Actes des Assises de la recherche stratégique 2020 au CNAM

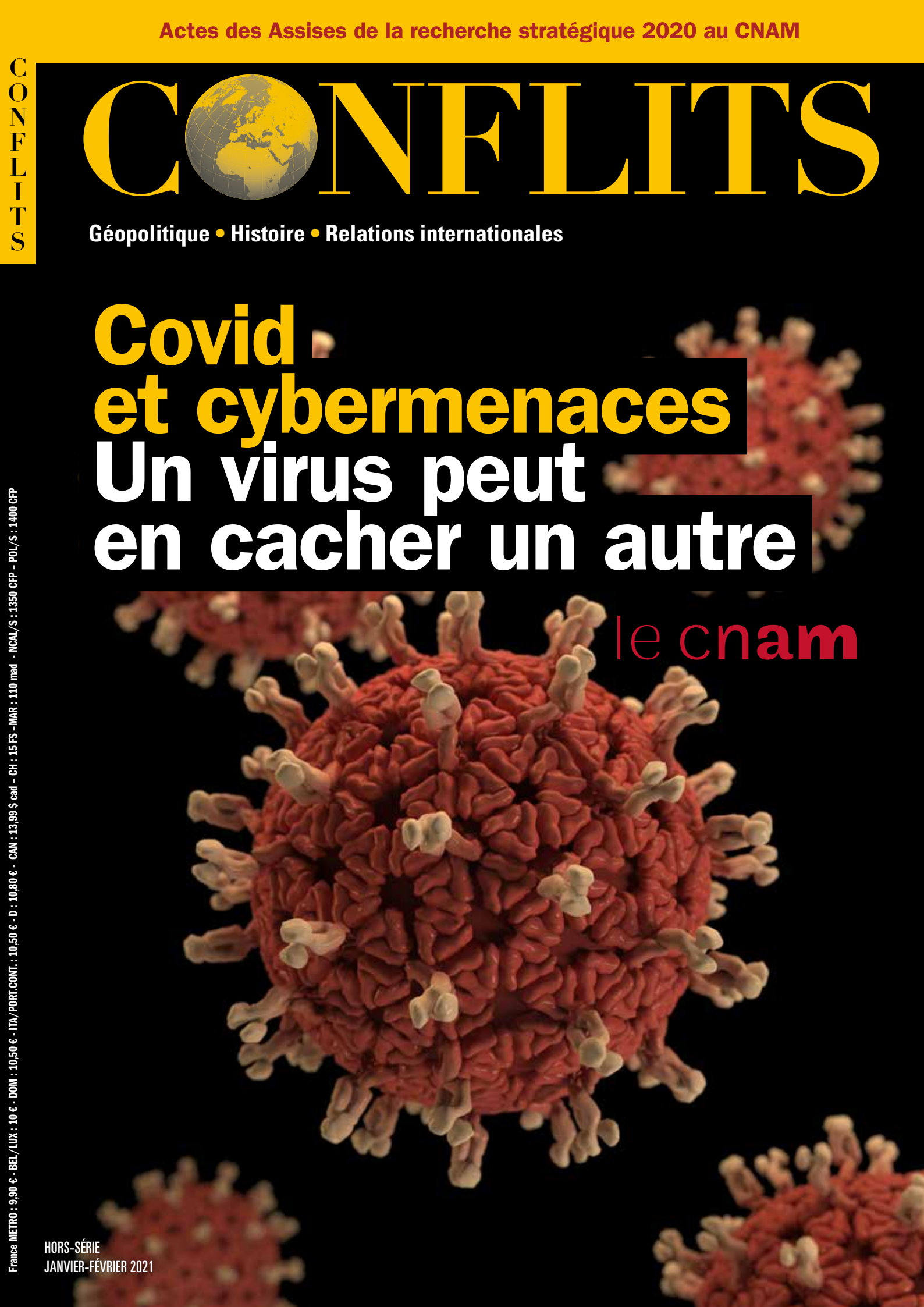
CONFLITS

CONFLITS

Géopolitique • Histoire • Relations internationales

Covid et cybermenaces
Un virus peut en cacher un autre

le cnam



France METRO : 9,90 € - BEL/LUX : 10 € - DOM : 10,50 € - ITA/PORT.CONT. : 10,50 € - D : 10,80 € - CAN : 13,99 $ cad – CH : 15 FS –MAR : 110 mad - NCAL/S : 1350 CFP – POL/S : 1400 CFP

HORS-SÉRIE
JANVIER-FÉVRIER 2021

CONFLITS
Géopolitique • Histoire • Relations internationales
Fondateur et premier rédacteur en chef : Pascal Gauchon

Janvier - Février 2021
32, rue du Faubourg-Poissonnière - 75010 Paris
01 84 79 01 35 - www.revueconflits.com

Conflits est heureux de proposer à ses lecteurs ce supplément rapportant les actes des Assises de la recherche stratégique, organisées le 17 septembre 2020 sous la direction du professeur Alain Bauer par le pôle et l'équipe sécurité défense, renseignement, criminologie, crises, cybermenaces, du CNAM. Les sujets abordés et la qualité des intervenants présents s'inscrivent pleinement dans les thèmes étudiés par *Conflits*.

La rédaction

Conflits est édité par la Société d'Édition et de Presse Antéios (SEPA), SARL au capital de 212 000 €.
Siège social : 32 rue du Faubourg Poissonnière, 75010 Paris.
Directeur de la publication : Gil Mihaely.
RCS Paris n° 802 072 504. Dépôt légal à parution.
Commission paritaire 0624I92339. Distribution MLP.
Impression : BLG Toul, 2780, route de Villey Saint-Etienne - 54200 Toul
Printed in France / Imprimé en France

Introduction générale aux Assises de la recherche stratégique

par Olivier Faron

Administrateur général du Conservatoire national des arts et métiers.

Le CNAM est, depuis 2009, un établissement pionnier du secteur sécurité-défense-renseignement. Il accueille en effet en son sein le pôle sécurité-défense, répondant à une demande du ministère des Armées du ministère de l'Intérieur : alimenter la réflexion stratégique sur des enjeux de sécurité-défense-enseignement au cœur de la sauvegarde de notre souveraineté nationale. Le pôle s'appuie sur deux piliers : formation et recherche.

Reflétant et s'appuyant sur des enseignants et intervenants reconnus, avec une forte expérience opérationnelle, le pôle SDR du CNAM désormais élargi aux questions de gestion de crise et aux cybermenaces, en complément de son pilier historique de criminologie, a ainsi créé un parcours LMD unique en Europe, car fondé simultanément sur les sciences criminelles, la cybersécurité, les relations internationales et la polémologie. Au sein du CNAM Bretagne, le pôle a ainsi développé, en partenariat avec les services de l'État, des licences professionnelles d'analyste criminel opérationnel - sécurité-défense-renseignement.

Dispensé sur deux ans, le master en criminologie, sécurité-défense-renseignement, permet aux auditeurs d'acquérir une connaissance approfondie et transverse des menaces sécuritaires modernes, de la politique de sécurité et de défense nationale, du renseignement et de la cybersécurité, dans des contextes nationaux et internationaux.

Appuyé depuis 2019 par l'équipe de recherche sécurité-défense, le pôle compte un vivier d'une vingtaine de doctorants pluridisciplinaires formés par ses soins. Dès 2014, une offre de formation doctorale dédiée a été mise en place avec la Gendarmerie nationale et différents services de l'État dont nous sommes un partenaire privilégié. À travers tout ce parcours, c'est la capacité de réflexion stratégique des auditeurs qui est stimulée. Des outils et des connaissances clés qui leur sont transmis, afin de permettre à des générations de décideurs d'appréhender les mutations complexes du champ criminel, du terrorisme, du cyber ou du renseignement, et de mieux y faire face.

Développant perpétuellement son offre, le pôle SDR 3C a enfin créé plusieurs certificats de spécialisations visant à offrir un parcours de haut niveau, ciselé et concentré autour d'une problématique précise de sécurité, faisant toute sa place à la prévention de la radicalisation, à l'analyse des cybermenaces, à la cryptographie et à la lutte contre la fraude. Il traite aussi des questions de renseignement économique ou de sécurité des sites et des flux. Le pôle sécurité-défense contribue enfin à l'animation d'une filière d'excellence de renseignement au sein de l'Académie du renseignement.

En parallèle du pilier éducatif, et depuis sa création en janvier 2019, l'équipe de recherche sécurité-défense (ERSD), renseignement, cybermenaces, crises, criminologie, porte une ambition forte : fédérer des centres de recherche internes au CNAM, nationaux et internationaux, spécialisés dans l'étude des problématiques terroristes, criminelles, de sécurité, de défense, de renseignement, de sortie de la violence, afin de contribuer plus efficacement à la compréhension et à la lutte contre ces menaces en perpétuelle mutation.

Forte de 11 chercheurs permanents et d'une cinquantaine de fellows et senior fellows venant des meilleures universités mondiales (Harvard, MIT, Stanford, Cambridge, etc.), l'ESD-R3C est rapidement montée en puissance. À la tête de plusieurs projets et consortiums de recherche portant sur des thématiques aussi variées que l'extrémisme religieux au Sahel, la cryptographie ou la lutte contre le trafic d'êtres humains, l'ESD conseille aussi bien ministères et agences publiques qu'institutions européennes et internationales.

À titre d'exemple, l'ESD-R3C fut choisie, dès octobre 2019, comme institution conseillère du Conseil de sécurité et de la Commission européenne pour la lutte antiterroriste et la cybercriminalité, ou encore, en novembre 2019, à la tête d'un groupe de travail sur les économies de la violence sous la tutelle de la FMSH et de la Fondation Carnegie. L'ESD-R3C organise enfin régulièrement des conférences et des séminaires de haut niveau, parmi lesquels le cycle sur la politique des drogues en partenariat avec le Lirsa ou des interventions de personnalités telles que le professeur John Mallery du MIT ou de Louise Shelley (George Mason University), tous deux senior fellows de l'équipe.

Créées en 2010 par le CSFRS, sous tutelle conjointe du président de la République et du Premier ministre, les assises de la recherche stratégique (ARS) sont désormais sous la responsabilité du pôle SDR 3C. Intervenants de haut niveau, échanges et débats sur l'évolution du contexte sécuritaire dans tous les espaces, les ARS répondent en effet aux besoins de création de nouveaux paradigmes et à l'encouragement de la réflexion interdisciplinaire indispensable pour parvenir à des projections et orientations stratégiques adéquates à moyen et long terme. Sans cette réflexion transdisciplinaire portant sur nos environnements et nos interactions, les crises et les menaces qui les traversent, parfois silencieusement, il est en effet impossible d'endiguer les risques propres à notre époque, de les anticiper et de soutenir les puissances publiques et privées pour qu'elles y répondent de manière adéquate.

En abordant lors de sa 9e session le thème des dissuasions ou celui quelques années plus tôt de l'hybridation des menaces, les ARS permettent ainsi d'identifier les axes stratégiques sur lesquels des ruptures sont susceptibles de se produire et de générer les réflexions indispensables pour aborder le monde de demain. Rappelant les objectifs du pôle sécurité défense et de ses équipes, à savoir le décloisonnement des disciplines et de perspectives, les ARS, organisées pour la première fois cette année par le pôle SDR 3C, l'ESD et le CNAM visent ainsi à créer une dynamique collective de réflexions indispensables pour aborder les changements de paradigme sociétaux et y repérer en amont menaces et opportunités.

Intervention du Préfet Stéphane Bouillon

Secrétaire général de la défense et de la sécurité nationale (SGDSN).

L'épidémie de Covid-19 est une crise systémique mondiale, aux effets économiques, politiques, sociaux mais aussi géostratégiques, affectant les relations entre les grandes puissances. Elle révèle des vulnérabilités jusqu'à présent asymptomatiques. Cette invisibilité de certaines évolutions de notre société est révélée par la crise sanitaire ; elle nous impose de mieux nous préparer et de pouvoir désormais réagir plus rapidement aux défis qui seront cybernétiques et écologiques. Cette crise sanitaire a dépassé nos scénarios, en partie à cause de son caractère inédit. En France, les plans de pandémie grippale, considérés comme aboutis depuis 2013, se sont avérés partiellement inadaptés face à une maladie sans vaccin ni traitement connus. Les divergences publiques entre scientifiques ont engendré de nombreuses polémiques sur la gravité de l'épidémie, les traitements adéquats, les masques, etc. Ces polémiques, combinées à une impression de manque de lisibilité partiel de la réponse à la crise, ont pu éroder le lien de confiance entre les citoyens et l'État et ralentir la prise de décision dans ce contexte d'urgence. D'ores et déjà, un travail d'analyse critique est à l'œuvre pour comprendre quelles ont été les imperfections de notre réponse et les améliorations à apporter pour l'avenir. Analyser une crise qui est toujours en cours n'est cependant pas une tâche aisée. La pandémie de Covid-19 rappelle ainsi l'importance de la planification « à froid ».

L'un des premiers enseignements à tirer de cette crise est le rôle central des États, toujours appelés en première ligne face aux crises majeures. Les crises peuvent avoir différentes origines (naturelle, technologique, sanitaire, etc.) et également résulter d'initiatives hostiles (agression armée, terrorisme, troubles graves à l'ordre public, cyberattaques, etc.). Dans chacune de ces configurations, l'État doit anticiper par la préparation de plans et réagir rapidement le moment venu. Le SGDSN est en charge de ce travail de préparation. L'articulation entre la nécessité de pouvoir réagir rapidement et la capacité de prévoir et penser des situations futures est essentielle. Il effectue ainsi un travail de veille pour détecter et anticiper les événements et les évolutions qui pourraient être générateurs de crise dans le champ de la défense et de la sécurité nationale, en France comme à l'étranger.

Les cybermenaces ont pris une ampleur considérable, non seulement dans leur dimension politique et militaire mais aussi sous un angle criminogène. L'Agence nationale de la sécurité des systèmes d'information est en charge de mener la réflexion sur la gestion des risques numériques. Notre économie est aujourd'hui de plus en plus numérisée et cette dépendance s'est accrue avec l'épidémie de Covid-19 et les restrictions de circulation. Chaque organisme, public comme privé, est ainsi amener à participer à ce travail d'analyse et de réflexion.

Comment l'État réagit-il en temps de crise ? Le Premier ministre peut activer une cellule interministérielle de crise. Il peut également désigner un ministre pour assumer en son nom la coordination opérationnelle de la réponse à la crise. Traditionnellement, la gestion des crises qui ont un impact majeur sur l'ordre public et la sécurité nationale relève du ministre de l'Intérieur. Cependant celle de Covid-19, différente de celles que l'État est habitué à gérer, a quelque peu chamboulé ce modèle. Ainsi, au début de la pandémie, c'est le ministère de la Santé qui a été désigné pour mettre en œuvre la réponse nationale ; une task force interministérielle assistant le directeur général de la santé dans cette mission. Plus tard, au stade 3 de la crise, la cellule interministérielle de crise a été activée pour gérer les aspects non sanitaires, dont ceux liés au confinement. Les principales mesures ont été prises en Conseil de défense, car cette instance présente l'avantage de réunir de façon opérationnelle et immédiate l'ensemble des ministres concernés, de pouvoir anticiper un certain nombre de décisions dans les relations extérieures de la France et enfin de coordonner efficacement la mise en œuvre des plans existants ou encore de les retravailler.

La gestion de la crise s'appuie sur les plans. La planification est une activité essentielle pour anticiper et réagir au mieux. L'une des missions premières du SGDSN est de rédiger des plans dans tous les secteurs, de les adapter le cas échéant, et de concevoir puis d'organiser des exercices pour préparer la réponse à une situation générique de crise. Ces plans, qui proposent donc des stratégies de réponse, constituent ainsi un guide d'aide à la décision. Cette planification est nécessairement imparfaite, certains événements pouvant modifier le schéma et entraîner un développement imprévu de la crise. Elle est cependant indispensable car elle fournit un mode de réflexion et d'organisation des moyens sur le territoire et de mise en œuvre des forces de sécurité qui permettra de réagir quel que soit le déroulement de la crise. L'objectif de ces plans est donc d'amener les professionnels sur le terrain à se connaître mutuellement, à développer des habitudes de réflexion, de prise de décision et des méthodes opérationnelles conjointes.

Les nécessités des dernières années, marquées par la prégnance de la menace terroriste, ont pu amener certains acteurs à perdre de vue le caractère indispensable de cette activité essentielle qu'est la planification. Il faut y revenir. Il s'agit moins de prévoir toute situation de crise possible que de créer les conditions d'une réaction rapide et efficace. Pour faire face aux prochains défis, notamment écologiques, il est indispensable de renouer avec une culture de la planification et de l'anticipation partagée interministériellement.

Gestion de l'ordre public terrorisme, radicalisation et délinquance l'ordre et les libertés au temps du Covid-19

par Cynthia Fleury et Alain Bauer

Professeur Alain Bauer, titulaire de la chaire de criminologie, directeur du pôle sécurité défense, renseignement, criminologie, crises, cybermenaces (PSD-R3C) du CNAM et la professeure Cynthia Fleury, titulaire de la chaire humanités et santé du CNAM, modération de Guillaume Soto-Mayor, IGE du PSD-R3C et de l'ESD-R3C du CNAM.

« À circonstances exceptionnelles, mesures exceptionnelles. » L'adage autour duquel s'est construit et justifié le principe d'urgence sanitaire est mis à mal par l'installation de la crise liée au Covid-19 dans la durée, comme l'illustre la deuxième vague de contaminations que nous sommes en train de traverser. La réponse à apporter à cette crise n'est donc plus celle d'une mesure d'urgence, et s'inscrit au contraire dans le temps long. De ce fait, les privations de libertés auxquelles ont consenti les citoyens français face à l'urgence sont de plus en plus difficiles à légitimer.

Une première observation à ce sujet porte sur la banalisation de l'exception :

l'outil d'état d'exception, bien que nécessaire au bon fonctionnement de l'État de droit face à diverses situations de crise inédites aux incertitudes fortes, doit voir son utilisation limitée par les principes permettant son recours consenti, à savoir : les principes de conditionnalité, proportionnalité et temporalité. Sorti de ce cadre, le recours à un état d'exception banalisé amène nécessairement vers une pente glissante et dangereuse. La mise en place d'outils d'audit permettant d'évaluer précisément le rapport entretenu entre les mesures d'exception décidées au niveau de l'État et les trois principes précédemment cités est alors souhaitable : ce, dans le but de préparer un calendrier visant la sortie de l'État d'exception mis en place. Sinon, le flou qu'une absence d'évaluation laisse s'installer risque d'entraîner la société toujours plus loin des limites de l'État de droit, vers une « nouvelle normalité » qui assoiraient une version désubstantialisée de la démocratie.

Les États de droit, dans le domaine de la gestion des crises doivent composer avec une position paradoxale consistant à devoir anticiper des circonstances exceptionnelles auxquelles, par ailleurs, ils ne croient pas. Ils se retrouvent ainsi dans l'incapacité de concevoir les outils de réponse adaptés car ils restent enfermés dans un mode de pensée où l'exceptionnel est considéré comme si improbable qu'il devient presque inutile de s'en soucier. Un exemple historique récent auquel nous pouvons penser est celui de la préparation de la gestion de la crise sanitaire. À la suite de l'épidémie de grippe aviaire H5N1 en 2006, avait été mis en place dès 2007 un établissement de préparation et de réponse aux urgences sanitaires (Eprus) qui, entre autres, avait permis le stockage du milliard de masques qui ont manqué lors de l'émergence de la pandémie de SARS-COV-2. Or, en 2008-2009, la crise sanitaire annoncée avec le début de pandémie de grippe H1N1 n'a finalement pas eu lieu. Considérant ainsi que la crise n'aurait de fait jamais lieu, l'intégralité du dispositif est démantelée progressivement par une bureaucratie tatillonne et revancharde. Ainsi, les dispositifs exceptionnels sont systématiquement dépassés par l'ampleur réelle de la circonstance exceptionnelle et par sa médiatisation. L'État se retrouve alors dans une incapacité de gestion normale de l'anormal, et valse d'un scepticisme à la limite du déni à une gestion panique de l'urgence qu'il devient impossible d'ignorer. Ce passage brutal entraîne une réponse étatique où l'anormal, pour rester sous contrôle, doit nécessairement devenir l'ordinaire. Cette « valse des extrêmes » se retrouve également avec la gestion sécuritaire comme le montre la gestion des peines de prisons coincées entre une « prison pour tous » impossible à mettre en place et aménagements de peines inefficaces.

Les mesures d'"exception doivent donc être mises en place dans un cadre contrôlé, sans quoi la démocratie risque d'être dévoyée : il s'agit de penser un dispositif de *checks and balances*, qui autorise le recours aux mesures d'exception uniquement dans des conditions mesurées.

Ce cadre contrôlé est d'autant plus important qu'il est au cœur des critiques portées à l'encontre de la réponse proposée par l'État français à la crise sanitaire, hautement liberticide. Le manque de confiance des citoyens vis-à-vis de l'État, lié à l'absence de ce *checks and balances* qui pousse ses représentants au mensonge et certaines de ses institutions aux abus, est aggravé par l'absence d'évaluation des conséquences des mesures de privations de libertés mises en place sur les populations. On en voit les limites avec l'apparition d'une « troisième vague psychiatrique » dénoncée récemment dans les médias à la suite du deuxième confinement. Se pose alors la question des solutions alternatives qui, bien qu'existantes, n'ont pas été privilégiées.

Cela s'explique tout d'abord par un biais cognitif classique consistant à considérer qu'une mesure efficace face à une situation exceptionnelle consiste nécessairement en une privation de droits. Peuvent être pointées la réputation de lenteur et de lourdeur des processus de décisions démocratiques, considérés comme peu adaptés aux temps de crises où l'urgence amène à privilégier une verticalité qui frise l'autoritarisme. Or, ce choix idéologique, par son manque intrinsèque de considération de la pluralité, entraîne un renforcement des discriminations préexistantes (violences domestiques, handicaps et comorbidités, précarité économique, etc.). Une approche plus collégiale de la question aurait ainsi pu permettre la prise en compte de la dimension préventive et socio-thérapeutique de la situation, plus que de sa seule dimension sanitaire.

La réaction autoritaire, marquée par la facilité, s'explique également par un biais culturel lié à la nature de l'État en France dans sa relation avec la société, où l'équilibre d'un contrat social établi par la confiance est concurrencé par le recours à la force caractéristique de l'État-nation. La relation de l'État français à la société française reste ainsi essentiellement un rapport de force sans compromis. Dans le cas de la gestion de la crise sanitaire, la perte de confiance des citoyens vis-à-vis de l'État engendrée par l'incohérence permanente de ses déclarations (sur le port du masque notamment) a ainsi déteint sur la confiance que portaient encore jusqu'alors les citoyens français au discours scientifique. Pour la première fois, le débat s'est orienté non pas sur la manière de régler le problème mais sur la nature même de celui-ci. La remise en cause systématique de la parole scientifique a ainsi eu pour conséquence la dissolution totale d'une vérité de référence pouvant servir de socle aux autres débats, poussant ainsi l'État à adopter ses mesures réflexes : l'autorité et la contrainte.

Toutefois, les recours aux experts ne permettront pas de renouer le lien de confiance nécessaire à la mise en place d'une politique publique de gestion de la crise sanitaire plus sereine et efficace. Les démocraties fonctionnent en effet sur une association primordiale entre vérité et liberté, l'une permettant de savoir où, quand et comment, définir les limites de l'autre. Concernant la crise sanitaire actuelle, il s'agit d'une vérité scientifique, argumentée, revue collectivement selon le processus habituel de la recherche scientifique. Or, la destitution récente de l'autorité scientifique va de pair avec une culture de l'information toujours plus rapide, binaire et spectaculaire en contradiction totale avec la logique d'éducation sur le temps long nécessaire à la création d'une confiance vis-à-vis du discours scientifique au sein de la population. Les recommandations tirées de ce même discours sont ainsi plus que jamais contestées. Le recours aux processus d'*open science* et de *mass self media* pourrait être utile contre ça, mais ces alternatives aux médias de masse n'ont pour l'instant pas encore suffisamment intégré la culture de l'information pour être efficaces en ce sens.

Or, avant de vouloir refaire vérité, il faudrait pouvoir refaire société. L'incapacité de la puissance publique à répondre à la pluralité des situations par l'application stricte d'une règle unique amène ainsi un questionnement sur la réponse de l'État aux contestations sociales. En effet, la disparition progressive au cours des trente dernières années de l'équilibre qui était jusqu'alors institué entre professionnels de la contestation et professionnels du maintien de l'ordre et les violences policières qui en ont résulté ont mis en exergue la difficulté de l'État à s'extirper de dispositifs obsolètes. La gestion du Covid-19 a ainsi été le point final de ce lent processus de désagrégation de l'État et plus spécifiquement de l'État profond. Mais cette désagrégation de l'État profond entendu comme garant institutionnel de la république n'amène pas l'extinction d'une autre forme d'État profond. Celui-ci, bien vivace, serait lié aux multinationales, au lobbying, et renverrait à un surpouvoir visant la confiscation totale de l'État par des intérêts particuliers. La restructuration de l'État profond tel que compris dans la première définition proposée, colonne vertébrale de l'État, nécessite une réflexion sur l'hypercentralisation qui dans les faits ne fonctionne plus, et donc sur la nécessaire révision des échelles de gestion. Cependant, la violence n'est pas un outil de régulation adéquat dans un État de droit, c'est pourquoi la contestation et la définition du juste doit redevenir une compétence des citoyens en démocratie tout comme la réconciliation ne doit plus être naïvement conçue comme un consensus d'emblée, mais comme ce qu'elle est réellement : un dissensus cathartique et mouvementé qui permet la construction d'une réponse et où la violence, essentiellement destructrice, n'a pas sa place.

Les principaux défis pour l'État dans la gestion de la pandémie du Covid-19 en matière sanitaire ainsi que les perspectives de sortie de crise

par Jean-François Zagury et Alain Toledano

Professeur Jean-Francois Zagury, titulaire de la chaire de bio- informatique du CNAM
et le docteur Alain Toledano, cancérologue, président de l'Institut Rafael. Professeur

Toute l'attention est aujourd'hui accaparée par le contrôle de l'épidémie et le traitement des cas graves. Il est cependant particulièrement nécessaire d'alimenter la réflexion post-covid et d'élaborer un projet de santé globale.

En effet, les patients infectés développent un cortège de symptômes (fatigue, gênes respiratoires, syndromes anxio-dépressifs, troubles sensoriels, atteintes multiples des fonctions cognitives, etc.) qui deviendront dans certains cas des pathologies

chroniques : 10 % des personnes infectées présentent des séquelles médicales significatives, 40 % constatent une baisse de leur qualité de vie[1].

Ce virus n'affecte pas seulement la santé des personnes infectées, une crise sanitaire au tel retentissement social et économique entraîne de facto de nombreux risques, souvent négligés. À la suite de la crise économique de 2008, les scientifiques ont constaté par exemple une surmortalité par cancers. Une étude menée par l'Inserm relève une surmortalité des chômeurs trois fois supérieure, représentant d'ores et déjà 14 000 décès en France par an[2]. Les 800 000 chômeurs supplémentaires au deuxième trimestre 2020[3] s'ajoutent ainsi à la longue liste de défis auxquels devra faire face notre système de santé publique en post-Covid.

Certaines pathologies de confinement ont déjà été clairement identifiées : dépression, addictions, surpoids entraîné par la sédentarité ou encore troubles de la sexualité. Enfin, il faut distinguer le risque, de la perception du risque. Une part non négligeable d'individus sont prisonniers de leurs peurs et refusent ainsi de travailler en présentiel ou bien saturent les centres de santé, d'où l'importance de la communication thérapeutique pour diminuer l'impact négatif sur la santé émotionnel.

Une approche en termes de santé intégrative qui prendrait en considération toutes les dimensions de la santé (sociale, psychologique, émotionnelle ou encore sexuelle) pour les intégrer dans un projet de santé globale est ainsi nécessaire afin de gérer au mieux cette période post-Covid. Cette approche multidisciplinaire de la santé émerge aux États-Unis dans les années 1990[4] face à la problématique des maladies chroniques. En quoi consiste-t-elle concrètement ? Il s'agit de coconstruire avec chaque patient un parcours de santé qui lui est propre, centré sur son projet de vie. Cette approche multidisciplinaire de la santé nécessite l'inclusion de nouveaux métiers et enseignements, qui relèvent ou non du domaine médical à proprement parler : sophrologie, psychologie, hypnose, nutrition, kinésithérapie, etc.

L'Europe accuse un retard sur ce sujet, alors même que le vieillissement des populations justifie une meilleure prise en charge de ces pathologies. En 1994, 3 700 000 personnes en France étaient suivies pour une affection longue durée, elles sont 11 millions en 2018[5], représentant une consultation sur deux. Le système de santé publique français doté d'un budget plus que significatif (208 milliards d'euros soit plus de 10 % du PIB[6], supérieur à la moyenne de l'OCDE) nourrit cependant le mécontentement des soignants et des usagers. L'inefficacité de ce système pourtant coûteux signe l'échec d'une médecine purement symptomatique et insuffisamment innovante.

La crise de Covid-19, comme expliqué auparavant, amplifiera drastiquement cette tendance d'augmentation des pathologies chroniques. Elle pourrait cependant être le catalyseur d'une nouvelle manière d'appréhender la médecine, indispensable au regard des nombreux défis auxquels devra faire face notre système de santé publique, déjà à la peine.

1. Stéphane Korsia-Meffre, « COVID-19 : quelles séquelles à long terme ? L'expérience du SRAS et du MERS », Vidal, 16 juin 2020.
2. Pierre Meneton, « Unemployment is associated with high cardiovascular event rate and increased all-cause mortality in middle-aged socially privileged individuals », *International Archives of Occupational and Environmental Health*, 2014.
3. Direction des études et statistiques du ministère de l'Emploi (Dares).
4. Snyderman R, Weil AT, *Integrative Medicine : Bringing Medicine Back to Its Roots*, Arch Intern Med, 2002.
5. Caisse nationale de l'assurance maladie.
6. *Les dépenses de santé en 2019 – Résultats des comptes de la santé*, Panorama Dress Santé, édition 2020.

Les missions élargies de la cyberdéfense pendant la crise globale de 2020

Entretien entre le général Didier Tisseyre[1], commandement de la cyberdéfense française (COMCYBER), et le professeur Philippe Baumard, directeur de l'équipe de recherche sécurité défense, renseignement, criminalité, crises, cybermenaces (ESD-R3C du CNAM).

Le 12 décembre 2016, Jean-Yves Le Drian alors ministre de la Défense présente dans une déclaration inédite les prémices de la nouvelle cyberdoctrine française. « *La défense de la France doit s'adapter aux enjeux actuels et futurs de ce champ de bataille* […]. *En temps de guerre, l'arme cyber pourra être la réponse* […] *à une agression armée, qu'elle soit de nature cyber ou non.* » Ce discours marque une rupture dans l'approche française de la cyberdéfense en annonçant les prémices de ce que sera la Lutte informatique offensive (LIO) officiellement dévoilée en janvier 2019.

À l'origine de cette évolution doctrinale, une prise de conscience de l'augmentation du nombre d'attaques, de l'étendue de leurs conséquences et de leur caractère parfois systémique pouvant affecter des intérêts vitaux et souverains de la France. La doctrine française conçoit dès lors la dimension cyber comme un instrument de projection, d'amplification ou de réduction des moyens de la puissance ; dans le strict respect du droit international. La seule posture défensive apparaissait alors insuffisante : il fallait décourager les potentiels attaquants en leur montrant la capacité de réaction de la cyber force française.

Après cette annonce, un certain nombre d'éléments de cette doctrine ont été rendus publics afin d'informer les citoyens sur la cyberdéfense française et d'établir le cadre dans lequel elle s'applique. À la différence d'autres doctrines de nations alliées, la doctrine française ne distingue pas la réponse cybermilitaire sur une échelle d'intensité, mais au contraire comme un moyen transversal de projection qui accompagne le conflit conventionnel. Dès lors, elle s'insère dans le cadre de doctrines militaires préexistantes ou vient les compléter. S'il y a bien une spécificité de ce milieu de conflictualité, par sa nature technique, le cyberespace est un espace d'opérations que l'on peut difficilement isoler ou contraindre comme on le ferait d'un terrain d'opérations traditionnel.

Le cyberespace est caractérisé par une contraction du temps et de l'espace, nécessitant une capacité de réaction rapide et d'anticipation. Les frontières se matérialisent moins bien rendant l'identification des attaquants et la portée des dommages plus complexes. Le Centre de coordination des crises cyber (C4), rattaché au SDGSN, a défini une grille d'analyse afin de mieux appréhender la nature de ces attaques et de définir le cadre d'une réponse nationale. Il est primordial de déterminer qui est l'attaquant (individu isolé ou groupe de cybercriminels) et s'il y a derrière lui un acteur étatique ou non. Il faut ensuite analyser la manière dont l'ennemi attaque. La réaction ne sera pas identique s'il s'agit de pénétrer un système mal sécurisé ou de lancer une offensive via des méthodes invasives pour casser un système. L'impact de cette attaque est le troisième élément de cette grille à visée opérationnelle. L'élaboration d'une riposte n'est pas un processus automatisé car chaque attaque est spécifique, mais cette grille permet entre autres d'éviter un risque d'escalade de la violence non souhaitée.

On peut distinguer trois composantes du cyberespace. La première est physique, il s'agit du matériel (ordinateurs, câble, etc.) auquel est associé la notion de territorialisation qui ouvre sur l'application des droits nationaux. Vient ensuite la dimension logique, qui fait l'objet des attaques visant les systèmes, avec l'exemple du traditionnel virus. Enfin, la troisième dimension est cognitive et correspond à ce que l'on appelle aujourd'hui la guerre de l'information. Dans le contexte actuel de crise pandémique majeure, cette dernière trouve un écho particulier. Les faux pavillons, sorte de robots qui investissent les réseaux sociaux afin de diffuser massivement des infox et autres théories du complot, sont aujourd'hui clairement identifiés comme une problématique majeure du cyberespace et des acteurs qui le composent. L'OMS a d'ailleurs parlé d'« infodémie ». À noter que le nombre d'attaques n'a pas drastiquement augmenté avec la pandémie, elles se sont cependant massivement concentrées sur la thématique Covid-19, avec une efficacité redoutable.

Nous travaillons actuellement à définir le positionnement de la France par rapport à cette guerre de l'information ou encore sur la question de savoir quel champ d'action la cyber doctrine française autorise-t-elle ? La France ne peut réussir dans ce combat sans travailler conjointement avec ses alliés stratégiques. Comme pour les attaques informatiques, le recoupement des informations dont chaque pays dispose sur son propre périmètre permet de cartographier ces pavillons et notamment d'identifier le style caractéristique de leurs auteurs. L'efficacité française dépend alors du maillage créé avec ses alliées.

Enfin, la conflictualité dans le cyberespace dépend de la manière dont chaque État appréhende traditionnellement la conflictualité et le rapport de puissance (avec ses alliés et ses ennemies), mais également des attaques subies par ces mêmes États qui peuvent faire évoluer leur position doctrinale. La cyberdoctrine française s'inscrit dans le cadre du droit international humanitaire et de ses principes comme ceux de proportionnalité et de discrimination des cibles

Le professeur Baumard précise également que les États-Unis, sous l'administration Trump, ont détaillé publiquement une stratégie basée sur le *defense forward* et le *persistent engagement* pour augmenter la sécurité nationale et conforter la supériorité stratégique des États-Unis partant du principe que les États sont en contact permanent avec leurs adversaires dans le cyberespace. Le professeur ajoute que, selon son avis, la France, de son côté, a promu une vision différente des équilibres cybermilitaires ; en refusant notamment l'idée qu'un positionnement déclaratif d'actions en dessous d'une conflictualité armée, difficile à définir en matière cyber, puisse être une carte blanche à la prolifération de micro-agressions cyberarmées. C'est pour cette raison que la France a adopté une doctrine équilibrée, s'inscrivant dans son savoir-faire militaire, reconnaissant la notion de souveraineté nationale numérique tout en utilisant la modernité pour servir ses buts stratégiques, en respectant le droit international, quel que soit l'intensité et le niveau d'intervention de ses interventions militaires cyber.

1. Le général de division aérienne Didier Tisseyre, a pris la tête du commandement de la cyberdéfense en septembre 2019, et conduit les forces de cyberdéfense des armées françaises, regroupant plus de 3 400 cybercombattants.

Synthèse du panel entre la professeure Véronique Legrand et le député Gérard Cherpion

Professeure Legrand, titulaire de la chaire de sécurité informatique du CNAM et directrice de l'équipe de recherche sécurité défense, renseignement, criminologie, crises, cybermenaces (ESD-R3C) et le député Gérard Cherpion (LR, 2e circonscription des Vosges).

Les enjeux de l'emploi et de l'innovation en cybersécurité, dans la perspective des JO 2024 sont au cœur du débat. Paris s'est en effet fixé le double objectif de « construire les Jeux les plus numériques de l'histoire olympique » et d'en faire un catalyseur de l'emploi. La cybersécurité sera au cœur de ce pari, sans aucun doute garante du succès de cette transition numérique des JO.

Les perspectives d'emplois des JO 2024 sont énormes, plus de 12 millions de personnes attendues au total. La cybersécurité emploie aujourd'hui 24 000 personnes en France, soit seulement 3 % des effectifs de l'industrie. C'est un chiffre insuffisant pour répondre à la demande croissante des acteurs privés et publics face à des menaces cyber toujours plus variées et sophistiquées. En vue des JO de Paris, l'objectif fixé est de 3 500 nouveaux emplois par an, pour atteindre 8 % des besoins en effectifs. Il est essentiel aujourd'hui de former et de recruter des professionnels dans ce domaine. Mais « former pour former » ne sert à rien, ces jeux ne doivent pas être une finalité en soi mais un tremplin pour le développement des nouveaux métiers de la cybersécurité.

La crise du Covid-19 a été révélatrice des forces et des faiblesses de la France dans la perspective des JO 2024. Les individus, les entreprises comme les États ont dû apprendre et s'adapter rapidement à une situation sanitaire inédite. Des capacités insoupçonnées se sont révélées, par exemple le télétravail qui, jusqu'à présent peu concevable dans la culture managériale française, s'est largement répandu pour laisser entrevoir de nouvelles opportunités. Il

convient néanmoins de veiller à réduire certaines difficultés et aspects négatifs qui l'accompagnent, comme la fracture numérique ou l'évolution des cybermenaces qui doivent être traitées en priorité.

À la suite du premier confinement, des mouvements de population ont été constatés allant des grandes villes vers des zones périurbaines voire rurales. De plus en plus d'individus souhaitent s'éloigner des métropoles, étant prêts à abandonner un certain niveau de service pour améliorer leur qualité de vie. Cela concerne évidemment une catégorie de population précise qui est en capacité de poursuivre son activité professionnelle à distance des grands centres urbains. Cette nouvelle tendance démographique, si elle se confirme, pourrait mettre en valeur des régions qui ont montré une avance notable sur leur numérisation comme c'est le cas de la région Grand Est qui sera 100 % « fibrée » en 2022.

Le besoin en formation et compétences cyber émane directement des citoyens comme des entreprises, notre société étant fortement dépendante du numérique. La formation cyber doit également répondre à l'enjeu extrêmement fort des JO les plus numériques afin de garantir la sécurité des personnes et de l'État. Les perspectives de formation aux métiers de la cybersécurité se présentent de façon très favorable, les formations cyber couvrent l'ensemble du territoire et des métiers et touchent des populations diversifiées.

Les compétences attendues en cybersécurité devront favoriser les plans de carrière afin qu'ils soient flexibles et adaptés aux différents métiers. Elles devront couvrir trois grands volets : bien sûr techniques comme la sécurité informatique mais également transverses et fonctionnels comme la protection des informations et transverses comme les métiers très attendus des domaines connexes à la cybersécurité. Par exemple, avec 12 millions de personnes transportées à l'occasion des JO, il convient d'ores et déjà de penser la formation à la gestion de crise des conducteurs ou pilotes des compagnies de transport, et d'apprendre comment réagir face à une prise d'otage ou travailler dans le contexte d'une crise sanitaire, etc. Des modules complémentaires de sécurité seront dispensés pour ces métiers, les premières formations devraient démarrer rapidement.

La formation en cybersécurité mettra en avant les parcours professionnels, chaque personne étant différente, et laisser la possibilité de choisir un parcours et d'en changer sera le challenge à relever pour assumer la pérennité de l'emploi avant et après les Jeux. Aussi, le panel de formations doit porter sur des formations initiales et la reconversion de certaines professions. C'est le cas chaque année pour environ 15 000 personnes qui quittent les rangs de l'armée, de la gendarmerie et de la police pour retourner à la vie civile. Ils peuvent être recrutés par des sociétés de sécurité intéressées par leurs compétences à condition de compléter leur formation par des modules en adéquation avec leurs nouvelles missions. Il est ainsi essentiel de penser la formation de cette catégorie de professionnels afin de valoriser au mieux les compétences qu'ils ont acquises tout au long de leur carrière militaire tout en répondant aux questions de pénurie du domaine de la cybersécurité.

Pour relever ce double défi des JO les plus numériques et de la pérennité de l'emploi, il convient de mettre en place un plan global et ambitieux de formation aux métiers de la cyber, ce plan en mesure d'intégrer une dimension numérique aux formations de la sécurité globale et de répondre au besoin impérieux de se protéger contre la cybermenace. Peu importe leur niveau de formation, intégrer intelligemment les évolutions de carrière des individus, c'est tirer vers le haut ces professions et leur donner des perspectives nouvelles.

Analyse rétrospective des cybermenaces au temps du Covid-19

par Julia Pieltant et Édouard Klein

Docteure Julia Pieltant, maîtresse de conférences au CNAM et le docteur Édouard Klein, ex-expert au C3N (Gendarmerie nationale).

Dans la continuité directe d'attaques à peine antérieures au premier confinement (la métropole d'Aix-Marseille ayant par exemple été victime d'un rançongiciel à très large portée, et l'AP-HP d'une attaque de type DDoS), la crise sanitaire liée au SARS-COV-2 a été révélatrice de vulnérabilités présentes au sein des systèmes d'information de nombreuses entreprises et administrations, ce qui a mécaniquement entraîné une augmentation des cyberattaques. La généralisation du télétravail, exigeant l'adaptabilité immédiate de l'organisation des tâches des différents agents pour assurer la continuité de leurs travaux, a entraîné le recours massif à du matériel personnel et à des logiciels gratuits, de fait peu sécurisés.

Pourtant, cette augmentation des cyberattaques peine à être pleinement connue et analysée par les services de

gendarmerie dédiés. Le C3N, unité de la gendarmerie nationale spécialisée dans la lutte contre la cybercriminalité à différentes échelles, reconnaît par exemple avoir rencontré des difficultés dans la gestion des cyberattaques en augmentation au cours de ces derniers mois. La centralisation opérée au sein du C3N de l'intégralité des plaintes liées à l'activité cybercriminelle en France, extrêmement utile lorsqu'il s'agit de détecter des tendances de fond et des modèles d'attaques répétés, ne permet l'accès

qu'à la partie émergée de l'iceberg des cybermenaces. Or, cette base de données reste malgré tout très parcellaire.

Les efforts accomplis par le C3N en partenariat avec l'institut SystemX de l'université Paris-Saclay pour déterminer l'ampleur de la partie immergée de l'iceberg ont donné des résultats édifiants : à travers une méthode de corrélation croisant le nombre de plaintes reçues, le nombre de recherches Google portant sur des expressions telles que « ransomware » ou « Loki » et les résultats d'un sondage mené par Philipe Wolff et Philippe Laurier (de l'institut SystemX) évaluant l'exposition d'un échantillon d'entreprises aux cyberrisques, il leur a été possible de déterminer que pour une plainte déposée, 251 victimes de cyberattaques n'en déposaient pas et restaient donc en dehors des radars du C3N. Pis, les 251 plaintes non recensées concernent des individus pleinement conscients d'avoir été victimes d'une cyberattaque. Le protocole d'évaluation concernait en effet les ransomwares, une forme d'attaque où le cybercriminel a tout intérêt à ce que sa victime soit tenue au courant du préjudice subi afin, précisément, qu'elle règle la rançon lui permettant de récupérer ses données. Ainsi, une large partie des cyberattaques prenant des formes plus sournoises (vols de données destinées à la revente dans les cas d'espionnage industriel par exemple), où le cybercriminel a au contraire tout intérêt à ce que l'individu ignore tout de son statut de victime afin que son attaque passe aussi inaperçue que possible, reste quasiment indétectable pour le C3N.

Or, la massification du télétravail a eu précisément pour conséquence d'augmenter le nombre de ce type de cyberattaques qui sont donc pour la plupart passées sous les radars. Cette massification a en effet eu pour principale conséquence l'augmentation de la surface d'attaque exploitable pour les cybercriminels, tout en révélant le sous-investissement chronique des responsables de la sécurité des systèmes d'information (RSSI) dans divers dispositifs de cybersécurité qui, dans cette situation, auraient été bienvenus. Subitement, le parc de machines qu'il incombe aux RSSI de gérer a été d'un même coup multiplié et dispatché entre les différents domiciles des employés d'entreprises et administrations qui se sont retrouvés confinés du jour au lendemain.

La continuité de missions nécessitant parfois le traitement de données sensibles (listes de clients, numéros de comptes en banque, etc.) a ainsi dû s'effectuer à partir d'un matériel potentiellement porteur de compromissions préalables, en dehors du réseau sécurisé de l'entreprise ou de l'administration concernée et loin du contrôle du RSSI.

La réorganisation de tâches en cours ou nécessitant le regard de plusieurs personnes à distance a également entraîné le recours massif dans l'urgence à diverses solutions de partages de documents (Google Drive, Dropbox, etc.) ou encore de réunions en visioconférence (Skype, Teams, Google Meet, etc.) qui ne permettaient ni le respect de normes de cybersécurité minimales, ni une quelconque cohérence entre les choix de logiciels à utiliser.

La mise en péril de la sécurité globale du système d'information des entreprises ou administrations concernées entraîne de fait l'augmentation d'attaques d'opportunité, car l'absence de logs, qui permettent habituellement au RSSI d'avoir un retour sur les activités des machines liées à son système d'information fermé et structuré, empêche la détection et la reconstruction des processus de cyberattaques.

Le recours au télétravail reste actuellement relativement large et semble s'installer dans la durée, au même titre que la crise sanitaire liée au Covid-19. Il s'agit donc, afin de limiter au maximum les cyberrisques évoqués précédemment, de rendre un certain nombre de précautions en amont.

Un premier pas consisterait à investir davantage dans la sécurité des systèmes d'information. Il est en effet fondamental que la cybersécurité, au même titre que la sécurité en général, ne soit plus considérée comme un coût (souvent perçu comme élevé et superflu) mais comme un investissement sur le long terme à privilégier autant que possible. Un système sécurisé est d'abord un système fiable et efficace, qui permet aux individus de travailler plus vite, plus efficacement, plus sereinement, et débouche à terme sur un retour sur investissement bénéfique pour tous. Sans cet effort d'investissement, et bien qu'il soit impossible à l'heure actuelle de déterminer le coût exact, les pertes liées à l'ensemble des préjudices liés aux cyberattaques sur les entreprises en France qui s'élèveraient à plusieurs milliards d'euros risquent encore d'augmenter dans les années à venir.

Il serait également bénéfique de corriger l'absence criante d'une culture des bons réflexes de cybersécurité dans le monde du travail. Il s'agirait de former et de responsabiliser davantage chaque utilisateur et ainsi, à terme, faciliter le traitement sécurisé des données tout en rendant la détection de potentielles cyberattaques plus immédiate et plus efficace en lien avec le RSSI et les services de sécurité informatique des entreprises.

Par ailleurs, le recours massif aux outils de partage de données gérés principalement par les Gafam (Google, Apple, Facebook, Amazon, Microsoft) amène à s'interroger sur les enjeux fondamentaux de souveraineté informatique de la France, et plus largement du continent européen. C'est dans cette optique que le projet de cloud souverain européen Gaia-X a été lancé sous l'impulsion commune de l'Allemagne et la France.

En l'état actuel des choses, le recours aux logiciels libres, ainsi qu'aux nombreux hébergeurs libres et collaboratifs déjà existants permettent d'ores et déjà d'assurer une architecture de systèmes sécurisée.

Il serait ainsi judicieux d'exploiter et d'aider au développement de ce savoir préexistant plutôt que de chercher à tout prix à développer un cloud en passant par une industrie qui, bien souvent, peine à offrir des performances équivalentes à celles que proposent la communauté agrégée de générations d'intelligences visant depuis déjà plusieurs décennies la liberté et l'indépendance de la sécurité des systèmes d'information. ◗

Pôle Sécurité Défense, Renseignement - Criminologie - Cybermenaces - Crises (PSD R3C) et Équipe de recherche (ESD R3C)

Des formations multidisciplinaires adaptées à tous les projets

Les équipes du pôle vous proposent des formations en format hybride, présentiel, à distance et sur mesure:

NCU HESAM (niveau bac +1/+2) pour le *middle management* de la sécurité

Ce diplôme s'intègre dans le processus de formation et de reconnaissance de compétences de la sécurité privée. Cette formation professionnalisante contribue à façonner des talents confirmés pour ce secteur en pleine transformation.

Licence professionnelle analyste criminel opérationnel/sécurité défense-renseignement

Le pôle sécurité défense implantée en Bretagne accueille cinq formations : analyste en sécurité des systèmes télécoms et réseaux informatiques, analyste opérationnel de données stratégiques, analystes linguistes (russe, chinois et arabe) et des formations spécialisées, opérées en étroite relation avec les structures étatiques partenaires.

Master criminologie, sécurité défense, renseignement, crises et cybermenaces (M1 et M2)

Le master criminologie est une formation pluridisciplinaire (sciences criminelles, droit, droit pénal, gestion, probabilités, etc.) permettant d'acquérir une large variété de compétences dans les domaines de la sécurité et de la défense. Le master de criminologie s'appuie sur un corps enseignant de haut niveau et a été progressivement reconnu comme la formation de référence par les acteurs du secteur.

Doctorat droit - sécurité défense – criminologie

L'équipe de recherche associée au pôle accueille une formation doctorale et compte 17 doctorants. Reflétant et s'appuyant sur le réseau international de recherche, ce programme doctoral traite aussi bien de l'étude de la criminalité organisée et du terrorisme, que des cybermenaces, du renseignement ou des affaires militaires.

Doctorate of Business Administration (DBA) sécurité défense - renseignement

Destiné à des professionnels, ce DBA est pour eux un travail d'exploration intellectuelle. Il conjugue la définition et la description sur le terrain d'une problématique managériale qui a retenu l'attention du praticien et la recherche élargie de cadres d'interprétation.

Certificats spécialisés :

Prévention de la radicalisation

Il vise à transmettre aux professionnels des outils de décryptage, d'analyse et d'intervention sur une problématique complexe. Cette formation comprend un volet théorique, permettant d'appréhender les différents paradigmes, mais aussi empirique avec le témoignage d'experts reconnus.

Gestion des crises complexes

Cette formation appréhende les techniques de négociation en situation dégradée ou en situation de crise. Elle s'adresse aux futurs négociateurs de crise ou médiateurs professionnels, mais également à ceux qui souhaiteraient développer leurs compétences dans la gestion des crises souvent moins dramatiques mais tout aussi complexes, dans les milieux touchés par les actes d'incivilité et les conflits interpersonnels dans lesquelles le recours à la violence se banalise.

Lutte contre la fraude comptable et financière

Réalisé en partenariat avec le Conseil supérieur de l'ordre des experts comptables et l'Association des directeurs financiers et contrôleurs gestion, ce certificat poursuit l'objectif de former des professionnels du chiffre. Il s'adresse ainsi à une large variété de profils : experts comptables, commissaires aux comptes, mais aussi des directeurs financiers ou des contrôleurs de gestion.

Sécurité des sites et des flux

La prévention situationnelle est en fait bien plus riche qu'il n'y paraît. Cette formation appréhende à la fois un contenu théorique très riche et explore les moyens de prévention situationnelle en préparant la perspective des JO de Paris.

Renseignement économique

L'objectif pédagogique de cette formation est d'acquérir une culture large de l'environnement géoéconomique et de sa complexité, de connaître l'ensemble des menaces pesant dorénavant sur une entreprise moderne, et de savoir y faire face en maîtrisant les techniques et outils d'acquisition et de traitement de l'information stratégique. Cette formation cherche à recentrer la problématique autour du renseignement économique afin d'apporter une véritable plus-value en matière de stratégie d'entreprise. La capacité d'anticipation est au cœur de cet enseignement.

Cybersécurité et analyse des menaces / cryptoologie

Ces formations entendent répondre au besoin grandissant d'acquisition de nouvelles compétences dans la gestion des cybermenaces. Ces compétences mobilisent un large champ de connaissances à la fois numériques, sociologiques et stratégiques. Afin de couvrir tous ces aspects de la cybersécurité et de la cryptologie, les formations font intervenir un panel de spécialistes académiques, ainsi que des experts reconnus.

Information et inscription :
par inscriptionsPSD-RMCC@lecnam.net

Présentation du partenariat entre l'Académie du Renseignement et le Pôle sécurité défense

par son directeur François Chambon

L'Académie du renseignement, créée il y a maintenant dix ans, concourt à la formation du personnel de la communauté du renseignement, c'est-à-dire des principaux services de renseignement, mais contribue aussi à la diffusion de la culture du renseignement. À la conjonction de ces deux missions, l'Académie du renseignement est de plus en plus attentive à entretenir des relations avec le monde de la recherche et de l'enseignement. À ce titre, l'Académie du renseignement a notamment pour mission :

– de concevoir, d'organiser et de mettre en œuvre des activités de formation initiale et continue au profit du personnel des services ;

– de favoriser la coopération entre ces services en matière de formation ;

– de participer aux actions de sensibilisation, à proximité et à l'extérieur de la communauté renseignement.

C'est dans ce contexte que le partenariat avec le Conservatoire national des arts et métiers est né, en 2017, avec une ambition transverse. L'objectif premier était de proposer à l'intention des cadres de la communauté du renseignement des parcours diplômants qui peuvent être réalisés en parallèle d'une poursuite d'activité professionnelle et qui s'inscrivent dans les modules de formation de l'Académie du renseignement. La coopération avec le pôle sécurité défense du CNAM sera amenée à s'étendre dans un avenir proche, notamment au vu des besoins identifiés par l'État et la communauté du renseignement, sur l'étude transverse de la thématique « renseignement » à la manière des recherches en *intelligence studies* implantés depuis plusieurs décennies dans les pays anglo-saxons.

Ce partenariat, aujourd'hui bien installé, illustre à la fois la qualité de la relation de confiance nouée entre la communauté du renseignement et le CNAM, mais également l'intérêt que les services de renseignement portent aujourd'hui à la recherche dans le domaine stratégique.

L'enjeu est double : intégrer de nouvelles méthodes de réflexion et d'analyse en enrichissant les formations de l'Académie des apports de la recherche et aller à la rencontre des chercheurs et des étudiants qui peuvent être intéressés par des parcours proposés par les services de la communauté du renseignement.

Crise du Covid-19 la crise de l'anticipation ? La nécessaire modélisation des risques

par Michel Béra et Olivier Lopez

Professeur Michel Béra, titulaire de la chaire de modélisation statistique du CNAM
et le Professeur Olivier Lopez, directeur de l'Institut de statistique de l'université Pierre et Marie Curie (ISUP).

La modélisation statistique est une manière simplifiée et mathématiquement formalisée de décrire un processus supposé aléatoire (ou stochastique) à partir de données pertinentes. L'application des méthodes de modélisation statistique à l'étude des risques a pour grand intérêt de permettre l'élaboration de prédictions à partir de l'approximation de la réalité représentée par le modèle établi. Cependant, les modèles statistiques restent des outils imparfaits dont l'utilisation doit être accompagnée d'une nécessaire humilité face aux aléas de la réalité. Malgré l'existence de grands modèles classiques en épidémiologie (on pense par exemple aux travaux de

Pierre-Yve Boëlle), la recherche désespérée d'un modèle dynamique fiable et fonctionnel au cœur de la crise du SARS-COV-2 nous offre en la matière un sujet d'étude de cas tout trouvé.

La récupération de données stables et fiables fut la première difficulté à laquelle se sont heurtés les statisticiens dans cette entreprise, révélant le caractère illusoire d'un accès facilité aux données à l'ère du big data. Il a fallu tout au contraire aller les chercher, non sans difficulté. Par ailleurs, leur rareté et leur instabilité a rendu le processus de discrimination entre données pertinentes et non pertinentes long et complexe, ce qui, au regard de la situation d'urgence traversée par la France lors de la première vague de Covid-19, a représenté un ralentissement non négligeable de l'effort de modélisation mis en œuvre. Les données relatives à l'épidémie comportaient en effet un certain nombre de biais liés aussi bien au processus de collecte qu'au comportement des acteurs en présence. Un biais supplémentaire lié à l'évolution temporelle de l'épidémie, fortement instable, est enfin venu s'ajouter. Cette instabilité des données pertinentes a représenté un défi de premier ordre pour sa modélisation statistique, qui suppose même dans le cas de processus évolutifs une certaine stabilité permettant de percevoir les prémices des évolutions à venir du modèle – et donc, d'en tirer des prédictions. La présence d'*outliers* ou « valeurs aberrantes » au sein des données recueillies font ainsi rapidement tomber les enseignements tirés de la modélisation dans la conjecture pure et simple.

À ces difficultés s'ajoutent les attentes trop élevées mises sur les modèles, en déconnection avec les réalités de la modélisation statistiques. La situation d'urgence liée à la crise sanitaire a renforcé le poids de ces attentes en faisant des modèles développés le point focal d'un grand nombre de décisions liées à la gestion de l'épidémie.

Cependant, ces difficultés ne se limitent pas à la modélisation statistique en période d'épidémie : on les retrouve ainsi par exemple dans le cadre de la modélisation statistique des cyberrisques, dès lors qu'il s'agit de proposer un modèle décrivant le processus de propagation d'un virus informatique. L'évolution des usages numériques et des comportements des acteurs, encore plus rapide que dans le cadre de l'épidémie de Covid-19, amène les statisticiens à lutter continuellement contre un décalage entre des données recueillies qui deviennent très vite obsolètes si non traitées correctement et l'exigence d'une capacité de prédiction toujours plus éloignée dans le temps.

Concernant l'épidémie de Covid-19, les orientations politiques de la gestion de la crise sanitaire ont eu un impact fondamental sur la qualité et la stabilité des données : retard dans la prise en compte des personnes décédées en Ehpad, délai de plus de trois mois pour recueillir les données concernant les personnes décédées à domicile, incertitude quant à l'intérêt des données concernant les personnes testées positives au SARS-COV-2 par rapport aux données concernant les patients des services de réanimation des hôpitaux… Ces contradictions ont eu pour double effet de complexifier le travail de modélisation des statisticiens et de renforcer la méfiance qu'une partie de la population française nourrissait déjà vis-à-vis du discours scientifique, devenu à leurs yeux simple discours émanant d'experts aussi légitimes que les premiers technocrates venus.

Il est néanmoins possible de renforcer le degré de confiance envers le modèle proposé pour l'épidémie actuelle : la documentation disponible en open data sur le site www.data.gouv.fr permet d'effectuer une généalogie des différentes étapes de construction de la base de données finalement constituée. Cet effort de traçabilité permet aux statisticiens de traiter a posteriori les données de façon pertinente, tout en permettant un calibrage du modèle proposé à l'équilibre entre imperfection des données prises en compte et obtention d'un résultat tout de même valide. La qualité du système de données médicales en France (à travers notamment le Système national de la santé) reste par ailleurs assez remarquable, malgré les défauts de comptabilisation d'un certain nombre de victimes du Covid-19 évoqués plus haut. Enfin, le marché ayant rarement tort face à la modélisation statistique, l'humilité dont savent faire preuve les statisticiens lorsque leur modèle est de facto mis en défaut par les faits nous assure leur capacité de remise en question en cas de nécessité d'adaptation à une réalité mouvante.

La comparaison entre modélisation statistique des risques sanitaires et des risques cyber peut par ailleurs être riche d'enseignements pour chacun de ces champs de recherche. Les virus cyber, contrairement aux virus virologiques humains, sont apparus très récemment dans l'histoire de l'humanité. Malgré le peu de recul que cela engendre sur ce phénomène, on note également que la durée d'une crise épidémique de virus cyber est bien plus courte que la durée d'une véritable crise épidémique. La qualité des données à disposition des chercheurs est assez similaire, mais l'évolution des cybermenaces est en règle générale plus volatile que celle des menaces virologiques. De même, le rôle joué par les acteurs et l'orientation de leur comportement sont décisifs dans un cas comme dans

l'autre, même s'ils sont plus facilement modélisables dans le cas de l'étude des virus cyber.

Ainsi, partant de cette comparaison, on peut par exemple pointer la difficulté spécifique liée à la modélisation de l'épidémie de Covid-19 sur laquelle, contrairement à un certain nombre d'épidémies récurrentes dans l'histoire de l'humanité (grippe notamment), les chercheurs n'avaient encore quasiment aucun recul au printemps dernier. De même, l'importance du comportement des acteurs doit être prise en compte également à l'aune de leur perception du risque qui, même dans les cas d'épidémies virologiques réelles, n'est pas nécessairement très aiguisée (on pense ici à l'exemple édifiant de l'entre-deux-vagues de grippe espagnole en 1918). Par ailleurs, déterminer les facteurs influençant le comportement des acteurs – et donc de prédire son évolution – revient souvent à se pencher sur des variables spécifiques au problème étudié : en l'occurrence, il s'agira pour les statisticiens concernés de prendre en compte les enseignements de l'épidémiologie comportementale en la matière – y compris dans les cas où c'est le modèle lui-même tel que présenté aux acteurs à un instant t qui influence l'évolution de leur comportement à l'instant t+1 !

Il est donc très important de ne pas se laisser aveugler par le modèle, qui n'a pas vocation à remplacer l'oracle de Delphes. Il s'agit simplement, en s'appuyant sur le sérieux de la démarche scientifique qui sous-tend son développement, de pouvoir lui accorder une confiance suffisante pour en faire un outil efficace et performant d'aide à la décision, sans qu'il ne se substitue jamais à l'humain qui, en dernière instance, prend la décision.

Les perspectives organisationnelles et managériales de la sortie de crise

par Patrick Boisselier et Yvon Pesqueux

Professeur Yvon Pesqueux, titulaire de la chaire de développement des systèmes d'organisation du CNAM et le professeur Patrick Boisselier, CNAM.

La question critique de la refonte des modes de management et d'organisation à l'aune des leçons tirées de la crise sanitaire récente suppose tout d'abord un état des lieux des domaines concernés.

Ainsi, il nous faut rappeler que la situation initiale du printemps 2020 avait été fondamentalement impréparée par les États comme par les entreprises, aussi bien sur le plan matériel qu'humain, et les réponses apportées ont été extrêmement contrastées en fonction des pays et des organisations concernées. Si l'on prend l'exemple de l'Allemagne, la réponse a été plus efficace que celles mises en œuvre en France, en Espagne ou encore en Italie notamment du fait de facteurs structurels et organisationnels ancrés dans la culture allemande. Dans les pays latins, le confinement a ainsi été une réponse d'urgence face à l'afflux de malades vers les hôpitaux débordés dans un contexte d'incertitude quasi total vis-à-vis du taux de contamination et de létalité du SARS-COV-2. L'incertitude était d'autant plus forte que les situations très contrastées entre les nombreux pays touchés rendaient vaine tout étude comparative. Ces différences, notamment en termes de nombre de morts, peuvent être reliées à des enjeux d'organisation que nous nous proposons d'étudier aux niveaux macro, micro et méso.

Sur le plan macro, on observe des réponses multiformes sans que ne se dégage un modèle unique pleinement efficace : « laissez faire » en attente de l'immunité collective au Royaume-Uni, ordres dispersés aux États-Unis, absence totale de réponse concrète au Brésil…

Certains facteurs, comme le niveau de centralisation du pays concerné ou la brutalité avec laquelle les mesures sanitaires y ont été imposées ont eu un impact moindre sur l'évolution locale de l'épidémie. D'autres facteurs, par exemple l'importance du clivage entre les niveaux de vie des populations concernées ont en revanche eu un impact bien plus grand : les difficultés d'accès aux soins pour les plus pauvres ont ainsi mécaniquement entraîné une augmentation du nombre de morts au sein des pays les plus clivés socialement. Dans cette perspective, c'est l'organisation des structures hospitalières en fonction des pays qui a été déterminante.

Sur le plan micro, l'organisation des entreprises en interne a été le point essentiel de difficulté tous pays confondus. Les conséquences en ont tout d'abord été humaines, avec un exil massif des populations vers les campagnes (30 % de la population parisienne lors du premier confinement), permis par ailleurs par la massification soudaine du télétravail. Mais les conséquences les plus profondes concernent l'économie : la Bourse a ainsi

connu un crack plus violent que ceux de 1929 ou de 2008, le trafic aérien et le tourisme de masse ont été anéantis, et les difficultés d'approvisionnement rencontrées au cours du premier confinement ont mis en évidence une situation de dépendance économique (notamment vis-à-vis de la Chine) impliquant une nécessaire restructuration de pans entiers du secteur industriel. De plus, l'injection massive de capitaux par les banques centrales dans les milieux financiers a entraîné une nouvelle augmentation de la masse financière, creusant encore davantage l'écart problématique entre masse financière et masse réelle du PIB et augurant par là même une crise financière à venir. Cependant, si beaucoup d'entreprises ont fait ou feront faillite à cause des suites de la crise sanitaire actuelle, certaines ont au contraire saisi l'opportunité de réorganisation massive qui s'offrait à elles pour maintenir, voire développer leurs activités : le paysage entrepreneurial est donc malgré tout contrasté.

Enfin, au niveau méso, la prise de conscience de l'importance du système hospitalier et de la nécessité de voir son coût comme un investissement nécessaire a été fondamentale dans la perspective de sa réorganisation pendant et à la sortie de la crise sanitaire.

Toutefois, il est important de noter que ces leçons durement apprises risquent surtout d'amplifier la crise sociale qui traverse la France depuis 2018 et que la pandémie de Covid-19 n'a calmée que pour un temps. Cette amplification serait paradoxalement le résultat de points par ailleurs considérés a priori comme positifs : un télétravail plus répandu qui rendrait les employés et étudiants plus libres et autonomes et qui en réalité les aliènerait plus qu'autre chose, les promesses de réhabilitation de l'hôpital public ou encore de reconnaissance vis-à-vis des franges de la population souvent démunies qui se sont retrouvées en première ligne en leur qualité de caissiers et soignants qui restent à tenir…

La refonte des organisations dans la perspective d'une sortie de crise doit donc être pensée de manière à englober tous leurs aspects problématiques préalables afin de répondre aux revendications sociales en jeu. Tout d'abord, le regain d'importance de l'espace géographique des nations par rapport à l'espace géographique mondialisé des marchés doit avoir pour conséquence la remise en cause des fondamentaux de la réflexion en stratégie d'entreprise, qui vont devoir s'adapter au prisme géopolitique de « retour des frontières ». Également, la primauté accordée à l'activité économique institutionnalisée sous la forme d'entreprises devra être discutée, avec plusieurs issues possibles : la fin du managérialisme (entraînant ainsi la réarticulation de la place des études de commerce et de gestion au sein de l'enseignement supérieur), la remise en cause de l'éclatement des chaînes de valeur et de la doctrine du « juste à temps », la faillite de la doctrine du *new public management* à l'origine de la confusion entre efficacité, rentabilité et missions de service public, et enfin la reformulation de la responsabilité sociale des entreprises.

Ces différentes issues possibles, si elles demeurent souhaitables, sont cependant dépendantes de décisions à la fois politiques et collectives. La réforme des représentations managériales suppose ainsi par exemple une réforme de représentations culturelles profondes concernant la formation, le rôle et la place des élites dans divers domaines de gestion. De même, la faillite de la doctrine du *new public management*, fragilisée par la récente crise sanitaire, doit nécessairement venir des pouvoirs publics tout en supposant une remise en cause globale de la métrologie comptable actuellement intégrée aux raisonnements des représentants de la nation.

Ainsi, de même qu'un retour vers l'espace géographique de nation en opposition à l'espace géographique de marché mondialisé, la crise sanitaire que nous traversons nous amène vers une remise en cause des catégories issues d'une métrologie purement comptable au profit d'une métrologie et de modalités de gestion plus adaptées à la mission des services publics – et, en priorité, des services publics hospitaliers. Cette métrologie comptable, par ailleurs très présente au sein des directions générales des grandes entreprises, est à interroger dans son ensemble afin que la période post-Covid-19 débouche sur une véritable remise en cause des modèles néoclassiques de management – aussi bien chez les élites économiques que politiques.

Les conséquences À long terme de la crise du Covid-19 sur l'économie française et mondiale

par Rémy Février et Jean-Philippe Denis

Docteur Rémy Février, maître de conférences au CNAM
et le professeur Jean-Philippe Denis, rédacteur en chef de la Revue Française de gestion (RFG).

Il s'agit de replacer cette question dans un contexte stratégique plus large, au contraire de la plupart des analyses qui, proposées à chaud au cœur de la crise, tenaient plus de la réaction immédiate sans plus d'approfondissement. Le concept de paradigme stratégique est fondamental : au même titre qu'un paradigme scientifique, un paradigme stratégique est constitué d'un ensemble d'hypothèses considérées comme allant de soi et guidant l'orientation des actions entreprises par un ou plusieurs agents à la manière d'un réflexe ancré. La principale conséquence de fond de la crise sanitaire que nous vivons depuis bientôt un an a été de voir s'effondrer le paradigme stratégique dans lequel nous agissions et réagissions aux risques jusqu'alors. En effet, la stratégie avance face à l'incertitude, or le principe même d'incertitude nous empêche d'anticiper pleinement les risques : ainsi, ce qui paraît acquis peut à n'importe quel moment être remis en cause, et c'est précisément l'effet produit par la crise du Covid-19 sur le paradigme qui prévalait jusqu'à présent : celui de la mondialisation des marchés. L'héritage de la chute du bloc de l'Est et la montée en puissance de la Chine et de sa nouvelle classe moyenne ont rendu ce paradigme, dans un tel contexte, particulièrement puissant.

Mais le changement de contexte nous amène à repenser jusqu'aux fondations de ce paradigme : ainsi, les pays désindustrialisés qui comptaient jusqu'alors sur les échanges avec leurs fournisseurs à l'autre bout du monde se sont retrouvés en difficulté logistique dès lors qu'il a été question de s'approvisionner, entre autres, en masques chirurgicaux. Cela nous invite à la réflexion quant à la reconstitution d'un nouveau paradigme stratégique plus adapté. De là, nous pouvons nous réapproprier un outil d'analyse qui, bien que parfois sous-estimé notamment en économie, nous offre dans le contexte actuel une puissance analytique extraordinaire : le PESTEL, avec son P pour politique, E pour économie, S pour sociologie, T pour technologie, E pour écologie, et enfin L pour légal.

Pris un à un, ces différents éléments permettent d'éclairer la crise sanitaire en en balayant chaque dimension. Le P de politique nous renvoie à la critique globale de la démocratie, cette dernière apparaissant presque comme un luxe que tous ne peuvent se payer avec le retour des hommes forts et d'une aspiration à l'autoritarisme lié à l'importance toujours plus grande des enjeux de puissance. Ainsi disparaît le « doux commerce » de Montesquieu, auquel fait place le retour de la rivalité sino-américaine, le débat sur la place de l'Europe au niveau mondial, et toutes les conséquences que ce retour en force des enjeux de puissance entraîne (en termes de droit de douanes ou d'enjeux de relocalisation de la production par exemple), et dont la crise sanitaire a surligné l'importance.

Le E d'économie nous amène à nous pencher sur l'effondrement du paradigme sur lequel se basaient jusqu'alors les réflexions des économistes les plus sérieux : taux d'intérêts négatifs et absence d'inflation qui côtoient l'explosion de la valeur d'actifs à certains endroits et des rachats d'actions aux États-Unis qui ont amené les médias à parler d'un grand renversement où c'est maintenant l'entreprise qui finance la Bourse, et non plus l'inverse. Dans un tel contexte, où se multiplient les entreprises de l'« économie zombie » sous perfusion étatique à la suite des diverses restrictions d'ouvertures des commerces et confinements successifs, la valeur même de l'argent comme ressource rare dans le paradigme économique habituel est mise en cause. Les économistes se retrouvent à prédire à l'aveugle tout en tentant de développer, au cœur de la crise, un nouveau paradigme.

Le S de sociologie est, quant à lui, fondamental pour quiconque souhaite analyser la situation actuelle dans son ensemble : de l'extension des nouveaux modes de consommation via internet à l'importance prise subitement par le télétravail au sein des entreprises et administrations en passant par l'émergence d'une aspiration à une plus grande simplicité au cœur des modes de vie ouvrent de nouveaux horizons. Les retombées sur le long terme restent à définir tant leur évolution, jusqu'à présent plus étalée dans le temps, a été fulgurante au cours des derniers mois.

Le T de technologie nous rappelle l'importance prise par ces dernières dans le cadre de l'organisation de la vie de nos sociétés (à travers la question du télétravail notamment), mais également l'augmentation des capacités technologiques qui étaient jusqu'alors réservées aux grandes entreprises et qui, avec l'apparition de smartphones toujours plus puissants et performants, sont maintenant à la portée de chacun avec les avantages et les risques que cela comporte.

Le deuxième E, pour écologie, rappelle de son côté l'importance de la menace du réchauffement climatique et met en avant la difficulté qu'ont encore nos sociétés à gérer et traiter plusieurs risques de grande ampleur à la fois.

Enfin, le L de légal, trop peu intégré dans le paradigme stratégique des entreprises jusqu'à présent. Souvent considéré comme simple droit des sociétés et droit du travail, on a redécouvert à l'occasion de cette crise sanitaire que le droit était d'abord et avant tout une arme : les exemples d'amendes colossales versées ces dernières années aux États-Unis par diverses grandes entreprises non américaines du fait de l'extraterritorialité de leur droit nous rappellent ainsi la puissance d'une telle arme stratégique.

L'un des exemples les plus transversaux de cette nécessité de changement de paradigme se trouve à travers les cyberattaques. Soudainement, sans anticipation, les entreprises, administrations et universités se sont retrouvées à devoir réorganiser tout leur mode de fonctionnement à distance et, ce faisant, ont dû s'équiper des outils informatiques adéquats en urgence. Or, il n'existe pas de logiciel sans faille. Les attaques coupant ou modifiant les flux vidéo menées par divers hackers, parfois par pure malveillance, ont ainsi été légion. Au-delà de ces seules vagues d'attaques, on a également pu observer de nombreuses attaques visant des hôpitaux et centres de soins (en République tchèque, Espagne, Royaume-Uni, États-Unis, France…). C'est un signe critique de ce changement de paradigme où le *gentlemen's agreement* des hackers concernant la sanctuarisation de la vie humaine qui restait jusqu'à présent relativement épargnée par les cyberattaques a volé en éclats. Le but purement financier de ces attaques, survenues sur le modèle classique du ransomware, a ainsi mis en danger de fait de nombreuses vies humaines. Enfin, on peut s'intéresser aux cas de cyberattaques visant des structures de recherche développant un vaccin contre le SARS-COV-2, dont la visée, loin d'être uniquement financière, était également géopolitique et géoéconomique.

Le choc représenté par la hausse des cyberattaques à l'occasion de la crise sanitaire a cependant permis une prise de conscience globale de notre vulnérabilité face à de telles armes. Toutefois, et l'histoire est en cela riche d'enseignements, il s'agit de ne pas se contenter de traiter le seul symptôme à l'immédiate sortie de crise, mais de chercher des solutions sur le long terme à une menace latente qui s'est révélée dans toute sa dangerosité. Il importe donc que nous prenions en main ce changement de paradigme afin qu'y soient intégrées pleinement toutes les menaces que le paradigme précédent ne nous permet pas de penser efficacement. L'intégration des hackeurs dans toute leur diversité au sein de la théorie des parties prenantes pourrait être un premier pas dans le bon sens.

Cet effort de développement d'un nouveau paradigme stratégique ne saurait être efficace sans être accompagné du développement d'une véritable culture stratégique, en accord avec les enseignements de cette dernière crise. Il s'agirait de remettre l'incertitude au cœur des préoccupations, de la culture et de la stratégie globale des entreprises et administrations, précisément afin de la rendre moins exceptionnelle en rappelant qu'elle est toujours latente. Pour ce faire, il est notamment urgent que les cadres et dirigeants d'entreprises et du secteur public soient mieux formés aux enjeux du renseignement économique, peu étudié en France.

La difficile gestion des menaces terroristes durant une pandémie

par Elyamine Settoul et Farhad Khosrokhavar

Docteur Elyamine Settoul, maître de conférences au CNAM et Farhad Khosrokhavar, directeur d'études à l'EHESS (École des hautes études en sciences sociales).

Quel est l'état des lieux de la radicalisation aujourd'hui en France, cinq ans après les événements tragiques de *Charlie hebdo* et à l'aune du débat sur le séparatisme ?

La neutralisation militaire de l'État islamique en 2017 eu un impact sur les phénomènes de radicalisation en France et en Europe ; il ne faut cependant pas surestimer cette disparition territoriale, l'idéologie perdurant au Califat. À son apogée en 2015, le territoire dont il disposait était équivalent à celui de l'Angleterre, avec entre 10 et 12 millions d'habitants sous son égide. C'est un véritable État qui s'est constitué, attirant une trentaine de milliers de jeunes du monde musulman, et environ 6 000 à 7 000 Européens. Les statistiques de l'adhésion des jeunes à l'islam radical en France démontrent le pouvoir d'attraction de l'État islamique, et l'importance de son implantation territoriale : entre 2000 et 2013, on dénombre environ 175 départs de jeunes pour faire le djihad au Moyen-Orient, contre 1 900 sur la seule période 2013-2016. L'augmentation de ces vocations n'est pas le fruit d'événements extraordinaires qui se seraient déroulés en France ou en Europe mais bien de l'établissement et de l'expansion de l'État islamique.

D'un point de vue idéologique, Daesh et Al-Qaïda diffusent un discours rela-

tivement semblable. La différence se situe au niveau du prestige incarné par le Califat, ainsi que sa violence de loin supérieure à Al-Qaïda. Aujourd'hui neutralisé d'un point de vue militaire et territorial, l'influence idéologique semble perdurer.

Pour lutter contre la radicalisation à tous les niveaux (prévention et resocialisation), il faut d'abord faire une lecture correcte du phénomène et s'intéresser au profil des personnes radicalisées, en brosser leur portrait sociologique. Les musulmans de classes populaires représentent la majorité de ces individus. Partout en Europe, des quartiers précis ont été des pourvoyeurs importants de candidats au départ avec pour une large part d'entre eux l'exclusion sociale et la ghettoïsation ethnique.

Le but n'est pas ici de retracer l'histoire des migrations musulmanes en Europe, mais il faut garder en mémoire que les États, notamment la France, ont incité les premières générations à migrer dans un souci de manque de main-d'œuvre et que les suivantes se sont ensuite heurtées à un chômage massif. La modernisation du modèle industriel français dans les années 1970-1980 a entraîné une réduction structurelle des emplois d'ouvriers non qualifiés.

La paupérisation de ces individus et le désintérêt des pouvoirs publics pour les problématiques urbaines et sociales ont conduit à une concentration de jeunes d'origine immigrée dans des quartiers de plus en plus homogènes du point de vue ethnique. L'absence de perspective d'avenir et le sentiment de stigmatisation poussent ces jeunes vers l'économie parallèle et donc la délinquance. L'anomie fait ensuite un excellent terreau pour la radicalisation et non pas seulement au sein des classes populaires de banlieues, les petites classes moyennes, écrasées par le haut et le bas, souffrant également.

Avec l'anéantissement territorial de Daesh, la problématique centrale n'est plus le départ d'individus radicalisés vers la Syrie ou l'Irak, mais bien leur retour. La France, comme d'autres pays, doit faire face dès maintenant à la question des *returnees* (environ 300 individus partis faire le djihad en Irak ou en Syrie). À cela s'ajoute la sortie d'incarcération d'individus radicalisés. La prison, et particulièrement la maison d'arrêt, est une sorte d'école de la radicalisation où la haine est sacralisée. En cause, la surpopulation carcérale mais aussi une proportion de musulmans (environ la moitié des détenus) bien plus élevée que dans la population française (estimé à seulement 6 %). On retrouve le même schéma d'homogénéité ethnique que dans les banlieues.

La question du séparatisme est aujourd'hui au cœur du débat public : peut-on parler de logiques séparatistes dans certains territoires de la République ? Il s'agit d'un débat purement idéologique. La notion même de séparatisme signifieraient que certains acteurs sociaux auraient des velléités de conquête et suffisamment de pouvoir pour y prétendre. Le séparatisme prend acte d'une séparation réelle en termes de géographie et de stigmatisation de la part de la société globale à l'égard de ces jeunes. Il est reproché aux salafistes de ne pas se mélanger (par la scolarité, le mariage, etc.), mais cette forme de séparation, de mise à l'écart, se produit déjà dans leurs conditions de vie. Il s'agit pour ces individus de prendre acte de manière agressive d'une situation de fait qui leur est imposée. Ils entérinent une situation préexistante en lui donnant un contenu nouveau : ils s'affirment dès lors eux-mêmes comme différents. Il s'agit d'un processus d'inversion des stigmates, pour reprendre le vocabulaire d'Erving Goffman. Le salafisme permet ainsi à des individus stigmatisés et qui n'entrevoient pas de perspective d'avenir, de donner un sens actif à une situation passive.

Pour lutter contre ces formes de sectarisme salafiste, la solution n'est pas de diaboliser davantage ces individus, qui seraient alors confortés dans leur sentiment de différence. Diaboliser le salafisme c'est accroître son degré de crédibilité en regard des populations stigmatisées. Comment s'étonner, avec une telle logique d'exclusion sociale, de rejet de la part de la société et de diabolisation de ces quartiers dans les médias, que ces populations souhaitent faire bande à part ?

Le salafisme est une manière de sacraliser le phénomène de faire bande à part, de s'affirmer contre une société qui exclut et enferme dans une situation d'infériorité insurmontable. Cette attitude n'est pas uniquement liée à l'islam, il s'agit plutôt d'une contre-sécularisation qui s'effectue au nom d'un islam d'importation dont les traits antagoniques vis-à-vis de la société française sont accentués. Il est essentiel de comprendre cela pour pouvoir lutter efficacement contre cette logique de repli sur soi et d'exclusivisme.

Dès lors que l'on a pleinement appréhendé le processus de radicalisation, la réponse pour lutter contre ce phénomène semble évidente. Les leviers sont principalement socio-économiques, également en termes de politiques urbaines, avec comme objectif un changement fondamental des conditions sociales d'insertion de ces individus dans la société. Pour qu'ils deviennent des citoyens à part entière, encore faut-il leur donner la possibilité d'exercer leur citoyenneté. ◗

La réponse de l'Union européenne à la crise du Covid-19

par la professeure Nicole Gnesotto et l'ambassadeur Baudouin Baudru,
chef de la représentation de la Commission européenne en France

L'Union européenne a produit une réponse très critiquée à la crise du Covid, car arrivée trop tardivement, mais qui s'est finalement montrée audacieuse, voire historique, avec un plan de relance inédit de 750 milliards d'euros. Cette défaillance initiale a une nouvelle fois révéler les insuffisances et les défauts structurels du modèle décisionnaire et des institutions européennes. Elle a fortement terni son image dans une addition de crises requérant plus que jamais sa présence visible dans le quotidien des citoyens européens. Afin de penser l'avenir, l'UE devra pérenniser et approfondir la coopération entre ses institutions clés, sans quoi elle se retrouvera dans l'incapacité de répondre rapidement aux prochaines crises, notamment environnementale.

Vis-à-vis de la crise du Covid-19, l'Union européenne a été capable du pire comme du meilleur. Les institutions ont tout d'abord minimisé cette crise et ses impacts, et ont fait preuve d'incrédulité avec un premier plan de seulement 24 milliards d'euros. Les sollicitations de l'Italie, premier pays européen touché par l'épidémie, sont restées trop longtemps sans réponse, alors même que la situation devenait critique. Ce n'est que six semaines après l'apparition des premiers cas, que l'Union européenne et ses institutions vont enfin prendre conscience de la gravité de cette crise et de la nécessité d'une action concertée. Le 12 mars, les pays membres arrivent à un accord inédit sur un plan de relance de 750 milliards d'euros : Next Generation EU. Il est nécessaire de comprendre pourquoi la réponse européenne est arrivée aussi tardivement et de tirer des leçons de cet échec afin de mieux anticiper les crises futures.

Premièrement, l'Europe n'a pas de culture du risque et c'est une lacune importante des institutions communautaires. Ce sont les États qui, traditionnellement, disposent de cette culture du risque (guerres, crises économiques, etc.). L'Union européenne est, elle, maître dans l'art des longues négociations, et se retrouve ainsi désemparée quand elle doit agir dans l'urgence. Il est donc impératif de réinsérer cette culture du risque au sein de ses institutions.

Les États membres n'ont quant à eux pas mieux réagi. Ils se sont en effet refermés sur eux-mêmes sans aucune concertation, fermant par exemple leurs frontières sans en avertir la Commission ou encore en s'appropriant des stocks de masques à destination d'autres pays. Enfin, il faut souligner les nombreuses oppositions à un plan de relance incluant une mutualisation de la dette, autrement dit à une solidarité fiscale. Le constat est sans appel, contrairement à ce que prévoyaient Schuman et Monnet, soixante-dix ans d'intégration européenne n'ont pas créé de solidarité de fait. Dès lors que la situation est critique, les États optent à nouveau pour le chacun pour soi. Pourtant, la crise du Covid-19 a démontré que l'Europe était seule et ne pouvait donc compter que sur le fonctionnement de l'Union européenne, son alliance de sécurité avec les États-Unis se révélant distandue.

La solidarité n'est donc pas spontanée au sein de l'UE, la présidente de la Commission, Ursula von der Leyen, s'est elle-même excusée auprès de la population italienne reconnaissant que trop peu avait été fait pour générer cette solidarité. Si les institutions communautaires ont tardé à réagir ce n'est pas seulement à cause d'une minimisation des risques. Leurs compétences en termes de santé publique et les moyens budgétaires mis à leur disposition ne sont pas appropriés pour répondre à une crise sanitaire d'une telle ampleur. L'UE n'a en effet pas de compétence à proprement parler en matière de santé, uniquement des compétences de soutien aux États membres et de coordination (art. 168 du Traité sur le fonctionnement de l'UE). Quant aux moyens, pour la période 2014-2020, le budget total était de 449 millions d'euros pour l'ensemble de l'Union, soit 12 € par an et par personne. Les États membres dans leur grande majorité n'ont pas souhaité transférer aux niveaux des institutions communautaires une compétence forte en matière de santé publique. Dotées de compétences et moyens budgétaires totalement insuffisants, elles n'ont ainsi pas pu répondre à l'urgence de la situation.

Après une période de léthargie, l'Union européenne, ayant pris la mesure des enjeux, a lancé une série d'initiatives au caractère inédit et historique. Les États ont ainsi été autorisé à s'endetter au-delà des limites imposées par le Pacte de stabilité et de croissance afin de soutenir massivement les économies et les systèmes de santé. Une flexibilité considérable dans les aides d'États a également été introduite afin d'éviter une vague de faillites d'entreprises. Enfin, le plan Next Generation EU prévoit que la Commission européenne emprunte jusqu'à 750 milliards d'euros sur les marchés financiers pour prêter cet argent aux États membres à un taux extrêmement bas.

Il faut souligner l'importance du couple franco-allemand dans l'impulsion et les négociations de ce plan de relance. La crise du Covid-19 montre, une fois de plus, que ce couple est un axe essentiel à la vitalité de l'UE et à ses ambitions. Le fait politique européen de cette année est sans aucun doute le changement d'attitude de l'Allemagne : elle abandonne un principe de discipline budgétaire qui a caractérisé sa position européenne depuis toujours. Autre fait nouveau, la République fédérale se positionne de plus en plus sur des questions de géopolitique.

Finalement, si la crise sanitaire a révélé une absence de solidarité de fait et des réticences face à une réponse concertée, elle a également rappelé à ces membres que l'Europe des nations serait une Europe plus pauvre, ce que personne ne souhaite. Les pays originellement réticents à ce plan de relance incluant une mutualisation de la dette l'ont finalement accepté, prenant conscience des pertes

qu'occasionnerait l'effondrement d'une partie de la demande européenne.

Qu'adviendra-t-il une fois ce plan de relance ratifié par les parlements nationaux et l'argent distribué ? Reviendrons-nous à l'Europe d'avant, celle des critères de Maastricht et du Pacte de stabilité et de croissance ou assisterons-nous à une remise en question de ces postulats, à la refonte des grands principes européens ? Le débat doit se poursuivre, car l'Union européenne et ses institutions seront bien sûr challenger par de nouvelles crises, notamment environnementale.

Conclusion Générale des Assises de la recherche stratégique 2020

par Laurent Nunez, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT).

La pandémie du Covid-19 a bouleversé nos vies quotidiennes, notre économie, notre système de santé ainsi que nos rapports sociaux, conséquence des mesures de restriction de circulation qui ont dû être imposées pour endiguer la progression de la maladie. Ce virus a également eu un impact sur les menaces et sur la délinquance. Depuis le début de la crise sanitaire, et notamment pendant la période de confinement qui a significativement réduit les déplacements, dont les flux internationaux, la délinquance a pris d'autres formes, pour s'adapter à cette nouvelle situation. La baisse des trafics de stupéfiants en est un exemple saillant, à la fois au niveau de la vente au détail mais aussi de l'importation des produits vers le territoire national, dû à la restriction des moyens de communication aériens mais aussi interfrontaliers par transport routier.

La crise sanitaire a fait évoluer la morphologie de la délinquance. Si elle a diminué sous sa forme traditionnelle (violence, cambriolage, etc.), elle s'est exprimée autrement. Les atteintes aux biens ont par exemple chuté, mais se sont concentrées sur un certain type de commerces, que l'on peut qualifier de stratégique dans ce contexte épidémique, tel que les pharmacies ou les producteurs de matériels sanitaires. Les entreprises porteuses de technologies et savoir-faire d'intérêt ont également fait l'objet de prédations. Ce type de menace persiste, la situation sanitaire étant toujours instable. Les services de renseignement restent ainsi attentifs à toute velléité, tentative de captation de savoir-faire en matière de traitement médicamenteux et de recherche médicale. Ces menaces, si elles ne sont pas nouvelles, sont cependant bien plus prégnantes depuis le début de la crise du Covid-19. Cette réorientation de la délinquance a nécessité une adaptation rapide des forces de sécurité.

La numérisation du monde et des communications, si elle est vectrice de progrès, porteuse d'amélioration de la qualité de vie, des échanges et de leur rapidité ainsi que du public touché, engendre de nouveaux risques, appelés de manière générique cybermenaces. Ces menaces qui se matérialisent sous des formes variées, se sont développées de manière exponentielle ces dernières années. Elles sont généralement le fait de groupes criminels, parfois même de puissances étrangères dans un but de déstabilisation étatique ou encore de groupes terroristes qui utilise ces cyberattaques pour porter atteinte à la souveraineté d'un État. Le développement des réseaux sociaux et des communications numérisées permet à certains groupes animés de mauvaises intentions de se structurer et de communiquer rapidement, parfois sans être détectés par les services de police et de renseignement grâce à la cryptographie. Pendant la crise sanitaire, la puissance de diffusion des réseaux sociaux a facilité la propagation de fausses informations, la décrédibilisation de la parole publique et l'élaboration de discours de contestation allant jusqu'au complotisme.

Face à ces nouvelles menaces, l'ensemble des services de sécurité (renseignement, police et gendarmerie) se sont adaptés ces dernières années, en développant des départements cyber et en augmentant leur capacité de détection dans le cyberespace. Les services de polices judiciaires ont également développé des techniques d'investigation propres au numérique. Les plateformes de signalement sont une des méthodes de riposte des pouvoirs publics, à l'image de Pharos mise en place par la Direction centrale de la police judiciaire pour centraliser les signalements de contenus illicites sur internet.

La conjugaison de deux phénomènes plus ou moins récents, crise sanitaire et cybermenaces, a fait émerger de nouvelles problématiques sécuritaires. La capacité d'adaptation et d'anticipation, tant des services de renseignement que des services répressifs, s'avère alors primordiale.

Enfin, la question de la responsabilité est commune face aux menaces cyber et sanitaires. Il convient aux citoyens d'appliquer des gestes barrières pour limiter la propagation du virus Covid-19, mais également contre les cyberattaques par leurs comportements vis-à-vis des outils informatiques, par la gestion des messageries électroniques ou encore des transmissions. Les mesures prises par l'État contre l'épidémie du Covid-19 (restrictions de circulation entre autres) et contre les risques cyber (obligation pour les opérateurs de réseaux sociaux de supprimer les contenus illicites) constituent des restrictions de liberté mais sont rendues nécessaires compte tenu des menaces qui peuvent exister.

Découvrez le dernier numéro de la revue *CONFLITS*

Chez votre marchand de journaux ou sur le site www.revueconflits.com