

RAPPORT

Résilience nationale :
Au-delà des constats, le temps de l'action

40 ANS HCFRN

18 OCTOBRE 2022



« Nous entrons dans un monde où l'intensité et la fréquence des perturbations, ruptures et parfois crises vont aller grandissantes. Cela va nous conduire à réfléchir mieux et plus vite sur les structures de gestion et d'anticipation à mettre en place.

Je pense que nous pouvons y apporter une modeste pierre, tant le chantier est titanesque. »

Christian Sommade, délégué général du HCFRN

Célébration des 40 ans du HCFRN le 18 octobre 2022 ©HCFRN

SOMMAIRE

4
LE MOT DU PRÉSIDENT

6
LES RENCONTRES EXTRAORDINAIRES DE MAURICE SCHUMANN

8
LE HAUT COMITÉ DE 1982 À NOS JOURS

18
ÉTAT DES MENACES ET RISQUES MAJEURS

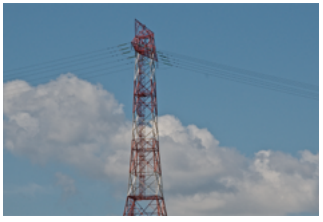
48
LA GESTION DE CRISE EN FRANCE

54
LES VOIES DE LA RÉSILIENCE

58
BILAN D'ACTIVITÉS 2021

64
REMERCIEMENTS



©HCFRN

LE MOT DU PRÉSIDENT



© Mairie de Paris

Le Haut comité n'en est pas à son premier rapport. Jouant son rôle de « veilleur », il a fait connaître ses travaux pour tirer les enseignements du passé et participer à l'amélioration de la préparation et de la gestion des évènements d'ampleur en France avec l'apport de ses membres, en particulier avec le soutien des opérateurs d'infrastructures critiques. Depuis les analyses du Gal(cr) Étienne Copel pour une meilleure prise en compte des risques technologiques ou NRBC et de la réponse aux actes terroristes, jusqu'à l'étude des grandes étapes et de la gestion de la crise sanitaire COVID-19 (2 rapports et plusieurs centaines d'infographies quasi-quotidiennes), l'action du Haut comité a été importante et reconnue.

Ma présidence a justement débuté en juillet 2020, année marquée par cette crise sanitaire et économique et je rappelais alors qu'il était urgent que la société civile prenne conscience des enjeux et soit impliquée dans la préparation face aux crises futures. C'est ce à quoi notre association contribue en accompagnant ses membres, en s'intéressant aux aspects aussi bien politiques que techniques et organisationnels de ces questions, et je tiens à souligner la qualité du travail réalisé par toute l'équipe et en particulier Christian Sommade, son délégué général, pour les y aider.

Ce nouveau rapport témoigne donc de 40 ans de réflexion et d'actions de notre association et propose un panorama des risques et menaces majeurs en France. Après le choc de la crise sanitaire, sur fond de guerre en Ukraine, mais aussi de défis énergétiques et sociétaux, il pousse à réinterroger le fonctionnement de nos organisations et habitudes et à tendre vers un modèle de résilience plus systémique.

Dans l'introduction du rapport « Risques et menaces exceptionnels - Quelle préparation ? » publié en 2012 à l'occasion des 30 ans de l'association, Jean-René Lecerf soulignait qu'il fallait « s'interroger sans cesse sur les efforts à entreprendre pour élever notre niveau de résilience nationale ». Je pense cet objectif inchangé comme nous l'exprimions lors de notre audition à l'Assemblée nationale[1] en novembre dernier.

(1) Général Étienne Copel, Vaincre la guerre, Edition Lieu Commun, Paris 1984

La prévention et la préparation de la France aux situations d'exception font bien partie de l'objet de l'association qui reste une plateforme unique d'information « 360° » sur les risques et de rencontres entre acteurs de la société civile : institutions, collectivités, entreprises, opérateurs, associations, experts intéressés et compétents sur les questions de résilience, de sécurité globale et de gestion de crise.

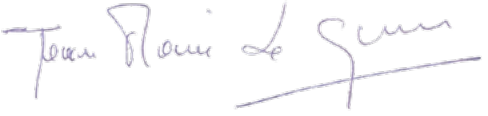
40 ans c'est aussi un âge on l'on regarde encore et toujours l'avenir. Celui-ci est porteur de risques et de menaces certes, mais aussi de beaucoup d'opportunités. Une grande politique de résilience nationale couvrant l'éducation, la participation citoyenne, le renforcement des réserves de tous types, l'investissement sur les infrastructures et sur les services liés à la résilience, permettra certainement de passer le cap des évènements difficiles qui peuvent survenir dans les prochaines années, notamment ceux liés aux phénomènes climatiques sévères ou extrêmes, mais aussi face à toute disruption sociétale majeure.

Face à l'incertitude, l'information est clef, la confiance également.

En cette matière le Haut comité a pu bénéficier du soutien de la Direction générale de la sécurité civile et de la gestion des crises du Ministère de l'Intérieur, du Ministère de la Transition écologique et de la Cohésion des territoires (qui a reconnu le label Résilience France collectivités comme axe stratégique pour le développement de la culture du risque) et du Secrétariat général de la défense et de la sécurité nationale, mais aussi de ses partenaires notamment la Brigade de sapeurs-pompiers de Paris, la Direction générale de la gendarmerie nationale et la Direction générale de la Police nationale.

Je souhaiterais enfin rendre hommage à Paul Girod qui avait pris la présidence du Haut Comité Français pour la Défense civile à la suite de Maurice Schumann et participé avec une forte implication et conviction à son rayonnement, ainsi qu'au Professeur Louis Crocq, également disparu cette année, et qui avait transmis à de nombreuses occasions lors de nos formations son expérience sur les effets psychologiques des « chocs ».

La Résilience de notre pays passe par renforcer la capacité d'agir de chacun, adapter nos moyens et chercher collectivement des solutions nouvelles.



Jean-Marie LE GUEN

Président du Haut Comité Français pour la Résilience Nationale

LES RENCONTRES EXTRAORDINAIRES DE MAURICE SCHUMANN

Fondateur du Haut Comité

« J'ai eu la chance unique de vivre plusieurs années aux côtés de Maurice Schumann et de bénéficier en direct de nombre de ses souvenirs. Aujourd'hui, au moment des quarante ans du Haut Comité il me semble opportun de rappeler le parcours de son fondateur et de retransmettre tels qu'il me les a narrés deux épisodes de sa vie au service de la France. »

Général Étienne Copel

PREMIÈRE RENCONTRE AVEC CHARLES DE GAULLE, LE VISIONNAIRE

Nous sommes dans les derniers jours du mois de juin 1940, me dit Maurice Schumann, je viens de débarquer en Angleterre et je me présente au général de Gaulle, au moment où, malgré l'évacuation réussie de Dunkerque, la plupart des experts prévoient l'invasion imminente de la Grande Bretagne par les troupes nazies qui ont terrassé les forces françaises en quelques semaines, je l'entends [le Général de Gaulle] encore me dire :

« Je suis vraiment ravi de vous accueillir aujourd'hui, pour plusieurs raisons et en particulier parce que, comme Hitler va sûrement perdre cette guerre, j'aimerais profiter de votre connaissance approfondie de la culture germanique, **pour que vous m'aidiez, dès aujourd'hui, à préparer la nécessaire réconciliation franco-allemande** » *!*

RENCONTRE AVEC MAO ET CHOU EN LAÏ

Le général de Gaulle ayant souhaité rapprocher la France et la Chine, je suis envoyé « tâter le terrain » à Pékin. Dès ma première rencontre avec le président chinois et son Premier ministre, Mao me demande de lui expliquer notre doctrine nucléaire, je la résume en disant « En gros, nous prévoyons que si les blindés soviétiques s'approchent du clocher de Strasbourg nous dirons au maître du Kremlin : « Si vous n'arrêtez pas vos troupes nous allons vitrifier Moscou, Stalingrad et Léningrad. » Alors, bien sûr, la conquête de la France ne valant pas la perte de leurs villes essentielles, les Soviétiques ne pourront que reculer. » *A ce moment Mao et Chou sont partis d'un grand éclat de rire et Mao m'a dit :* « **Comment pouvez-vous espérer faire croire aux Soviétiques, que je connais, que vous allez commencer une guerre nucléaire contre eux alors qu'ils sont mille fois plus puissants que vous et que leur population est en partie protégée et la vôtre pas du tout.** »

De retour à Paris je n'ai trouvé personne pour admettre que protéger les populations rendrait la menace du passage à l'acte, c'est-à-dire l'ouverture du feu nucléaire, plus crédible et par conséquent le discours dissuasif deviendrait plus efficace. Pour tous les apôtres de la dissuasion pure : protéger les populations voudrait dire que le discours dissuasif peut échouer ce qui, pour eux, est le crime suprême. On n'a pas le droit d'envisager que la Dissuasion puisse échouer ! Heureusement, en lisant votre livre , mon général, j'ai trouvé quelqu'un qui osait prôner l'idée que face à une attaque classique des Soviétiques il valait mieux profiter de la nouvelle efficacité des armes antichar pour se défendre par des moyens classiques plutôt que de risquer la fin de la France voire de l'Humanité en initiant un terrifiant feu d'artifices nucléaire.

C'est pour cela que j'ai souhaité vous voir rejoindre le Haut Comité et que j'ai fait modifier ses statuts pour que les parlementaires ne soient plus les seuls autorisés à en faire partie.

LE HAUT COMITÉ : DE 1982 À NOS JOURS

S'il n'est pas possible d'être exhaustif pour décrire 40 ans d'activités, il nous est paru nécessaire d'en rappeler les temps forts, les constantes et évolutions, les actions phares qui font le cœur et la « marque » de notre association ainsi que les partenariats solides qui sans aucun doute contribuent à sa longévité.

DU CONCEPT DE DISSUASION À LA RÉSILIENCE

1982-1991

Le concept de dissuasion et la crise des euromissiles

Renforcer la protection des populations

Créé en 1982 par le sénateur Maurice Schumann et le général Pierre Billotte, le « Haut comité français pour la défense civile » (HCFDC) a alors vocation, dans un contexte de guerre froide entre les États-Unis et l'URSS, à être un lieu de réflexion pour les décideurs publics et privés, en vue de protéger les citoyens français en cas de guerre nucléaire, chimique et conventionnelle.

1991-1998

Les problèmes de société et les risques

Mobiliser la société civile

Ouverture de l'association avec la création de différents collèges.
Le Haut comité poursuit ses travaux sur les risques majeurs naturels et technologiques et favorise la réflexion sur la doctrine, l'organisation et les techniques de notre pays en matière de défense et sécurité civile.

1998 - 2018

Risques et menaces sociétales

Professionnaliser l'association

L'association met en place ses propres outils (veille, cartographie) et méthodologies (exercices, formations), sa fonction de think tank se développe (événements, salons, médias, publications, voyages d'études). Elle propose une session nationale annuelle sur les questions de « Résilience et sécurité sociétales ». Elle accompagne l'État et les opérateurs à la gestion de crise et est également présente dans les projets européens.

2018 - 2022

Résilience

Informer et préparer les acteurs à la compréhension et la gestion des crises complexes face à un avenir incertain

Devenue en 2018 « Haut comité français pour la résilience nationale (HCFRN) » ou « Résilience France », l'association est le premier réseau d'acteurs professionnels publics et privés de la résilience en France. Elle s'attache à l'analyse des grands risques et des menaces, au développement de la résilience des organisations en termes de gestion de crise et post-crise, de continuité d'activité et de robustesse. Elle réfléchit également à plus long terme aux problématiques de résilience structurelle et à l'adaptation aux risques et menaces majeurs et hybrides qui impacteront notre société.

NOTRE APPROCHE ET DÉFINITION DE LA RÉSILIENCE

En vue de favoriser la prise de décisions « résilientes », dimensionner les actions et adapter selon les besoins la planification, nos travaux portent à la fois sur la résilience organisationnelle et la résilience structurelle.

La **résilience organisationnelle** est l'ensemble des mesures qu'une organisation ou un individu peut prendre pour réduire l'impact d'un choc. Professionnellement, ce sont les actions suivantes : l'analyse des risques et menaces auxquels on est exposé, la planification, la prévention, la préparation, la veille, l'alerte, la gestion de « crise », la continuité d'activité ou de services, les actions post-crise, le retour d'expérience.

La **résilience structurelle** prend en compte l'anticipation et la prospective des scénarios, mais surtout la réduction des vulnérabilités (par des leviers structurels, organisationnels et/ou comportementaux). Elle inclut aussi l'adaptation dynamique aux changements environnementaux, technologiques et sociétaux.

NOS THÈMES D'INTÉRÊT


Environnement géopolitique et stratégique


Mutations technologiques et environnementales


Risques et menaces majeurs


Résilience des organisations


Sécurité nationale


Veille et analyse


Prévention et planification


Gestion de crise


Communication de crise


Continuité d'activité et de services


Anticipation & Prospective

NOS RÉALISATIONS ET ACTIONS

Depuis 1998, le Haut comité français pour la résilience nationale a organisé plus d'une centaine de colloques techniques, dont plusieurs internationaux. Ces colloques sont l'occasion de participer avec l'ensemble des acteurs publics et privés concernés, à la réflexion sur la doctrine, l'organisation et les techniques de notre pays en matière de sécurité globale, de résilience et de protection des populations.

+ de 200
petits-déjeuners / rencontres au restaurant des Sénateurs

+ de 100
colloques en France et à l'International

+ de 200
webinaires

+ de 10
voyages d'études à l'international

7
sessions nationales de formation (2010-2017)

>100
formations à la gestion de crise et à la continuité d'activité

+ de 100
exercices de crises

4
projets européens de recherche

1
projet ANR
(Agence Nationale de la Recherche)

+ de 100
interventions médias

21
sessions de certification

35
certifiés
(tous niveaux confondus)

36
nouveaux labellisés depuis 2021

368
labels décernés depuis 2009

Veille

Depuis sa création en 1982, le Haut comité français pour la résilience nationale s'intéresse à l'évolution des risques et des menaces majeurs pesant sur le territoire national et à l'étranger. Adaptant constamment ses outils de veille, le Haut comité français pour la résilience nationale **offre à ses adhérents une plateforme interactive** permettant à chacun de personnaliser sa veille selon ses centres d'intérêt. Cette plateforme joue également un rôle de « mémoire » puisque les articles, même s'ils ne sont plus diffusés sur internet, restent accessibles sur notre plateforme et il est possible d'effectuer des recherches précises sur les années précédentes, depuis 2012.

Résilience territoriale

Le **label Résilience France Collectivités** est un label décerné par le Haut comité français pour la résilience nationale aux communes qui répondent à certains critères en termes de sauvegarde et de protection des populations face aux risques et menaces majeurs. Le développement du label Résilience France Collectivités a été présenté en octobre 2021 comme un des 3 grands axes stratégiques du Ministère de l'Écologie pour faire émerger une véritable culture du risque en France. Cette reconnaissance du label est le fruit de plus de 10 ans de travail auprès des collectivités.

FF72 « Faire Face 72 » est un site internet qui permet à chaque commune ou intercommunalité de créer facilement son propre site pour la préparation des populations en cas d'événement exceptionnel. Trois rubriques sont proposées aux citoyens afin de les initier à la résilience individuelle et collective : s'informer, s'adapter, se préparer. 72 heures, c'est le temps durant lequel les services essentiels aux populations sont susceptibles d'être affectés suite à un événement majeur. Chaque citoyen doit alors être le plus autonome possible, afin que les secours puissent se concentrer sur l'essentiel : sauver des vies.

Le **label Résilience France Entreprises** doit permettre aux entreprises d'évaluer leur propre dispositif de prévention des risques et des crises et de continuité d'activité, sur la base des meilleurs référentiels nationaux.

Certification professionnelle en Gestion de crise

Cette certification professionnelle lancée en 2021 comprend 3 niveaux : collaborateur de cellule de crise, responsable de cellule de crise, directeur de crise. Elle est à la fois une garantie de connaissances et de compétences, tant pour la structure d'emploi que pour le cadre de la cellule de crise.

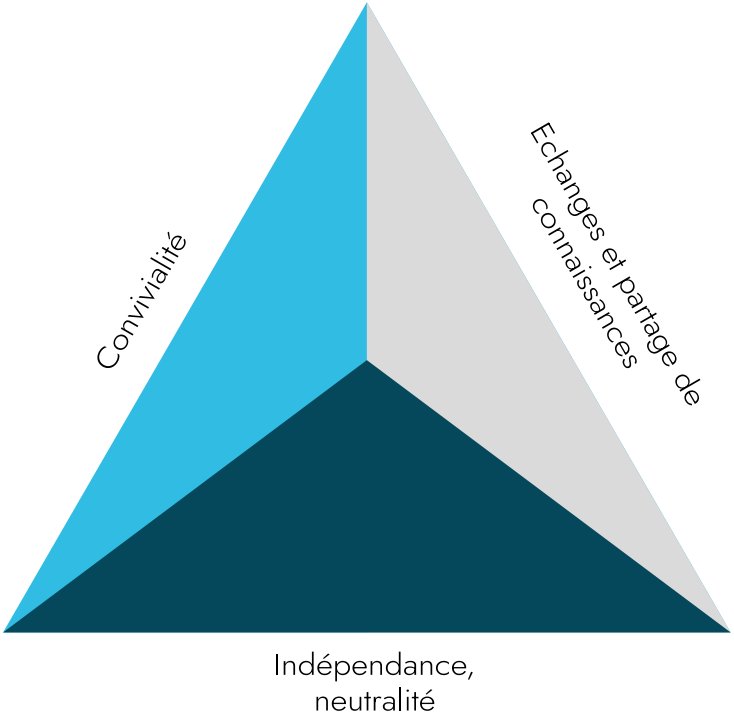
Études, recherche, accompagnement

Le Haut comité français pour la résilience nationale met en œuvre des projets ou réalise des études sur la continuité d'activité, la gestion des risques et des crises au profit de ses membres, notamment des grands opérateurs d'infrastructures. Il a ainsi travaillé au cours des dernières années sur des projets portant sur l'approche des phénomènes de résilience territoriale, avec l'appui du ministère de l'Intérieur (DGSCGC) et du ministère de la Transition écologique. Nos équipes développent aussi des méthodologies, des outils d'analyse, de visualisation des résultats et de dissémination. En 2021, le Haut comité français pour la résilience nationale a réalisé, dans le cadre d'une mission confiée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), une étude visant à identifier les entreprises essentielles, dans un contexte post COVID-19, pour permettre de mieux appréhender ensuite les axes d'amélioration de leur résilience.

Projets européens

Le Haut comité français pour la résilience nationale travaille sur des projets d'étude et de recherche afin d'innover et anticiper les problématiques de demain. L'association participe régulièrement à des projets européens (FP7, H2020, Horizon Europe) où son expertise et son savoir-faire peuvent s'exercer au travers de son réseau d'experts et de ses capacités de mobilisation d'acteurs publics, privés, de donneurs d'ordres ainsi que d'utilisateurs finaux, particulièrement dans les domaines : résilience, gestion de crise et NRBC.

NOS VALEURS



NOS OBJECTIFS

Favoriser la résilience nationale

En développant la capacité des organisations publiques et privées à faire face aux crises majeures : diminuer les vulnérabilités, mieux gérer les situations d'exceptions et en réduire les impacts.

Comment ?

En animant un réseau de professionnels autour de 8 axes :

1. Continuer d'assurer une veille permanente sur notre environnement tant national qu'international, en l'adaptant aux besoins de nos adhérents
2. Poursuivre les échanges de connaissances et techniques au travers de nos activités événementielles : rencontres mensuelles au Sénat autour de hautes personnalités, colloques, webinaires, visites … en tenant compte des nouveaux enjeux
3. Mettre en place de nouvelles formations, pour mieux préparer les cadres de demain à cette thématique globale de la résilience
4. Mesurer la résilience et la récompenser, tant pour les territoires et les organisations - au travers des labels Résilience France Collectivités et Entreprises - que pour les individus (certifications en gestion de crise)
5. Repenser les exercices de crises
6. Développer les coopérations nationales et internationales sur des sujets d'intérêt commun pour favoriser l'expertise
7. Poursuivre l'action européenne et les travaux de recherche
8. Accompagner nos membres (entreprises ou services de l'État) sur ces sujets, notamment au travers d'études et d'analyses

RÉSEAU INTERNATIONAL

Le Haut comité français pour la résilience nationale s'appuie sur son réseau pour proposer à ses adhérents des visites et voyages d'études en France ou à l'international. Il est le représentant en France du réseau international TIEMS (The International Emergency Management Society).

NOTRE PRÉSENCE SUR INTERNET

Nos sites internet

Site institutionnel : www.hcfrn.org

Certifications en gestion de crises : www.certifications-gestion-crise-hcfrn.org

Label Résilience France :

- pour les collectivités : www.label-resilience-france-collectivites.fr
- pour les entreprises : www.label-resilience-france-entreprises.fr
- le DICRIM pour les communes : www.ff72.org

Plateforme de veille : www.votresalledecrise.fr

Nos réseaux sociaux

@Résilience France - HCFRN

@Resilience France (HCFRN)

@Fr_Resilience

@Veilleint_HCFRN

@FranceLabelColl

@FranceLabelEnt



Célébration des 40 ans du HCFRN le 18 octobre 2022 © HCFRN

ÉTAT DES MENACES ET RISQUES MAJEURS

INTRODUCTION

Depuis sa création en 1982, le Haut comité français pour la résilience nationale (HCFRN) a toujours porté une vigilance particulière à l'évolution des risques et menaces majeurs qui pèsent sur les populations.

L'accumulation des crises endogènes et exogènes au territoire en ce début du 21ème siècle rend le concept de défense et de sécurité nationale plus prégnant tant au plan national qu'européen.

Loin de faire un panorama exhaustif des risques et menaces majeurs, le présent chapitre a pour objectif de présenter les grandes tendances sur les questions sociétales, sécuritaires, sanitaires et environnementales, principaux défis auxquels notre pays est confronté.

Les perspectives du changement climatique constituent un enjeu d'adaptation majeur pour notre société. Elle devra s'appuyer sur des mesures structurelles qui porteront leurs fruits sur un horizon à plusieurs dizaines d'années. Dans l'intervalle, les risques naturels : tempêtes, inondations, canicules risquent de se multiplier et de gagner en intensité. Les niveaux de prévention face à ces aléas, et de préparation face aux conséquences de ces crises, doivent être améliorés et renforcés.

Les menaces terroristes, notamment liées à l'islam radical et à d'autres radicalités, constituent une menace permanente dont la population doit être consciente et à laquelle elle doit être préparée. Les modes opératoires terroristes pourraient aussi évoluer dans les années à venir, notamment via le détournement des usages des drones, des nouvelles technologies ou encore le recours aux agents biologiques ou chimiques, ou de produits radioactifs.

Le risque sanitaire est réapparu sur le devant de la scène avec la crise de la COVID-19. La multiplication des virus et autres agents pathogènes - favorisée par le changement climatique et les échanges internationaux continuera de poser des défis au regard des pénuries du secteur de la santé, tant en termes de personnels de santé, que d'établissements de soins, de capacités de recherche et développement ou encore de production de contre-mesures médicales. Les défis « Santé » et « Santé face aux événements exceptionnels » demeurent majeurs face au vieillissement de la population.

La menace cyber constitue une préoccupation grandissante, compte tenu de la forte transition numérique de nos sociétés. La multiplication et la diversification des cyberattaques représentent une menace certaine pour l'économie, mais aussi pour la sûreté des infrastructures critiques. Tous les acteurs sont concernés, en particulier l'État et les entreprises qui concourent à la sécurité de la Nation. La difficulté d'attribution des attaques - réseaux criminels ou actions de déstabilisation d'États - rend la menace cyber très difficile à gérer. C'est dans ce domaine que le concept de « protection » (et aussi de remédiation) prend tout son sens, car il faut en général agir « avant ». Les capacités technologiques, d'innovation et de formation se révèlent indispensables pour endiguer la menace. C'est donc un secteur essentiel d'investissement en matière de sécurité nationale.

Le risque sociétal a connu une évolution majeure avec la crise des gilets jaunes. Cette dernière a révélé l'ampleur du phénomène de défiance envers les autorités. D'autres tendances comme les violences urbaines, l'économie parallèle des trafics, et la multiplication de cas de forcenés, témoignent d'une crise profonde que traverse la société française. Ces fragilités sont largement accentuées par les réseaux sociaux, eux-mêmes instrumentalisés par des puissances étrangères dans un objectif de déstabilisation.

Enfin la guerre en Ukraine n'a pas simplement posé la question de la menace que fait peser la Russie en Europe. Sur le plan militaire, l'instrumentalisation de la dissuasion nucléaire dans le cadre d'une guerre conventionnelle met en exergue les enjeux des seuils et de la co-belligérance. Mais cette guerre a surtout révélé les questions de dépendances en matière énergétique, économique et alimentaire. Cette crise va nous affecter quelques années avec les conséquences de l'inflation et la perte de pouvoir d'achat pour une grande partie de nos citoyens. Elle pose aussi le problème de la révision de notre outil de défense et de son intégration européenne et de la place « nouvelle » que doivent prendre la défense territoriale et la protection des populations en cas de conflit de haute intensité. Ce dernier point ne doit pas être oublié des politiques de défense et de sécurité nationale comme il l'est depuis plus de 70 ans.

L'ensemble de ces risques et menaces font peser sur les infrastructures vitales et critiques de notre pays un niveau d'incertitude jamais atteint, surtout si on ajoute les notions de souveraineté, d'autonomie stratégique, de vieillissement de nos infrastructures critiques, d'interdépendances connues ou non.

Les temps sont donc à l'analyse, la vision à moyen et long terme, au renforcement des capacités de défense et de protection en profondeur. Pour cela il convient d'avoir une vision claire de ces risques et menaces, de les veiller quotidiennement, de préparer les planifications de court et long termes, d'avoir des capacités de gestion de crise et d'anticipation dans la durée et sur l'ensemble du spectre des risques et menaces et enfin d'avoir une vision globale et stra-

tégique des enjeux et du positionnement de chacun des acteurs, à son niveau. La faiblesse de l'un sera la faiblesse de l'autre. Il faudra donc « plus » investir dans la préparation pour perdre « moins » dans la crise à tous niveaux.

CHANGEMENT CLIMATIQUE ET AGGRAVATION DES RISQUES NATURELS ET TECHNOLOGIQUES

[Axe 1] NaTech et sauvegarde des populations - [Propositions] Revoir la planification sur les risques naturels et technologiques à l'aune du changement climatique, en apportant une vigilance particulière sur les infrastructures critiques.

Depuis de nombreuses années, le Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC) alerte sur l'accroissement de la fréquence, de la durée et de l'intensité des événements climatiques extrêmes associés au changement climatique. Ce dernier est responsable, selon la plupart des experts, des vagues de chaleur records de l'été 2022. Il est donc nécessaire d'anticiper une aggravation des risques naturels liée à l'évolution du climat.

Le Ministère de la Transition Écologique estime que les deux tiers des 36 000 communes françaises sont exposées à au moins un risque naturel. Le risque d'inondation constitue le principal aléa en France, concernant 64 % du territoire et causant d'importants dommages humains, matériels et économiques. Il faut par ailleurs noter que 6 000 communes sont classées à risque feux de forêt.

En outre, la tendance à la concentration des populations dans les centres urbains et à l'artificialisation des sols constituent des facteurs aggravants de ces risques. Les évolutions plus lentes induites par le changement climatique telles que l'érosion côtière, l'assèchement des sols, les glissements de terrain ou la pollution atmosphérique auront également des impacts majeurs sur le niveau de risque.

Bien que la mortalité liée aux risques naturels soit limitée, les dommages économiques sont considérables et amenés à exploser. Le Centre de recherche sur l'épidémiologie des désastres (CRED) estime à plus de 224 milliards de dollars les pertes engendrées par les catastrophes naturelles en 2021 au niveau mondial. Une étude conjointe de la Caisse Centrale de Réassurance et Météo France basée sur le scénario RCP 8.5 du GIEC conclut à une hausse de 50 % du coût des catastrophes naturelles à l'horizon 2050.

Les pertes annuelles moyennes augmenteraient de 23 % pour les sécheresses, de 38 % pour les inondations et de 82 % pour les submersions. Les valeurs assurées pourraient alors atteindre 30 000 milliards d'euros, contre environ 14 000 milliards d'euros aujourd'hui.

D'autre part, découle également du changement climatique un accroissement des risques potentiels sur les sites industriels. Le concept de risque « NaTech » (qui regroupe l'impact d'une catastrophe naturelle et ses conséquences sur les installations industrielles) est apparu dans les années 2000 pour refléter cette nouvelle réalité. S'ils ne représentent qu'une part minimale des accidents industriels, les accidents NaTech ont eu tendance à augmenter ces dernières années selon l'Institut national de l'environnement industriel et des risques (Ineris). En effet, on en comptait 100 en 2021, contre seulement 30 en 2010.

À cet égard, les installations classées pour la protection de l'environnement (ICPE), notamment les sites classés Seveso, ainsi que les installations nucléaires font l'objet d'une surveillance particulière, mais le cadre de référence - des actions de prévention en impliquant les collectivités concernées, au dimensionnement des moyens de secours en passant par la planification - ne devrait-il pas être révisé pour certains d'entre eux, soumis à des risques naturels grandissants ?

D'autres installations critiques pour la société comme les datacenters ou les infrastructures de réseaux (électrique, transport, télécommunications) devront aussi s'adapter aux contraintes posées par le changement climatique. À ce jour, les réglementations ne concernent que les IPCE et opérateurs d'importance vitale. Or plusieurs secteurs deviennent aussi critiques, sans que ceux-ci soient réellement réglementés dans une approche « tous risques ».

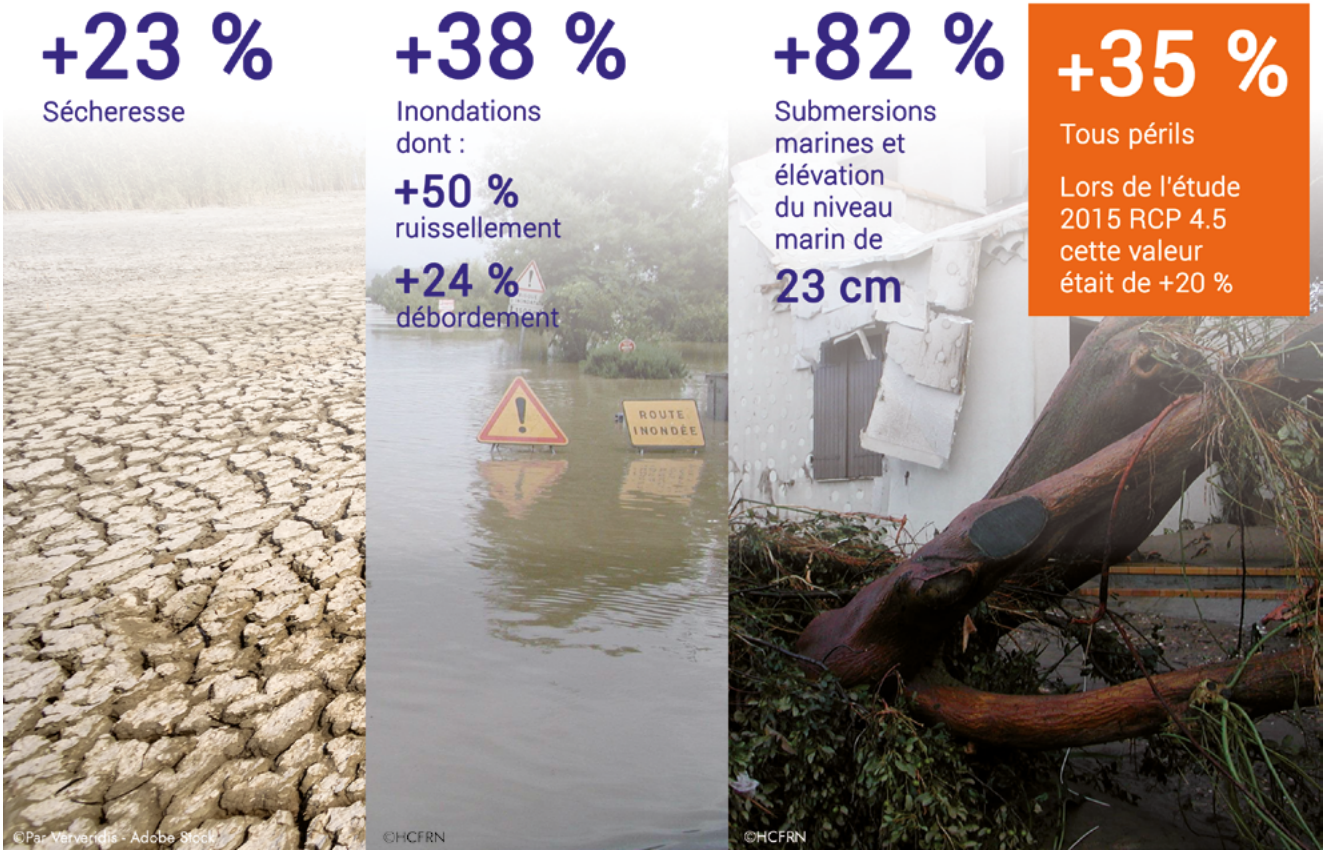


@HCFRN



Echelle historique du pont Wilson dans la ville de Tours @HCFRN

Évaluation 2050 des pertes annuelles moyennes par péril liées aux évolutions du climat sur les valeurs assurées actuelles



Données : @CCR - Production : @HCFRN

Par ailleurs, l'interdépendance des infrastructures et des réseaux est une vulnérabilité majeure car susceptible de provoquer des défaillances en cascade avec des impacts sociaux et économiques démultipliés.

Plus largement, le changement climatique affecte tous les domaines de l'activité humaine et amplifie les risques naturels mais aussi sanitaires (pandémies, pollution) et socio-économiques (instabilité des marchés, accès à l'eau, menace sur les systèmes alimentaires). Dans cette perspective, la France a porté au niveau européen la problématique du changement climatique. Durant sa présidence, Paris a fait de la transition écologique un axe stratégique de sa politique. Ainsi, le Pacte Vert a vocation à atteindre la neutralité carbone pour l'ensemble des États membres à horizon 2050.

ÉTAT DE LA MENACE TERRORISTE ET NOUVELLES FORMES DE TERRORISME

[Axe 2] Vigipirate et engagement de la population - [Propositions] Démocratiser les exercices anti-terroristes auprès de la société civile pour former aux bons comportements (RETEX Bataclan). Renforcer la résilience des OIV face à la diversification de la menace, notamment la menace portée par les drones et les nouvelles technologies.

La menace terroriste est toujours persistante, avec presque 300 morts et 1200 blessés sur les dix dernières années. Ces chiffres placent la France comme le pays le plus touché de l'Union européenne. Les conflits en Afrique subsaharienne et au Levant associés à la politique étrangère de la France sont instrumentalisés par les groupes terroristes qui font de la France un de leurs adversaires majeurs.

Les crises géopolitiques liées aux conflits armés, aux changements climatiques, aux risques sanitaires et pénuries alimentaires se multiplient et sont un terreau favorable à la menace terroriste.

Dans cette perspective, la crise sanitaire a été riche d'enseignements. Les mesures de restrictions - confinement, couvre-feu et isolement - ont été exploitées par les groupes terroristes pour propager massivement leur propagande. Ce qui pose des questions sur les pratiques et les cheminements de la radicalisation violente.

De plus, la COVID-19 a été l'occasion pour les groupuscules terroristes d'étendre leur champ d'action, personnels et infrastructures hospitalières étant désormais pris comme cibles en Occident. À ce titre, la planification antiterroriste, en particulier sur la résilience des infrastructures sanitaires et hospitalières, doit être améliorée.

À l'aune des grands événements sportifs de 2023 et 2024, la menace terroriste constitue une préoccupation majeure dans tous les modes d'actions possibles. Le risque d'usage de nouveaux vecteurs comme les drones représente de nouveaux modes opératoires auxquels il faut se préparer.

Les flux migratoires continueront d'être exploités par les groupes terroristes, comme a pu le révéler le RETEX des attentats du 13 novembre 2015. Certains des terroristes avaient emprunté des routes connues : arrivée par la Turquie, puis sur l'île de Leros en Grèce et enfin arrivée en Europe occidentale. Ces tragiques événements ont conduit à repenser la coopération entre les services de renseignement européens et les dispositions juridiques d'entrée sur le territoire européen. Le résultat est très incertain au regard des flux illégaux qui perdurent venant de l'Afrique du nord ou du Moyen-Orient.

En outre, le développement des nouvelles technologies, en particulier celles du metavers vont très certainement être exploitées par les groupes terroristes. L'utilisation de la réalité virtuelle et de la réalité augmentée permet aux groupes terroristes d'améliorer et d'intensifier leurs stratégies de recrutement et de mieux planifier des attentats. À ce titre, la diffusion de fatwa (avis juridique par un imam légitime) doit faire l'objet d'une surveillance accrue. Les tristes exemples de Salman Rushdie, de Charlie Hebdo et de Samuel Paty sont là pour le démontrer. L'accessibilité des données numériques, fort utile au développement économique, doit également être imaginée à l'aune du détournement de ces dernières par des groupes terroristes. Ainsi, si les services de renseignement commencent déjà à réfléchir à des solutions techniques pour surveiller l'activité sur ces nouveaux espaces numériques, la coopération public-privé sur ces champs d'activité devra être renforcée.

Face à ce constat, la France a pris un certain nombre de mesures pour endiguer la menace terroriste avec notamment la promulgation de la loi renseignement en 2015, de la loi SILT en 2017 et de la loi portant sur le retrait de contenus à caractère terroriste en ligne en 2022. Le RETEX du Bataclan a montré la nécessité de revoir la planification opérationnelle qui s'est traduite par la révision du Schéma national d'intervention. En plus de l'arsenal juridique français, les entreprises ont un rôle à jouer, en particulier au niveau de la sécurité physique des bâtiments et de la prévention du risque de radicalisation. Enfin, la société civile joue également un rôle dans la prévention et dans la réaction face à la menace terroriste, d'une part en se familiarisant avec le plan Vigipirate et d'autre part en signalant aux autorités des comportements suspects et/ou violents. Des exercices existent réunissant la population et les acteurs compétents contre la menace. Seulement, ils sont trop peu nombreux et réservés à une partie de la population. Une démocratisation de ces exercices permettrait une meilleure réponse sur la planification antiterroriste.



GAO à l'entrainement @HCFRN

La France dans la lutte contre le terrorisme

Présidence de Nicolas Sarkozy

Présidence de François Hollande

Présidence de Emmanuel Macron

Rébellion touarègue au Mali de janvier à avril 2012

Printemps arabe de décembre 2010 à décembre 2012



11 - 22 mars 2012

Attentats Merah à Toulouse et Montauban

11 janvier 2013

Début de l'opération Serval

25 mai 2013

Attentat à la Défense à l'arme blanche contre un militaire

21 décembre 2012

Promulgation de la loi relative à la sécurité et à la lutte contre le terrorisme pour poursuivre les auteurs d'actes de terrorisme commis à l'étranger par des Français ou des personnes résidant habituellement en France

30 avril 2014
Transformation de la DCRI en DGSI

1er août 2014
Fin de l'opération Serval, début de l'opération Barkhane

19 septembre 2014
Début de l'opération Chammal

13 novembre 2014
Promulgation de la loi renforçant les dispositions relatives à la lutte contre le terrorisme qui prévoit l'interdiction du territoire français des suspects candidats au djihad et crée un délit d'entreprise terroriste individuelle

26 juin 2015
Attentat dans une usine de production de gaz industriel à Saint-Quentin-Fallavier

3 février 2015
Attentat à Nice contre 3 militaires positionnés à un centre communautaire juif

7 janvier 2015
Attentats contre Charlie Hebdo et contre l'Hyper Cacher

20 décembre 2014
Attentat contre un commissariat à l'arme blanche à Joué-lès-Tours

24 juillet 2015

Promulgation de la loi sur le renseignement qui définit le cadre dans lequel les services de renseignement sont autorisés à recourir à des techniques d'accès à l'information

21 août 2015

Attentat du Thalys

13 - 14 novembre 2015

Attentat au Stade de France et au Bataclan

13 novembre 2015

L'état d'urgence est décrété dans la nuit du 13 au 14 novembre pendant 12 jours

22 mars 2016

Promulgation de la loi relative à la prévention et à la lutte contre les incivilités, les atteintes à la sécurité publique et actes terroristes dans les transports collectifs de voyageurs

24 mars 2016

Attentat déjoué avant l'Euro de foot

7 janvier 2016

Attentat contre un commissariat dans le 18e arrondissement de Paris

16 novembre 2015

Présentation du projet de loi prolongeant l'état d'urgence, intensification des opérations françaises en Syrie

3 juin 2016

Promulgation de la loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale

13 juin 2016

Attentat contre des fonctionnaires de police à Magnanville

21 juin 2016

Promulgation de la loi prorogeant l'état d'urgence et durcissement des mesures

3 février 2017

Attentat contre des militaires au musée du Louvre

19 décembre 2016

Promulgation de la loi prorogeant l'état d'urgence jusqu'au 15 juillet 2017

3-4 septembre 2016

Attentat déjoué contre Notre-Dame de Paris

14 juillet 2016

Attentat à Nice au véhicule bélier et contre une église à Saint-Étienne-du-Rouvray

28 février 2017

Promulgation de la loi relative à la sécurité publique

18 mars 2017

Attentat perpétré contre un militaire de l'opération Sentinelle à l'aérogare d'Orly

20 avril 2017

Attentat contre des fonctionnaires de Police sur les Champs-Élysées

14 juin 2017

Création de la CNRLT : Coordination nationale du renseignement et de la lutte contre le terrorisme

1er octobre 2017

Attentat à la gare de Marseille à l'arme blanche

9 août 2017

Attentat contre des militaires à Levallois-Perret

11 juillet 2017

Promulgation de la loi prorogeant l'état d'urgence jusqu'au 1er novembre 2017

19 juin 2017

Attaque terroriste à Notre-Dame de Paris visant les forces de l'ordre

30 octobre 2017

Promulgation de la loi renforçant la sécurité intérieure et la lutte contre le terrorisme, dite loi SILT

23 mars 2018

Attentat à Carcassonne et à Trèbes

12 mai 2018

Attentat à l'arme blanche à Paris dans le 2e arrondissement

11 décembre 2018

Attentat au marché de Noël de Strasbourg

13 janvier 2020

G5 Sahel, conférence de presse conjointe à l'issue du sommet de Pau

3 janvier 2020

Attentat à Villejuif à l'arme blanche

3 octobre 2019

Attentat à l'arme blanche à la préfecture de police de Paris

24 mai 2019

Attentat à la bombe artisanale à Lyon

février 2020

Début de la pandémie de COVID-19 en France

27 avril 2020

Attentat à l'arme blanche à Romans-sur-Isère et à la voiture bélier à Colombes

10 août 2020

Promulgation de la loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine.

24 décembre 2020

Promulgation de la loi qui vise à prolonger différentes mesures de lutte contre le terrorisme

16 octobre 2020

Attentat de Conflans-Sainte-Honorine (assassinat de Samuel Paty) et à la basilique Notre-Dame à Nice

25 septembre 2020

Attentat à proximité des locaux de Charlie Hebdo

23 avril 2021
Attentat à l'arme blanche contre un commissariat de police à Rambouillet

30 juillet 2021
Promulgation de la loi relative à la prévention d'actes de terrorisme et au renseignement

15 août 2021
Prise de pouvoir des Talibans en Afghanistan

16 septembre 2021
Neutralisation de l'émir de l'Etat Islamique au Grand Sahara (EIGS)

8 septembre 2021
Ouverture du procès du Bataclan

24 août 2021
Promulgation de la loi confortant le respect des principes de la République en réponse à l'assassinat terroriste de l'enseignant Samuel Paty en octobre 2020, établit un délit d'entrave à la fonction d'enseignant

21 octobre 2021

Neutralisation de Nasser Al Tergui, chef de la Katiba du Gourma du Rassemblement pour la victoire de l'Islam et des musulmans (RVIM)

25 - 16 février 2022

Neutralisation de Yahia Djouadi, un des leader d'Al-Qaïda au Maghreb islamique (AQMI)

28 mars 2022

Neutralisation de Boubacar Banon, chef de la Katiba Gourma du Jama'at Nusrat al-Islam wa al-Muslimeen (JNIM)

16 août 2022

Loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne

30-31 juillet 2022

Neutralisation du leader d'Al-Qaïda, Al-Zawahiri à Kaboul, en Afghanistan

13 juillet 2022

Nouvelle organisation de la Direction générale de la Sécurité extérieure (DGSE)

5 septembre 2022

Ouverture du procès des attentats de Nice

LE RISQUE SANITAIRE EN FRANCE

*[Axe 3] Réformer et sensibiliser - **[Propositions]** Engager les réformes nécessaires de l'hôpital et des urgences, renforcer les capacités de gestion de crise sanitaire, notamment au sein des ARS ; développer une culture citoyenne de santé publique face aux épidémies.*

La COVID-19 a mis en lumière le risque d'une crise sanitaire mondiale. Plusieurs rapports prévoyaient un tel scénario, et les signaux faibles apparus dès octobre 2019 posent la question de l'anticipation et de la planification par les autorités françaises. Il s'avère en effet que Wuhan est une ville bien connue de Paris au regard de l'implantation d'une multitude de sociétés françaises et des relations stratégiques avec Pékin concernant les différents laboratoires P3 et P4. Soit l'ambassade française n'a pas perçu ces signaux, soit après évaluation la situation n'a pas été qualifiée de majeure, soit c'est en administration centrale qu'il en a été décidé ainsi. Dans tous les cas, cela montre une défaillance dans le dispositif de gestion de crise.

Le 17 mars 2020, le gouvernement déclare un confinement général en réponse à la crise pandémique. Si les signaux faibles étaient perceptibles dès octobre 2019, le centre de crise sanitaire du Ministère des Solidarités et de la Santé n'était activé que le 27 janvier, tandis que la cellule interministérielle de crise n'était opérationnelle que le 17 mars 2020. Deux ans plus tard, alors que l'on peut s'attendre à des reprises épidémiques, la COVID-19 est « gérée » dans un cadre sanitaire « à bout de souffle » : médecins personnels soignants, structures hospitalières… malgré des efforts de gestion notables (Tous anti-covid, centres de vaccination…).

En mai 2022, quelques mois après les vagues pandémiques les plus importantes, la France déclare son premier cas de Monkeypox (variole du Singe) sur le territoire national. Identifié pour la première fois dans les années 1950 en Afrique centrale, un premier rebond épidémique a été observé au Nigéria en 2017. Entre 2018 et 2021 plusieurs cas ont été notifiés en Occident (États-Unis et Royaume-Uni). En août 2022, plusieurs milliers de cas étaient recensés en France.

Les retours d'expérience des différentes crises sanitaires montrent une concentration des épicentres autour de l'Afrique et de l'Asie du Sud-Est. L'évolution démographique, les migrations, les échanges économiques et touristiques s'intensifiant, le risque que de nouvelles vagues épidémiques voire pandémiques liées à l'émergence ou la réémergence d'agents pathogènes voient le jour dans les prochaines années est une réalité. Face à cette situation, les capacités de veille, de recherche, de production et de stocks stratégiques de contre-mesures médicales sont des champs à investir, tant au niveau européen que national. Il s'agit surtout de ne pas perdre notre souveraineté stratégique, tant le risque sanitaire est crucial pour la sécurité globale du pays.

La France doit donc revoir sa politique de santé publique, dans ses nombreuses composantes.

Bien évidemment, les points les plus vulnérables - l'hôpital et les urgences - constituent une priorité, mais aussi les capacités de gestion de crise sanitaire, notamment au sein des ARS qui ont montré leurs faiblesses durant la crise COVID, la gestion des stocks stratégiques… mais il faut aussi développer une culture citoyenne de santé publique face aux épidémies d'origine naturelle ou liées au bioterrorisme.

ÉTAT DE LA MENACE CYBER : TENDANCES ET AGENTS DE LA MENACE

*[Axe 4] Former et protéger - **[Propositions]** Démocratiser la cybersécurité pour qu'elle ne soit plus réservée aux seuls techniciens. Mieux éduquer et mieux former les agents à la menace cyber en particulier dans les collectivités et établissements publics. Améliorer l'attractivité de la filière pour favoriser une pérennité des emplois. Mieux comprendre et anticiper les menaces portées par les APT.*

L'environnement de la cybersécurité est particulièrement fluctuant. Voilà une décennie, les pratiques communes reposaient en majorité sur l'usage de scams, de spams ou sur l'exploitation de réseaux de botnets, et avec presque systématiquement la recherche d'un gain économique. Si la motivation économique demeure majoritaire au cours des dernières années, les finalités de la cybermenace relèvent désormais aussi de l'espionnage, du sabotage, de la concurrence étatique, en faisant un réel enjeu de souveraineté. En outre, la tendance à l'accroissement de la cyber malveillance en ligne s'est largement confirmée durant la décennie, atteignant chaque année un nouveau pic en termes d'attaques et de pertes. La transformation numérique accrue du secteur privé, y compris des secteurs critiques, comme celle des services de l'État se poursuit à un rythme soutenu pendant la crise COVID-19. Cela a permis des gains d'efficacité remarquables mais a aussi engendré l'apparition de vulnérabilités généralisées et inédites pour les administrations.

Aujourd'hui, la menace se structure principalement autour de deux types d'agents malveillants. Dans les deux cas, l'intensité de leur activité tout comme les dommages occasionnés suivent la même tendance haussière. La cybercriminalité demeure la source la plus courante de cybermalveillance. Sa motivation première étant le gain financier, ses cibles prioritaires sont les systèmes d'information essentiels d'entreprises ou de services publics, grâce auxquels les pirates optimisent leurs profits (principalement par le rançonnage). La numérisation constante des dernières décennies - dans les domaines public comme privé

- pas systématiquement accompagnée de mesures de protection efficace des systèmes d'information, ni d'une sensibilisation suffisante des publics, a permis aux cybercriminels une forte intensification de leur activité et de sa rentabilité.

Parallèlement, d'autres groupes, eux aussi acteurs de la malveillance, poursuivent des objectifs différents, plus stratégiques, voire politiques. Généralement qualifiés d'APT (Advanced Persistent Threat), ces groupes dont on soupçonne qu'ils sont soutenus par les États, mettent en place des pratiques d'espionnage sur le long terme à l'encontre de services et d'infrastructures stratégiques. Ils ont aussi la capacité de saboter des systèmes d'information stratégiques dans le but d'accompagner une action étatique. La cybermenace d'origine étatique, puisqu'elle correspond aux logiques de la géopolitique mondiale, peut être considérée comme une prolongation de celle-ci dans un nouvel espace de conflictualité. L'Iran, la Russie, la Chine et la Corée du Nord sont les quatre États qui entretiendraient le plus de groupes APT. Ils forment dans le champ cybernétique un axe anti-occidental et anti-libéral menaçant. En face, les USA semblent aussi entretenir des entités cyber d'action clandestine, réunies sous le nom d'Equation Group (à l'origine de Flame, de Stuxnet…).

Pour ces raisons, la cyber-résilience des infrastructures et services stratégiques français doit être une priorité. Bien que les travaux de modernisation et de prévention soient très fréquents, force est de constater que la crise de la COVID-19 a révélé la vulnérabilité généralisée des systèmes d'information français et accentué celle-ci. Assurer une cyber-résilience efficace nécessite en premier lieu le renforcement des défenses face à des attaques toujours plus innovantes et efficaces, et en second lieu l'adoption généralisée de plans de continuité d'activité solides et versatiles. Ce renforcement nécessite la mise en place de solutions souveraines automatisées, pour assurer une réactivité optimale palliant aux défaillances humaines et techniques.

De manière générale, la conception française de l'environnement cyber s'est longtemps limitée à celle de la posture de défense. En 2019, Florence Parly a dévoilé la doctrine française de lutte informatique offensive (LIO). La LIO doit permettre le soutien des intérêts français sur un plan stratégique ou militaire. Elle permet le renseignement, la riposte et l'action de première initiative. Au vu de l'intégration constante de l'outil cyber dans l'action des puissances concurrentes, régulièrement dans un cadre clandestin, il semble nécessaire que la France s'approprie elle aussi ce spectre hybride de la conflictualité afin d'assurer sa compétitivité sur la scène internationale.

RISQUE SOCIÉTAL : FRACTURES SOCIALES ET DÉFIANCE ENVERS LES AUTORITÉS

[Axe 5] Transparence et communication - [Propositions] Lutter contre la manipulation des discours. Créer un comité indépendant chargé de déconstruire les récits visant à instrumentaliser les discours. Mieux former les agents de l'État à la communication de crise.

Assurément, la crise sociale la plus marquante de ces dix dernières années est celle des gilets jaunes. Le mouvement s'est véritablement construit fin 2018 à la faveur d'une popularité numérique inédite, tout à la fois reprise, provoquée et accentuée de manière décisive par les médias et les réseaux sociaux. Au plus fort de son activité, il a réuni au moins 287 000 personnes selon le Ministère de l'Intérieur (chiffre contesté par d'autres entités).



@HCFRN

Le mouvement des gilets jaunes est un remarquable témoignage du phénomène pluriel et multifactoriel de crise sociale que connaît la France aujourd'hui. Cette crise sociale dormante abrite un risque réel de défaillance de la gouvernance française. Multivectoriel, ce mouvement repose sur plusieurs piliers fondamentaux : des fractures culturelles au sein de la population française, la présence quotidienne de millions de Français sur les réseaux sociaux, un mécontentement croissant envers les politiques gouvernementales. Ces trois facteurs expliquent plusieurs phénomènes observables au quotidien : défiance face au politique et à son autorité, désinformation et vulnérabilité aux fakes news, scènes de violence au quotidien, particulièrement dans des zones urbaines populaires.

La crise de la COVID-19 a mis au jour de nombreuses défaillances du système français. Parmi elles, on retrouve celle d'une rupture du lien entre le gouvernement et une partie de la population. Face à une communication hasardeuse de la part des structures officielles, alimentée par des discours mal combattus sur les réseaux sociaux, une forme de défiance de l'autorité et du gouvernement a rapidement émergé

au sein d'une partie de la population. Elle reposait, d'une part, sur une forme de complotisme entretenu sur le web (mentionnons pour exemple le documentaire Hold Up) et d'autre part, sur la présence antérieure d'un « terreau de mécontentement », propre à la contestation.

Cette forme d'hostilité envers les pouvoirs publics doit toutefois être distinguée des violences urbaines, généralement considérées elles aussi comme des marqueurs d'opposition à l'autorité. Il faut souligner que tant les causes sociologiques que les modes d'expressions de ces formes de défiance sont radicalement différents. Toujours est-il qu'elles ont en commun d'exister grâce à la constitution de cultures parallèles. De nombreux analystes observent un phénomène de disparition des matrices traditionnelles communes du peuple français au profit de groupes variés et aux intérêts divergents.

Depuis quelques années, les violences envers les personnes dépositaires de l'autorité publique semblent suivre la même tendance à la hausse. En même temps, on assiste à une recrudescence très forte des cas de forcenés violents, s'élevant à 205 % sur le premier semestre 2022. Le recours aux échelons spécialisés d'intervention (GIGN et RAID) gagne en fréquence. Si les cas ont généralement eu des conséquences graves mais contenues, souvent en zone rurale, rien n'exclut une diversification des modes opératoires en zone urbaine. Le RETEX des ces évènements indique que ces individus souffrent de pathologies psychologiques, qui ont notamment été exacerbées durant la crise sanitaire.

En parallèle, on peut observer une généralisation dans la pratique des opérations de manipulation de l'information. D'origines diverses et propres à polariser les opinions et les positions au sein de la population, elles constituent une menace pour l'ordre public largement exploitée par les puissances extérieures. À l'approche des élections présidentielles, le Kremlin avait ainsi lancé, par le biais d'un parti politique turc, une fausse information faisant état de la mort de 50 soldats français en Ukraine, que le président E. Macron aurait cherché à cacher pour préserver sa campagne. Les opérations d'influence informationnelle exploitent, s'immiscent dans les failles présentes au cœur des sociétés civiles pour déstabiliser les pouvoirs concurrents. La fondation de Viginum est un premier pas dans la lutte informationnelle. Elle n'a pour autant pas pour objectif de résoudre les problématiques profondes de la société française, pour lesquelles des politiques publiques sont nécessaires.

LE RISQUE ET LA MENACE NRBC

*[Axe 6] Planification - **[Propositions]** Repenser la doctrine d'emploi des forces. Revoir la planification NRBC à l'aune de la guerre en Ukraine. Penser la résilience des centrales nucléaires au regard des conséquences du changement climatique.*

L'évolution du contexte international vers une compétition stratégique et militaire conduit à une recrudescence de la menace nucléaire, radiologique, biologique et chimique (NRBC).

Ces dernières années ont vu l'emploi répété d'armes chimiques et biologiques par divers acteurs, y compris non étatiques et terroristes. L'usage d'armes chimiques en Syrie et en Irak, ainsi que les tentatives d'empoisonnement au Novitchok menées par la Russie témoignent de l'actualité de la menace.



@HCFRN

L'adoption croissante par les États de stratégies hybrides visant à rester sous le seuil de conflit ouvert encourage également le recours tactique aux armes NRBC, ce qui augmente le risque d'escalade et interroge le concept de cobelligérance. Ainsi, l'affirmation de doctrines n'excluant plus l'usage d'armes nucléaires tactiques remet en cause le paradigme classique de la dissuasion nucléaire. Dans le cadre du conflit en Ukraine, le Kremlin a par exemple fait un usage récurrent du chantage nucléaire dans une vision offensive de la dissuasion.

Toutes ces pratiques contribuent à l'érosion des normes et traités internationaux régulant l'emploi des armes de destruction massive (FNI, CABT). Les postures de l'Iran et de la Corée du Nord continuent d'affaiblir le régime international de non-prolifération nucléaire et le TNP, tout comme la modernisation des arsenaux et des vecteurs par les États.

En outre, la pandémie de COVID-19 a révélé les vulnérabilités inhérentes à un système fondé sur la mondialisation et les flux de population, particulièrement vis-à-vis d'une menace biologique. L'opportunité pourrait être saisie par des acteurs malveillants profitant des progrès réalisés dans le domaine de la biologie de synthèse.



@HCFRN

D'autre part, le risque NRBC n'est pas totalement négligeable, malgré l'absence de catastrophe majeure ces dernières années. En 2022, c'est le risque d'accident nucléaire autour de la centrale de Zaporijia qui ravive les inquiétudes de la communauté internationale. Une frappe de missile sur un réacteur, mais surtout une coupure de l'alimentation en électricité, pourraient provoquer la fusion du cœur de réacteur.

Le risque nucléaire est également présent en France, pays le plus nucléarisé au monde en proportion de sa population. Par ailleurs, la gestion des déchets radioactifs, notamment des 10 % ne disposant pas de site de stockage définitif, représente un défi pour les autorités. Le démantèlement des installations nucléaires en fin de vie, amené à prendre de l'importance dans les prochaines années, constitue également un enjeu majeur en France. En 2021, 35 installations nucléaires étaient arrêtées ou en cours de démantèlement. Ce type d'opération comporte des risques spécifiques en matière de radioprotection des personnels, de pollution et de perte de mémoire de conception et d'exploitation et du maintien des compétences. En outre, les installations nucléaires doivent se préparer à faire face à de nouvelles menaces telles que le survol de drones, les cyberattaques, les intrusions ou encore les sabotages.

Enfin, la multiplication des événements climatiques extrêmes liés au changement climatique amplifie le risque nucléaire. Ainsi, les enjeux principaux concernent la capacité des centrales nucléaires françaises à produire de l'électricité dans les conditions climatiques futures, mais aussi la sûreté des installations, c'est-à-dire le maintien de leur intégrité lors d'événements naturels extrêmes. Une réflexion doit donc être engagée sur la résilience de nos infrastructures critiques.

DÉFENSE TERRITORIALE

[Axe 7] Capitaliser et agir - [Propositions] Renforcer l'esprit de défense avec le Service National Universel. Créer une réserve territoriale et la former aux menaces hybrides. Former les maires à des exercices d'agression contre une puissance régulière. Capitaliser sur les stratégies développées en Ukraine.

La guerre en Ukraine a révélé de nombreux enseignements sur le concept de défense nationale notamment les faiblesses de la dissuasion nucléaire (instrumentalisation, multiplication des armes nucléaires tactiques, enjeux des seuils…) et l'importance d'une défense territoriale face à une agression terrestre. Plus largement, elle nous invite à repenser la doctrine française, en particulier sur le spectre capacitaire et industriel face à la recrudescence des conflits de haute intensité.

Le nouvel ordre mondial post guerre froide et la nouvelle géopolitique ont entraîné un détournement de l'usage de nos armées contre des ennemis asymétriques, en particulier contre des groupuscules terroristes dans le cadre d'OPEX. Ce constat explique en partie pourquoi le concept de défense territoriale est resté au placard.

En effet, dans le cadre de la guerre russo-ukrainienne, force est de constater que l'intégration et la préparation des civils à la défense ont été au moins aussi efficaces que l'usage des moyens traditionnels de la guerre : infanterie, blindés, artillerie, aviation … Un autre avantage de la défense territoriale réside dans la maîtrise de son environnement : face à une méconnaissance des zones d'engagements, notamment urbaine, l'armée russe a éprouvé de grandes difficultés opérationnelles. Alors que la « résistance ukrainienne » maîtrisait parfaitement son environnement.

La préparation des civils au regard des conflits de haute intensité, notamment sur la partie défense apparaît donc primordiale. Il faut néanmoins associer ces capacités à celles des stocks. De très nombreux rapports et constats partagés par des autorités militaires nous indiquent que la BITD française accuse de grandes difficultés. Les engagements pris par le président de la république, Emmanuel Macron lors du salon international de défense Eurosatory et plus récemment lors de la table ronde « Économie de guerre » pilotée par le Ministre des Armées, doivent véritablement se traduire par des mesures concrètes - notamment sur la partie financière et sécurisation des chaînes d'approvisionnement - pour s'assurer d'une autonomie stratégique sur la filière défense.

Une défense territoriale formée et préparée ainsi qu'une BITD résiliente apparaissent donc comme des composantes complémentaires et essentielles dans la dissuasion pouvant ainsi changer la donne stratégique vis-à-vis d'un agresseur.

Ceci pourrait se traduire par une armée de « réserve territoriale » formée aux enjeux des nouvelles menaces hybrides - NRBC, cyber et informationnelle notamment - et positionnée aux points stratégiques (sécurisation de sites sensibles) à proximité de nos frontières. C'est en faisant cet effort que l'on pourrait ré-élever le niveau de la dissuasion qui serait alors ultime.

SOUVERAINETÉ : OPPORTUNITÉS ET CONTRAINTES

[Axe 8] Réalisme et offensive - [Propositions] Élargir le régime SAIV à l'ensemble des secteurs stratégiques. Ré-industrialiser pour gagner en compétitivité. Assumer une politique offensive, notamment par le droit européen et national à l'instar des États-Unis ou de la Chine. Agir au niveau européen sur l'influence des normes pour défendre et promouvoir les intérêts français.

La crise de la COVID-19 et la guerre en Ukraine ont repositionné les questions de souveraineté au cœur de la politique française. La pandémie de COVID-19 a exposé les vulnérabilités de la France en matière d'approvisionnement des médicaments, des principes actifs et des équipements de protection individuels. La guerre en Ukraine, quant à elle, questionne sur la sécurité des approvisionnements en énergie, sur l'agroalimentaire et sur les capacités des forces armées françaises au regard de conflits dits de haute intensité. D'une manière générale, la France accuse des retards depuis 40 ans sur une multitude de secteurs : santé, défense, énergie, numérique pour n'en citer que quelques-uns.

Fruit d'une politique assumée dans les années 1980 - 1990, où les élites de Bercy ont contribué à l'abandon de l'industrie française au profit d'une économie de service, les nouveaux enjeux de la mondialisation remettent en question l'autonomie stratégique française. De crises sectorielles locales à cinétique courte, nous sommes passés à des crises multiples transverses à cinétique longue. Ce changement de paradigme impose une modernisation de la doctrine où la souveraineté apparaît comme étant un facteur prépondérant à la résolution des crises. La souveraineté peut également être perçue comme un vecteur offensif, permettant au monde économique français de pénétrer de nouveaux marchés, favorisant ainsi le soft power de Paris.

Les secteurs stratégiques sont plus que jamais la cible de stratégies d'intelligence économique à l'heure où la compétition internationale est exacerbée. Aussi, la protection de ces entreprises revêt de la défense des intérêts vitaux de la Nation. Même si la France dispose d'un arsenal juridique qui a connu des avancées significatives ces dernières années, les stratégies menées

par les États-Unis ou la Chine continuent d'enregistrer des succès notables. Les entreprises ont en ce sens un rôle important et doivent être moteur dans la défense de leurs intérêts.

C'est dans ce contexte que le gouvernement a adopté des premières réformes : le plan de relance, le plan de résilience et la stratégie nationale de résilience (SNR). Ces actions se sont poursuivies au niveau politique avec une nouvelle doctrine énoncée par le Chef d'État-major des armées : du concept de guerre-paix et amis-ennemis, nous nous inscrivons désormais dans celui de compétition, contestation et affrontement qui reflète mieux le contexte géopolitique actuel.

Peut-être moins significatif, mais qui témoigne bien d'une prise de conscience politique, la souveraineté est à présent inscrite dans le nom de deux ministères : le ministère de l'Économie, des finances et de la souveraineté industrielle et numérique ; et le ministère de l'Agriculture et de la souveraineté alimentaire.

Toutefois, être souverain sur l'ensemble du spectre est totalement illusoire, ce qui sous-entend de faire un choix et de privilégier un secteur ou des chaînes d'approvisionnement. Cela n'empêche pas de conduire des analyses de risques et de prendre des mesures palliatives pour réduire le risque de dépendance.

Aussi, la souveraineté peut s'entendre au niveau européen, ce qui semble désormais être le cas pour le domaine du numérique ou de la transition écologique avec des succès plus ou moins relatifs, comme les paquets législatifs sur les données numériques. Des initiatives ont été poussées en ce sens lorsque la France présidait le Conseil de l'Union européenne. Seulement cette idée est bien franco-française, peu de pays de l'Union européenne la partagent. La dépendance, notamment Outre-Atlantique, ne semble pas être un problème stratégique pour la plupart d'entre eux. Il convient dès lors de mener une politique d'influence pour convaincre nos partenaires européens et de renégocier les traités existants pour s'assurer que les marchés européens bénéficient aux pays membres de l'UE. Il faut tout de même garder à l'esprit que la compétition économique intra-européenne est féroce et que les entreprises françaises en ont souvent payé les frais.

La souveraineté de la France en chiffres

Résilience des chaînes d'approvisionnement

En 2022 **40%**

En 2012 **29%**

des intrants* utilisés pour l'industrie française sont importés

80%

des principes actifs pharmaceutiques sont importés de Chine et d'Inde



La France est à

100%

dépendante des terres rares qui proviennent de

Amérique du Sud | Afrique | Chine

Résilience des infrastructures numériques

5 entreprises américaines représentent

50%

du trafic internet en France

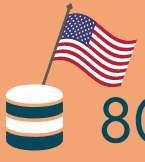
Netflix Google Akamai Facebook Amazon

La France est dépendante à

100%

d'entreprises étrangères sur les câbles sous-marins

TE SubCom américains | NEC japonais | ASN finlandais



80%

des données françaises stockées aux États-Unis

(*) L' ensemble des ressources utilisés dans les processus de fabrication (matières premières, main d'oeuvre, etc...)

Données : ©Sénat - Production : ©HCFRN

Résilience des infrastructures énergétiques

La France a importé **25** jours d'électricité en 2019 **78** jours d'électricité en 2021

La France produit

70%
d'énergie nucléaire

56 réacteurs

10%
de gaz

- sept points d'interconnexion principaux
- quatre terminaux méthaniers et douze sites de stockage

10%
d'énergie hydraulique

257,7 GW

Souveraineté de la politique commerciale



352 milliards



178 milliards

de marchés publics ouverts en 2021



4,3 milliards

de manque à gagner pour l'UE en raison de la non application des accords commerciaux

LA GESTION DE CRISE EN FRANCE

La crise de la COVID a démontré l'insuffisance de la préparation de l'État et d'une grande partie des acteurs publics, voire parfois privés, pour articuler une gestion de crise efficace dans un contexte systémique et global.

Cette situation a été mentionnée par plusieurs rapports qui notent à la fois, la faiblesse des formations et entraînements de la plupart des personnels engagés, ainsi qu'une insuffisance en termes d'outils et de méthodologie. Cette dernière est notamment due à une planification de niveau gouvernemental peu adaptée aux conditions de gestion de crise en haute intensité.

Cette situation n'était pas nouvelle, elle était connue, nous l'avions notamment explicitée dans notre rapport de 2012, il y a 10 ans. Elle est consécutive d'une volonté de ne pas considérer les scénarios « extrêmes » comme probables, et ce tant au sein de l'administration que de la classe politique (le turn-over étant très grand dans les deux branches de notre exécutif… le long terme a peu sa place), et en conséquence de ne pas investir, ni dans les hommes, ni dans les moyens permettant une gestion plus performante et plus respectueuse des acteurs et des victimes.

Il aura fallu attendre plusieurs mois pendant cette crise COVID pour voir une mécanique et des actions plus fluides et plus optimisées se mettre en place. Les premiers mois ont été une débauche de moyens et parfois d'argent pour une « suractivité » globale peu performante.

Le leadership politique est apparu relativement tardivement, des erreurs de communication ou de stratégie ont été commises (les masques, notamment). Il a fallu attendre environ deux mois pour voir se dégager une stratégie, une cohérence et des actions, qui même si elles n'étaient pas toutes parfaites, démontraient une « conduite » de la crise. C'est au travers du professionnalisme des acteurs locaux : sapeurs-pompiers, urgentistes et hospitaliers que le dispositif a tenu. Le grand public retiendra également le soutien économique apporté par l'État aux entrepreneurs et salariés les plus fragiles. La classe politique a bien évidemment joué son rôle, et de manière plutôt positive. Il n'en demeure pas moins que le « retard à l'allumage » a été important et que de très nombreuses familles ont été endeuillées. Une meilleure gestion de crise initiale aurait sans doute permis de sauver plus de vies.

Le système doit donc être revu. Sans pour autant changer l'organisation globale de l'administration française, il convient de rechercher une bien plus grande efficacité et une meilleure articulation entre les différents échelons : État, collectivités et entreprises, sans oublier le citoyen qui est à la base du dispositif, à la fois victime et acteur de la crise.



Exercice de sauvetage sur la Seine par la Sécurité Civile et la BSPP @HCFRN

Au premier rang de cette « révision » se pose la question de la planification gouvernementale, qui a déjà fait l'objet d'une réflexion. La planification va être revue pour se concentrer sur un concept de fiches d'actions informatisées, et pouvant s'appliquer à toute nature de crise, les problématiques étant parfois communes. Sans oublier évidemment les aspects singuliers propres à chaque typologie de crise, et ceci pour éviter de tomber dans la lourdeur de plans souvent inadaptés et trop longs à la mise en œuvre.

Cette nouvelle planification que met en place le SGDSN va certainement dans le bon sens. Elle doit s'articuler dans une stratégie nationale de résilience qui ne doit pas être, seulement, une réponse aux insuffisances constatées, mais qui doit devenir une véritable ambition nationale pour la gestion des situations d'exception qui ne manqueront pas de toucher notre pays dans les années à venir.

La stratégie nationale de résilience doit être ambitieuse. Elle doit associer l'État dans ses différentes composantes nationale, zonale (et/ou régionale), départementale, mais aussi les collectivités territoriales : régions et départements - ainsi que les collectivités locales : intercommunalités et communes. Un énorme travail reste à faire pour préparer ces différentes structures à la gestion des crises ; notamment face à des scénarios aigus et longs. Il faudrait que cette stratégie associe toutes les parties prenantes pour faire réellement consensus.

Sur le point particulier, au sein de cette stratégie, qu'est la gestion de crise, la formation, l'entraînement, ainsi que les salles et outils - bref les capacités techniques de gestion de crise, et de télécommunications - doivent faire l'objet d'une attention et d'un investissement importants pour permettre aux équipes de travailler en mode nominal, mais aussi dégradé et résilient.

Cette stratégie ne peut évidemment faire l'impasse sur l'échelon européen qui prend une place de plus en plus grande, tant dans les moyens de secours avec le MEPC (Mécanisme Européen de Protection Civile) et RescEU qu'en matière sanitaire avec HERA (stocks stratégiques) et dans la gestion de crise elle-même, avec le SITCEN et l'IPCR (Integrated political crisis response) notamment pour les crises systémiques et/ou internationales. Ces ressources et capacités européennes sont certes essentielles dans la montée en puissance et la mutualisation de la réponse, mais elles ne doivent pas nous laisser penser que nous pouvons nous permettre un investissement au rabais en France en la matière.

Nous sommes en effet aujourd'hui très loin du compte, et cette stratégie nationale de résilience ne pourra réellement voir le jour que si elle est accompagnée d'un véritable budget pour la concrétiser. Ce qui n'a jamais été le cas depuis maintenant plus de 50 ans. Le « texte » ou l'incantation ne suffiront pas. On ne pourra juger que sur l'implémentation de cette stratégie. La crise COVID a laissé au sein de la population des traces aussi lourdes que le nuage de Tchernobyl et il est peu probable que la population ne sanctionne pas la prochaine gestion de crise majeure qui serait fortement déficiente.

Dans cette stratégie, la planification est certes importante, mais elle ne constitue pas la réponse unique. Elle doit être associée à une architecture juridique qui permet tant à l'État qu'aux autres acteurs publics et privés d'agir dans une sécurité juridique qui, même



@HCFRN

relative, doit prendre en compte le cadre « particulier » de la crise, dérogatoire du droit commun. Elle doit aussi être lisible, claire et accessible pour tous, et ce sans méconnaitre la légitimité du « secret » sur des points particuliers.

Mais cela ne suffit évidemment pas. Il convient aussi de bien connaître la résilience « globale » des acteurs partenaires de l'État qu'ils soient du secteur public ou privé, et de favoriser l'émergence de cette résilience au travers des mesures particulières qui pourraient parfois déroger d'une logique économique « à flux tendus », peu propice à cette résilience, voire du droit commun si nécessaire. Par exemple, la constitution de stocks tampons, de stock d'urgence, de moyens de gestion de crise, ou de communication en mode dégradé, pourrait faire l'objet de mesures fiscales particulières. Les modes de fonctionnement « 12/24H » qui dérogent au droit social devraient également être prévus dans ce droit spécifique de la crise qui reste à écrire.

Des facilités de fonctionnement pour les opérateurs qui assurent des fonctions vitales telles que énergie, eau, santé, etc... restent encore à écrire, et à en permettre l'application. Cela pourrait également concerner des entreprises spécifiques et essentielles à la résolution de certaines typologies de crises ou, pour les collectivités, dans le cadre de leurs compétences de sauvegarde ou de gestion spécifiques et essentielles (eau, routes, etc...).

Cette démarche de « moyens » ne sera utile que si le niveau de formation et d'entraînement des équipes en charge de la résolution de ces situations exceptionnelles est suffisant. Nous constatons fréquemment, tant au sein de certaines administrations que du secteur privé, une méconnaissance au sein des équipes dites « de gestion de crise » des conséquences des agressions (que celles-ci soient d'origine naturelle ou autres) et de leurs effets cascades, mais aussi des dispositifs de gestion de crise publique ou privée en interface avec leurs propres structures. Il y a là souvent tout autant un manque de connaissances de base que de compétences réellement opérationnelles, sans oublier les comportements de savoir-être en crise, qui doivent aussi faire l'objet d'une formation spécifique. La stratégie du silo propre à chaque administration ou des calculs politiques à courte vue ne doivent plus être la règle. Ce travail de formation doit aussi être associé à un travail de labellisation des organisations et de certification des personnes compétentes. Ceux-ci sont essentiels à la construction de cette stratégie de résilience.

Les nouvelles technologies vont évoluer dans les années à venir - et certaines sont déjà opérationnelles et capables d'apporter des capacités nouvelles et complémentaires essentielles. Les réseaux satellitaires de basse altitude permettant un accès rapide et simple à internet sur les zones sinistrées vont devenir essentiels pour la communication. De même si les nouvelles constellations permettent l'acquisition du renseigne-

ment à un niveau de détail extrêmement précis, offrant au gestionnaire de crise une connaissance en temps quasi réel, les moyens téléphoniques satellitaires qui existent déjà vont devenir moins chers et plus communs. Les réseaux IOT (Internet of things) vont également apporter leurs lots d'informations, voire des capacités de détection et de signaux faibles, capacités extrêmement intéressantes sur tout un domaine couvrant les risques majeurs naturels ou industriels, voire terroristes.

La gestion de crise ne doit plus être considérée comme s'appliquant « après la réalisation d'un événement marquant ou exceptionnel » nécessitant une coordination particulière. La gestion de crise doit s'appliquer dans un dispositif permanent de veille et de détection des signaux faibles, permettant une montée en puissance extrêmement rapide (24/7), à la hauteur de l'analyse qui est faite de l'événement ou de la situation potentielle qui peut en découler.

À cet égard, la doctrine française sur les feux de forêt que l'on peut résumer à « éteindre immédiatement le feu naissant » doit s'appliquer à tout type de risque ou menace et éviter - ou réduire au minimum - le temps de sidération et de montée en puissance des structures de gestion de crise, qui est aujourd'hui toujours trop long.

Cela réclame une pensée nouvelle, plus pragmatique, plus professionnelle, accompagnée des moyens à la hauteur des enjeux, ce qui n'est pas encore le cas. Ces enjeux sont et seront malheureusement de plus en plus lourds pour notre société contemporaine à l'aune du changement climatique, du terrorisme de masse, du délitement sociétal, voire du conflit de haute intensité.

Il convient aujourd'hui pour toutes les structures responsables d'être prêt à faire face « vraiment » et c'est peut-être cet adverbe qui change tout par rapport à ce que nous avons vécu lors des 20 dernières années.



@HCFRN

LES VOIES DE LA RÉSILIENCE

La résilience est le « buzz Word » de l'année. Le changement climatique, la guerre en Ukraine, la crise énergétique, les difficultés sociétales… font que ce terme est de plus en plus utilisé tant par la classe politique que médiatique, pour faire comprendre à la population qu'il va falloir faire plus avec moins et surtout que les conditions de vie seront susceptibles d'être plus compliquées à l'avenir.

Or la résilience c'est peut-être cela, mais pas forcément, et surtout si on a pris le problème à bras le corps et au bon moment. En fait, la résilience a pour objet et vocation de nous préparer à anticiper des difficultés, voire des crises, qui peuvent être conjoncturelles ou structurelles. Et ce quelles que soient les origines de la « crise », même si ce terme lui-même ne veut plus dire grand-chose tant il est galvaudé. Elle a aussi pour fonction d'atténuer les effets disruptifs de l'événement ou de la situation. Mais la résilience n'est pas seulement un concept qui arrive « après » un événement majeur et douloureux et qui nous permettrait d'oublier, de repartir grâce à quelques formules magiques, ou de travail psychique, même si ce dernier est bien évidemment utile et nécessaire pour la majorité des personnes affectées par un traumatisme.

La résilience est aussi un méta-concept qui s'applique aux systèmes complexes, l'homme en est un, tant à titre individuel que collectif, mais elle s'applique aussi aux systèmes complexes qui organisent notre société : réseaux, flux, équipements, etc… qui permettent aujourd'hui d'assurer le fonctionnement d'une société moderne. Dans ce cadre, toute rupture d'un système (énergie, transport, santé…) a des conséquences graves et engendre le plus souvent la défaillance d'un de ces systèmes par effet cascade d'autres ruptures, mettant ainsi en danger les populations et les économies.

La résilience d'un système doit donc se considérer à l'aune des autres systèmes. C'est un concept systémique positif dans lequel chaque élément travaille donc sa propre résilience. Dans ce cadre, on distingue la résilience dite « organisationnelle » dont l'objet est la capacité à faire face à un choc avec des mesures internes puissantes : veille, alerte, gestion de crise, continuité d'activité, restauration etc. et la résilience dite « structurelle », c'est à dire la capacité à s'adapter en permanence et en anticipation aux nouvelles conditions auxquelles fait face son activité présente ou future, telles que le changement climatique, la rupture d'approvisionnement de matières premières, l'apparition de technologies disruptives, ou encore d'évolutions sociétales ou juridiques majeures…

L'approche des États a été depuis 2001 de « sanctuariser les infrastructures dites critiques ou vitales » face

à la menace terroriste. Mais aujourd'hui le spectre des menaces et des risques s'est considérablement élargi posant de nouvelles questions tant aux gouvernements qu'aux opérateurs de ces systèmes. Les risques naturels majeurs ou extrêmes, les menaces cyber, le vieillissement des infrastructures, les pénuries possibles de certaines matières premières agricoles ou industrielles, le cadre géopolitique en pleine évolution avec les impacts du changement climatique et son cortège de risques de conflits directs ou hybrides imposent une nouvelle approche plus globale et systémique de la sécurité des États et des populations. Cette nouvelle approche s'impose aussi pour les risques de sécurité intérieure liés au délitement sociétal, au terrorisme ou au crime organisé.

Cette approche nécessite de penser la résilience à plusieurs niveaux, notamment en termes de territoires et de population.

Une illustration de ce concept de résilience est le nid d'abeille. La structure modulaire reproduite à l'infini assure un niveau de résistance particulier et optimum, c'est cela la résilience, et chacun fait sa part dans la hiérarchie des structures.

Il nous faut une résilience « locale » qui permet de protéger les populations et structures du territoire (le quartier, la commune, l'intercommunalité…) et d'être en mesure, dans la plus grande autonomie possible, de faire face à une situation difficile, qu'elle soit passagère ou plus structurelle. Bien sûr, la solidarité doit jouer à plein qu'elle soit à l'échelon départemental, régional, zonal, national ou européen et heureusement, le progrès apporté par 2000 ans de civilisation ne s'arrête pas à ce début du 21ème siècle. Mais cette solidarité sera d'autant plus forte et efficiente, que tous les niveaux auront fait ce travail de réflexion, de prévention, de préparation et d'adaptation. A ce titre, face aux enjeux, la résilience est à l'inverse du survivalisme, centré sur l'individu et non sur la collectivité, quelle que soit sa taille.

Il nous faut aussi une résilience des institutions, des organisations, des réseaux techniques essentiels, des flux. Bref il faut que toute activité humaine nécessaire pour « l'autre », puisse aborder la question du choc et de l'adaptation au travers d'une vision partagée et construite, et puisse avoir les moyens de créer la résilience « raisonnable » de son activité. Pour cela il faut une vue à 360°, les silos ne peuvent plus être de mise, chacun peut être touché par un événement perturbateur à tout moment. La veille, le professionnalisme et la rapidité de réaction seront clés pour toutes les organisations aujourd'hui, mais encore plus demain.

Et il nous faut par-dessus tout une résilience humaine pour être prêts à gérer ce concept et ses attributs humains, organisationnels et techniques. Cette résilience s'apprend, elle s'exerce et elle doit permettre la confiance en l'autre, le voisin, les institutions, les organisations… Elle doit être enseignée dans une optique de progrès et non de recul ou de sectarisme.

Il faut aussi penser la résilience pour les scénarios les plus extrêmes. Les préparer et y penser n'est pas un traumatisme, au contraire. Une préparation face à un événement peut permettre de contribuer à la résolution d'un autre. Dans ce cadre, les scénarios de défense nationale et de défense civile ne peuvent être exclus. Des révisions d'approche stratégique de notre défense nationale doivent être posées sur la table, la dissuasion nucléaire seule ne pouvant couvrir objectivement la variété des menaces.

C'est un chantier énorme, nous devons passer d'une société de consommation globalisée à une société plus continentale où l'on doit aujourd'hui prévoir, planifier, compter plus sobrement, réagir et intégrer « vraiment » la prévention et la préparation aux situations d'exceptions, qui le seront de moins en moins, ou complètement nouvelles. L'adaptation aux enjeux, notamment climatiques, nous demandera des efforts importants. Ceci aura un coût, personnel et sociétal, pas seulement celui de l'assurance, mais aussi celui du progrès dans un monde fini où peut-être la résilience environnementale nous montrera la voie... si l'on sait la voir et la respecter.

Comment faire pratiquement ? La première chose à faire consiste à renforcer à bon niveau sa résilience organisationnelle en vérifiant bien la qualité de la planification de crise, de l'organisation de la gestion de crise, et notamment celle de la formation et de l'entraînement des personnels affectés. Cela a l'air un peu trivial, mais c'est plus compliqué et plus consommateur en temps et en ressources que l'on peut souvent l'imaginer pour maintenir une organisation à bon niveau. Il faut également ne pas voir trop petit dans le dimensionnement des équipes ou des moyens. La crise peut durer et il faut des équipes en nombre suffisant pour assurer une continuité de gestion 24/7. Il convient également de travailler en amont et durant la crise sa communication tant externe qu'interne... cela se prépare aussi ; sans oublier la résilience financière (provisions, assurances, plan de contingences) et surtout la continuité d'activité dans toute la mesure du possible.

Bref, ces métiers de la résilience sont, dans les organisations publiques ou privées, de vrais métiers, mais qui ne sont malheureusement pas toujours considérés comme tels. Or ils sont essentiels. **Sans bonne préparation, planification et conduite, les organisations se retrouvent très rapidement en défaut sur une crise majeure, avec des conséquences très lourdes à tous niveaux : gouvernance, image, finances...** Cela est valable tout autant pour les gouvernements, les autorités régionales ou locales, que pour les entreprises cotées ou importantes sur leurs marchés.

La seconde est liée à la résilience structurelle et aux scénarios d'anticipation sur le moyen et long terme.

L'adaptation au changement climatique souhaitablement imposée au niveau international et national, la responsabilité sociétale des entreprises, les attentes de la société, notamment des jeunes générations,

ont pour conséquence, compte tenu des scénarios annoncés par les scientifiques et notamment le GIEC, d'accélérer les mutations techniques et sociétales pour un monde plus décarboné et plus respectueux de l'environnement.



Ligne électrique @HCFRN

Au-delà de ces attentes légitimes, cela veut dire accélérer les mutations dans un monde complexe, où les choix ne sont pas toujours évidents, compte tenu de l'environnement mouvant en termes politique ou technologique. Mais il convient d'avancer en prenant en compte les aménagements vertueux en matière environnementale, sans oublier des sujétions de sécurité structurelle, face à des risques rares et extrêmes, mais pour lesquels les coûts doivent être engagés à l'occasion d'une construction ou d'une rénovation, même si leur amortissement peut prendre des décennies. **La résilience dans ce cadre est un « investissement » et doit être considérée comme tel.** À titre d'exemple, les Pays-Bas travaillent aujourd'hui sur des infrastructures qui prennent en compte des scénarios de remontée de niveau de la mer face à un risque qui n'est pas centennal mais millénale.

En conclusion, les voies de la résilience passent par une prise de conscience des risques et des menaces qui s'exercent sur l'Europe, la France, nos territoires, nos entreprises et nos populations à court et long termes. Une fois cette prise de conscience faite, **la résilience nationale doit devenir une véritable stratégie nationale dans laquelle l'État et l'ensemble des forces vives de la nation s'engagent ensemble. La résilience n'est pas un concept étatique, il s'agit réellement d'un concept sociétal et stratégique pour aborder les temps difficiles** qui s'annoncent et surmonter une époque charnière dans l'histoire de l'humanité avec humanisme mais réalisme.

BILAN D'ACTIVITÉS 2021

L'année 2021 a encore été impactée par la crise sanitaire. 8 rencontres en présentiel ont toutefois pu être organisées (petits-déjeuners rencontres au Sénat, dîner-débat et visite du GIGN) et 17 à distance proposées à nos adhérents qui ont également apprécié nos nouveaux produits de veille. L'intérêt continu pour nos activités est marqué par le renouvellement des adhésions malgré la crise.

71
Personnes morales adhérentes
(institutions, entreprises, associations et collectivités - hors communes labellisées Résilience France)

+

30
Experts

=

1 300
Personnes physiques membres

11
Petits-déjeuners / Rencontres
(6 au Sénat, 5 webinaires)

11
Talks Vidéo

1
Dîner-débat

1
Colloque international

1
Visite de site : GIGN

6 844
Articles publiés en veille France

10 772
Articles publiés en veille internationale

3
Bulletins d'informations sécurité

17
Note d'alertes

5
Analyses à chaud

2
Points de situation

1
Projet européen : «Respondrone»

Rétrospective de nos événements 2021

Petit-déjeuner (webinaire)

Gendarmerie et crise permanente
avec le général Hubert Bonneau

Talk-vidéo

Cyberattaques et collectivités, avoir anticiper pour mieux se défendre

M. Nicolas Arpagian, M. Cyril Bras et le général Marc Watin-Augouard

Petit-déjeuner (webinaire)

Gestion de la crise COVID-19, impact et regard sur les activités quotidiennes de la BSPP
avec le général Jean-Marie Gontier

Talk-vidéo

Le rôle des associations agréées de sécurité civile dans la gestion du Covid-19
avec M. François Richez, M. Alain Rissetto, M. Philippe Sauzey, M. le préfet Alain Thirion

Petit-déjeuner (webinaire)

Les missions du commandement spécialisé pour la sécurité nucléaire
avec le général Laurent Phélip

Talk-vidéo

Covid et Big data
avec le Dr Bruno Boyer, M. Guillaume Rozier et Mme Valérie Peugeot

Talk-vidéo

Feux de forêts : y a t-il encore une saison ?
avec le Contrôleur général Grégory Allione, le Contrôleur général François Pradon et M. Jean-Louis Pestour

Petit-déjeuner

Résilience énergétique de la France
avec M. le préfet Jean-François Carenco

Talk-vidéo

Nouvelle IGI 1300 : quels enjeux pour les directeurs sûreté ?
avec la Capitaine Louis Doumenjou, M. Philippe Le Fahler et M. Philippe Muller Feuga

Talk-vidéo

Résilience économique : Comment les collectivités se préparent-elles ?
avec M. Nicolas Bauquet, M. Simon Karleskind, M. Sébastien Le Maire et M. Frédéric Rose

Petit-déjeuner

ANCCLI : le constat choc sur la préparation des Français au risque nucléaire
avec M. Yves Lheureux

Talk-vidéo

Tempêtes solaires : quelle préparation possible ?
avec M. Sébastien Bourdarie, M. Eric Degny, Mme Marie Ponsart et Mme Nicole Vilmer

Petit-déjeuner

Changement climatique : quel impact sur les risques naturels et technologiques ?

avec M. Cédric Bourillet

Talk-vidéo

Horizon Europe : quel programme après la pandémie ?

avec M.Géraud Canet, M. Frédéric Perlant, M. Philippe Quevauviller, M. Ludovic Pinganaud

Petit-déjeuner

Le rôle de la Délégation ministérielle aux Partenariats, aux Stratégies et aux Innovations de Sécurité (DPSIS)

avec M. le préfet Olivier de Mazières

Petit-déjeuner

Quelles nouvelles orientations pour la planification de sécurité nationale après le COVID ?

avec M. le préfet Nicolas de Maistre

Petit-déjeuner

La Police nationale et les crises

avec M. Frédéric Veaux

Talk-vidéo

Les différentes applications du drone dans les missions de sécurité

avec M. Laurent Terramorsi, M. Hugues d'Ales, le Commandant Eric Rodriguez et M. Romain Bevillard

Dîner

Forces d'intervention : quel équilibre national et régional ?

avec M. le général Ghislain Réty

Talk-vidéo

Culture du risque : comment impliquer les populations ?

avec Mme Ludivine Gilli, M. Frédéric Rose, M. Florent Vallée et M. Laurent Vibert

Petit-déjeuner

Les missions de l'Armée de l'Air et de l'Espace pour la sécurité nationale

avec le général de brigade aérienne Dominique Tardif

Petit-déjeuner

Présidence française de l'Union européenne : Quelles priorités de la France dans les domaines de la sécurité intérieure et de la protection civile face aux risques et menaces majeurs ?

avec M. Bruno Cruchant

Talk-vidéo

Alerte des populations : évolutions et calendrier

avec le Pr. Johnny Douvinet, M. Yves Hocdé, M. Karim Karzazi, Lcl Romain Moutard et M. Yann Chevalier

Colloque international

New emergency management in a Resilience era facing health, climate and energy challenges

en partenariat avec TIEMS


PETIT DÉJEUNER
MARDI 12 OCTOBRE - 8H30/10H
AU RESTAURANT DU SÉNAT


TALK-VIDÉO
TRÈS SECRET
NOUVELLE IGI 1300 :
JEUDI 15 AVRIL - DE 11H À 12H


TALK-VIDÉO
LE RÔLE DES ASSOCIATIONS AGRÉÉES DE SÉCURITÉ CIVILE
DANS LA GESTION DU COVID-19
JEUDI 10 MARS - DE 11H À 12H


INTERNATIONAL CONFERENCE
NEW EMERGENCY MANAGEMENT IN A RESILIENCE ERA FACING HEALTH, CLIMATE AND ENERGY CHALLENGES


PETIT DÉJEUNER
MARDI 15 JUIN - 8H30/10H
AU RESTAURANT DU SÉNAT
OU EN WEBINAIRE
CHANGEMENT CLIMATIQUE :


PETIT DÉJEUNER
MARDI 16 MARS - 9H/10H
WEBINAIRE


TALK-VIDÉO
TEMPÊTES SOLAIRES :
MARDI 11 MAI - DE 11H À 12H


PETIT DÉJEUNER
MARDI 13 AVRIL - 9H/10H
WEBINAIRE
RÉSILIENCE ÉNERGÉTIQUE DE LA FRANCE


PETIT DÉJEUNER
MARDI 6 JUILLET - 8H30/10H
AU RESTAURANT DU SÉNAT


PETIT DÉJEUNER
MARDI 14 DÉCEMBRE - 8H30/10H
AU RESTAURANT DU SÉNAT


PETIT DÉJEUNER
MARDI 21 SEPTEMBRE - 8H30/10H
AU RESTAURANT DU SÉNAT
POLICE NATIONALE


TALK-VIDÉO
HORIZON EUROPE :
MERCREDI 16 JUIN - DE 11H À 12H


PETIT DÉJEUNER
JEUDI 8 JUILLET - 9H/10H
EN FORMAT WEBINAIRE


TALK-VIDÉO
CULTURE DU RISQUE : COMMENT IMPLIQUER LES POPULATIONS ?
JEUDI 28 OCTOBRE DE 11H À 12H


TALK-VIDÉO
ALERTE DES POPULATIONS : ÉVOLUTIONS ET CALENDRIER
VENDREDI 3 DÉCEMBRE DE 11H À 12H

REMERCIEMENTS

NOS PARTENAIRES

NOTRE ÉQUIPE

Christian Sommade
Délégué général
christian.sommade@team-hcfdc.org

Bureau parisien

Lauriane Abriat
Déléguée générale adjointe
lauriane.abriat@team-hcfdc.org

Manon Rifaï
Graphiste
manon.rifai@team-hcfdc.org

Bureau nîmois

Claire Menon
Chargée de mission Senior
Projets européens, labels et certifications
claire.menon@team-hcfdc.org

Benjamin Roman
Responsable veille et prospective
benjamin.roman@team-hcfdc.org

CONSEIL D'ADMINISTRATION

BUREAU

Président
Jean-Marie Le Guen
Ancien secrétaire d'État, député et conseiller de Paris

Présidents d'honneur
Membres honoraires du Parlement
Paul Girod † - Jean-René Lecerf - Jacques Gautier

Vice-président
Thomas Peaucelle
Président de KAIROS-c2i

Secrétaire général
Muriel Reus
Présidente, MRC Conseil

Secrétaire général adjoint
Germain Gauthier
Chargé d'enseignement, Sciences Po Paris

Trésorier
Jean-Yves Cousin
Membre honoraire du Parlement

REPRÉSENTANTS DES COLLÈGES

Collège des services de l'État
Christian Desprès,
Service du Haut fonctionnaire de défense et de sécurité, MTES

Collège des entreprises sociétés commerciales et EPIC
Éric Marion
Vice-président opérations Sûreté, Prévention, Secours et santé, Disneyland Paris

Collège des opérateurs d'infrastructures critiques
Philippe Daguzan
Directeur du cabinet de la présidence, ENEDIS

Collège des collectivités locales et territoriales
Frédéric Rose
Conseiller municipal délégué à la prévention, médiation, risques majeurs, Mairie d'Orléans

Collège des start-ups
Philippe Bardon
Dirigeant fondateur, CIM HOLIS

Collège des partenaires thèmatiques
Lidia Gabor
Mission risques naturels (MRN)

Collège des experts
Gal (2S) Étienne Copel

ADMINISTRATEURS

Alexis Arif
Directeur, AUDACIA

Delphine Buffard
Directrice de la communication et des relation institutionnelles, Deveryware

Dr. Catherine Bertrand
Présidente de la société française de Médecine de Catastrophe (SFMC)

Jean-Yves Cannesson
Vice-président CESER Hauts-de-France

Contrôleur général Éric Faure
Chef d'État-Major de Zone et de Protection Civile, Préfecture de La Réunion

Guy Lacroix
Président, GLX Consulting

Philippe Muller Feuga
Secrétaire général, CLUB des officiers de sécurité

Cyril N'Guyen
Directeur de la sûreté, ENGIE

Jacques Poinas
Conseiller sûreté, Inspecteur général de la Police Nationale (er), ancien directeur de l'UCLAT

NOS MEMBRES

Le collège des services de l'État

Le collège des entreprises

Le collège des opérateurs d'infrastructures critiques

Le collège des collectivités locales et territoriales

Le collège des start-ups

Le collège des partenaires thématiques

Le collège des experts

Il regroupe une trentaine de personnalités reconnues pour leurs compétences et leurs actions dans le domaine de la sécurité, ainsi que des étudiants et doctorants des filières spécialisées sécurité, défense ou gestion de crise.



Haut comité français pour la résilience nationale

www.hcfrn.org - hcfdc@hcfdc.org

PARIS

Siège de l'association
Pôle communication, relations membres
et institutionnelles :
162, rue du Faubourg-Saint-Honoré
75008 Paris
Tel : +33 (0)1 78 95 83 39

NÎMES

Pôle veille, labels, certifications
et projets R&D :
78, chemin de la Tour de l'Évêque
30000 Nîmes
+33 (0)4 30 31 79 00

Nos réseaux sociaux : @Résilience France HCFRN - @Fr_Resilience
@Veilleint_HCFRN - @Resilience France (HCFRN)