux massif de victimes.
L'entraînement des décideurs diffère sensiblement, tant leur rôle est différent lors d'une crise. Il est indéniable que le directeur et le directeur médical de crise vont devoir avoir une réaction beaucoup plus élaborée que la dissimulation ou la fuite. Leur préparation est plus subtile et relève d'actions répétées et d'échanges réalisés en amont des phases de simulation avec les divers partenaires de secours et de sécurité. Cela commence par un dialogue avec les partenaires avec lesquels ils collaboreront en cas de crise (police, gendarmerie, sapeurs-pompiers, samu, préfecture, et ARS), pour leur faire préciser leurs attentes au moment de la crise. Cela passe ensuite par des exercices internes, mais qui cette fois, peuvent revêtir un caractère purement intellectuel (exercice sur table).

Quel est le point de rupture ?

Connaître le point de rupture de son établissement de santé constitue le troisième élément à intégrer pour assurer le moment venu une gestion efficace d'un événement terroriste. Il est plus facile de déterminer les limites d'un service que d'un individu. À cette fin, on mettra en œuvre le recensement d'éléments objectifs : capacités du service (nombre de lits, nombre de blocs opératoires, etc.), compétences du service (traumatologie, pédiatrie, etc.), besoins du service (électricité, fluides, personnels soignants), qui définiront de facto une ligne rouge au-delà de laquelle le ou les services de l'établissement hospitalier ne seront plus en mesure de fonctionner. Il sera du ressort du directeur d'établissement de signaler aux autres acteurs de gestion de crise (police, pompiers, préfecture) ce point de rupture ainsi défini pour envisager des transferts de charge.
Il paraît utile de travailler sur cet outil afin d'envisager la réponse en cas de flux spontané de victimes. Tous les exemples montrent qu'une grande majorité de victimes impliquées dans des catastrophes se précipitent vers les établissements de soins et les urgences de proximité [8]. Cet afflux massif de victimes a lieu avant même le déclenchement du moindre plan et quel que soit le contexte y compris NRBC. La saturation immédiate de la structure peut avoir des conséquences dramatiques qu'il est important d'envisager. Cette notion de point de rupture permet de modéliser, d'anticiper et d'investir en priorité sur des stratégies de réponse hospitalière à un afflux massif et spontané de victimes.

QU'EST-CE QU'UNE INTRUSION ?

Les bases de la préparation ayant été posées, il faut désormais savoir identifier précisément une attaque terroriste le jour venu. Or, il n'existe pas de signe précurseur clairement détectable d'une attaque jusqu'à ce que les premiers coups de feu retentissent ou que des témoins/victimes se présentent. Toutes les attaques terroristes ayant touché la France depuis 2015 le prouvent : les assaillants misent sur l'effet de surprise et la sidération créés par une attaque éclair, le caractère terroriste de l'attaque n'étant affiché et clamé que dans un deuxième temps, généralement peu avant la confrontation finale avec les forces de l'ordre.
Ceci étant dit, quelques signes peuvent permettre de reconnaître des intrusions hors norme au sein des établissements hospitaliers. On encouragera seulement quelques catégories de personnels à les connaître (agents de sécurité, agents d'accueil) afin de ne pas alourdir la charge du personnel soignant, qui doit déjà intégrer les modalités d'action en cas d'attaque comme on l'a vu précédemment. Au-delà d'éléments d'identification indubitables (port visible d'armes à feu ou d'arme blanche, de gilets pare-balle), des faits comme une arrivée rapide en groupe, le transport de grand sacs de sports, la prise à partie physique ou verbale du personnel dès leur rencontre peuvent constituer des signaux d'alarmes. La liste de ces caractéristiques ne saurait être certaine ni exhaustive, aussi faut-il se raccrocher à son bon sens (est-ce que je trouve cela normal ?).
Les évidences méritent d'être rappelées : voir quelque chose de suspect n'a de sens que si cette information est communiquée à quelqu'un qui a un levier d'action en termes de sécurité. Un agent de sécurité le fera sans aucun doute, car ce « process » fait partie de son travail habituel et ce d'ailleurs quelle que soit l'échelle de gravité du fait (des incivilités aux actes de violence les plus graves). Pour un personnel d'accueil ou un personnel soignant, l'évidence est moindre, car la culture du compte rendu n'est pas naturelle en la matière. On en revient au principe d'entraînement et de préparation à la crise que l'on évoquait auparavant. Le destinataire de la remontée d'informations doit être un responsable de la sécurité ou un directeur.
L'identification de la personne ou du service à contacter est primordiale et son contact doit être simple, pour encourager le signalement du fait. Ainsi, il n'y a pas de sens à ce que le moindre incident ou doute soit remonté au directeur de l'hôpital en personne et quand bien même cela serait décrété, il est évident que le personnel réfléchirait à deux fois avant de saisir son téléphone. Or, c'est bien l'effet inverse que l'on recherche : on doit pouvoir appeler le responsable ou le service chargé de la sécurité sans commencer sa phrase par : désolé de vous déranger.

COMMENT RÉAGIR DANS LES PREMIÈRES MINUTES ?

Lorsque la crise survient, le plan de sécurité doit être appliqué individuellement et collectivement. Le personnel hospitalier appliquera (ou pas) les consignes de réaction préconisées dans le plan de sécurité et répétées lors des exercices : s'enfuir, se confiner, alerter [9]. Les décideurs (directeur d'établissement et directeur médical de crise) constitueront quant

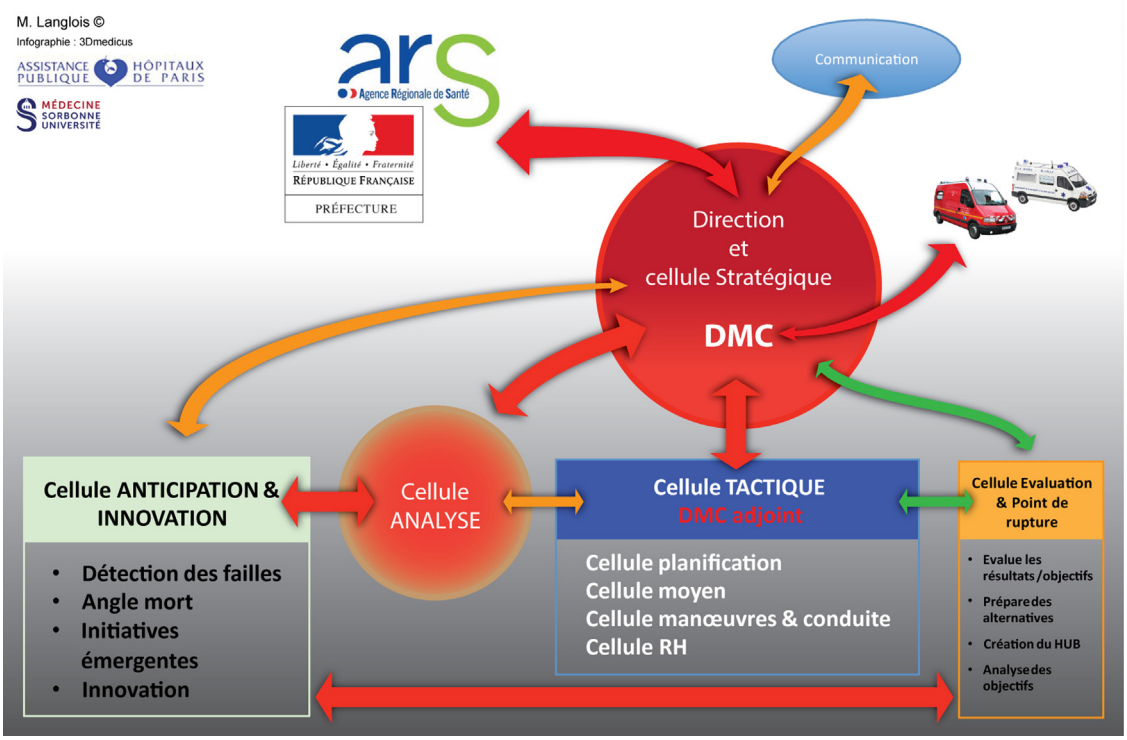

Figure 1. Proposition d'une cellule de crise hospitalière.

à eux une cellule de crise et prendront les premières mesures de sécurité dans l'attente des forces de police ou de gendarmerie. La sidération frappe inévitablement ceux qui sont impliqués dans un attentat terroriste et même les décideurs n'échapperont pas à un sentiment de confusion et d'impuissance inaugurale. Il faut donc se raccrocher à des principes réflexes très simples pour gérer les premières minutes de l'attentat tels qu'alerter les services de police ou de gendarmerie, prévenir l'ensemble du personnel, donner la consigne à tenir pour eux et les patients, évacuer le bâtiment ou le service dans lequel l'attentat a lieu (mais pas l'ensemble de l'hôpital !), favoriser l'évacuation, empêcher l'accès au bâtiment ou au service où a lieu l'attentat, etc. Des fiches réflexes aident le décideur à réduire la phase initiale de chaos [10].

L'établissement d'un centre de crise ou poste de commandement (PC) (*Fig. 1*) est évidemment un bon réflexe à avoir en cas d'attaque terroriste. Le choix de son emplacement doit être prévu à l'avance dans le plan de sécurité et se situer évidemment à l'écart du lieu de crise (le cas échéant, on choisira un lieu de repli s'il s'avère que l'attaque se passe juste à côté de l'implantation prévisionnelle du PC). Un poste de commandement idéalement placé est situé loin de la crise, mais reste au sein de l'établissement. Rester au sein de l'établissement est stratégique : cela permet de continuer à s'informer de la situation par des sources directes (vidéosurveillance) ou indirectes (témoignage des salariés, compte rendu radio ou téléphonique du personnel de sécurité), d'avoir à disposition des ressources précieuses (plans de l'établissement, renvoi des caméras) et d'être un point de passage obligatoire des services partenaires qui contribueront à résoudre la crise.

Dès lors, on l'aura compris, le lieu d'implantation du PC devra être défini et connu des décideurs. Il centralisera l'information et c'est bien de ça dont il va s'agir jusqu'à l'arrivée des secours extérieurs : centraliser l'information, la vérifier, la synthétiser. Le PC peut aussi initier des actions plus élaborées : définition d'un périmètre de sécurité, identification des nids de blessés, sanctuarisation des blocs opératoires, transfert des patients, etc. La seule limite étant de ne pas prendre d'initiative élaborée sur la zone de crise elle-même (la zone d'exclusion ou zone rouge), dont la gestion relève définitivement des forces d'intervention spécialisée. Idéalement, la zone PC doit pouvoir regrouper plusieurs bureaux pour une organisation en cellule (*Fig. 1*). Cette organisation doit être anticipée.

COMMENT SE METTRE À DISPOSITION DES FORCES DE SÉCURITÉ INTÉRIEURE ?

Une fois les partenaires de sécurité et de secours sur les lieux, leurs responsables doivent être dirigés au PC. Ils pourront prendre connaissance de la situation sous son double aspect : que s'est-il passé, que peut-il encore se passer ? Cette deuxième partie du questionnement renvoie aux capacités de l'établissement à surmonter la crise (sans doute peut-il traiter des blessés sur place et offrir une réponse adaptée) ou à contrario à ne plus être en état de fonctionner (la fameuse identification du point de rupture). Seul le directeur de l'établissement et directeur médical de crise peuvent répondre à cette question, car les services extérieurs ne possèdent ni

la connaissance structurelle ni la connaissance médicale. En revanche, les services extérieurs offriront au directeur des solutions et des idées de manœuvre en cas de rupture de la structure. Dans la réponse apportée à la crise, les forces de sécurité intérieure vont intégrer dans leur processus d'analyse, les conditions nécessaires pour maîtriser la menace, priorité absolue, mais également la capacité pour le secours de porter assistance aux victimes, la gestion des mouvements de foule et la prévention du sur-attentat.
Le Directeur de l'établissement et le directeur médical doivent intégrer que la gestion opérationnelle de la crise relève ensuite du commandant des opérations de police et de gendarmerie (COPG). Au niveau des services de l'État, c'est lui qui est « menant » face aux sapeurs-pompiers et au samu, qui sont quant à eux « concourants ». L'ensemble de ces acteurs agissent sous l'autorité du Préfet, directeur des opérations. C'est donc le COPG qui sera l'interlocuteur naturel des deux managers de crise de l'hôpital dans le PC. À son arrivée, il va s'enquérir auprès d'eux de la situation (quoi ?) et de la localisation (où ?). En fonction de leurs réponses, le COPG prendra les premières mesures de sécurité : fixation ou confinement des terroristes, établissement d'un périmètre de sécurité, évacuation des impliqués et victimes en dehors de la zone d'exclusion. Le COPG prendra soin de garder le directeur d'établissement et le directeur médical de crise à ses côtés dans le PC tout au long de l'événement. Il les questionnera pour approfondir sa connaissance des lieux et les informera de l'évolution de la situation pour anticiper d'autres problèmes qu'eux seuls peuvent anticiper. Les propositions seront les bienvenues : zone à protéger en priorité (urgences, blocs…), les zones de danger, les recommandations de circuits internes, des points de rassemblement, etc.

QU'EST-CE QUE LA FORCE D'INTERVENTION SPÉCIALISÉE ATTEND DE L'HÔPITAL ?

Les managers de crise de l'hôpital auront affaire à un autre interlocuteur un peu plus tard. En effet, la force d'intervention spécialisée sera celle qui arrivera en dernier sur les lieux (son temps de projection est plus long, car sa base est plus éloignée de la crise que ceux des services primo-intervenants). Mais, c'est à cet acteur que revient la résolution finale de la crise, c'est-à-dire, l'interpellation et la suppression des menaces. Au PC, il sera incarné par un cadre de l'unité, baptisé pour la circonstance commandant des opérations d'intervention spécialisée (COIS). Tout comme le COPG, le COIS aura absolument besoin de la coopération du directeur d'établissement pour connaître les lieux et utiliser les ressources de l'établissement.
La connaissance des lieux va permettre au groupe d'intervention de fixer au mieux les terroristes : itinéraire rapide pour arriver jusqu'à eux, points hauts pour placer des tireurs de haute précision, localisation des points de fuite possibles, détermination des zones pouvant présenter des risques d'explosion en cas de tirs, etc. Cette connaissance sera transmise par les deux autorités du site à l'aide d'outils simples : cartographie, descriptif verbal, mise à disposition des clefs d'accès, retours de la vidéosurveillance, etc. Le COIS cherchera à agir avec l'avantage tactique maximal sur les terroristes. Un assaut d'urgence ne sera lancé qu'en cas de péril immédiat, comme par exemple une reprise de la tuerie par les terroristes. L'assaut planifié sera la stratégie recherchée au maximum par le COIS, c'est-à-dire, une intervention décidée au moment opportun, lorsqu'un certain nombre de facteurs seront remplis (qu'on ne saurait divulguer dans cet article par souci de préservation de leur efficacité). Sans trop s'étendre, il faut savoir que certains de ses facteurs seront favorisés par le directeur de l'établissement et le directeur médical de crise de par leur connaissance des lieux.
Le COIS aura besoin d'utiliser les ressources de l'établissement parallèlement à la gestion de l'assaut. En effet, en zone d'exclusion, c'est le groupe d'intervention qui gère le secours, le triage et l'extraction des victimes. S'appuyant sur un officier de secours tactique (médecin du RAID, officier du GIGN), le COIS va déterminer les circuits d'évacuation jusqu'au point d'extraction des victimes (PEV) en zone contrôlée. D'anticiper les besoins tactiques pour maîtriser la menace tel que l'incendie et des risques particuliers liés à l'hôpital (fluides médicaux, laboratoire, radiologie, etc.) et d'anticiper d'autre blessés lors des assauts [11].

COMMENT PRÉPARER LA REPRISE DE L'ACTIVITÉ ?

Le directeur et sa cellule de crise vont rapidement laisser la gestion immédiate de la crise aux forces de sécurité intérieure et service de secours. Ils vont ainsi pouvoir se projeter dans l'après crise. Des outils d'aide à la sortie de crise sous forme de check-list peuvent aider à la planification. Il est impératif de garder à l'esprit que la planification de l'après crise ne veut pas dire que la crise n'est pas encore évolutive. Il faut donc éviter de mettre en place des manœuvres lourdes et peu modifiables. Il est nécessaire de garder une réelle agilité dans un univers chaotique tout en se projetant sur l'avenir.
Le COPG interviendra auprès du directeur hospitalier uniquement pour faciliter, sur le plan sécuritaire, le retour à l'activité normale. Une attaque terroriste dans un centre hospitalier aura de toute manière une cinétique de crise lente pour sortir de la phase aiguë. Les caractéristiques propres de la structure et de son fonctionnement 24 h/24 ne permettent ni un arrêt complet ni aucune modification structurelle brutale pour permettre un retour à la normalité très rapide.
Enfin, la notion de point de rupture va s'inscrire dans la durée. Il permet simplement d'anticiper un basculement rapide vers un délestage des circuits de patients hospitalisés ou d'afflux de nouveaux blessés. Si ce choix s'avère indispensable à réaliser, il doit être rapidement communiqué par le directeur médical de crise (DMC) au commandant des opérations de secours (COS) et au samu. Car c'est à eux que reviendront la charge de l'organiser y compris à distance de la phase aiguë de l'évènement. De toute évidence, une intrusion terroriste dans l'hôpital entraînera un saut dans l'imprévu [12]. L'agilité dans la décision et le commandement sera déterminante, mais notre obligation est de s'y préparer.

CONCLUSION

Les centres hospitaliers doivent bâtir une réflexion interne sur la réponse en cas d'agression et d'attaque terroriste et ne pas uniquement se reposer sur les plans tuerie de masse des services extra hospitaliers [13]. Des plans intrusion semblent indispensables au sein de chaque établissement de soins. Ils

aideront le directeur et son équipe de crise à réduire la durée de la phase initiale de chaos et à initier une réponse adaptée à la menace.
Cette culture du risque n'est pas assez enseignée chez le personnel hospitalier. Cela ne s'improvise pas le jour d'un acte malveillant, mais se travaille régulièrement avec exigence. En cas d'agression, le lien opérationnel entre le directeur de l'établissement, le directeur médical de crise et les services de l'État (sécurité intérieure, service d'incendie et de secours, samu et ARS) doit être connu, mis en œuvre et efficace.
Chaque acteur a son rôle avec d'un côté le pilotage de la crise et de l'autre la poursuite de l'activité hospitalière. C'est la coordination au niveau du PC de crise qui permet de répondre à l'agression en organisant la maîtrise de la menace et simultanément le secours, les soins et la gestion des flux de victimes sur le site hospitalier. Pour garder sa capacité opérationnelle, l'hôpital doit se préparer à recevoir à tout moment un afflux massif de blessés sans préavis, tout en connaissant/maîtrisant ses limites capacitaires pour anticiper une rupture qui ajouterait de la crise à la crise. On doit tous ensemble se préparer de manière rigoureuse et planifiée, mais en gardant beaucoup d'agilité face à l'incertitude. L'enjeu est de taille !

Déclaration de liens d'intérêts
Le docteur Langlois déclare un lien d'intéret avec le laboratoire Teleflex. L'autre auteur déclare ne pas avoir de liens d'intérêts.

RÉFÉRENCES

[1] Kelen GD, Catlett CL, Kubit JG, Hsieh YH. Hospital-based shootings in the United States: 2000 to 2011. Ann Emerg Med 2012;60(6). doi: 10.1016/j.annemergmed.2012.08.012 [790–8. e1. Epub 2012 Sep 19].
[2] Riou B, Vivien B. S'organiser et se former pour faire face à l'afflux massif de victimes à l'hôpital. Ann Fr Med Urgence 2019;9:141–2.
[3] Lettre conjointe des ministres des Affaires sociales et de la Santé et de l'Intérieur relative à la sécurisation des établissements de santé; 2016 [lettre institutionnelle].
[4] Sécurisation des établissements de santé — Guide d'aide à l'élaboration du PSE. [Disponible sur : https://solidarites-sante.gouv.fr//IMG/pdf/guide_d_aide_a_l_elaboration_du_pse_-_version_avril_2017.pdf]
[5] Guide d'aide à la préparation et à la gestion des situations sanitaires exceptionnelles au sein des établissements de santé. [Disponible sur : https://solidarites-sante.gouv.fr/IMG/pdf/guide_situation_sanitaire_exceptionnelle.pdf]
[6] Wexler B, Flamm A. Lessons learned from an active shooter full-scale functional exercise in a newly constructed emergency department. Disaster Med Public Health Prepardness 2017;11:522–5.
[7] Vigilance attentats : les bons réflexes — Guide à destination des personnels de santé, sociaux et médico-sociaux; 2016 [Disponible sur : http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/07/guide_pratique_pour_les_personnels_des_etablissements_de_sante_sociaux_et_medico-sociaux.pdf].
[8] Wang JC, Tsai SH, Chien WC, Chung CH, Dai NT, Tzeng YS, et al. The crowd-out effect of a mass casualty incident: experience from a dust explosion with burn injuries. Medicine (Baltimore) 2019;98(18):e1547.
[9] [p. 42–45. Disponible sur : https://www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf]
[10] Service médical du RAID. Antenne médicale spécialisée de Satory, F Lapostolle, T Loeb, E Lecarpentier, B Vivien, P Pasquier, M Raux. Comment appréhender une tuerie de masse par les équipes SMUR primo intervenantes. Ann Fr Med Urgence 2018;8:16–25.
[11] Service médical du RAID. Médicalisation de l'extrême-avant au cours d'une intervention des forces de l'ordre pour prise d'otages : principes régissant la prise en charge médicale et retour d'expérience du RAID. Ann Fr Med Urgence 2015;5:166–75.
[12] Lagadec P. Le continent des imprévus. Journal de bord des temps chaotiques. Ed Manitoba. Les belles lettres; 2015.
[13] Shah A, Rehman A, Sayyed R, Haider A, Bawa A, Zafar S, et al. Impact of a predefined hospital mass casualty response plan in a limited resource setting with no pre-hospital care system. Injury 2015;46:156–61.