

AUDIT DE SURETE  
STATION DE PRIMATOLOGIE  
DE LA DELEGATION PROVENCE ET CORSE DU CNRS

RAPPORT D'AUDIT : ANALYSE DES ANOMALIES RELEVÉES ET PRECONISATIONS



DEPARTEMENTALE 56, 13790 ROUSSET

# Sommaire

Introduction.....	3
1 Méthodologie.....	3
1.1 Évaluation du niveau de maîtrise.....	3
1.2 Évaluation du risque résiduel.....	3
1.2.1 Définition des barèmes.....	4
1.3 Classification des préconisations.....	4
2 Le site de la station de Primatologie de la délégation Provence et Corse du CNRS.....	6
2.1 Identification des menaces possibles.....	7
2.1.1 Radicalisation.....	8
2.1.2 Terrorisme.....	11
2.1.3 Enlèvement et/ou séquestration.....	15
2.1.4 Dégradations ou destructions volontaires.....	16
2.1.5 Vol de données sensibles.....	17
2.1.6 Ingérence économique.....	20
2.1.7 Troubles à l'ordre public.....	22
2.1.8 Agressions – coups et blessures volontaires – violences au travail.....	23
2.2 Prise en compte des risques à l'international/ En déplacement.....	24
2.3 Hiérarchisation des risques.....	25
3 Audit de la sûreté du site : analyse des anomalies relevées et préconisations.....	26
3.1 Moyens architecturaux et mécaniques.....	26
3.1.1 Les accès.....	26
3.1.2 Eclairage.....	29
3.1.3 La périphérie du site.....	30
3.2 Les bâtiments.....	31
3.3 MOYENS ORGANISATIONNELS.....	37
3.3.1 Procédures d'accueil.....	38
3.3.2 Procédures de recrutement.....	39
3.3.3 Gestion du personnel de gardiennage.....	39
3.3.4 La gestion des badges et des clés.....	39
3.3.5 Gestion du personnel externe.....	40
3.3.6 Politique et culture de sûreté.....	40
4 SUIVI DES RECOMMANDATIONS PAR CRITERES ET PRIORITES.....	42
5 CONCLUSION.....	44

## INTRODUCTION

Le 26 avril 2022 de 14h à 17h30, nous avons audité la Station de Primatologie à Rousset de la délégation Provence et Corse du CNRS

### Personnes rencontrées :

- M. MOLINA VILA Pau, Directeur adjoint de la Station
- Mme MASSA Annie, Secrétaire générale
- M. GUIOL Sébastien, responsable technique, hygiène et sécurité
- M. DESOR Grégory, responsable informatique
- M. KOURILSKY responsable service informatique (accompagnateur de la délégation Provence et Corse)

### Documentations fournies :

- Plan de masse de la station
- Plans d'implantation des caméras de vidéosurveillance et systèmes de sûreté

## 1 METHODOLOGIE

### 1.1 ÉVALUATION DU NIVEAU DE MAÎTRISE

Pour chaque composante du système de sûreté du site, il vous est proposé une évaluation du **niveau de maîtrise**. Celle-ci est appréciée au regard du nombre d'anomalies relevées et de leur gravité, tout en prenant en compte les mesures de sûreté existantes.

Le niveau de maîtrise est obtenu par la soustraction de la valeur pondérée des anomalies à la valeur absolue de 100%.

Le niveau de maîtrise est mesuré sur une échelle de 0 à 100% selon le barème suivant :

De 0 à 33%	<b>Faible</b>	De 34 à 66%	<b>Moyen</b>	De 67 à 100%	<b>Élevé</b>
------------	---------------	-------------	--------------	--------------	--------------

#### Exemple : niveau de maîtrise de la périphérie

Valeur absolue	100 %
Hauteur de la clôture insuffisante	- 15 %
Portails / portillons de mauvaise qualité	- 10 %
Absence de système de détection d'intrusion	- 20 %
Niveau de maîtrise estimé	<b>55 %</b>

Dans le cas présent, le niveau de maîtrise obtenu est coté « **moyen** ».

**NB :** la valeur attribuée à chaque anomalie diffère en fonction de la sensibilité du site et de son environnement direct. Ces critères sont appréciés lors de l'audit sur place et à travers les échanges avec les responsables du site.

Les préconisations formulées par la suite ciblent la réduction de l'écart entre le niveau de maîtrise et la valeur absolue.

### 1.2 ÉVALUATION DU RISQUE RESIDUEL

Les composantes sont elles-mêmes regroupées au sein de catégories de moyens : architecturaux, technologiques et organisationnels.

Pour chacune de ces catégories, un **risque résiduel** est calculé, selon la méthodologie de *Kinney*, adaptée à la sûreté, de la manière suivante :

- **Risque résiduel** ( $R_r$ ) = **Danger** ( $D$ ) – **Risque maîtrisé** ( $R_m$ )
- **Danger** ( $D$ ) = **Gravité** ( $G$ ) X **Fréquence** ( $F$ )
- **Risque maîtrisé** ( $R_m$ ) = **Danger** ( $D$ ) X Niveau de **Maîtrise** ( $M$ )
- Niveau de **Maîtrise** ( $M$ ) = moyenne des niveaux de maîtrise des composantes

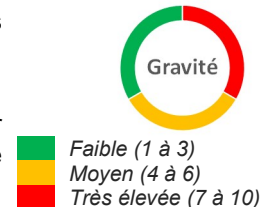
### 1.2.1 Définition des barèmes

- **Gravité :**

C'est l'importance ou le degré de participation du moyen audité dans le dispositif sûreté global du site.

Elle est estimée sur une échelle de 1 à 10.

Exemple : la périphérie du site (Gravité = **10**) car c'est le premier obstacle contre les malveillances : des failles dans la périphérie facilite les intrusions dans le périmètre du site.

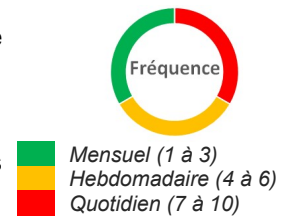


- **Fréquence :**

C'est la récurrence de l'utilisation ou de la présence du moyen de sûreté audité sur le site.

Elle est également estimée sur une échelle de 1 à 10.

Exemple : les systèmes de sûreté (Fréquence = **10**) car ils sont utilisés quotidiennement et d'une manière quasi-permanente.



- **Danger :**

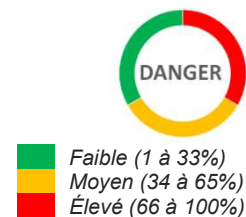
C'est le résultat multiplicateur de **Gravité** ( $G$ ) et **Fréquence** ( $F$ )

Exemple : Moyens organisationnels

Gravité = 10/10, Fréquence = 10/10

Danger = Gravité X Fréquence

Danger = (10 X 10) = 100 %



- **Risque résiduel :**

C'est le niveau de risque final, en dépit des mesures mises en place pour le réduire.

C'est le résultat de la soustraction du niveau de **Risque maîtrisé** ( $R_m$ ) à la valeur du **Danger** ( $D$ ).

Celui-ci est évalué sur échelle de 0 à 100%, selon le barème suivant :

De 0 à 33%	<b>Faible</b>	De 34 à 66%	<b>Moyen</b>	De 67 à 100%	<b>Élevé</b>
------------	---------------	-------------	--------------	--------------	--------------

### 1.3 CLASSIFICATION DES PRECONISATIONS

Le présent rapport dresse un état des lieux objectif de la sûreté du site tout en y apportant, pour chacune des catégories et rubriques, un certain nombre de préconisations.

Celles-ci sont hiérarchisées par code couleur indiquant l'ordre des priorités dans les travaux ou la mise en place des mesures organisationnelles proposées.

En fin de document, un tableau récapitulatif des préconisations vous est proposé. Il reprend l'ensemble des recommandations selon la codification suivante :

- Par ordre de priorité :

**URGENT**

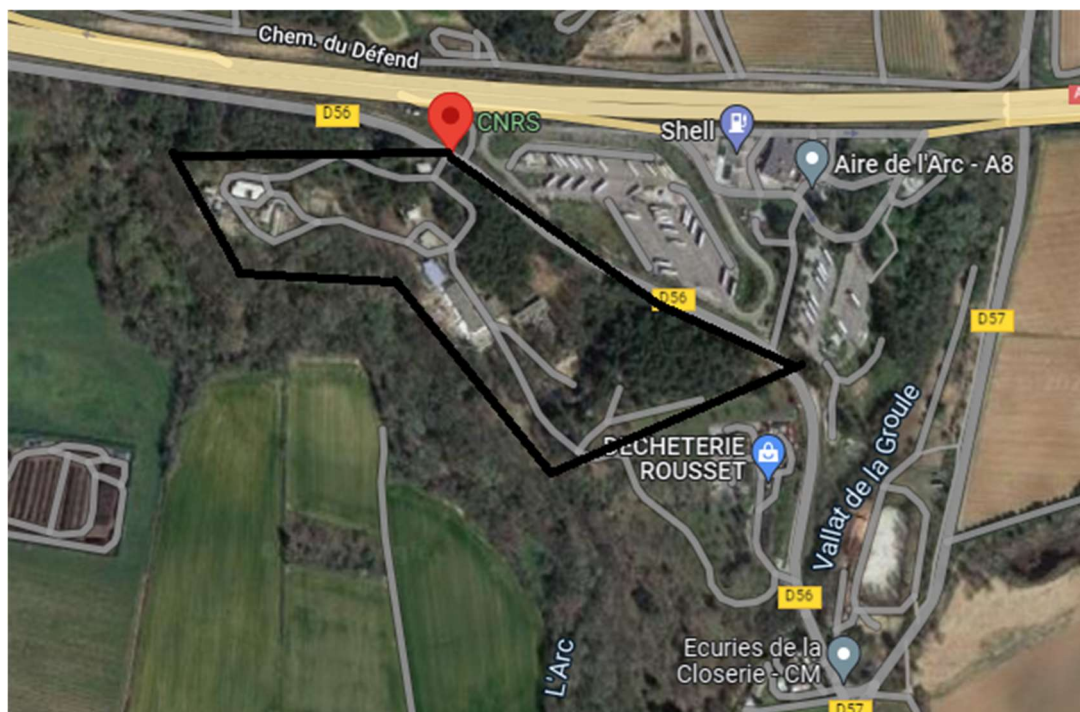
- Par trigramme :

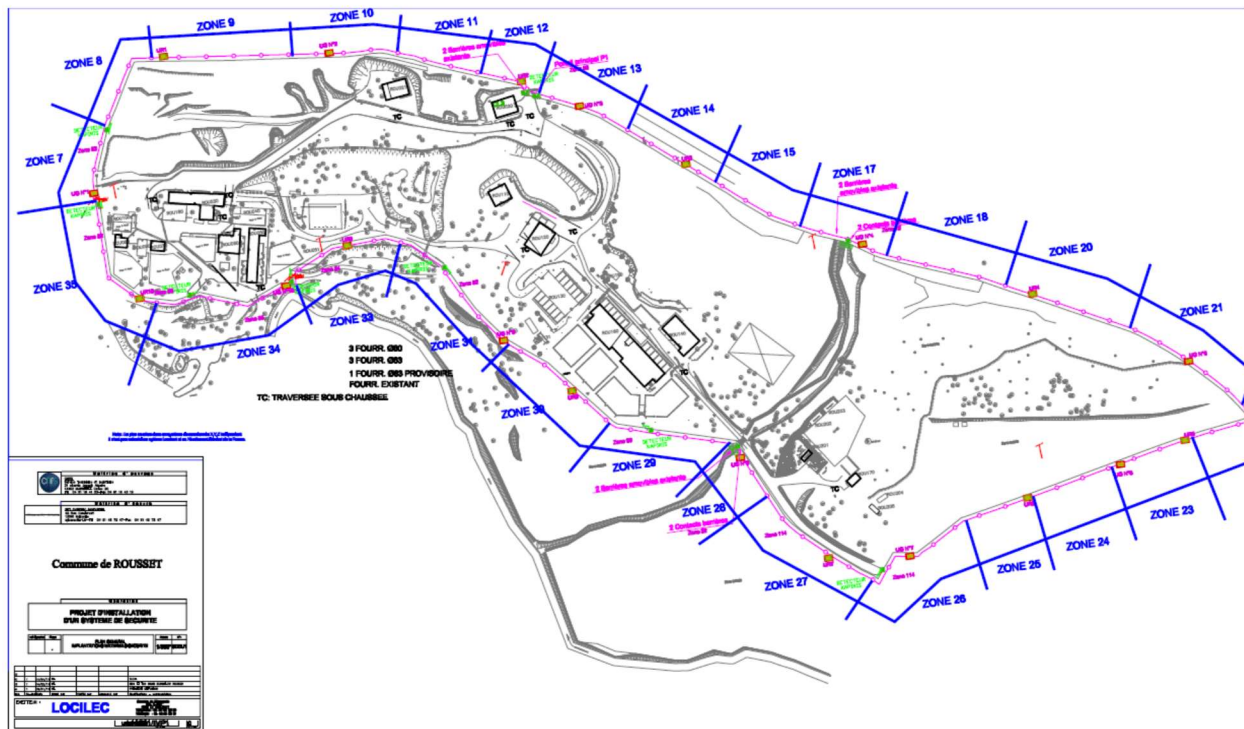
<b>A</b>	<b>Moyens Architecturaux</b>
AA	Moyens Architecturaux / Accès
AAP	Moyens Architecturaux / Accès / Accès principaux
AAI	Moyens Architecturaux / Accès / Accès intérieurs
AP	Moyens Architecturaux / Périphérie, Périmétrie
APP	Moyens Architecturaux / Périphérie, Périmétrie / Volumétrie
AE	Moyens Architecturaux / Éclairage
AEC	Moyens Architecturaux / Éclairage / Réseau d'éclairage
AL	Moyens Architecturaux / Locaux
ALS	Moyens Architecturaux / Locaux sensibles
ASC	Moyens Architecturaux / Ascenseurs
<b>T</b>	<b>Moyens Technologiques</b>
TVD	Vidéosurveillance
TAL	Alarme anti-intrusion
TCA	Contrôle d'accès, interphones et systèmes de fermeture
TCO	Moyens de communication
<b>O</b>	<b>Moyens Organisationnels</b>
OG	Moyens Organisationnels / Moyens généraux
OGS	Moyens Organisationnels / Moyens généraux / Surveillance
OGL	Moyens Organisationnels / Moyens généraux / Liaisons
OGA	Moyens Organisationnels / Moyens généraux / Accueil
OC	Moyens Organisationnels / Gestion des Clés
OP	Moyens Organisationnels / Gestion des Prestataires
OAI	Moyens Organisationnels / Accès / Procédures Internes
OIA	Moyens Organisationnels / Procédures Internes / Accueil
OIS	Moyens Organisationnels / Procédures Internes / Surveillance
OPE	Moyens Organisationnels / Gestion des Prestataires / des Externes
OPG	Moyens Organisationnels / Personnel de Gardiennage
OSI	Moyens Organisationnels / Sécurité de l'Information

## 2 LE SITE DE LA STATION DE PRIMATOLOGIE DE LA DELEGATION PROVENCE ET CORSE DU CNRS

La station de primatologie est implantée au Sud Est de la ville d'Aix en Provence à environ 20 km, sur le ban de la commune de Rousset, à proximité de l'autoroute A8, en bordure de route départementale 56, dans un environnement rural (Ecuries de la Closerie, Ecuries Welcome). On relève toutefois la présence voisine de la déchèterie de Rousset et d'une aire d'autoroute SHELL en mitoyenneté de la station. Ces deux sites génèrent beaucoup de passages, éventuellement de curieux.

### Localisation





## 2.1 IDENTIFICATION DES MENACES POSSIBLES

Les menaces possibles identifiées correspondent à des risques que l'on peut retenir comme probables ou possibles sur un site abritant à un laboratoire de recherches dépendant de la délégation régionale Provence Corse du CNRS. Les menaces retenues sont identiques à celles traitées au Campus Joseph Aiguier du CNRS à Marseille. Nous retiendrons tout particulièrement les actes de radicalisation et notamment ceux liés au droit des animaux (cf paragraphe 2.1.1) et l'écoterrorisme (cf paragraphe 2.1.2).

Ce ne sont pas forcément des risques constatés sur la station de Primatologie, mais des risques contre lesquels il est préférable de se prémunir préventivement.

Légende d'analyse des menaces :

	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.1.1 Radicalisation

De nombreux pays connaissent un phénomène de radicalisation croissant, qu'il soit religieux, politique et/ou social. La France n'est malheureusement pas exempte et fait notamment face à la menace des filières terroristes islamistes. Selon le gouvernement, plus de 2000 personnes seraient aujourd'hui impliquées dans des phénomènes de radicalisation religieuse violente ou auraient rejoint des filières de recrutements djihadistes. Les entreprises et les administrations y sont par conséquent potentiellement exposées à plusieurs titres.

L'enjeu pour la station de Primatologie est triple :

*Premier enjeu* : Il est tout d'abord sécuritaire, dans la mesure où une menace extrémiste évolutive et mouvante peut avoir un impact sur certains secteurs stratégiques (recherches, énergie, informatique etc.) ou entraîner des conséquences sur son activité.

*Second enjeu* : la radicalisation menant à la violence influence aussi la gestion interne et des ressources humaines. Cet aspect se confond parfois avec la question du vivre-ensemble sur le lieu de travail, de la convergence entre croyances individuelles, du respect du cadre organisationnel. Ce qui peut entrer en tension avec des opinions ou des pratiques religieuses ou politiques au sein du campus. Dans ce contexte sensible, il est essentiel de pouvoir mieux s'outiller afin de répondre aux enjeux de gestion organisationnelle qui peuvent surgir dans les la fonction publique.

*Troisième enjeu* : Enfin, la radicalisation menant à la violence pose un enjeu de responsabilité sociale pour des structures comme le CNRS en général. Parce qu'elle est le lieu de vie d'environ 32 000 personnes au quotidien, le CNRS possède une responsabilité vis-à-vis de la société, et a un rôle à jouer dans la prévention de ces phénomènes. Il lui faut s'assurer que ses collaborateurs ne représentent pas une menace pour la collectivité ou pour eux-mêmes.

Il est de la responsabilité des employeurs publics de renforcer la détection et le traitement des situations signalées de radicalisation violente chez les agents publics.

Les campus peuvent également être les cibles directes d'actes de terrorisme. Le risque de radicalisation constitue donc une menace à prendre en compte, mais aussi une nouvelle responsabilité sociale des employeurs publics.

Les idéologies sources de passage à l'acte ont des origines variées, toutefois la radicalisation islamiste est aujourd'hui la plus constatée.

### **La radicalisation des militants des « droits des animaux ». Un véritable enjeu pour le CNRS :**

Il ne faut pas cependant oublier les militants des "droits des animaux". Un grand nombre d'entre eux ont fait le choix d'actions directes et spectaculaires pour atteindre leur but. Ainsi, depuis deux décennies, s'observe une radicalisation croissante des groupes animalistes, de leur discours et de leurs actes.

Le « credo » des animalistes radicaux est que « la vie d'un animal équivaut à la vie d'un homme », les premiers ont donc pour eux les mêmes droits que les seconds. Les extrémistes de la cause animale se comparent ainsi aux grands mouvements de libération et de résistance – contre l'esclavage des Noirs, contre le nazisme, etc. – ce qui justifie à leurs yeux l'usage de la violence : les animaux, dominés et ne pouvant se défendre eux-mêmes, les animalistes le font à leur place et en leur nom.

Quatre modes d'action sont au cœur du répertoire confrontatif des activistes de la cause animale : l'espionnage militant, la libération d'animaux, la dégradation de locaux et les pressions psychologiques et physiques contre les personnes. Certains ultras n'hésitent pas à préconiser également le meurtre de scientifiques.

Par le biais de l'espionnage militant et l'infiltration d'objectifs ciblés, les activistes multiplient les opérations afin de rendre compte de faits de maltraitance dont sont victimes les animaux et dénoncer les « atrocités » qui se cachent derrière les portes des laboratoires, des usines et des fermes de l'exploitation animale.

Par exemple, dans son manuel intitulé Comment devenir un bon activiste ? le groupe People for the Ethical Treatment of Animals (PETA) explique comment se faire engager dans un laboratoire pharmaceutique soupçonné de ne pas respecter les droits des animaux et préconise de transmettre toutes les informations obtenues au PETA's Research, Investigation & Rescue Department.

L'infiltration des laboratoires de tests sur les animaux est également la tactique favorite du mouvement British Union Against Vivisection (BUAV). Son travail de pénétration débute toujours par des recherches documentaires, tant sur les bases de données que sur Internet. Il revendique l'infiltration de nombreux laboratoires travaillant au profit de l'industrie pharmaceutique : Huntingdon Research Centre, London Hospital Medical College, Shamrock Ltd, Hazleton UK Laboratories, Wickham Research Laboratories and Harlan UK

Au-delà de la destruction ou de la détérioration de biens matériels, les activistes radicaux recourent également aux pressions psychologiques et physiques sur les personnes. Ils s'en prennent en particulier aux dirigeants, au personnel, aux actionnaires et aux partenaires des entreprises qu'ils ciblent afin de les forcer à changer de politique ou renoncer à leurs activités : chantage et agressions, envois de lettres et de colis piégés, menaces de mort ou d'enlèvement des enfants des dirigeants, séquestrations, etc. Les actes d'intimidation se multiplient et les animalistes radicaux s'emploient à terroriser les personnes travaillant dans des structures exploitant les animaux.

Détecter ce type d'extrémiste devient également plus complexe car les individus radicalisés ont de plus en plus conscience de leur intérêt à dissimuler leur rattachement aux causes extrémistes derrière un comportement en apparence normal.

Si des doutes existent il ne faut pas hésiter à avoir recours aux innovations technologiques et en aviser très rapidement la DGSI. Une structure comme la délégation régionale collecte ou voit transiter un très grand nombre de données sur ses collaborateurs : historiques de sites fréquentés, rapports d'étonnements, enregistrements d'appels téléphoniques, arrêts maladies, etc. Parmi toutes ces données, certaines peuvent contenir des informations sur la présence d'individus aux comportements radicalisés. Le lieu de travail constitue ainsi le deuxième cercle social, après la famille, où détecter la radicalisation d'un individu. Des innovations technologiques, visent à améliorer la capacité de l'entreprise à exploiter et à analyser ces quantités de données, à des fins de veille transversale et d'alerte. Ces outils fonctionnent selon les principes du datamining : ils explorent des données internes et externes à l'entreprise (médias sociaux par exemple) pour détecter des « anomalies », ou dans notre cas, des comportements de personnes radicalisées ou en cours de radicalisation. Cela peut permettre de corroborer les observations humaines, voire de détecter des processus de radicalisation passés inaperçus.

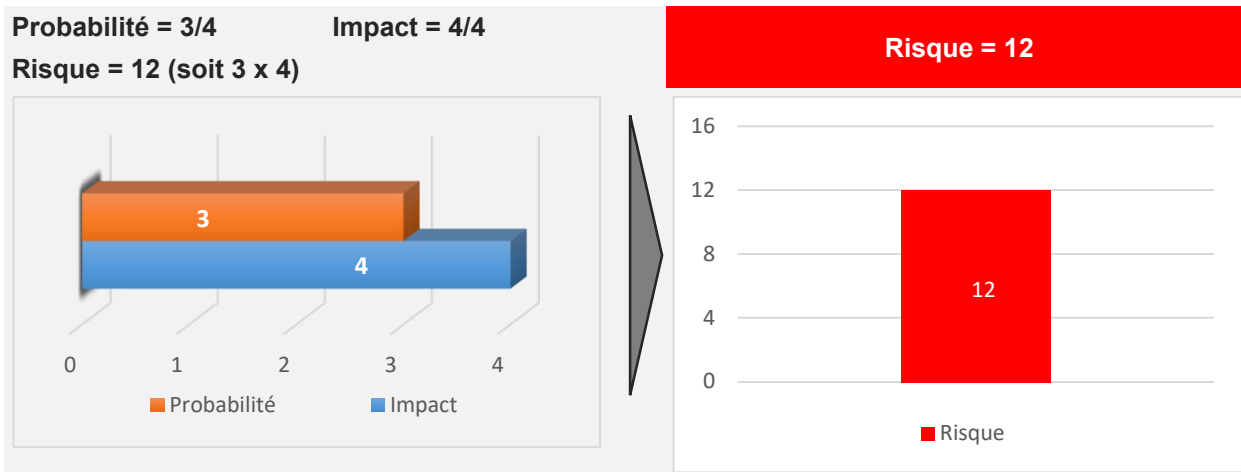
Utilisés à bon escient c'est-à-dire en conformité avec la réglementation, les outils d'analyse sont à considérer comme des atouts venant renforcer le dispositif de sûreté de l'entreprise. Afin de s'en assurer, il est conseillé de se faire accompagner juridiquement.

## Cotation du risque initial :

### Impact :

La radicalisation d'un individu conduisant à un ou des actes de violences ou de détériorations graves pourrait causer des pertes humaines considérables et paralyser en partie le site. Nous qualifierons l'impact de ce risque « **extrêmement grave** ».

### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.1.2 Terrorisme

Le terrorisme ciblé ou d'opportunité consiste en la tuerie suivie ou non d'une prise d'otages avec souvent un retranchement, avec ou sans otages, en attendant l'intervention des forces de police.

Il y a trois grands types de menaces terroristes en France :

- La menace « traditionnelle » que faisaient peser des mouvements « historiques » comme le FLNC (Front de libération nationale de la Corse), l'ETA, à peu près tous les mouvements insurrectionnels de la planète qui ont une représentation officielle ou clandestine en France ;
- La menace « islamique radicale » en distinguant les sunnites d'Al-Qaïda et de Daech et les chiites inspirés par Téhéran ;
- Les menaces « de demain » alimentées par les mouvements insurrectionnels issus des mouvances altermondialistes, écologistes et anarchistes auxquelles il convient d'ajouter les extrémistes de toutes tendances.

La chronologie des attentats en France nous permet de voir que de tout temps la menace terroriste a été présente sur le territoire national, connaissant des évolutions substantielles dans les procédés utilisés. L'affaire Merah en 2012, a mis en lumière la menace du terrorisme islamiste, depuis les attentats de janvier 2015 et leurs tragiques suites, toutes les attaques considérées comme terroristes qui ont été perpétrées sur le territoire français sont du terrorisme islamiste.<sup>1</sup>

- La ville de Marseille n'a pas été épargnée, l'attentat de la gare Saint-Charles de Marseille est un acte terroriste commis le 1er octobre 2017 à la gare de Marseille-Saint-Charles au cours duquel deux jeunes femmes sont tuées à l'arme blanche. L'assaillant est tué par des militaires d'une patrouille de l'opération Sentinelle. L'attaque est revendiquée par l'État islamique dans les heures qui suivent les assassinats

Paris est la ville la plus touchée, suivie de Lyon, Nice et Marseille. Mais la majorité de cette menace, parfois accomplie, se concentre en province qui enregistre 54% des événements. Les grandes villes sont davantage visées dans les chiffres, ce qui n'épargne pas les petites villes comme Trèbes encore récemment. »<sup>2</sup>

### L'écoterrorisme :

L'écoterrorisme, ce sont des actes violents comme des sabotages, des incendies ou des attentats à la bombe justifiés par des positions extrêmes sur des problèmes environnementaux et les droits des animaux. Le but est d'infliger des dommages économiques, matériels, voire psychologiques et physiques à ceux qui profitent de l'exploitation de l'environnement ou qui contribuent à sa destruction.

L'écoterrorisme existe déjà au niveau mondial à travers des mouvements comme l'Animal Liberation Front (ALF) ou l'Earth Liberation Front (ELF), qui pratiquent beaucoup d'opérations de sabotage. En France, l'écoterrorisme n'en est qu'au stade de l'hypothèse sérieuse mais les premiers signes annonciateurs d'une radicalisation sont apparus notamment lors des événements entourant la future construction de l'aéroport de Notre-Dame-des-Landes. Certains activistes vindicatifs et réactifs étudient et s'inspirent de ce qui se passe ailleurs dans le monde. Ils utilisent les mêmes technologies que celles des printemps arabes.

Au chapitre des méthodes, il est d'ailleurs intéressant de constater que, sauf exceptions, l'écoterrorisme exploite généralement des techniques visant principalement à détruire des biens. Ainsi, les attentats menés par ces groupes ne sont que très rarement mortels.

Cependant l'idéologie des groupes violents ne leur interdit pas de nuire à l'homme : elle préconise seulement un effort pour « minimiser » le préjudice aux humains. Ainsi, en 2007, des cadres d'Air France

<sup>1</sup> Global Terrorism Database : <https://start.umd.edu/gtd/>

<sup>2</sup> Centre d'Analyse du Terrorisme (CAT) : <http://cat-int.org/index.php/2018/06/29/terrorisme-projets-tentatives-attentats-la-carte-du-jihadisme-en-france/>

ont retrouvé des inscriptions menaçantes près de leur domicile parce que leur compagnie transportait des animaux de laboratoire. De même, à l'occasion de ses campagnes contre le laboratoire britannique Huntingdon Life Science (HLS) – le principal centre européen d'expérimentation animale – le groupe Stop Huntingdon Animals Cruelty (SHAC) recourait à des méthodes variées :

Il lançait des appels, via son site web, afin d'obtenir un maximum d'informations concernant les salariés et les clients du laboratoire ;

- des virus informatiques malveillants étaient adressés aux entreprises, aux salariés et aux clients
- des lettres de menaces étaient envoyées aux bureaux de l'entreprise et aux employés ;
- les résidences des salariés étaient tagguées avec des inscriptions les accusant de crimes terribles (torture, pédophilie, etc.) ;
- les activistes organisaient des « visites à domicile » pour intimider leurs cibles et leur indiquer qu'elles les surveillaient

Bien que n'ayant encore causé aucun décès, cette progressivité de l'action violente conduit clairement à substituer des objectifs « humains » aux cibles matérielles.

Une minorité activistes va encore plus loin, n'hésitant pas à préconiser d'éliminer directement certains individus. Jerry Vlasak, porte-parole de l'Animal Liberation Front (ALF) aux Etats-Unis, justifie le meurtre de scientifiques dans un texte surprenant où il va jusqu'à comparer la vivisection au traitement des juifs par les nazis : « Je pense que la violence fait partie de la lutte. Si quelque chose de regrettable arrive à un chercheur sur les animaux, cela découragera les autres. C'est comme cela que nous y arriverons. (...) Je ne pense pas qu'il faudra tuer beaucoup de chercheurs. (...) Pour cinq à quinze vies humaines nous pourrions sauver plusieurs millions de vies animales »<sup>3</sup>. Il ajoute « les personnes qui torturent des êtres innocents devraient être stoppées. Et si elles ne s'arrêtent pas lorsque vous leur demandez poliment, et si elles ne s'arrêtent pas lorsque vous leur démontrez que ce qu'elles font n'est pas correct, dans ce cas, elles devraient être stoppées par tous les moyens nécessaires ».

Progressivement, les ultras radicaux accroissent donc la violence de leurs actions, allant jusqu'à s'en prendre directement aux individus ou acceptant de plus en plus facilement l'hypothèse de victimes humaines collatérales. Ils sont donc clairement entrés dans le champ du terrorisme et sont devenus de véritables criminels. C'est donc bien un « djihad » environnementaliste auquel nous avons affaire. En conséquence, aux Etats-Unis comme au Royaume-Uni, ces groupes figurent sur la liste noire des organisations terroristes au même titre que Daesh ou Al-Qaïda et cela a conduit le FBI et Scotland Yard à créer des unités spécialisées afin de lutter contre la menace qu'ils représentent pour nos sociétés

### **Modus Operandi :**

Une variété de modes opératoires sont à prendre en compte, ainsi la politique sûreté de l'établissement doit être à même de répondre avec une seule et même politique à l'ensemble de ces modes opératoires :

- **Voiture-Bélier :** Une voiture-bélier est une automobile qui est utilisée comme arme par destination, par exemple contre une foule, notamment par des groupes terroristes. C'est actuellement l'un des modes opératoires les plus utilisés comme le montre ces différents événements en France dans lesquels une voiture-bélier a été utilisée.
- **Attaque à l'arme blanche :** Les attaques à l'arme blanche font partie des modes opératoires les plus utilisés du fait de la facilité d'acquisition, de dissimulation et d'usage. Aucun temps de préparation n'est nécessaire et rend absolument imprévisible ce genre d'attaque. L'année 2020 a été marquée par 7 attaques terroristes, 6/7 des attaques ont été commises à l'arme blanche ce qui représente donc 85%.<sup>4</sup>

Il est important de noter que la tendance terroriste est à l'utilisation d'armes blanches et de véhicules béliers. De plus les profils des attaquants sont de plus en plus jeunes et les attaques sont régulièrement faites par des individus seuls.<sup>5</sup>

<sup>3</sup> The Observer, 25 juillet 2004

<sup>4</sup> « Terrorisme en France en 2020 : analyse de la menace dans un contexte de crise » - Alexandre Rodde

<sup>5</sup> Ibid

- Utilisation d'armes à feu : L'utilisation d'armes à feu ne se fait pas toujours durant les attaques terroristes, les différentes attaques susmentionnées en sont la preuve. Toutefois le risque est grand et les cas de fusillades, pas forcément liés au terrorisme, sont réguliers à Marseille. Depuis 2012, et la création d'un préfet de police des Bouches-du-Rhône, cette moyenne est de 22 fusillades par an pour une petite vingtaine de victimes.
- Explosifs :
  - Le colis piégé : engin explosif envoyé par voie postale ou déposé à un endroit stratégique qui vise à blesser ou à tuer le destinataire lorsqu'il ouvre le colis. Très utilisé par l'ETA son usage se fait de plus en plus rare. L'un des derniers cas est celui de Lyon en 2019, où un individu dépose un sac ou un colis explosif contenant des vis, des clous et des boulons devant un commerce de la rue Victor Hugo faisant 14 blessés par suite de l'explosion. Les derniers chiffres concernant le déminage font état du fait que seules 0,6% des interventions correspondent à une réelle menace.<sup>6</sup>
  - Le gilet explosif : gilet porté par un kamikaze qui soit pour déclencher une explosion et/ou une sur-explosion, soit lorsqu'il est acculé, déclenche la charge explosive portée pour faire le plus de dégâts possibles. Cela faisait notamment partie des modes opératoires utilisés lors de l'attaque de novembre 2015 à Paris.
  - Les drones : les drones sont aujourd'hui une menace à part entière, pour les sites industriels notamment, il n'est pas nécessaire d'avoir un REAPER (drone américain de 11m) pour occasionner des dégâts considérables, matériels comme humains. Nous n'avons pas d'exemple à ce jour en France, néanmoins, les terroristes et criminels utilisent d'ores et déjà des drones de petite taille pour frapper des sites sensibles ou des cibles humaines. Faute de ressource, une charge explosive et un drone de petite taille suffisent.
  - Empoisonnement/Biologique/Chimique : Nous le voyons avec la crise COVID19, le risque biologique est grand, un virus peut occasionner des pandémies, avoir des impacts considérables sur tous les pans de la société. Aussi, il s'érige logiquement comme une menace car est un « outil » de choix pour les organisations terroristes tout comme le risque chimique. Parmi les procédés les plus redoutables, l'utilisation de canaux d'approvisionnement existants, notamment en eau potable. Bien que marginal l'aqua-terrorisme est une menace à prendre en compte puisque différentes tentatives ont déjà été faites :
    - En 2018, tentative d'empoisonnement de l'eau potable de Sardaigne
    - En 2017, tentative d'empoisonnement de l'eau potable de Rome ;
    - Mars 2016, une cyber-attaque modifie la quantité de composants chimiques présents dans l'eau d'une usine d'eau potable de la société Verizon ;
    - Le 11 juillet 2015, des membres de l'organisation Etat Islamique tentent d'empoisonner un réservoir d'eau au Kosovo

La liste faite des différents modes opératoire ne peut être exhaustive car elle est en constante évolution, il est important de noter que ces différents modes ne s'emploient pas forcément de manière isolée, un même individu peut utiliser différents modus operandi et différents individus peuvent, stratégiquement, déclencher des effets en chaîne en combinant différents modes opératoires. De nouveau : une politique sûreté globale doit être mise en place.

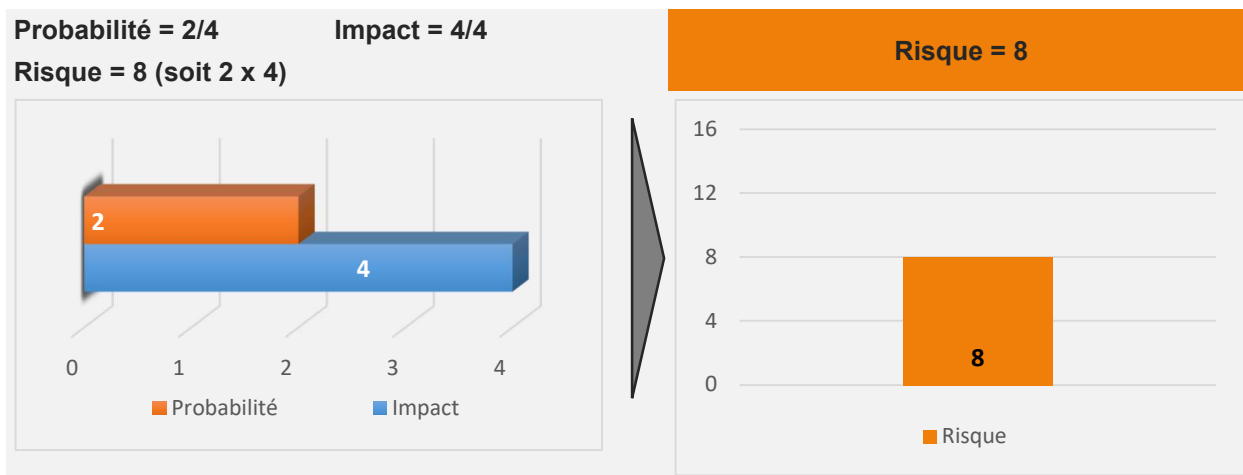
<sup>6</sup> « Combien de colis suspects s'avèrent être des bombes », Libération, 27/06/2018  
[https://www.liberation.fr/checknews/2018/06/27/combien-de-colis-suspects-s-averent-etre-de-vraies-bombes\\_1661967/](https://www.liberation.fr/checknews/2018/06/27/combien-de-colis-suspects-s-averent-etre-de-vraies-bombes_1661967/)

### Cotation du risque initial :

#### Impact :

Si un tel acte venait à être exécuté, il pourrait causer des pertes humaines considérables et endommager gravement les installations. Nous qualifierons l'impact de ce risque « **extrêmement grave** ».

#### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

### 2.1.3 Enlèvement et/ou séquestration

L'enlèvement, ou kidnapping, est un acte criminel, qui commence par le rapt d'une personne dans le but de la séquestrer afin d'en retirer un avantage, souvent financier en demandant une rançon à ses proches ou bien des revendications politiques par rapport à un état avec des menaces d'exécution d'une personne.

Les enlèvements peuvent viser une personne propre ou son entourage proche (enfants, conjoint etc.) afin de posséder un moyen de pression et les motivations sont variées, un groupe criminel peut cibler la famille d'un grand dirigeant pour obtenir une rançon. On qualifie de séquestration le fait par des salariés de retenir contre leur gré des cadres d'une entreprise lors de conflits sociaux.

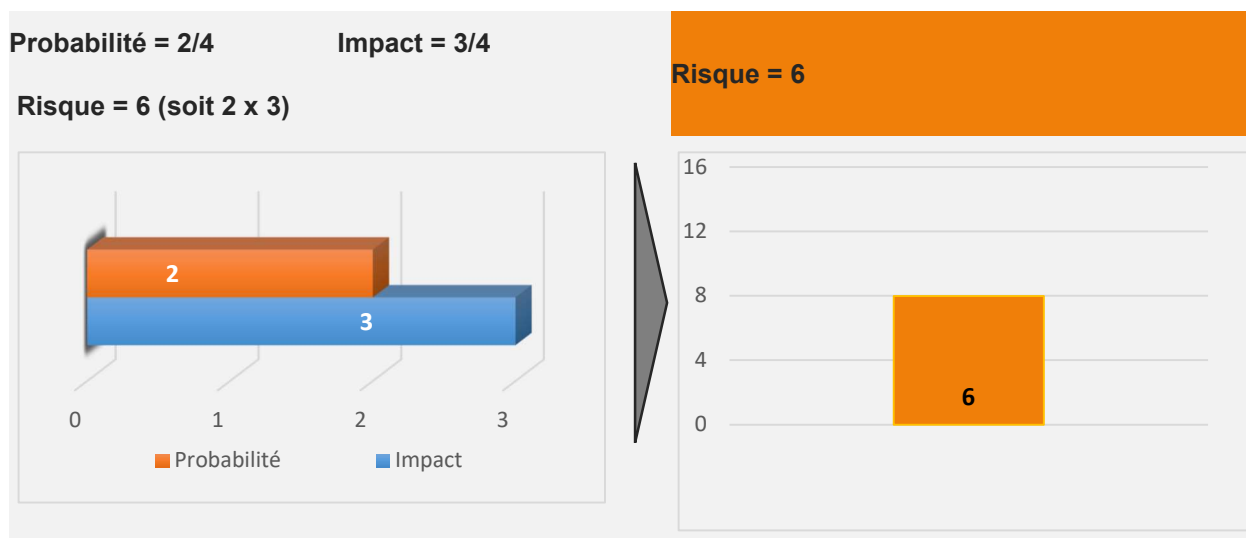
Comme nous l'avons vu précédemment certains groupes extrémistes animalistes et antispécistes n'hésitent pas à porter atteintes aux personnes. Ainsi en 2001, des membres britanniques d'ALF séquestrèrent pendant une demi-journée les enfants des dirigeants de l'entreprise pharmaceutique danoise Lundbeck dans leur école de Copenhague en leur exhibant de nombreuses photos d'animaux sanguinolents exposés aux tests.

Des menaces ont par ailleurs été proférées à l'encontre du vétérinaire référent de l'animalerie.

#### Cotation du risque initial :

**Impact :** la séquestration d'un chercheur outre les symptômes post-traumatiques dont pourrait souffrir la victime, pourrait aussi avoir un effet désastreux en termes d'image pour la délégation régionale du CNRS. Nous qualifierons l'impact de ce risque « **très grave** ».

#### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.1.4 Dégradations ou destructions volontaires

Juridiquement, l'acte accompli par malveillance est celui accompli avec l'intention de nuire. Ici la dégradation désignera donc le dommage matériel subi par un bien mobilier ou immobilier, provenant d'un acte volontaire, tout comme pour la destruction.

Les activistes animalistes notamment, dans le cadre de leurs actions préconisent et pratiquent la dégradation et la destruction de locaux. En recourant au sabotage ou à la destruction des infrastructures (incendies criminels principalement),

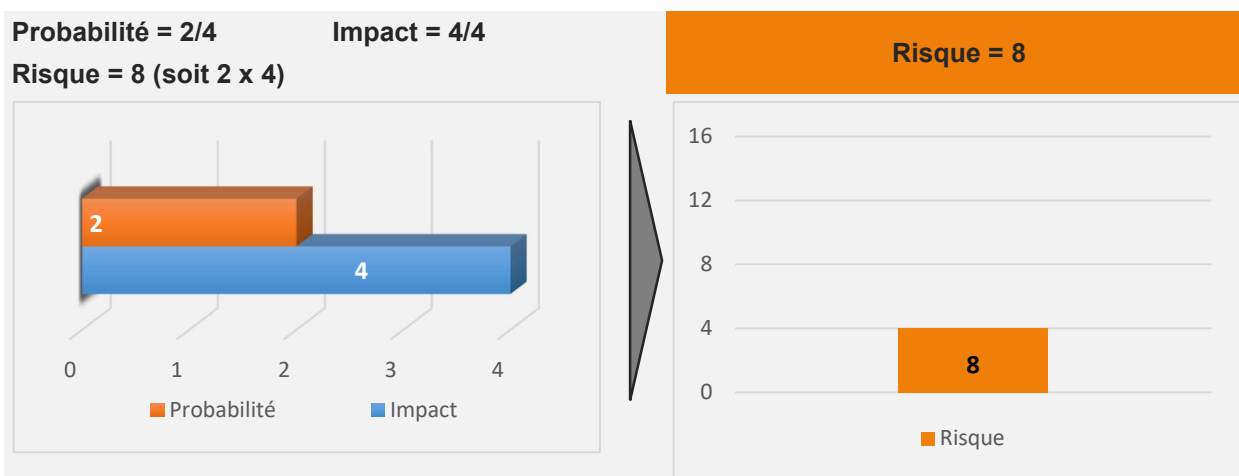
- En mai 2007, des activistes de l'ALF sont à l'origine d'un incendie criminel des locaux lyonnais de l'entreprise Tecniplast, qui fabrique des cages et de l'équipement d'animalerie, et qui est accusée de travailler avec l'entreprise britannique d'expérimentation animale Huntingdon Life Sciences (HLS), l'une des cibles favorites des mouvements de libération animale.<sup>7</sup>
- Un an plus tard, le laboratoire Charles River, filiale du groupe américain du même nom qui élève des animaux de laboratoire à Saint-Germain sur l'Arbresle (Rhône) est victime lui aussi d'un incendie volontaire qui détruit trois véhicules et une partie de ses locaux à la suite de l'explosion d'une bouteille de gaz.<sup>8</sup>
- Enfin, en décembre 2010, les locaux administratifs de Biomatech Namsa, société spécialisée dans l'évaluation des produits de santé à l'aide de tests toxicologiques, sont incendiés à Chasse-sur-Rhône, dans l'Isère, et cette action est revendiquée par l'ARM.<sup>9</sup>

### Cotation du risque initial :

#### Impact :

Des détériorations et dégradations graves pourraient causer des pertes humaines et endommager les installations paralysant la direction, le service informatique et le service recherches et développement. Nous qualifierons l'impact de ce risque « **extrêmement grave** ».

#### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

<sup>7</sup> [https://www.lexpress.fr/actualite/societe/les-enrages-de-la-cause-animale\\_476038.html](https://www.lexpress.fr/actualite/societe/les-enrages-de-la-cause-animale_476038.html)

<sup>8</sup> [https://www.francetvinfo.fr/faits-divers/l-attentat-d-un-commando-antivivisection-francais\\_1642797.html](https://www.francetvinfo.fr/faits-divers/l-attentat-d-un-commando-antivivisection-francais_1642797.html)

<sup>9</sup> <https://www.ledauphine.com/isere-nord/2011/02/01/des-ecoterroristes-revendiquent-un-incendie-a-chasse-sur-rhone>

### 2.1.5 Vol de données sensibles

Dans le cadre de notre étude sont appelées « données sensibles » toutes données personnelles relatives aux personnes physiques ou morales travaillant au profit du CNRS, celles relatives aux opérations, de tous ordres, menées par le CNRS (recherches fondamentale, brevets etc.).

La masse de données traitées augmente chaque jour et les risques de fuite qui vont avec également. Au premier semestre 2019, il y a eu en moyenne 5,7 violations de données par jour en France contre 4,5 au deuxième semestre 2018. Dans 54% des cas, les fuites de données ont été d'origine malveillante avec 69,8% de piratage en ligne et 15% de vol physique.

Dans le cadre de la prise en compte de la menace « Vol de données sensibles », il est important de citer les différents moyens mis en œuvre :

#### ➤ Cambriolages :

Le contexte sanitaire engendre une présence diminuée au sein des structures et, souvent de ce fait, une surveillance moindre.

L'actualité nous prouve, que les laboratoires de recherches ne sont pas épargnés.

- 2016 cambriolages au laboratoire de Biochimie de l'hôpital la Pitié-Salpêtrière et plus précisément dans une pièce où sont entreposées des cellules souches et des bactéries <sup>10</sup>

#### ➤ Vols en interne :

La malveillance interne ne procède ni de la même motivation ni n'a les mêmes objectifs que la malveillance externe. Autant cette dernière est essentiellement tournée vers le profit de celui ou celle qui l'engendre, autant les motivations et les objectifs peuvent aller bien au-delà dans le cas de la malveillance interne. Les matériaux entreposés peuvent s'avérer tentant pour des personnes dénuées de scrupules.

#### ➤ Cyberattaque :

Les impacts d'une cyberattaque pourraient avoir de lourdes conséquences sur la délégation régionale Provence Corse du CNRS. Les attaques peuvent se traduire de manières différentes. :

- Les détournements de fonds : pour ce faire, un employé ou une personne extérieure à l'organisation débite malhonnêtement les comptes de celle-ci ;
- Les virus informatiques : leur introduction du fait d'un système de sécurité inexistant ou défaillant peut entraîner la destruction complète ou partielle des fichiers de l'entreprise. Ainsi, des mois ou des années de travail seraient irrécupérables. Parmi les fichiers les plus fréquemment exposés aux virus, notons les documents Word, les feuilles de calcul Excel, les sauvegardes et les fichiers exécutables à extension EXE ;
- Le piratage de données sensibles telles que les recherches, les partenariats avec les entreprises finançant la recherche et des DCP (données à caractère personnel) ;
- La soustraction de documents d'importance pour les livrer contre de l'argent, à d'autres organismes de recherches ;
- Les attaques par déni de service distribuées : le site web du CNRS est inondé d'informations inutiles, par un réseau d'ordinateurs. Ce qui conduit à un crash et rend le système non fonctionnel.
- L'hameçonnage ou le dévoiement : une personne ou entité essaye de recueillir des données confidentielles en apparaissant frauduleusement comme digne de confiance. L'hameçonnage s'opère par courriel. Quant au dévoiement, il se fait au moyen de sites ou serveurs fictifs.

<sup>10</sup> <https://www.rtl.fr/actu/justice-faits-divers/hopital-de-la-pitie-salpetriere-etrange-cambriolage-au-laboratoire-de-biochimie-7783391670>

Les attaques informatiques ont redoublé d'intensité depuis janvier 2020, notamment dans le contexte de pandémie. Ces attaques permettent d'accéder à différentes données sensibles et peuvent être des attaques externes (souvent liées à des facteurs internes), des malveillances internes ou encore des erreurs internes. Les attaques peuvent prendre différentes formes : phishing, malwares, matériel infecté, cryptolocking ... et peuvent avoir des conséquences désastreuses qui n'ont pas toutes encore été identifiées. Les chiffres le prouvent : plus que jamais, la cybersécurité doit être considérée comme un outil de travail et s'imposer dans la stratégie globale de l'entreprise.

Pour l'année 2019, la cybercriminalité était estimée à plus de 600 milliards de dollars (en détournements de données, demandes de rançons, etc.), soit 1% du PIB mondial détourné.

Depuis janvier 2020, l'augmentation constatée des cyberattaques est de plus de 30 000 %. De 1200 en début d'année, elles sont passées à 380 000 début avril. Ce sont principalement de l'hameçonnage (phishing en anglais), et des logiciels malveillants (malwares), des sites malicieux qui ciblent des utilisateurs à distance.

Il n'y a aucun milieu professionnel épargné par les attaques cybercriminelles qu'il s'agisse du vol de données, du blocage de données ou de piratage provoquant des arrêts de production, ainsi le milieu scientifique ne fait pas exception.

Les chercheurs ont par ailleurs décrit une cyberattaque potentielle qui pourrait être utilisée pour tromper des scientifiques sans méfiance et les amener à produire des substances biologiques dangereuses, des toxines et des virus synthétiques.<sup>11</sup>

- janvier 2021 L'Institut Pasteur a été victime d'une campagne malveillante via des attaques qui ont ciblé ses partenaires de recherche sur un vaccin contre le Covid-19<sup>12</sup>
- février 2021 cyberattaque sur les laboratoires de biologie de l'université d'Oxford<sup>13</sup>
- Mars 2021 cyberattaque sur les laboratoires Pierre Fabre à Castres<sup>14</sup>

<sup>11</sup> <https://www.welivesecurity.com/fr/2020/12/02/cyberattaque-tromper-scientifiques-substances-dangereuses/>

<sup>12</sup> <https://www.usine-digitale.fr/article/des-cyberattaques-ont-cible-l-institut-pasteur-qui-vient-d-abandonner-son-projet-de-vaccin-contre-le-covid-19.N1054079>

<sup>13</sup> [https://www.sciencesetavenir.fr/high-tech/les-recherches-de-l-universite-d-oxford-pas-affectees-par-une-cyberattaque\\_152112](https://www.sciencesetavenir.fr/high-tech/les-recherches-de-l-universite-d-oxford-pas-affectees-par-une-cyberattaque_152112)

<sup>14</sup> <https://www.ladepeche.fr/2021/03/31/castres-lentreprise-pierre-fabre-victime-dune-cyberattaque-9461485.php>

## Cotation du risque initial :

### Impact :

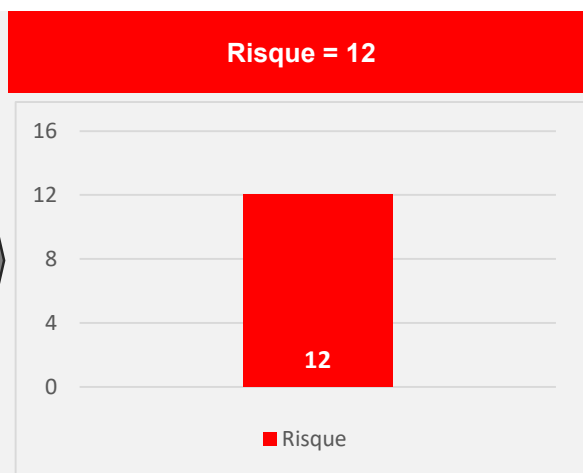
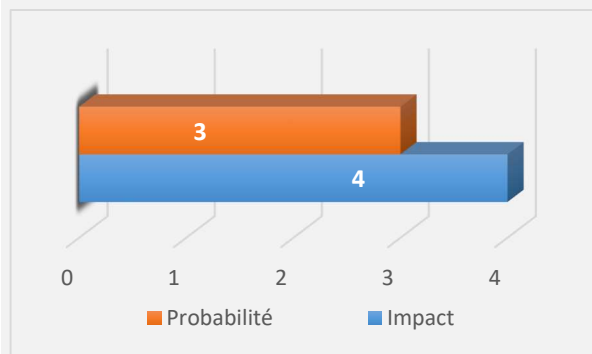
L'impact pourrait être important et il pourrait en résulter des dommages financiers, une dégradation de la réputation et de l'image du CNRS, une activité à l'arrêt ( une attaque informatique oblige de mettre l'activité principale d'une organisation en suspens, le temps d'éliminer tout risque potentiel.), une perte de données, un manque de confiance des entreprises partenaires en la sécurité de la délégation, les investisseurs seront plus enclins à s'engager avec d'autres laboratoires et centres de recherches, ce qui entrainera une baisse de la capacité à développer des projets. Une cyberattaque pourrait être extrêmement dommageable. Nous qualifierons l'impact de ce risque « **extrêmement grave** ».

### Probabilité :

Probabilité = 3/4

Impact = 4/4

Risque = 12 (soit 3 x 4)



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.1.6 Ingérence économique

L'ingérence économique est un ensemble d'actions, avec un but de captation d'informations, auxquelles les secteurs de recherches scientifiques peuvent être, et sont, confrontés.

Ce risque peut être mis en lien avec le risque de vol de données sensibles, mais cela ne se passera pas sur le site du CNRS. De même des procédés permettent la soustraction d'informations à une personne de son plein gré ou à son insu.

- Les salons scientifiques : Les salons sont une excellente opportunité pour les scientifiques de présenter leurs technologies et innovations, et de se faire connaître des autres spécialistes du marché.

Cependant, ces dernières années, la DGSI a constaté une recrudescence d'approches ou de démarches offensives conduites à l'encontre d'entreprises françaises par des sociétés ou des services de renseignement étrangers<sup>15</sup>. Ces derniers peuvent en effet réaliser, lors de ces salons, une veille concurrentielle active et mettent parfois en œuvre de réels stratagèmes de captation de données et d'informations.

Les techniques d'ingérence économique déployées lors de ces événements sont très diverses, passant, entre autres, de la collecte d'information au vol de matériels, à la captation de données et aux actions cyber et électroniques.

- Les entretiens rémunérés : En échange d'une compensation financière attractive, plusieurs employés d'entreprises et d'agences institutionnelles françaises ont récemment été contactés afin de participer à des entretiens visant à recueillir des informations précises relatives à leurs activités. Ces sollicitations émanent la plupart du temps de sociétés ou de cabinets de conseil étrangers.

Cette méthode permet en effet d'obtenir des informations à haute valeur ajoutée sur des filières d'importance, en ciblant notamment des acteurs stratégiques tricolores.

Véritable vecteur de captation d'informations, ce procédé peut faire perdre aux entités ciblées, via leurs collaborateurs, leur éventuel avantage concurrentiel et technologique.

- Le manque d'encadrement des stagiaires. Les entreprises et laboratoires ont tous recours à des personnels temporaires étudiants (stagiaires ou alternants), présents dans leurs locaux pour une durée s'étalant parfois sur plusieurs mois. Leur présence constitue une potentielle source de vulnérabilité pour le patrimoine d'une entreprise ou le potentiel scientifique technique national. En outre, il est à noter que certains concurrents ou pays tiers n'hésitent pas à « placer » des stagiaires dans le but de capter des informations ou de les faire bénéficier de formations à bon compte sur des technologies non maîtrisées. Le traitement de ces personnels temporaires est trop fréquemment négligé alors qu'ils devraient être informés et soumis aux mêmes obligations que l'ensemble du personnel de l'entreprise (signature de charte informatique, accord de confidentialité...). Leurs accès physiques et informatiques doivent également être précisément déterminés et restreints aux seuls travaux qui les intéressent. Par ailleurs, il est important de sensibiliser les référents de stage à la nécessité de remonter tout comportement anormal aux personnes en charge de la sécurité.

L'ingérence économique est difficilement quantifiable statistiquement car beaucoup d'actions ciblées ne sont pas considérées comme telles par leurs victimes, ne s'en rendant pas compte, et ne font donc pas l'objet de remontées. Toutefois c'est une menace importante de plus en plus répandue.

---

<sup>15</sup> Liste des Flashs Ingérence Economique de la DGSI <https://www.cyberocc.com/approfondir/intelligence-economique/flash-de-la-dgsi/>

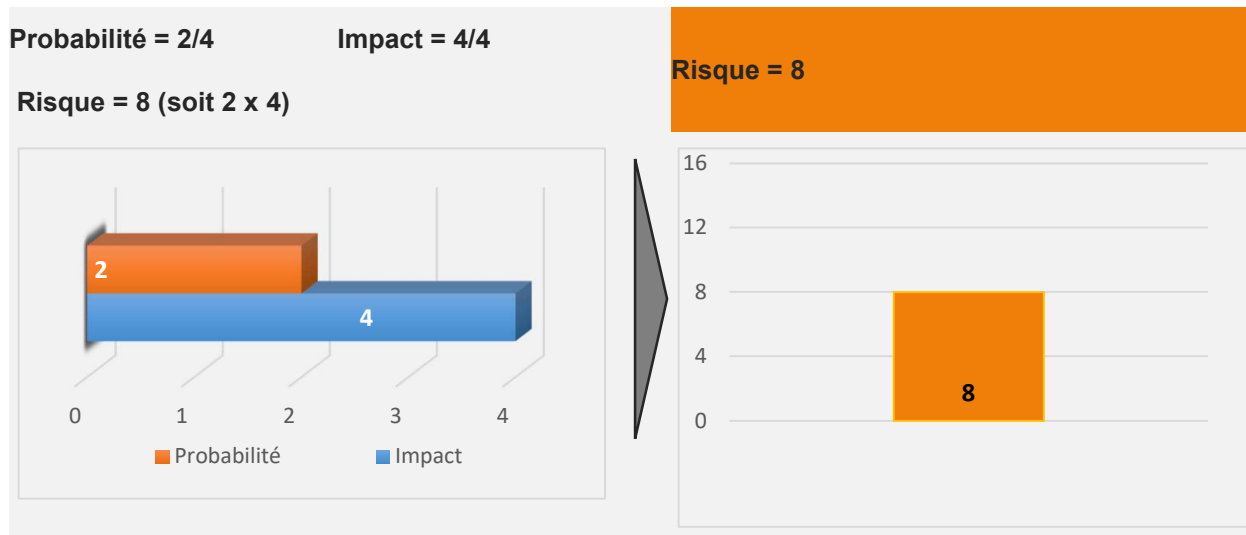
### Cotation du risque initial :

#### Impact :

Les conséquences de tels actes peuvent être nombreuses, perte de financement de la part d'entreprises partenaires, discrédit, déstabilisation du top management, lancement d'enquêtes publiques.

Nous qualifierons l'impact de ce risque « **extrêmement grave** ».

#### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.1.7 Troubles à l'ordre public

L'activisme animaliste est de plus en plus présent et virulent en France comme à l'étranger, différents groupes comme L214, PETA France, 269 life France, 269 libération animal et ALF, prennent pour cibles des laboratoires de recherches et activités liées :

Notons également la présence de groupes activistes à Marseille dont certains sont spécialisées dans des actions de rue :

- L214 Marseille/Aix
- ALARM Marseille
- 269 Life France Marseille
- The Earthling Expérience Marseille
- Anonymous for the Voiceless Marseille

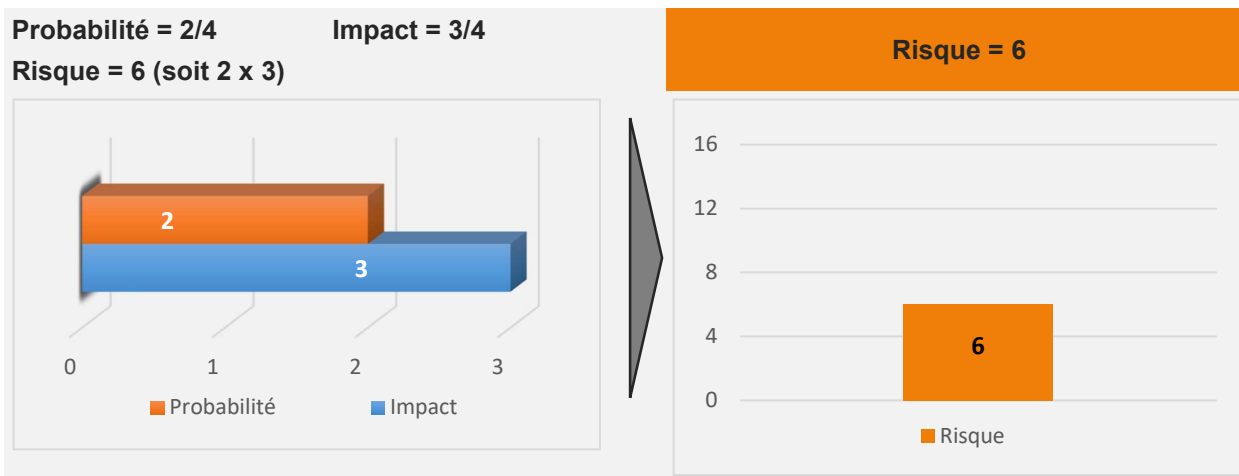
### Cotation du risque initial :

#### Impact :

Des manifestations et des troubles à l'ordre public assorties de blocage du site de la délégation attireraient l'attention des médias et pourrait modifier l'opinion publique sur le CNRS qui réalise des efforts de communication sur l'expérimentation animale et a signé en février 2021, la Charte de transparence sur le recours aux animaux à des fins scientifiques et réglementaires. Le blocage du site pourrait engendrer également des retards sur l'avancée de certains programmes scientifiques. Il ne faut pas négliger également les risques de dégradations et de rixes pouvant en résulter.

Nous qualifierons l'impact de ce risque « **très grave** ».

#### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.1.8 Agressions – coups et blessures volontaires – violences au travail

L'agression est une attaque, souvent soudaine et brutale, avec une atteinte réactionnelle de l'organisme. Les formes d'agressions peuvent être multiples dans le cadre du travail. Le plus souvent verbales, les agressions peuvent dégénérer en atteintes physiques ou morales, portant atteinte à l'intégrité de la personne.

Dans le cadre de notre analyse de risque les agressions sont celles pouvant intervenir sur le site ou ses abords.

Des agressions peuvent être commises sur le site de fait de circonstances personnelles (rixes, règlements de comptes) ou de manière ciblée (intimidation, revendications).

La violence et le harcèlement dans le monde du travail constituent un problème tenace et pernicieux. Il se manifeste entre collègues, entre les cadres et leurs subordonnés. La violence et le harcèlement peuvent prendre des formes diverses et changeantes, et pas seulement physiques ou sexuelles. Le harcèlement psychologique peut être particulièrement insidieux et abusif d'une manière extrêmement subtile, et le prix à payer au niveau psychique peut parfois conduire jusqu'au suicide.

Pendant la crise sanitaire que nous traversons actuellement, les cas de violence et de harcèlement semblent être en augmentation. En effet, les restrictions sans précédent qui ont été imposées à la population durant la pandémie ont accentué les niveaux de stress.

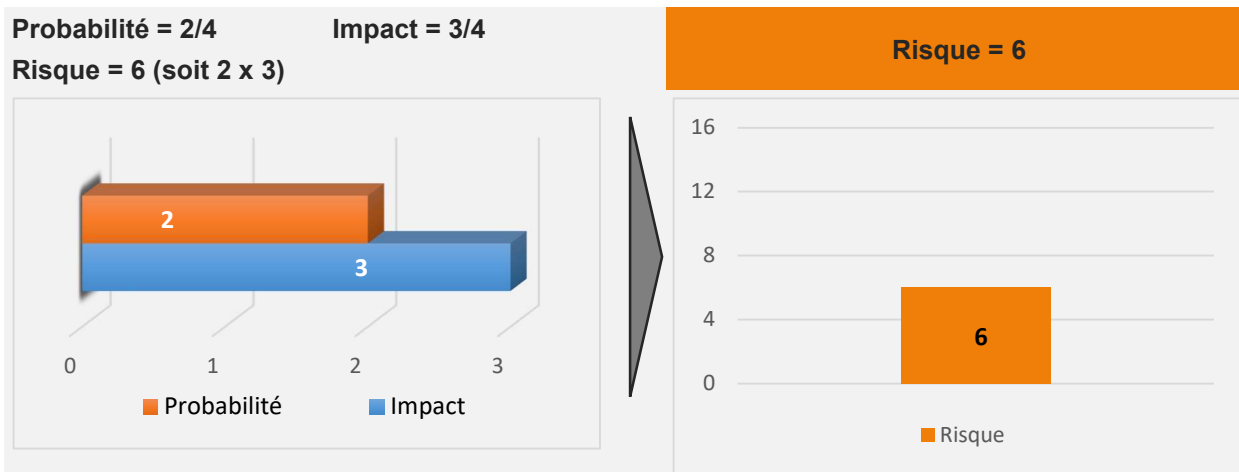
### Cotation du risque initial :

#### Impact :

Si un tel acte venait à être perpétré au sein de la station de Primatologie, l'impact psychologique sur les autres employés serait considérable (stress post-traumatique) et pourrait contribuer à relayer l'image d'une structure incapable de protéger ses employés.

Nous qualifierons l'impact de ce risque « **très grave** »

#### Probabilité :



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

## 2.2 PRISE EN COMPTE DES RISQUES A L'INTERNATIONAL/ EN DEPLACEMENT

Par suite d'une évolution favorable de la situation sanitaire, les voyages depuis et vers l'étranger sont de nouveau possibles selon des modalités qui varient en fonction de la situation sanitaire des pays tiers et de la vaccination des voyageurs

Le CNRS effectue chaque année environ 55 000 missions dans quasiment tous les pays du monde. En effet, l'archéologue ou le chercheur travaille sur des sources documentaires (bibliothèques, archives, musées...) qui se passent sur le terrain, dans des contrées et des situations souvent complexes. Les risques spécifiques potentiels imposent une attitude responsable et une vigilance auxquelles le chercheur n'est pas toujours préparé. Ainsi le Moyen-Orient devient de plus en plus dangereux pour les chercheurs européens.<sup>16</sup> L'Amérique du Sud n'est pas non plus exempte de danger pour les scientifiques.<sup>17</sup>

En temps normal, il ne fait pas bon voyager dans tous les pays du monde. Mais avec le coronavirus, cette liste s'est fortement développée. Les pays les plus à risques en 2021 seront donc surtout ceux qui disposent d'une infrastructure sanitaire fragile et qui ont été ou sont très touchés par le virus SARS-CoV-2.

Chaque pays n'a pas le même contexte, les mêmes mœurs, la même histoire, ainsi chaque menace est à appréhender différemment tant en termes d'impact que de probabilité d'occurrence. Aussi avant tout départ à l'étranger, une préparation doit être faite. Des bonnes pratiques doivent absolument être assimilées tout comme une connaissance du territoire et des risques majeurs auxquels nous pouvons être confrontés, des formations doivent être dispensées.

### Cotation du risque initial :

#### Impact :

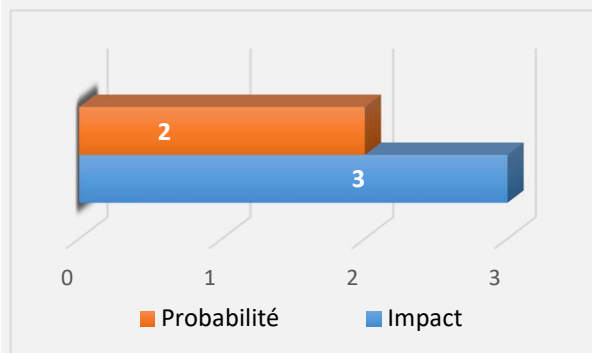
L'enlèvement d'un chercheur aurait un fort impact psychologique sur tous les personnels de la Station de Primatologie et de la délégation Provence-Corse du CNRS. Il générerait une situation de crise avec un impact fort dans les médias et pourrait remettre en question d'autres missions. Nous qualifierons l'impact de ce risque « **très grave** »

#### Probabilité :

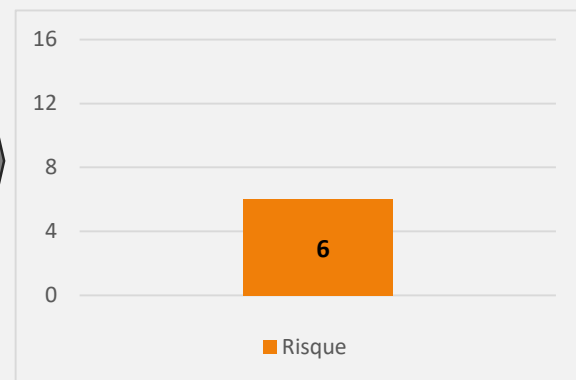
Probabilité = 2/4

Impact = 3/4

Risque = 6 (soit 2 x 3)



Risque = 6



	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

<sup>16</sup> <https://www.lemonde.fr/blog/filiu/2019/11/03/le-moyen-orient-de-plus-en-plus-dangereux-pour-les-chercheurs-europeens/>

<sup>17</sup> <https://www.lefigaro.fr/international/liberation-du-chercheur-espagnol-enleve-en-colombie-20201208>

## 2.3 HIERARCHISATION DES RISQUES

Les risques suivants ont été retenus en raison des antécédents de l'établissement, de sa situation géographique et socio-économique, et de ses caractéristiques propres (population, activité, biens mobiliers...).

L'échelle de cotation de la probabilité de survenu d'un risque est une échelle de 1 (peu probable) à 4 (extrêmement probable) ; celle de cotation de l'impact d'un risque est également une échelle de 1 (peu grave) à un 4 (extrêmement grave).

L'échelle de cotation du risque est une échelle de 1 à 16 (faible à extrême) :

	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

Scénarios	Risques malveillants pour l'établissement	Probabilité	Impact	Risque
1	Radicalisation	3	4	12
2	Terrorisme	2	4	8
3	Enlèvement	2	3	6
4	Dégradations.	2	4	8
5	Vol de données	3	4	12
6	Ingérence économique	2	4	8
7	Troubles à l'ordre public	2	3	6
8	Agressions	2	3	6
9	Risques à l'international	2	3	6

### 3 AUDIT DE LA SURETE DU SITE : ANALYSE DES ANOMALIES RELEVÉES ET PRECONISATIONS

La Station de Primatologie est située sur la route départementale 56 à Rousset 13790.

Le site est installé sur une parcelle d'une surface totale de 32 hectares (propriété du CNRS), dont 8 hectares clôturés par du grillage souple d'une hauteur de 2 mètres, le reste étant de la forêt. La Station de Primatologie dispose d'une douzaine de bâtiments (4.500 m<sup>2</sup> de surface habitable), le bâtiment de l'administration construit en 2011 qui accueille la direction, l'ensemble des personnels administratifs et un poste d'accueil, un bâtiment détente avec cuisine et 6 chambres d'hôtes, des laboratoires, des bâtiments techniques (ateliers), 2 villas d'habitations dédiées à des agents logés sur place, un garage, et principalement des animaleries (enclos fermés abritant des primates – Babouins Olives, babouins), et quelques bungalows type Algecco. Le tout accueillant environ 30 personnes (personnels CNRS, chercheurs, et étudiants).

La Station de primatologie héberge par ailleurs dans un bâtiment qui leur est dédié, la société ANIMALIANCE composée d'une dizaine d'agents et ayant pour tâches, l'entretien, l'alimentation, la santé, le nettoyage des primates.


La Station de Primatologie est en terrain mitoyen avec la déchetterie de Rousset, et voisine de l'aire d'autoroute SHELL située sur l'A8.

Nous évaluons les moyens de sûreté existants selon trois catégories définies comme suit :

1. **Les moyens architecturaux et mécaniques** : dans cette rubrique, nous abordons les moyens architecturaux physiques ou mécaniques mis en œuvre pour protéger les bâtiments à l'aide de clôtures, portails, barrières, murs, portes, serrures, vitrages, barres de sécurité ou de blocage.
2. **Les moyens technologiques** : dans ce chapitre, nous évaluons tous les moyens électroniques prévus dans un souci de sûreté des biens et des personnes fréquentant l'agence, et notamment ce qui concerne le contrôle d'accès, la détection d'intrusion, les moyens de communication et le système de vidéosurveillance.
3. **Les moyens organisationnels** : dans cette troisième catégorie, nous étudions les moyens organisationnels et notamment le personnel de sécurité (gardiennage) et toutes les procédures à mettre en œuvre tant en gestion de clés que d'interventions de personnels extérieurs.

#### 3.1 MOYENS ARCHITECTURAUX ET MECANIQUES

##### 3.1.1 Les accès

Points forts	
ACCES PERIPHERIQUES	
<ul style="list-style-type: none"> <li>• L'accès principal au site de la station de primatologie est sécurisé par un lourd portail coulissant en acier barreaudé, fermé en permanence.</li> <li>• Horaires d'accès au site de 8h à 12h et de 14h à 16h.</li> <li>• L'ouverture du portail se fait à l'aide d'un badge Bipper remis à chaque accédant disposant d'un véhicule (environ 30 bippers activés à ce jour et remis à des personnes identifiées)</li> </ul>	

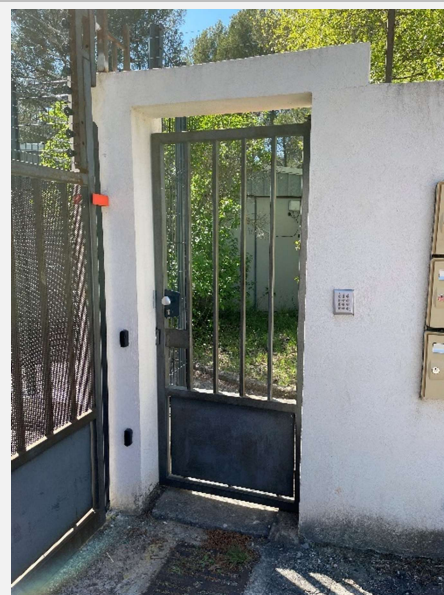
- Il est complété par un second portail faisant office de SAS en mode de fonctionnement normal. Ce portail n'était pas fonctionnel (en cours de maintenance) lors de notre audit.
- Détection au sol pour ouverture du 2<sup>e</sup> portail.



- Portail en position ouverture



- L'accès principal des piétons se fait par un portillon en acier barreaudé de bonne facture verrouillé en permanence et soumis à contrôle d'accès par digicode. Chaque accédant au site (piéton) dispose d'un code d'accès personnalisé ;



- Bonne signalétique, pas d'affichage des zones sensibles (animaleries)



- Le site dispose de 4 portails secondaires (vers déchetterie et arrière des bâtiments animaleries ROU140, ROU150 et ROU160) en grillage souple d'une hauteur de 2 mètres sur châssis métallique à double vantaux. Ces portails secondaires ne sont pas utilisés et sont verrouillés par une chaîne avec cadenas. Les portails sont surmontés de bavolets
- Le dispositif est complété par un système infrarouge de détection intrusion **désactivé.**



- Le site est également équipé sur sa périphérie de 5 portillons identiques en grillage souple de 2 mètres environ sur châssis métallique. Comme les portails secondaires, ces portillons sont surmontés de bavolets électrifiés. Ces portillons ne sont pas utilisés et sont fermés à clef.



#### Anomalies/Vulnérabilités constatées

##### ACCES PERIPHERIQUES

- L'accès au site est fermé en permanence par un lourd portail mais l'absence de contrôle et de filtrage permet l'accès au site à un visiteur ou un intrus au passage d'un entrant autorisé (personnel Station de Primatologie ou visiteur attendu) accédant au site.
- La circulation sur site étant libre, elle peut permettre à un visiteur de s'égarer dans les zones sensibles (animaleries)
- Sortie libre par bouton poussoir pour visiteurs, par Bipper pour détenteurs.
- Barrières infra-rouges non fonctionnelles

Niveau de maîtrise estimé		80% (élevé)
<b>Nos préconisations</b>		
<b>AAP1</b>	Remettre en état de fonctionnement le 2 <sup>ème</sup> portail afin de favoriser l'unicité de passage avec un contrôle des accès par véhicules.	
<b>AAI1</b>	Envisager un circuit pour les flux sur site permettant de mieux sanctuariser les zones sensibles	

### 3.1.2 Eclairage

Points forts	
<ul style="list-style-type: none"> <li>Le réseau d'éclairage couvre l'ensemble du site avec des projecteurs allumés à la tombée de la nuit.</li> </ul>	
Les extérieurs (allées, parkings) sont peu éclairés au motif de respect du confort des primates sur le site.	Spots à leds 20 watts éclairent le parking de l'administration
Anomalies/Vulnérabilités constatées	
Néant	
Niveau de maîtrise estimé	80% (Elevé)

	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

	Avant mise en œuvre des recommandations			Après mise en œuvre des recommandations (AAP1 ; AAI1 )		
MENACE	PROB.	IMP.	RISQUE	PROB.	IMP.	RISQUE
RADICALISATION	3	4	12	3	4	12
TERRORISME	2	4	8	2	4	8
ENLEVEMENT / SEQUESTRA.	2	3	6	1	3	3
DEGRADATION / DESTRUCTION	2	4	8	1	4	4
VOL DE DONNEES SENSIBLES	3	4	12	3	4	12
INGERENCE ECONOMIQUE	2	4	8	2	4	8
TROUBLES A L'ORDRE PUBLIC	2	3	6	2	3	6
AGRESSIONS / COUPS ET BLES.	2	3	6	1	3	3
RISQUES A L'INTERNATIONAL	2	3	6	2	3	6

### 3.1.3 La périphérie du site

#### Points forts

- L'enceinte périphérique du site « Station de Primatologie », est intégralement fermée et protégée. Sur toute sa périphérie, présence d'une clôture de grillage souple (1,7 km de clôture) de 2m environ surmontée d'un bavolet à 4 fils électrifiés.



#### Anomalies/Vulnérabilités

Le site est équipé d'un système de détection d'intrusion par câble sensible depuis 2011 mais le système est désactivé à cause de problèmes d'exploitation.

Niveau de maîtrise estimé

80% (élevé)

#### Nos préconisations

- Voir préconisations techniques

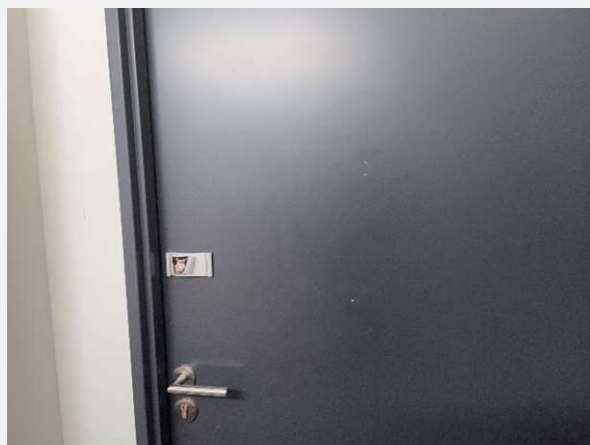
## 3.2 LES BATIMENTS

### MOYENS ARCHITECTURAUX

#### Points forts

#### Accès principaux

- Horaires d'ouverture d'accès au site de 8h à 12h et de 14h à 16h mais accès au bâtiment administration libre 24/7.
- Présence d'une porte vitrée à deux vantaux
- 2<sup>e</sup> porte vitrée formant un SAS mais libre d'accès.
- Toutes les portes en bois sont en très bon état général, elles ne sont pas systématiquement verrouillées au départ des personnels.



- Aile d'accès au couloir des bureaux administratifs et de la direction










- Aile permettant l'accès à la zone d'hébergement des hôtes



- Cuisine, salle de repos donnant sur terrasse ouverte en rez de jardin accessible par larges portes fenêtres vitrées. Pour une dizaine de personnes



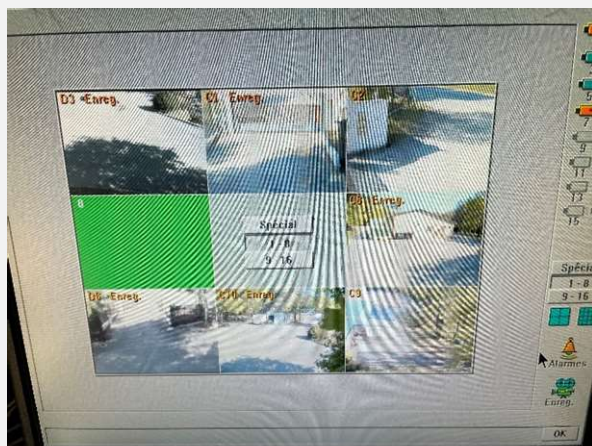
	
<ul style="list-style-type: none"> <li>• Logement d'agent logé</li> </ul>	
<ul style="list-style-type: none"> <li>• Bâtiment ANIMALIANCE</li> <li>• Passe commun pour tous les cadenas déposé par 3 personnes</li> </ul>	
<ul style="list-style-type: none"> <li>• Animaleries (zones sensibles) interdite d'accès aux personnes non autorisées délimitée par traçage bleu au sol.</li> <li>• Bâtiments B1 à B6 accessibles nuit et jour</li> <li>• Portes verrouillées par clef mécanique.</li> </ul>	

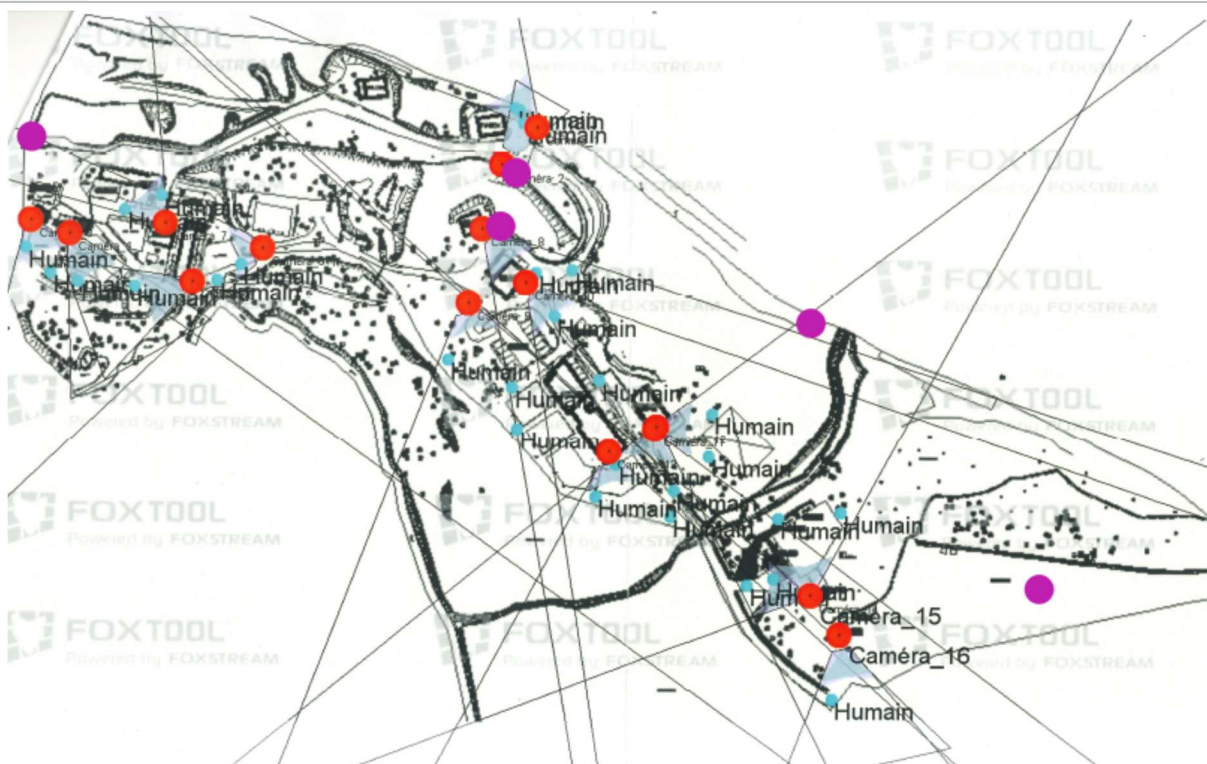
	 
<ul style="list-style-type: none"> <li>Atelier</li> </ul>	
<b>Anomalies Vulnérabilités</b>	
<ul style="list-style-type: none"> <li>Accès libre l'ensemble des locaux du bâtiment administration</li> </ul>	
<ul style="list-style-type: none"> <li>Pas de détection d'intrusion ni d'alarme volumétrique de l'ensemble des bâtiments du site</li> </ul>	
<b>Niveau de maîtrise estimé</b>	<b>70% (élevé)</b>
<b>Nos préconisations</b>	
<b>APP1</b>	<ul style="list-style-type: none"> <li>Verrouiller à clef le bâtiment administration le soir au départ des agents</li> </ul>
<b>APP2</b>	<ul style="list-style-type: none"> <li>Sanctuariser les bureaux de l'administration par rapport à l'accueil hébergement et la salle de cuisine par cloison</li> </ul>
<b>MOYENS TECHNOLOGIQUES</b>	

## Points forts

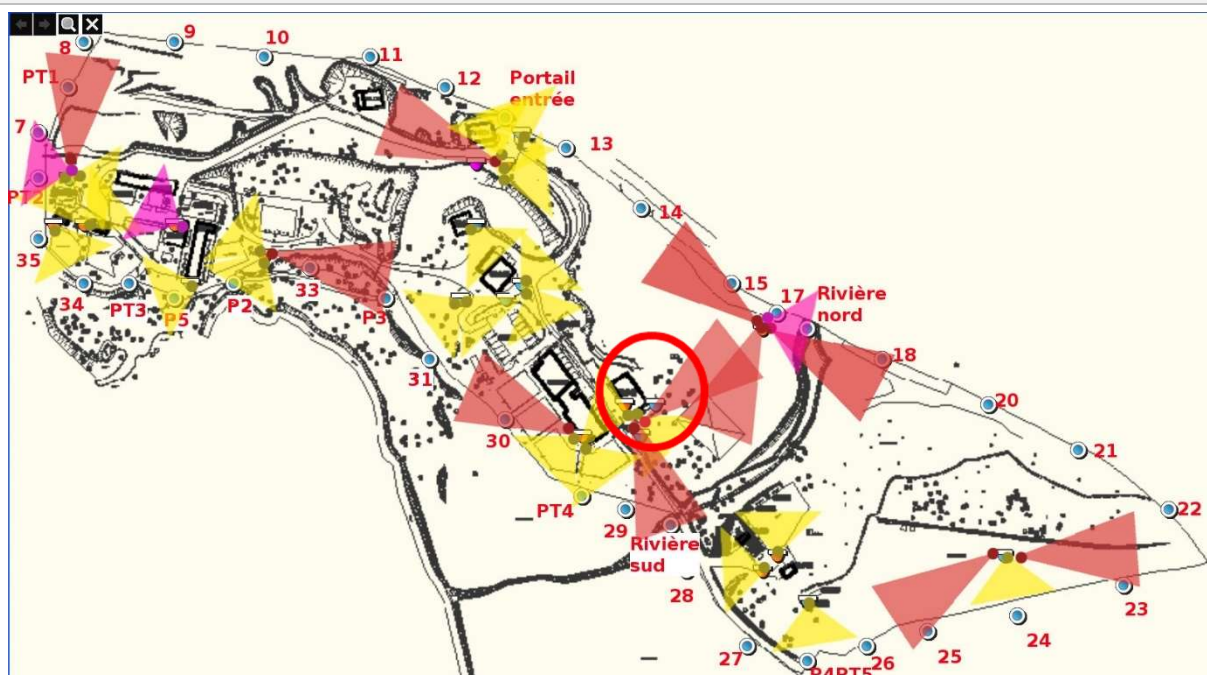
La Station de Primatologie est équipée à ce jour d'un dispositif de vidéosurveillance (système analogique avec 4 enregistreurs et supervision dans les locaux des 2 agents logés).

16 caméras couvrent correctement le site mais le matériel de marque BOSCH et l'ensemble du système commence à souffrir de vétusté.





En 2022, un projet est en cours de remplacement du matériel de vidéosurveillance et passage à une technologie IP/ Haute résolution avec l'ajout de caméras sur des points non couverts lors de l'audit (environ 30 caméras fixes et dômes au total)



- Existence d'un système de détection d'intrusion par barrière infra-rouges sur site au niveau du portail déchetterie (**désactivé**)

#### Anomalies/Vulnérabilités

- L'accès aux bâtiments n'est pas soumis à contrôle d'accès, les locaux sensibles (animaleries) sont verrouillés à clef
- Le bâtiment administration ne dispose pas de contrôle d'accès, il reste ouvert et accessible en permanence.

Niveau de maîtrise estimé

70% (élevé)

## Nos préconisations

<b>TVD1</b>	<ul style="list-style-type: none"> <li>Remplacer l'actuel système de vidéosurveillance analogique obsolète par du matériel IP Haute résolution (projet en cours)</li> </ul>
<b>TAL1</b>	<ul style="list-style-type: none"> <li>Remettre en état de fonctionnement le système de détection d'intrusion (barrières infra-rouges, câble sensible sur périphérie) existant</li> </ul>
<b>TCA1</b>	<ul style="list-style-type: none"> <li>Installer un système de contrôle d'accès par badge sur l'ensemble des bâtiments administratifs et locaux sensibles (zones animaleries) – <b>en mode renforcé</b></li> </ul>
<b>TCA2</b>	<ul style="list-style-type: none"> <li>Installer un interphone avec visiophone pour visualiser les demandes d'accès au site à l'entrée principale</li> </ul>
<b>TCA3</b>	<ul style="list-style-type: none"> <li>Installer un interphone à la place du bouton poussoir de sortie libre du site à l'accès principal.</li> </ul>

	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

	Avant mise en œuvre des recommandations			Après mise en œuvre des recommandations APP1 ; APP2 ; TVD1 ; TAL1 ; TCA1 ; TCA2 et TCA3		
MENACE	PROB.	IMP.	RISQUE	PROB.	IMP.	RISQUE
RADICALISATION	3	4	12	3	4	12
TERRORISME	2	4	8	2	4	8
ENLEVEMENT / SEQUESTRA.	2	3	6	1	3	3
DEGRADATION / DESTRUCTION	2	4	8	1	4	4
VOL DE DONNEES SENSIBLES	3	4	12	2	4	8
INGERENCE ECONOMIQUE	2	4	8	2	4	8
TROUBLES A L'ORDRE PUBLIC	2	3	6	2	3	6
AGRESSIONS / COUPS ET BLES.	2	3	6	1	3	3
RISQUES A L'INTERNATIONAL	2	3	6	2	3	6

### 3.3 MOYENS ORGANISATIONNELS

Nous traitons dans cette partie les points suivants :

- Procédures d'accueil
- Procédures de recrutement
- Gestion du personnel de gardiennage
- Gestion du personnel externe

### 3.3.1 Procédures d'accueil

#### Points forts

- Procédure d'accueil existante : arrivée d'un visiteur ou d'un prestataire qui s'annonce à l'interphone situé à l'entrée du site et qui est invité à se présenter à l'accueil situé dans le bâtiment Administration du site, ouverture à distance du portail par agent d'accueil.



- Enregistrement des visiteurs dans cahier de suivi



#### Anomalies/Vulnérabilités constatées

- L'accueil se fait directement à l'interphone situé au portail de l'entrée du site. Vulnérabilité liée à l'intrusion d'un visiteur non annoncé ou d'un intrus derrière un agent disposant d'un badge ou d'un visiteur attendu

Niveau de maîtrise estimé		60% (Moyen)
Nos préconisations		
OGA1	<ul style="list-style-type: none"> <li>Il est souhaitable que les procédures d'accès aux différents sites du CNRS Provence Corse soient uniformisées pour tous les sites dans la mesure du possible. Comme sur le campus de Joseph Aiguier il convient de mettre en place une procédure visant à bien maîtriser les flux de personnes sur le site de la station de Primatologie.</li> </ul>	
	<ul style="list-style-type: none"> <li>Voir préconisations techniques, mise en place d'un visiophone à la place des interphones pour visualiser les personnes entrantes sur le site avant ouverture du portail.</li> </ul>	


### 3.3.2 Procédures de recrutement

Points forts	
<ul style="list-style-type: none"><li>Le recrutement des scientifiques se réalise via le portail spécifique lié à la recherche EURACCESS : <a href="https://www.euraxess.fr/fr">https://www.euraxess.fr/fr</a></li><li>Procédure de recrutement encadrée. Pas d'enquête spécifique menée par le service RH mais sollicitation du fonctionnaire de sécurité de défense (FSD) attaché au CNRS</li></ul>	
Anomalies/Vulnérabilités constatées	
<ul style="list-style-type: none"><li>Néant. les procédures de recrutement sont soumis à des protocoles stricts</li></ul>	
Niveau de maîtrise estimé	90% (élevé)

### 3.3.3 Gestion du personnel de gardiennage

Le site de la station de primatologie ne dispose pas de service de gardiennage. En revanche, 2 agents techniques logés sur place assurent une astreinte pour levées de doutes techniques et de sûreté. Les 2 agents disposent d'un écran de supervision de images de vidéosurveillance du site. Ils assurent par ailleurs une ronde extérieure de l'ensemble des bâtiments chaque soir. Ils doivent assurer une présence sur site 24h/24h, 7 jours/7 jours.

### 3.3.4 La gestion des badges et des clés

Points forts	
<ul style="list-style-type: none"> <li>Absence de badges</li> </ul>	<ul style="list-style-type: none"> <li>Présence d'une boîte à clefs dans le bâtiment administration</li> </ul>
Anomalies/Vulnérabilités constatées	
<ul style="list-style-type: none"> <li>Boîte à clefs libre d'accès</li> </ul>	

### 3.3.5 Gestion du personnel externe

Points forts	
	<ul style="list-style-type: none"> <li><b>Personnel de nettoyage. Société KDS PACA</b> Une même personne de l'entreprise de nettoyage assure le nettoyage des bureaux et laboratoires lors des heures d'ouverture du site.</li> <li>Le nettoyage est procédé durant les heures de service de 8h à 16h</li> </ul>
Anomalies/Vulnérabilités constatées	
	<ul style="list-style-type: none"> <li>Il n'a pas été demandé à l'entreprise de réaliser une vérification des antécédents des personnels employés et de fournir un extrait de casier judiciaire</li> </ul>
Niveau de maîtrise estimé	
60% (moyen)	
Nos préconisations	
OP1	<ul style="list-style-type: none"> <li>Il serait utile d'envisager pour les futurs contrats de nettoyage d'inclure une clause supplémentaire concernant une obligation de vérification des références et la fourniture de l'extrait de casier judiciaire pour les personnels amenés à travailler sur le site.</li> </ul>

### 3.3.6 Politique et culture de sûreté

Les responsables du site Station de Primatologie du CNRS Provence Corse sont assez sensibles à la sûreté, comme en atteste leur projet de rénovation du système de vidéosurveillance. Des progrès, notamment par la remise en fonctionnement des moyens de détection d'intrusion pourraient faire évoluer sensiblement le niveau de sûreté du site de la direction de la délégation Provence Corse est soucieuse de développer la culture de sûreté, ses démarches en cours (audit de sûreté des sites CNRS de la délégation, réalisation du Plan de Mise en Sûreté – Attentat Intrusion PMS-AI) en sont la démonstration.

Points forts	
	<ul style="list-style-type: none"> <li>Des procédures (gestion des accès) sommaires mais qui sont bien appliquées.</li> <li>Désignation du responsable technique en tant qu'Assistant Hygiène Sécurité</li> </ul>
Anomalies/Vulnérabilités constatées	
	<ul style="list-style-type: none"> <li>Pas de véritable politique de sûreté : <ul style="list-style-type: none"> <li>- absence de plan de sûreté</li> <li>- absence de charte sûreté</li> <li>- absence de procédure normalisée de sûreté</li> </ul> </li> <li>Manque de sensibilisation des collaborateurs à la sûreté et la gestion des menaces</li> </ul>
Niveau de maîtrise estimé	
60 % (moyen)	
Nos préconisations	
OPS1	<ul style="list-style-type: none"> <li>Rédiger le PMS concernant le site Station de Primatologie Rousset (en cours)</li> </ul>
OPS2	<ul style="list-style-type: none"> <li>Procéder à la rédaction, d'un plan et d'une charte sûreté</li> </ul>



### OPS3

- Mettre en place des sensibilisations pour le personnel afin de les sensibiliser aux problématiques sûreté

	PROBABILITE P	IMPACT I	RISQUE P x I
1	Peu probable	Peu grave	Risque 1 à 4 : Faible
2	Probable	Grave	Risque 5 à 8 : Modéré
3	Très probable	Très grave	Risque 9 à 12 : Elevé
4	Extrêmement prob.	Extrêmement grave	Risque 13 à 16 : Extrême

	Avant mise en œuvre des recommandations			Après mise en œuvre des recommandations : OGA1, OP1 ; OPS1 ; OPS2 ; OPS3 ;		
MENACE	PROB.	IMP.	RISQUE	PROB.	IMP.	RISQUE
RADICALISATION	3	4	12	2	4	8
TERRORISME	2	4	8	2	4	8
ENLEVEMENT / SEQUESTRA.	2	3	6	2	3	6
DEGRADATION / DESTRUCTION	2	4	8	2	4	8
VOL DE DONNEES SENSIBLES	3	4	12	2	4	8
INGERENCE ECONOMIQUE	2	4	8	2	4	8
TROUBLES A L'ORDRE PUBLIC	2	3	6	2	3	6
AGRESSIONS / COUPS ET BLES.	2	3	6	2	3	6
RISQUES A L'INTERNATIONAL	2	3	6	1	3	3

#### 4 SUIVI DES RECOMMANDATIONS PAR CRITERES ET PRIORITES

MOYENS			Urgent	Court terme	Moyen terme
Bâtiments (s) audité(s)	Code	Recommandation (s)	Coût estimatif		
Site STATION DE PRIMATOLOGIE					
Moyens architecturaux – Accès principaux	AAP1	Remettre en état de fonctionnement le 2ème portail afin de favoriser l’unicité de passage avec un contrôle des accès par véhicules.	Contrat de maintenance		
Moyens architecturaux – Accès intérieurs	AAI1	Envisager un circuit pour les flux sur site permettant de mieux sanctuariser les zones sensibles	Néan		
Moyens architecturaux – périphérie périmétrie	APP1	Verrouiller à clef le bâtiment administration le soir au départ des agents	Néan		
Moyens architecturaux – périphérie périmétrie	APP2	Sanctuariser les bureaux de l’administration par rapport à l’accueil hébergement et la salle de cuisine par cloison	A évalué		
Moyens Technologiques – Vidéosurveillance	TVD1	Remplacer l’actuel système de vidéosurveillance analogique obsolète par du matériel IP Haute résolution (projet en cours)	Projet en cours		
Moyens Technologiques - Alarme	TAL1	Remettre en état de fonctionnement le système de détection d’intrusion (barrières infra-rouges, câble sensible sur périphérie) existant	A évalué		
Moyens Technologiques – Contrôle d’accès	TCA1	Installer un système de contrôle d’accès par badge sur l’ensemble des bâtiments administratifs et locaux sensibles (zones animaleries) – en mode renforcé	A évalué		

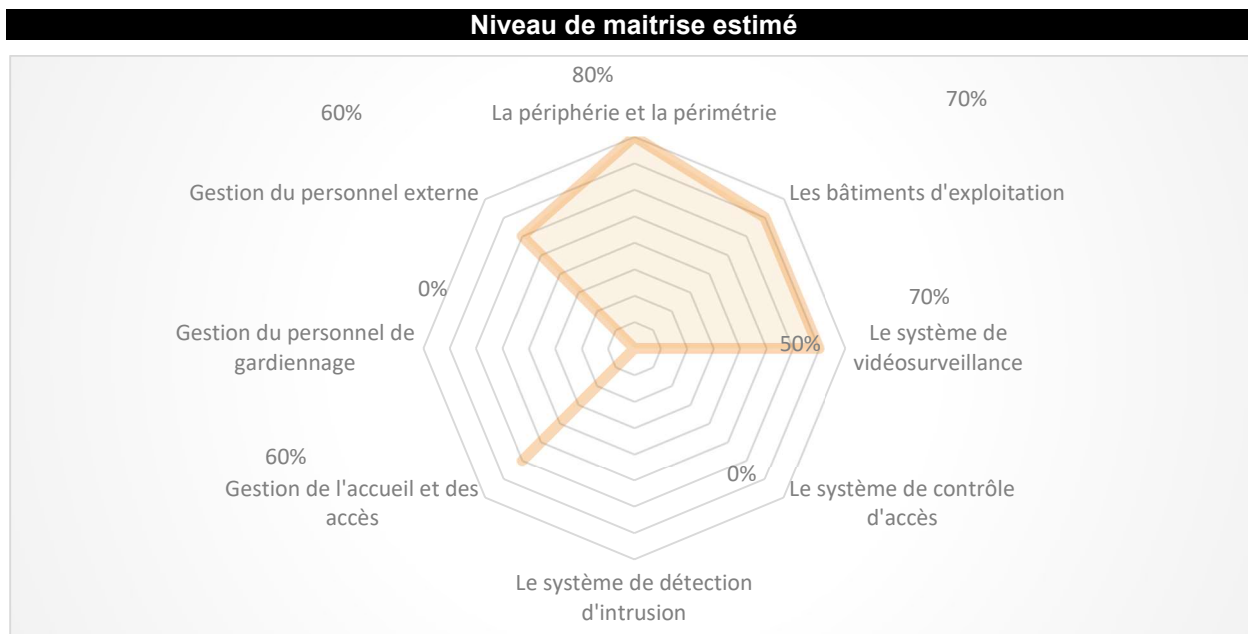
Moyens Technologiques – Contrôle d'accès	<b>TCA2</b>	Installer un interphone avec visiophone pour visualiser les demandes d'accès au site à l'entrée principale	1.000 €
Moyens Technologiques – Contrôle d'accès	<b>TCA3</b>	Installer un interphone à la place du bouton poussoir de sortie libre du site à l'accès principal.	1.000 €
Moyens Organisationnels Procédures Internes - Accès	<b>OGA1</b>	Il est souhaitable que les procédures d'accès aux différents sites du CNRS Provence Corse soient uniformisées pour tous les sites dans la mesure du possible. Comme sur le campus de Joseph Aiguier il convient de mettre en place une procédure visant à bien maîtriser les flux de personnes sur le site de la station de Primatologie.	Sans coût
Moyens Organisationnels Prestataires externes	<b>OP1</b>	Envisager pour les futurs contrats de nettoyage d'inclure une clause supplémentaire concernant une obligation de vérification des références et la fourniture de l'extrait de casier judiciaire pour les personnels amenés à travailler sur le site.	Sans coût
Moyens Organisationnels – politique et culture sûreté	<b>OPS1</b>	Rédiger dans délais assez brefs le PMS concernant le site (en cours)	
Moyens Organisationnels – politique et culture sûreté	<b>OPS2</b>	Procéder à la rédaction d'un plan et d'une charte sûreté	Sans coût sauf si recours prestataire externe
Moyens Organisationnels – politique et culture sûreté	<b>OPS3</b>	Mettre en place des sensibilisations pour le personnel à la problématique sûreté	A évaluer avec prestataire

<b>TOTAL ENSEMBLE SITE STATION DE PRIMATOLOGIE</b>	<b>1</b>	<b>5</b>	<b>8</b>	<b>14</b>
--	----------	----------	----------	-----------

## 5 CONCLUSION

L'audit que nous avons effectué le 26 avril 2022 sur le site de la Station de primatologie de la délégation régionale Provence Corse du CNRS nous amène à un certain nombre de conclusions devant être prises en compte pour garantir un niveau de sûreté optimal du site.

Le graphe ci-dessous met en évidence le niveau de maîtrise évalué sur chaque moyen audité.



Afin de rendre compte d'une situation globale de la sûreté, nous avons évalué les moyens humains et organisationnels de la sûreté mais également les moyens techniques et architecturaux participant à la sûreté du site hébergeant la Station de Primatologie de la Délégation régionale Provence Corse du CNRS et qui constitue une aide opérationnelle pour la direction du site. Cela nous a conduit à formuler 14 préconisations dont :

- 4 mesures concernant les moyens architecturaux et mécaniques,
- 5 mesures concernant les moyens technologiques,
- 5 mesures concernant les moyens organisationnels.

Parmi ces préconisations, nous constatons :

- 1 mesure urgente :

Elle concerne la mise en œuvre de moyens organisationnels par la rédaction du PMS- Attentat Intrusion.

- 5 mesures à court terme :

Il s'agit principalement de remplacer la vidéosurveillance, remettre en service le système anti-intrusion et de mettre en place une véritable culture de la sûreté au du CNRS,

- 8 mesures à moyen terme :

La plupart des préconisations concernent les moyens organisationnels et architecturaux en vue d'une protection renforcée du site et la mise en place de formations et de sensibilisations du personnel aux risques.

La mise en place des mesures proposées dans le cadre de ce rapport ne peut qu'optimiser les moyens et outils mis à disposition pour assurer la sûreté des personnes, des biens et des informations du site Station de Primatologie Rousset de la délégation régionale Provence et Corse du CNRS.