ÉTATS DE CHOC

L'intelligence économique au service des organisations

major

Photos couverture © Marek Piwnicki via Unsplash

Média en ligne créé en 2021, Major se donne pour mission de mettre l'intelligence économique et la cybersécurité, leurs enjeux et leurs bonnes pratiques à la portée des entreprises et organisations de toutes les tailles. Major analyse aussi bien les grandes tendances de la cybersécurité d'entreprise et de la protection des affaires, que les évolutions à l'œuvre en matière de souveraineté économique, ou les perspectives et opportunités stratégiques offertes par différents secteurs d'activité.

Pour en savoir plus : **www.major.com**

major

ÉTATS DE CHOC

L'intelligence économique au service des organisations

Sommaire

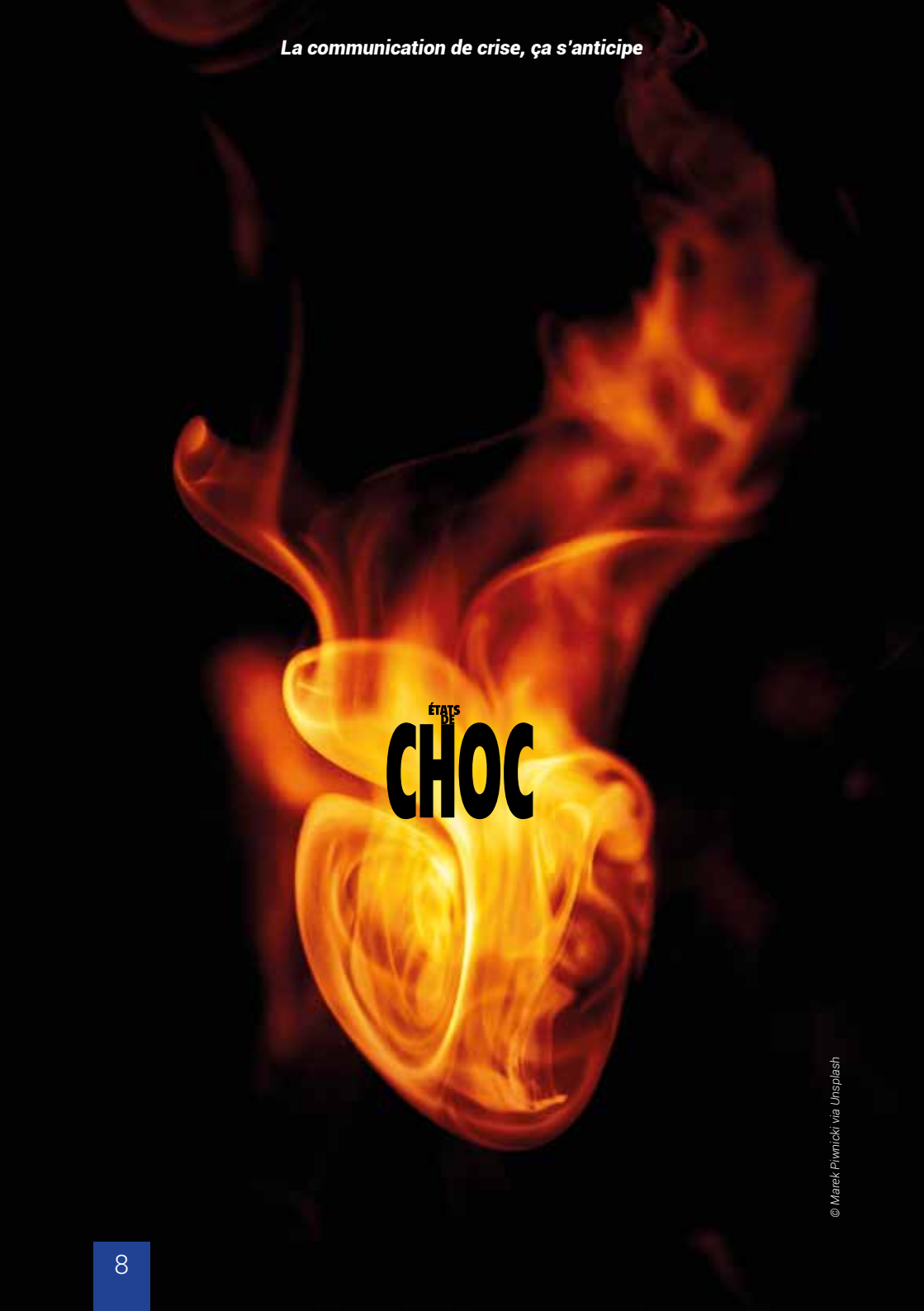

ÉTATS
DE
CHOC

La communication de crise, ça s'anticipe

DOSSIER N°15 ■ 9 mai 2022

Comme en a témoigné l'exemple d'Orpea, communiquer en situation de crise est une mission périlleuse. Pourtant, pas question de laisser passer l'orage sans réagir. Pour réussir cet exercice d'équilibriste, les organisations doivent travailler en amont pour se préparer au mieux. Message à faire passer, timing et canaux de communication : rien ne doit être laissé au hasard. La rédaction de Major a pensé ce dossier comme un guide afin d'accompagner les entreprises de toutes tailles dans leur communication de crise. Quand et comment se former ? Quelles erreurs éviter ? Quels acteurs mobiliser ? Ces articles, vidéo et bibliothèque de contenus devraient vous aider à vous approprier ce sujet crucial.

© Andrei Slobtsov via Unsplash



© Marek Piwnicki via Unsplash

4 questions pour organiser ses équipes de communication de crise

Géraldine Russell ■ 9 mai 2022

Une bonne répartition des rôles de chacun permet de garder la maîtrise du temps et du discours. Alors, avant et pendant la crise, qui doit faire quoi ?

© Prostock-Studio via iStock

« La communication de crise consiste à maîtriser au mieux la situation, en un minimum de temps et sous un maximum de pression, et à le faire savoir », résume Jean-Marc Atlan, associé du cabinet spécialiste de la communication Ekno. Or, l'un des enjeux de cette maîtrise, c'est de pouvoir compter sur une équipe solide.

QUI DOIT SE CHARGER DE LA COMMUNICATION EN SITUATION DE CRISE ?

« Pour limiter l'effet de surprise, il faut organiser à l'avance la gestion de la communication. Qui sont les experts thématiques à mobiliser ? Qui doit faire partie de la cellule de crise ? Qui parlera en public ? », liste Jean-Marc Atlan. « C'est en priorité l'équipe dédiée – s'il y en a une – qui va porter le volet communication », répond Stéphanie Ledoux, fondatrice de l'agence Alcyconie, spécialisée dans la gestion de crises cyber.

« Les ressources humaines, l'équipe technique ou les chargés de comptes clients peuvent être mobilisés sur des points spécifiques également. » Cette pluralité est indispensable pour avoir accès à toutes les expertises, notamment dans le cas de crises techniques. Par exemple, « lors d'une crise cyber, les personnes qui portent la parole de l'entreprise doivent être formées pour ne pas commettre d'impair », illustre la fondatrice d'Alcyconie. De la même manière, si des infrastructures techniques d'un fournisseur d'énergie sont touchées, ce seront les experts qui fourniront les éléments-clés concernant le rétablissement du service.

QUI DÉCIDE DE LA STRATÉGIE DE COMMUNICATION À MENER ?

Le terme même de crise, dérivé du grec krisis qui signifie « jugement », renvoie à l'importance de la décision. « Lors d'une crise, tout le monde a peur de faire une bêtise. Le pouvoir de décision est une vraie problématique », observe Jean-Marc Atlan. Il est donc indispensable de définir, lors de la cartographie des risques, la chaîne décisionnelle, y compris en matière de communication. « Avoir quelqu'un en interne qui décide de la posture à adopter sert la cohérence des méthodes et du discours », atteste Stéphanie Ledoux. « La cellule de crise doit disposer d'une personne qui a le pouvoir de décision et peut trancher rapidement : la direction de l'entreprise, ou du site concerné, ou quelqu'un qui a un pouvoir de représentation, comme un directeur des ressources humaines », suggère l'associé d'Ekno. Dans tous les cas, quelqu'un « qui a la légitimité pour décider ». Les entreprises les plus précautionneuses nommeront même un suppléant, si le décideur pré-déterminé n'était pas disponible.

LA DIRECTION DE L'ENTREPRISE DOIT-ELLE FORCÉMENT ÊTRE IMPLIQUÉE ?

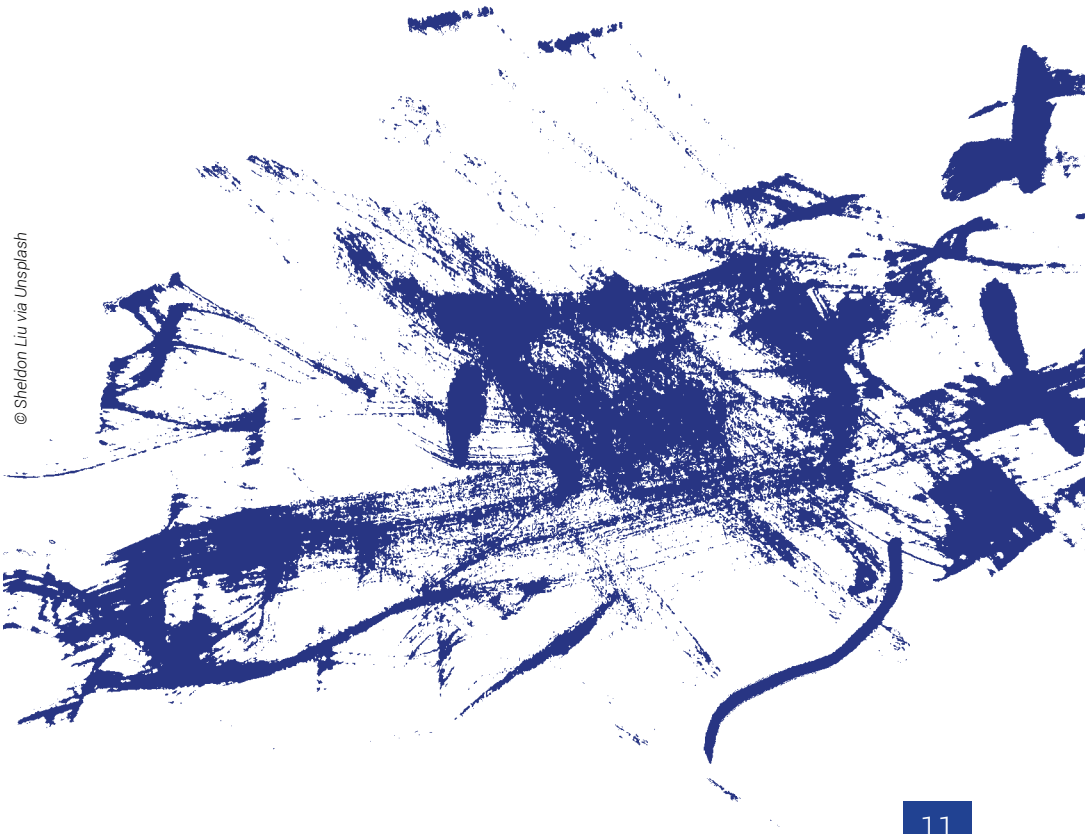
La réponse dépend de la taille de l'entreprise. Dans les TPE-PME, « la décision remonte vite au dirigeant », constate Jean-Marc Atlan. Pourtant, l'expert conseille de « le garder comme recours en cas d'escalade médiatique de la crise ». Mieux vaut ne mobiliser le dirigeant qu'en cas de crise grave, insoluble par un autre collaborateur. Cela permettra de calmer le jeu en montrant que l'entreprise passe un cap dans sa communication.

Dans les grands groupes, une communication très centralisée pose d'autres problèmes. « Dans le cas où la maison-mère n'est pas dans le pays où se situe la crise, il faut penser au décalage horaire, aux différences de culture, aux problèmes de traduction des contenus », alerte Laurent Vibert, fondateur de l'agence Nitidis, spécialiste de la communication de crise. Mieux vaut donc déplacer le centre de décision au plus près de la crise. « Le décideur doit être celui qui porte la responsabilité de la crise, par exemple le directeur du site où la crise se déclenche. Il doit avoir les mains libres. »

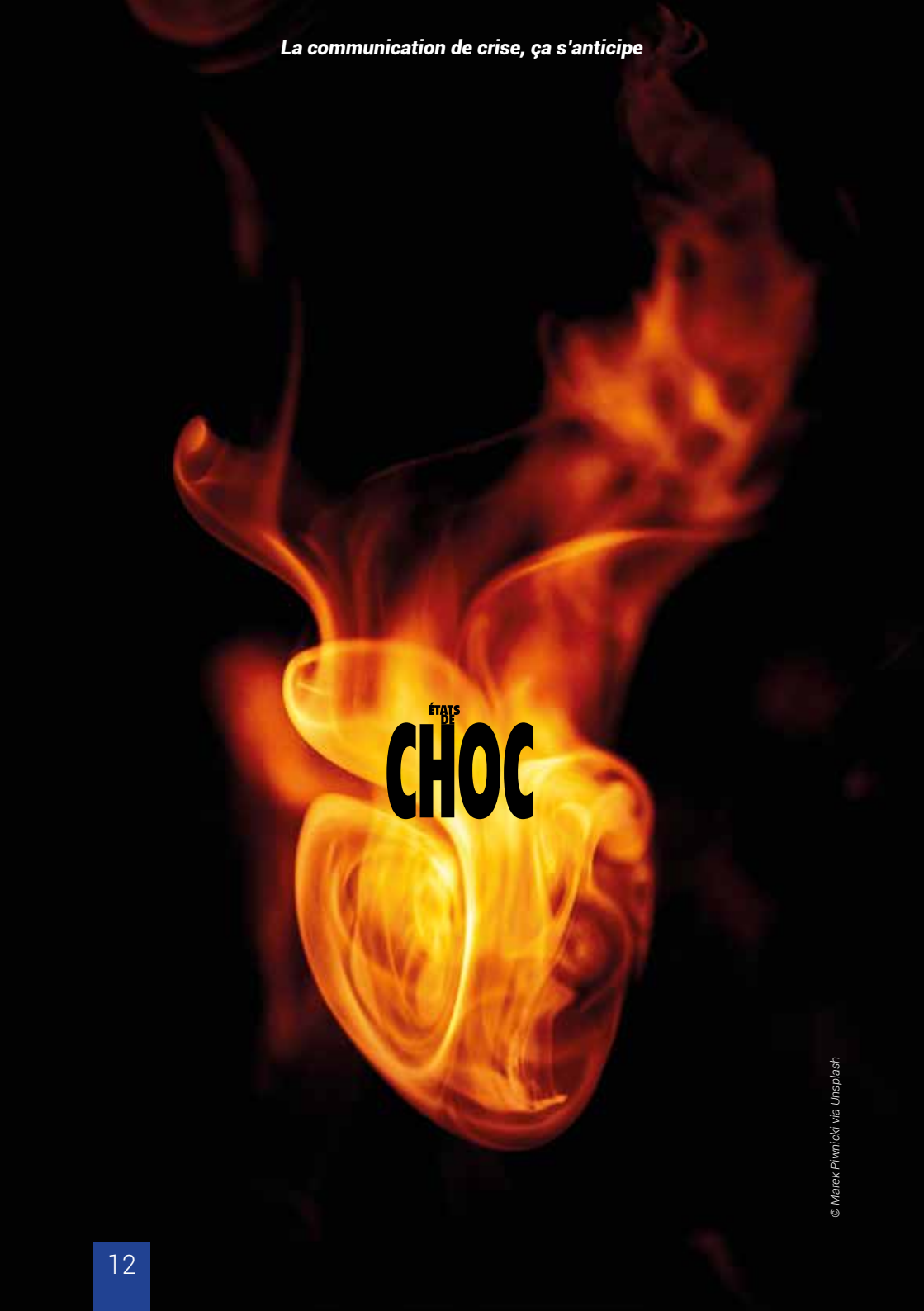
QUAND FAIRE APPEL À UN PRESTATAIRE EXTÉRIEUR ?

Parfois, l'entreprise ne dispose pas de toutes les compétences nécessaires en interne. Parce que la communication de crise impose des ressources pléthoriques. « Rester en veille, définir des éléments de langage, rédiger les supports de communication… Tout cela est hautement consommateur de ressources », observe Stéphanie Ledoux. « Avec la pression médiatique et les demandes entrantes à gérer, toutes les entreprises n'ont pas les ressources en nombre suffisant », ajoute Jean-Marc Atlan. Recourir à des agences ou cabinets experts permet donc de démultiplier les bras disponibles.

Mais aussi les cerveaux à mobiliser. C'est un moyen « d'ouvrir le champ des possibles », estime Laurent Vibert. « Ce qui peut paraître urgent à l'entreprise ne l'est pas forcément. Un prestataire extérieur a cette capacité à prioriser l'importance des différentes communications, tout en délivrant l'entreprise du poids hiérarchique, fonctionnel ou émotionnel des enjeux de la crise. » Pour rester maître en sa demeure, il faut parfois savoir déléguer. ■



© Sheldon Liu via Unsplash



© Marek Piwnicki via Unsplash

Bien préparer sa communication de crise en 3 étapes

Géraldine Russell ■ 9 mai 2022

© WeeDezign via iStock

Anticiper est crucial pour ne pas perdre ses moyens lorsque la crise survient. Les entreprises doivent jongler entre des procédures balisées et une certaine flexibilité pour réagir rapidement et efficacement.

La crise est-elle « devenue la normalité » ? En matière de communication, « les entreprises vivent une situation de crise permanente », confirme Jean-Marc Atlan, associé au sein du cabinet de communication Ekno. « Mais cela ne veut pas dire qu'il y a plus de crises qu'avant », nuance-t-il. C'est en fait la multiplication des instruments de mesure et de diagnostic, mais aussi la viralité des réseaux sociaux, qui amplifient le bruit des crises, ainsi que leurs conséquences.

Pour autant, considérer n'importe quel incident mineur comme une crise potentielle serait contre-productif. « La crise est un événement qui affecte l'entreprise au point qu'elle n'est plus en capacité de poursuivre, au moins sur un périmètre significatif, ses activités. Elle a un caractère exceptionnel

et associe des problématiques de continuité d'activité à des répercussions médiatiques, réputationnelles, juridiques », décrit Stéphanie Ledoux, fondatrice d'Alcyconie, cabinet de gestion de crise spécialisé dans les crises cyber. Contrairement à une mauvaise passe, la crise met en péril la légitimité ou la survie de l'entreprise à court terme. Pour ne pas risquer la sortie de route, mieux vaut être bien préparé.

ÉTAPE 1 : IDENTIFIER LES CRISES POTENTIELLES

Première étape : « identifier les crises auxquelles l'activité de l'entreprise l'expose, les enjeux qu'elles recouvrent et la façon de communiquer si elles surviennent », conseille Jean-Marc Atlan. De cette cartographie découle la réponse à apporter, en interne, en externe mais aussi en matière de communication réglementaire – comme dans le cas d'une violation de données personnelles, qui impose d'alerter la Cnil. L'exercice permet aussi d'éviter « l'effet domino qui réside dans l'addition de plusieurs facteurs de crise », prévient Laurent Vibert, fondateur de l'agence de communication Nitidis. « L'objectif d'une communication de crise réussie est de circonscrire le plus tôt possible la crise à un seul facteur. »

Cette cartographie doit intégrer les deux grands types de risques : les crises d'opinion – qui portent sur les activités de l'entreprise – et les crises accidentelles. Pour les premières, « l'idéal est de se préparer sur le fond en s'interrogeant sur les sujets qui peuvent devenir critiques », précise Jean-Marc Atlan. Ils peuvent être transversaux (financiers, sociaux, RH) ou liés au secteur d'activité de l'entreprise. « Cela permet d'avoir des éléments de langage pré-établis, quelques phrases-types préparées en concertation avec les juristes et les équipes opérationnelles », détaille Stéphanie Ledoux.

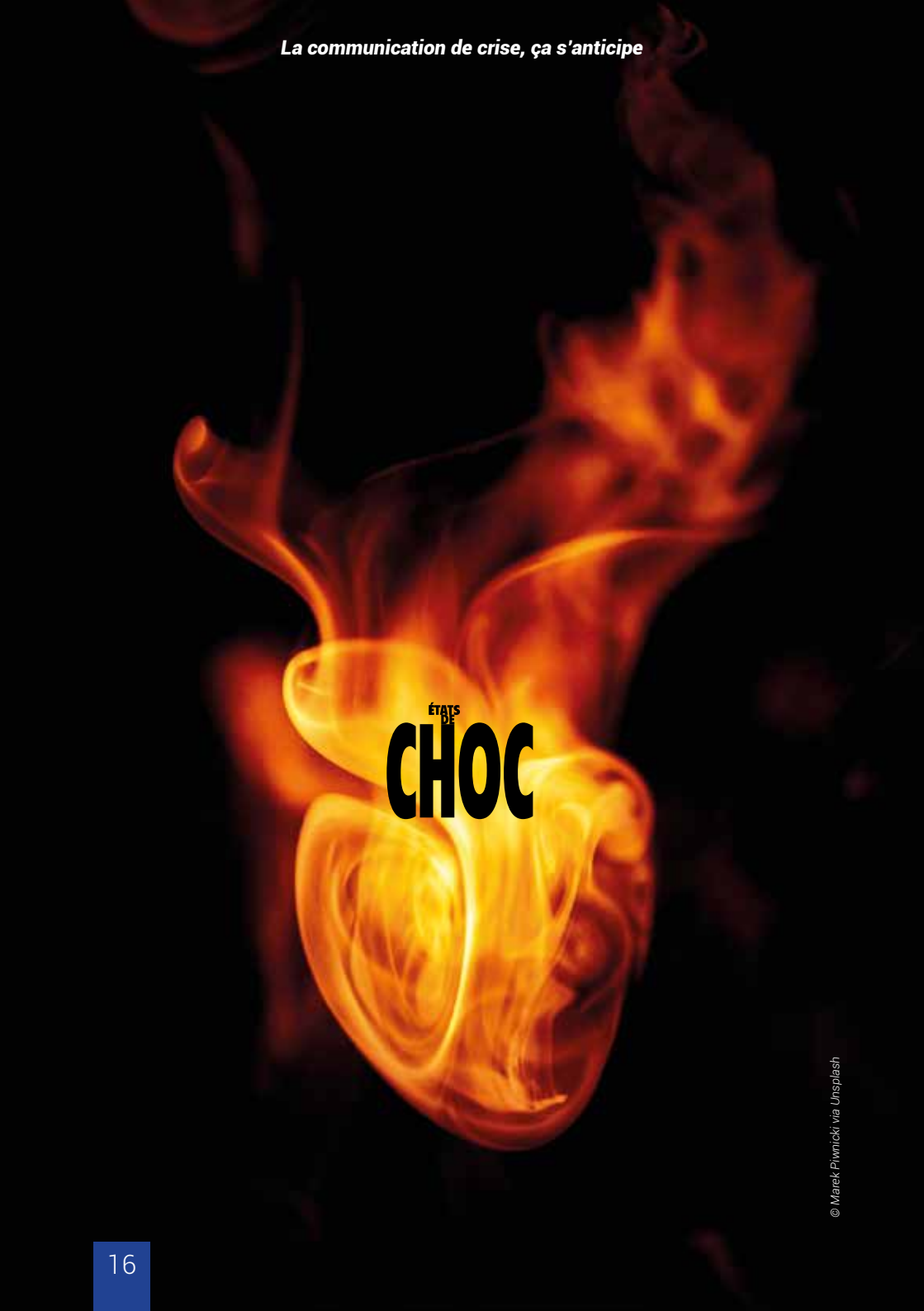
ÉTAPE 2 : RÉFLÉCHIR À DES DISPOSITIFS OPÉRATIONNELS

« La communication constitue un des piliers de la gestion de crise », rappelle Laurent Vibert. Elle doit donc être intégrée aux procédures de réponse à la crise. L'objectif ? « Éviter l'effet de surprise, parce qu'il paralyse les décideurs », observe Jean-Marc Atlan. Préparer des procédures à suivre lorsque la crise survient doit être un élément-clé des plans de continuation d'activité. « Tout ce qui permet de gagner du temps et de maîtriser les choses dans des conditions de très forte pression est un bon point », souligne l'associé d'Ekno. Et cela passe autant par de grandes interrogations (qui doit porter le volet communication de la cellule de crise ?) que de petits détails (où l'équipe communication peut-elle se réunir pour résoudre la crise ?). Dans le cas d'une crise cyber qui priverait l'entreprise de moyens de communication internes, par exemple, des questions très pragmatiques se posent à l'entreprise : quel canal utiliser ? Comment transmettre les premiers éléments aux employés, aux partenaires ou aux clients ? Tout cela doit être prévu en amont.

Dans le cadre d'une crise accidentelle, ces procédures aident également l'entreprise à ne pas commettre d'impair. « Les communications de crise ratées le sont dès les premières prises de parole parce que des organisations non préparées diront des bêtises dont elles ne pourront pas se remettre », estime Jean-Marc Atlan. C'est le cas d'Orpea, qui a récemment dû faire face à la publication d'un livre-enquête révélant des maltraitances au sein des établissements du groupe. Première réaction du groupe ? Nier l'évidence et invoquer de possibles poursuites en justice. En étant sur la défensive, l'entreprise n'a fait qu'attiser les doutes et les ressentiments sur un sujet hautement inflammable.

ÉTAPE 3 : S'ADAPTER

Tous ces éléments doivent aider l'entreprise à conjurer l'effet de paralysie lorsque la crise survient. Mais il convient de les adapter à chaque situation. « Il faut à tout prix éviter les copiés-collés dénués d'empathie et qui ne cadrent pas avec la situation en cours, juge Laurent Vibert. La communication de crise est autant une affaire d'anticipation que de modélisation : il faut être capable d'imaginer ce que seront les effets de la crise demain, dans un mois comme dans trois. » De nombreux outils existent désormais pour rédiger, programmer ou mesurer l'effet des éléments de langage mais aucun robot n'a la flexibilité et l'empathie d'un humain. ■



© Marek Piwnicki via Unsplash

Communication de crise : 3 réussites dont s'inspirer

Géraldine Russell ■ 9 mai 2022

Certaines entreprises ont su déjouer les pièges de la communication de crise avec brio. Voici 3 exemples à copier.

SAINT-GOBAIN ET LA CRISE DU CORONAVIRUS (2020)

En mars 2020, quand la France décrète un confinement drastique en réponse à la pandémie de Covid-19, les activités du groupe Saint-Gobain sont durement affectées. Contrairement à d'autres entreprises qui ont tardé à réagir – seules 10% des entreprises avaient communiqué en interne sur les mesures sanitaires avant le premier confinement, selon une étude réalisée par l'agence Qapa en mars 2020 – Saint-Gobain a d'emblée pris le parti de la transparence. Dès le premier jour, le président du groupe s'est exprimé auprès de l'ensemble des salariés. « Le top départ d'une stratégie volontariste de sur-communication en direction de nos publics internes », a raconté la directrice de la communication du groupe, Laurence Pernot, au blog The Brand New, spécialisé dans la communication des marques. « Montrer un management mobilisé, à la barre, partageant les décisions prises chaque jour était essentiel pour répondre à ces objectifs de réassurance et de maintien de la dynamique. »

Tout au long des périodes de confinement puis de déconfinement, la direction a tenu les salariés informés des mesures sanitaires à respecter et de l'évolution de l'activité. Saint-Gobain a réparti entre son président et son directeur général les différentes prises de parole : au premier « la vision stratégique » donnée à chaque tournant de la crise (prolongement du confinement, déconfinement et les fluctuations de l'activité qui allaient avec), au second « la gestion opérationnelle de la crise » au quotidien.

Ce qu'il faut retenir : soigner la communication interne. Il est primordial de soigner la communication interne. « Beaucoup d'entreprises oublient la communication interne pour se concentrer sur l'externe et leur image : c'est une maladresse fréquente », résume Stéphanie Ledoux, fondatrice de l'agence de gestion de crise Alcyconie. D'autant que la communication interne permet aussi de préparer l'après-crise. « Après la crise, ce sont les ressources internes qui permettront de redémarrer l'activité. Il est primordial de ne pas perdre la

confiance des salariés.» Garder le lien avec les équipes et en faire des ambassadeurs de la marque une fois la crise passée est donc crucial. « Si les salariés estiment que le patron a bien parlé et l'expriment comme tel, c'est un signal fort que la communication de crise a été réussie », note Laurent Vibert, directeur de l'agence de communication de crise Nitidis.

FLEURY MICHON, VICTIME D'UNE CYBERATTAQUE (2019)

Dans la nuit du mercredi 10 au jeudi 11 avril 2019, Fleury Michon se rend compte que ses systèmes informatiques ont été affectés par un virus. Les équipes opérationnelles réagissent rapidement et, dès le 11 avril au matin, les fournisseurs et partenaires de l'usine sont mis au courant de l'incident et des mesures prises en réaction. Quatre jours plus tard, lorsque l'entreprise publie un communiqué de presse pour rendre l'incident public, la production a déjà redémarré. Et Fleury Michon travaille de concert avec ses partenaires, dans une communication harmonisée, pour répondre aux questions des journalistes et des clients.

Ce qu'il faut retenir : maîtriser son timing. Difficile de garder une telle crise secrète à l'ère des réseaux sociaux et de la communication instantanée. Mais à l'impossible nul n'est tenu ! Fleury Michon a réussi le tour de force de jongler entre l'immédiateté de la communication interne et légale – notamment la déclaration de l'incident à l'Anssi – et l'ajournement de la communication publique. Une bonne façon d'éviter une pression trop intense et de travailler plus sereinement à résoudre la crise. « Le principal enjeu de la communication de crise, c'est de montrer qu'on maîtrise la situation et le faire savoir », rappelle Jean-Marc Atlan, associé du cabinet de communication Ekno. Aligner sa communication avec celle de ses partenaires et choisir – lorsque c'est possible – de communiquer lorsque la crise est déjà en voie de résolution permet d'éviter un sur-incident médiatique.

FINDUS ET LA CRISE DE LA VIANDE DE CHEVAL (2013)

Le 8 février 2013, Findus révèle que les lasagnes surgelées vendues au Royaume-Uni contenaient de la viande de cheval et non de bœuf comme indiqué sur les produits. La marque a choisi de communiquer avant d'être mise en cause par un tiers, et alors même que l'épisode n'a donné lieu à aucun incident sanitaire.

Quelques semaines plus tard, la marque se paye une grande campagne de presse sur la transparence. Une partie de son site internet est dédiée à la vérification de la conformité des produits. Findus s'engage publiquement à

© kiliweb pour Open Food Facts

défendre une meilleure traçabilité des produits. Puis finit par pointer du doigt la responsabilité de ses fournisseurs, notamment l'entreprise Spanghero. Celle-ci est placée en liquidation judiciaire à la suite de l'affaire, tandis que Findus voit son chiffre d'affaires augmenter.

Ce qu'il faut retenir : faire preuve de transparence. En prenant les devant, Findus a fait coup double. D'abord, l'entreprise s'est donné la maîtrise du tempo de communication. Et elle a fait montre de transparence, ce qui est important autant vis-à-vis des partenaires que des clients. « On ne doit pas tout dire mais, si l'on choisit de parler, il faut se cantonner à la vérité et à des éléments factuels », conseille ainsi Stéphanie Ledoux. Findus a gagné des points dans l'opinion publique, tout en se donnant du temps pour préparer des éléments de réponse immédiats mais aussi une opération de communication de longue haleine. ■

POUR ALLER PLUS LOIN

© DR

[VIDÉO] Jean-Marc Atlan *(Ekno)*
« En temps de crise, ce n'est pas parce que vous n'avez rien à dire qu'il faut vous taire »

© Shunya Koide via Unsplash

La grande bibliothèque de la communication de crise

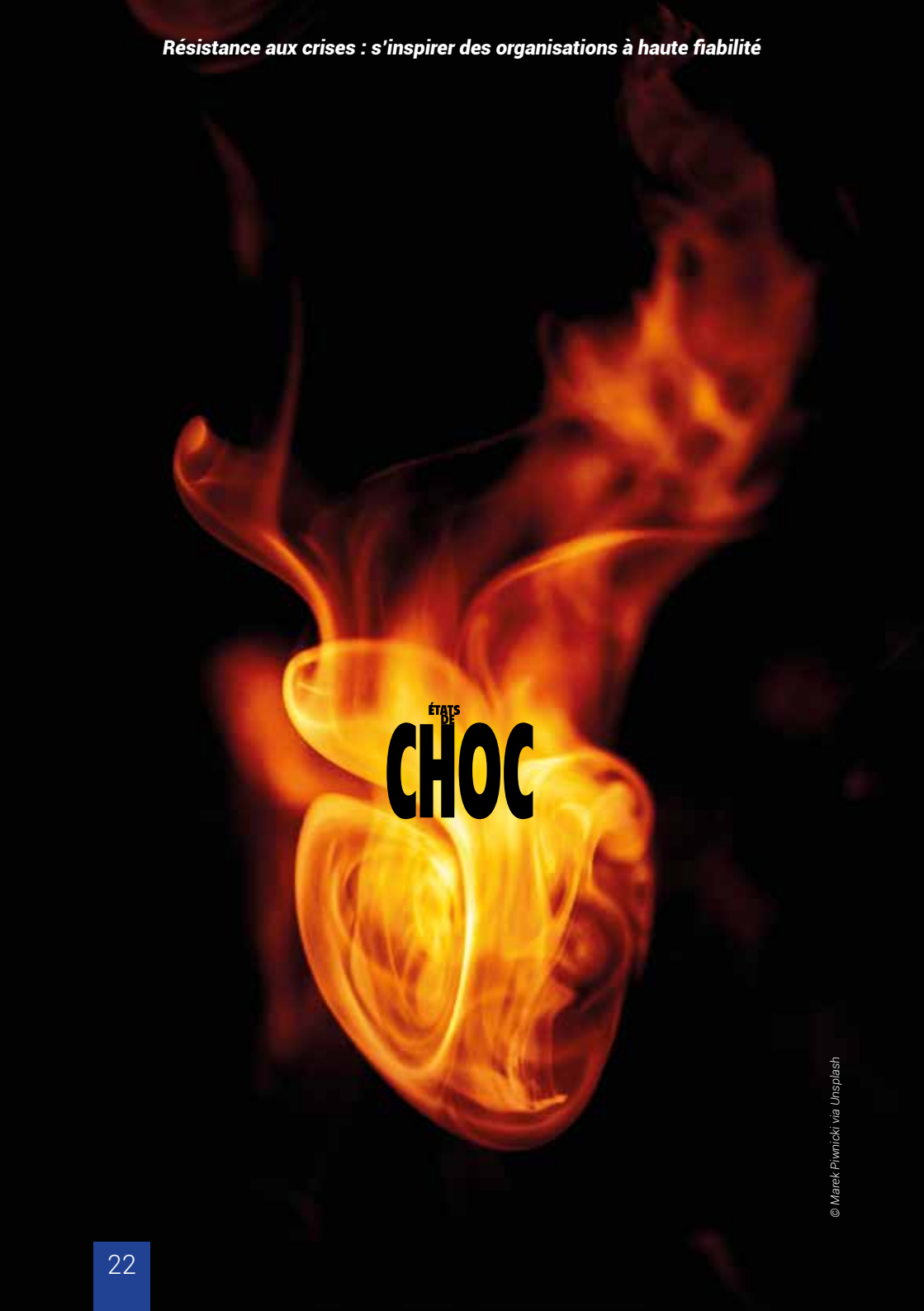
© Markus Winkler sur Unsplash

ÉTATS DE CHOC

Résistance aux crises : s'inspirer des organisations à haute fiabilité

DOSSIER N° 13 ■ 25 avril 2022

Crise après crise, les entreprises cherchent des façons de maintenir leur activité. C'est pourquoi certaines regardent ce qui se fait du côté des organisations à haute fiabilité. Désignées par l'acronyme HRO (High Reliabily Organizations, en anglais), il s'agit d'organisations publiques ou privées qui évoluent en milieu risqué. Centrales nucléaires, compagnies aériennes, hôpitaux... Leur résistance et leur faible taux d'accidents au regard des dangers qui entourent ces structures suscitent l'admiration, au point que certains chercheurs ont théorisé la recette qui faisait leur succès en 5 principes dans les années 90. Depuis, les entreprises tentent de s'en inspirer. Mais attention : selon le contexte et les parties prenantes, il faut adapter la formule avec intelligence.



© Marek Piwnicki via Unsplash

Quels sont les principes des organisations à haute fiabilité ?

Mélanie Roosen ■ 25 avril 2022

Se préoccuper des erreurs et des défaillances, favoriser les expertises… Le succès des organisations à haute fiabilité et leur résistance aux crises reposent sur 5 principes. Quels sont-ils ?

© Jason Goodman via Unsplash

Au début des années 90, les universitaires américains Karlene Roberts et Karl Weick ont théorisé ce qui faisait la force et la résistance des organisations à haute fiabilité – high reliability organizations en anglais, désignées par l'acronyme « HRO ». Les HRO, ce sont ces organisations qui évoluent dans des environnements périlleux. Hôpitaux, aéroports, centrales nucléaires… Comment expliquer que, malgré les risques constants, les dégâts et les accidents graves soient limités ?

D'après Karlene Roberts et Karl Weick, ce serait grâce à un mode de fonctionnement particulier. Le principe ? Récolter un maximum d'informations, à toutes les strates de l'organisation, les connecter les unes aux autres et les utiliser à bon escient pour prendre les meilleures décisions possibles.

LES 5 PRINCIPES DES HRO

1er principe : se préoccuper des erreurs et des défaillances

Le premier principe pour éviter les accidents, c'est d'avoir conscience qu'ils peuvent exister. Il ne faut pas se voiler la face, et s'assurer de pouvoir détecter les premiers signes d'échecs, s'en préoccuper, afin de déployer les efforts nécessaires pour les éviter si possible. L'idée, c'est qu'un « gros problème » n'arrive jamais tout à coup. Il est en général précédé de problèmes plus anodins ou de petites anomalies, qui, s'ils étaient détectés à temps, pourraient permettre de désamorcer les grosses difficultés. Il ne faut pas considérer l'erreur comme taboue : son signalement doit être encouragé.

Par exemple : en 1992, une explosion dans la mine de Westray au Canada tue 26 mineurs. L'enquête révèlera de nombreuses défaillances en termes de règles de sécurité, liées à des pratiques informelles mises en place par le management. Celles-ci, renforcées par une acceptation tacite des mineurs et une forme de « pression » interne, ont poussé les mineurs à négliger leur propre sécurité. Certains éléments extérieurs ont aggravé la situation : les mineurs étant eux-mêmes fils de mineurs avaient l'impression de pouvoir maîtriser les risques. Le professeur de l'université de Saint Mary (Halifax) David Wicks estime qu'au-delà des défaillances managériales, l'imaginaire collectif, la culture locale et le contexte économique ont contribué au drame.

2e principe : ne pas simplifier

Une fois qu'un échec, potentiel ou avéré, est identifié, les HRO s'attachent à ne pas en simplifier les causes ou les origines. Ainsi, un incident ne sera jamais (ou très rarement) le fait d'une seule personne. Les défaillances sont systémiques et concernent une organisation dans son ensemble. Par ailleurs, il convient d'encourager un dialogue ouvert et respectueux, qui donnerait la voix aux idées dissonantes, afin d'explorer les divergences potentielles.

Par exemple : en 1989, un Convair 580 de la compagnie aérienne Partnair quitte Oslo pour Hambourg. En plein vol, la queue de l'appareil tremble avant de se détacher du reste de l'appareil, qui devient incontrôlable et s'écrase en pleine mer. Aucun passager ne survit et Partnair doit déposer le bilan après quelques mois. Des spéculations affirment rapidement que l'avion a été abattu par des explosifs, renforcées par des témoignages affirmant avoir entendu un grand bruit en voyant l'avion tomber. Celui-ci s'étant désintégré dans les airs, la théorie de la bombe est reprise notamment par la presse et les discours politiques. Plus tard, un scénario dans lequel l'avion aurait été abattu par un exercice de l'OTAN voit le jour. Il aura fallu une longue enquête pour s'intéresser aux vibrations enregistrées par l'appareil sur plusieurs mois. Un examen des dossiers de maintenance de l'avion a révélé que lors d'une révision, un mécanicien avait découvert une usure sur un boulon maintenant l'aileron vertical.

Le boulon remplacé ainsi que les trois autres présents sur cette partie de l'avion ont été examinés par les enquêteurs. Verdict : les trois boulons étaient contrefaits, et avaient subi un traitement thermique incorrect pendant la fabrication. Ils ne pouvaient supporter que 60% de leur résistance à la rupture prévue.

3e principe : être sensible aux opérations

Les systèmes ne sont jamais statiques, monolithes et linéaires. Par essence, ils sont dynamiques. Plus une organisation est complexe, plus il est important de comprendre comment chaque élément qui la compose réagit par rapport aux autres. Il est aussi crucial de comprendre que chaque action ou opération peut entraîner une réaction, ou avoir une incidence sur une activité éloignée de l'organisation. Tous les niveaux hiérarchiques de l'entreprise doivent se sentir concernés par les activités et opérations de l'entreprise afin que chacun participe au maintien d'une attention renforcée.

Par exemple : en 1984, à Bhopal en Inde, un accident chimique survient à la suite de l'explosion d'une filiale de la firme américaine Union Carbide, qui produit des pesticides. Ce sont 40 tonnes de produit toxique (isocyanate de méthyle) qui seront déversées dans la ville, causant la mort de plusieurs milliers de personnes. Le P-DG de l'époque Warren Anderson fut accusé de « mort par négligence ». L'origine technique de la catastrophe semble être le lavage d'un tuyau à grande eau. En dépit des consignes de sécurité, l'opérateur et le superviseur en charge de l'opération auraient oublié d'isoler le tuyau à nettoyer du reste de l'installation. Le réservoir d'isocyanate de méthyle s'est rempli d'eau jusqu'à l'explosion.

4e principe : s'engager vers la résilience

La résilience, c'est la capacité d'une organisation à absorber les tensions tout en préservant son activité dans l'adversité. Il s'agit donc de développer des capacités d'improvisation. Mais pas seulement. Être résilient, c'est pouvoir faire preuve d'agilité et se remettre en service après des événements inattendus. Enfin, c'est prendre du recul sur les événements passés, et en tirer des leçons pour apprendre et grandir afin de prévenir et de contenir de futures erreurs.

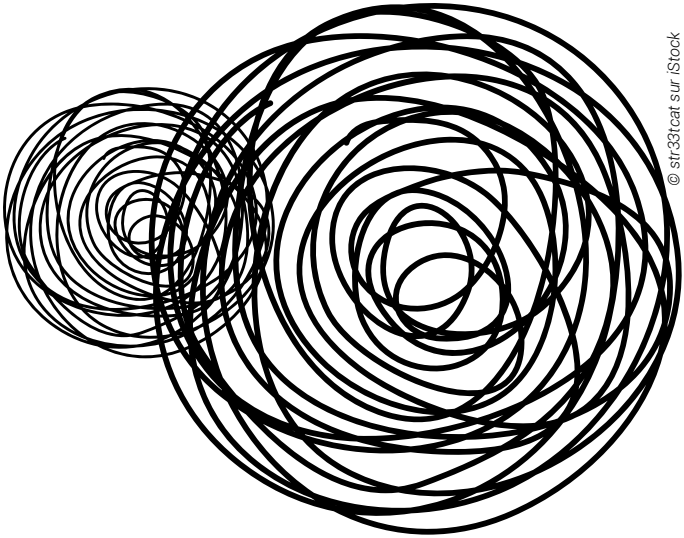
Par exemple : entre 1984 et 1995, le Bristol Royal Infirmary (BRI), unité de chirurgie cardiaque pédiatrique, est pointé du doigt pour ses mauvaises performances – alors qu'au début des années 80, l'équipe chirurgicale en place avait une performance comparable à celle des autres unités du pays. Au cœur du problème : un refus de modifier son fonctionnement alors que les autres unités améliorent leurs performances en continu. Il aura fallu le déclenchement d'une enquête en 1996 suite à la demande de nombreux parents pour que la situation évolue. Un rapport publié en 2001 a montré l'importance de modifier la gouvernance de l'hôpital.

5e principe : favoriser toutes les expertises

Le 5e principe des HRO, c'est de considérer l'ensemble de l'organisation comme autant d'expertises. Il faut donc être capable de faire confiance à celles et ceux « qui font » au quotidien ou qui possèdent la meilleure connaissance d'un sujet, même si ces personnes ne sont pas haut placées dans la hiérarchie. En acceptant que l'expertise et l'expérience priment sur la hiérarchie, il s'agit ensuite de faire appel aux principes de l'intelligence économique, et de faire circuler l'ensemble des connaissances et des informations pour prendre les décisions les plus éclairées possibles.

Par exemple : en 1999, un avion-cargo de la Korean Air s'écrase après 60 secondes de vol. L'enquête menée révélera une défaillance de l'horizon artificiel du commandant, mal réparé avant le décollage. Signalée par une alarme, la défaillance a été ignorée par le commandant que ne prit en compte que son instrument. Le commandant a par la suite incliné l'appareil de 90 degrés… croyant être à 2 degrés. La défaillance, mineure, a été aggravée par une réaction inappropriée de l'équipage : le copilote, au lieu de prendre les commandes, a préféré respecter l'autorité du commandant de bord plutôt que de le contredire.

Autant de principes qui peuvent s'appliquer aux entreprises du secteur privé : les récentes crises secouent toutes les organisations, sans réelle distinction, et ont des conséquences diverses mais concrètes sur les entreprises. En 2019, McKinsey identifiait les HRO comme des structures capables de se démarquer de la concurrence. Une pandémie et une guerre en Ukraine plus tard, au-delà de l'avantage concurrentiel, le sujet pourrait bien être un enjeu de survie. ■



© Pixabay via Pexels

Comment s'inspirer des organisations à haute fiabilité

Mélanie Roosen ■ *25 avril 2022*

À l'heure où les crises se multiplient, les entreprises peuvent s'inspirer des organisations à haute fiabilité pour repenser leurs modèles. Comment ? En apprenant à développer une force de réflexion rapide et en comptant sur l'ensemble des équipes.

« Nous sommes entrés dans un monde où la crise est devenue la normalité. » Avec la pandémie de Covid-19 et le conflit qui sévit en Ukraine, difficile de donner tort à Marius Bertolucci. Ce maître de conférences en sciences de gestion à l'IMGPT (Aix-Marseille Université) est passionné par les organisations à haute fiabilité (High Reliability Organizations en anglais, désignées par l'acronyme HRO). Quand on l'interroge sur la façon dont les entreprises peuvent s'en inspirer, il insiste sur deux points : « leur capacité à réorienter le sens de l'action pour éviter les accidents graves, et le besoin de considérer les

équipes dans leur ensemble. » D'après lui, la période entraîne une nécessité de repenser les modèles. « Sans chercher à copier-coller les principes des HRO, il est important de savoir qu'ils existent. C'est une première étape. Je pense que nous allons voir émerger de nouveaux principes, qui viendront enrichir ou remplacer ceux qui existent », explique-t-il.

TOUTES LES ENTREPRISES SUBISSENT DES CRISES

« Je ne pense pas m'avancer en affirmant que chaque entreprise va un jour se retrouver face à une crise. Il y a bien sûr les mégacrises comme les pandémies ou les guerres, mais il y a aussi les crises quotidiennes qui sont portées par une nouvelle définition de l'innovation. Aujourd'hui, les entreprises ne cherchent plus à innover mais à disrupter. Nous vivons dans un monde qui devient obsolète à chaque seconde qui passe. Nous l'avons bien vu avec les compagnies de taxis qui se sont retrouvés complètement démunis face à l'arrivée des applications de VTC. Tous les secteurs – et pas uniquement ceux qui se trouvent dans un environnement risqué – vont devoir apprendre à absorber les chocs. » À ce titre, il devient nécessaire que les entreprises apprennent à faire preuve de résilience dans l'urgence. Le chercheur Patrick Lagadec, spécialiste de la gestion du risque et de la gestion de crise, insiste dans ses travaux sur le besoin de développer une force de réflexion rapide. Les crises, précise-t-il, ont tendance à causer des déstructurations qui affectent les capacités de réponse. Paradoxalement, il faut accepter l'idée d'être toujours dépassé pour pouvoir prendre des décisions en temps réel.

MOBILISER TOUTES LES PARTIES PRENANTES

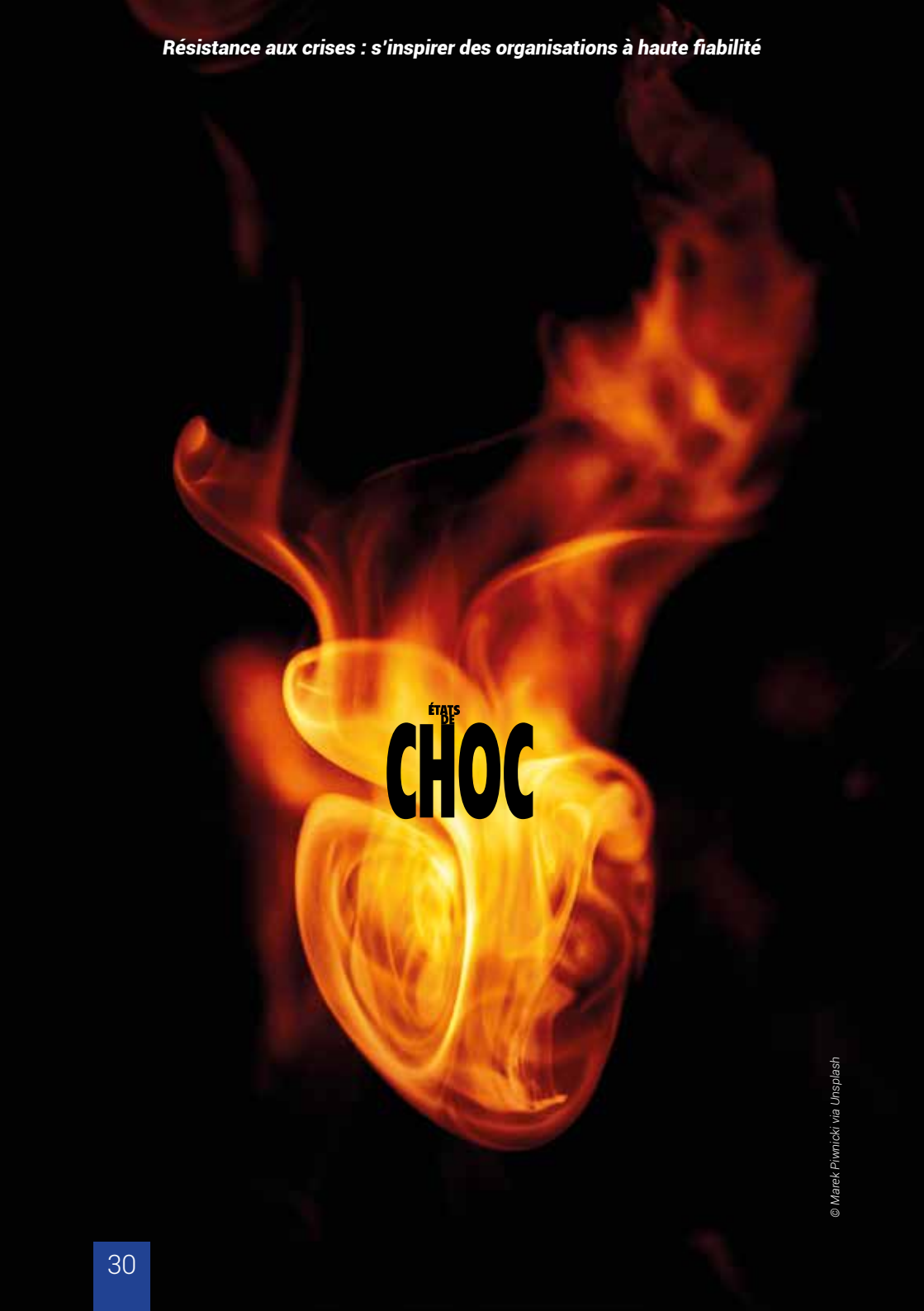
Cette prise de décision rapide ne doit pas se faire sans la considération de l'ensemble des acteurs qui constituent l'entreprise. « Lorsqu'un accident advient dans une organisation, on a tendance à pointer du doigt les hommes et les femmes qui sont en première ligne. Il ne faut pas oublier que lorsque tout fonctionne – c'est-à-dire la plupart du temps –, c'est aussi grâce à eux », poursuit Marius Bertolucci. Il rappelle que la force des HRO, c'est de ne pas confiner aux seules mains des dirigeants les sujets de crise.

Bonne nouvelle : la pandémie a accéléré la prise de conscience sur ce point, témoigne Arnaud Marion, « serial-redresseur d'entreprises » et fondateur de l'Institut des Hautes Études en Gestion de Crise. « La pandémie a révélé, de façon insoupçonnée, la capacité des entreprises à être agile et proactive. Cela vaut pour les dirigeants et les salariés, qui ont découvert une nouvelle façon de travailler ensemble. » C'est aussi parce que la crise a surpris tout le monde, et que toutes les parties prenantes des organisations se sont retrouvées à œuvrer pour une cause commune. « Je pense que cette manière de travailler, main dans la main et en considérant beaucoup plus l'opérationnel, va rester. C'est la première fois qu'une crise de cette ampleur entraîne si peu de conflits sociaux. »

LE RISQUE DU FILET DE SÉCURITÉ

Est-ce à dire que toutes les entreprises qui ont survécu au Covid-19 sont devenues des HRO ? « Tous les stagiaires que je forme m'assurent qu'ils savent désormais gérer une crise », s'amuse Arnaud Marion. Loin d'être dupe, il rappelle que la crise sanitaire a été abondamment soutenue par l'État. « Le danger a été surcompensé. Gérer une crise se fait souvent sans moyens, ou à périmètre très restreint. C'est ce qui permet en général aux concernés d'apprendre, de progresser. Là, on a intégré que l'État était une espèce d'assureur de dernier recours. Les dirigeants les plus sensibilisés au sujet iront chercher des solutions et voudront changer leurs façons de travailler, les autres vont se penser tranquilles pendant un moment. C'est un vrai risque », conclut-il. ■

© Sheldon Liu via Unsplash



Raphaël de Vittoris *(Michelin)*

« Pour être résilientes, les entreprises doivent comprendre que les crises sont multi-facettes »

Par Mélanie Roosen ■ 25 avril 2022

Il faut s'y faire : les crises sont protéiformes. Et pour y survivre, pas question de cantonner sa stratégie à de grands principes figés : les entreprises doivent accepter d'évoluer. Chaque année.

© Xerfi

Depuis plusieurs années, Raphaël de Vittoris apprend à naviguer entre les crises. Celles-ci sont de plus en plus difficiles à catégoriser : leurs implications sont tout de suite multiples. Pour cette raison, il valorise assez peu les théories qui permettraient d'expliquer comment y résister à coup sûr. Explications.

Comment intervenez-vous sur les différentes crises du groupe Michelin ?

Raphaël de Vittoris : Mon poste de group crisis manager a été créé en 2015. À l'époque, il s'agissait plutôt de profiter des « temps de paix » pour former les équipes. Mais le monde a changé : il est devenu instable. Un des problèmes des entreprises est qu'elles cherchent à développer des stratégies stables dans un régime turbulent. Selon moi, une telle approche est comparable à vouloir cultiver des terres sans se soucier des saisons. Nous nous retrouvons dans une situation où de trop nombreuses entreprises utilisent les mêmes leviers d'optimisation qu'il y a quelques années alors que tout le système a changé. Elles sont encore beaucoup à délocaliser, à amenuiser leurs stocks, à externaliser les expertises… Aujourd'hui, j'ai l'opportunité d'avoir une implication directe sur le terrain : je peux être sollicité pour tout type de crise, quel que soit l'endroit où elle a lieu. Il peut s'agir d'un incendie dans une usine, d'une attaque cyber, d'une rupture d'approvisionnement, d'une crise sociale ou d'un problème géopolitique qui peut bloquer le sourcing.

Y a-t-il un danger à catégoriser les crises ?

R. d. V. : Il serait inexact de vouloir cantonner chaque crise à une seule thématique. La réalité, c'est qu'elles ont toutes plusieurs dimensions. Une crise qui éclatera à cause du non-respect des règles antitrust aura par exemple des conséquences juridiques, économiques, sociales ou médiatiques. De même, il serait réducteur de parler de la crise du Covid-19 comme d'une crise purement sanitaire : elle a des implications en termes de mobilité, de sécurité, d'économie ou de souveraineté. Le risque, c'est surtout de catégoriser les méthodologies. Ce serait inadapté au monde moderne. Mon rôle est d'être un facilitateur : d'identifier les bons experts, en interne et en externe, de les faire monter à bord et cohabiter avec d'autres pour résoudre les crises. Mais attention : quand on parle d'expertise, la situation n'est pas exactement la même qu'il y a 30 ans. Aujourd'hui, tout le monde peut aisément se considérer expert de quelque chose. La crise du Covid l'a bien montré : d'un coup, nous avions 70 millions d'épidémiologistes. Et quand tous les experts prennent la parole en même temps, et qu'ils ne sont pas d'accord entre eux, ça crée beaucoup de confusion.

Miser sur l'expertise, c'est justement l'un des principes des organisations à haute fiabilité (HRO). Diriez-vous que les entreprises doivent s'en inspirer ?

R. d. V. : Oui… et non. Le problème avec les HRO, c'est que personne n'a cherché à les redéfinir depuis les années 90. Les technologies ont beaucoup évolué. Par ailleurs, les organisations censées être HRO ont montré des failles, ces dernières années. Elles sont supposées être davantage soumises aux accidents majeurs et d'être pourtant capables d'en éviter la survenue. Que dire,

alors, des crashs aériens qui ont secoué les compagnies aériennes ces dernières années, du Concorde à la Germanwings ? Ou des catastrophes nucléaires de Fukushima, de Tchernobyl ou de Three Miles Island ? Il faut admettre que le concept de HRO, au bout de trois décennies, doit se confronter aux tristes manifestations du réel.

Les HRO sont-elles (déjà) dépassées ?

R. d. V. : Pas forcément. C'est un modèle qui fournit des règles simples qui satisfont aussi bien les académiciens que les professionnels. Aujourd'hui, ils nous apparaissent comme des évidences, mais à l'époque, c'était la première fois que ces principes étaient ainsi énoncés. Ce que je préconise, c'est donc de s'éloigner de la théorie pour plonger à fond dans la pratique. Le savoir des anciens n'est pas toujours applicable au monde moderne. Les vrais experts, ce sont les praticiens. Si ces derniers font des recommandations, il faut les écouter. Je recommande aux entreprises de réfléchir leur identité en plusieurs dimensions : quelle approche doivent-elles adopter en fonction de leurs départements ? Une approche antifragile ? Résiliente ? Horizontale ? Le plus important, c'est aussi d'envisager sa structure à un instant T, et ne pas considérer qu'elle est ensuite figée. Une stratégie pourra s'avérer bonne une certaine année, et obsolète la suivante. Il faut donc être capable de démystifier la théorie, car parfois, elle ne passe pas l'épreuve des faits.

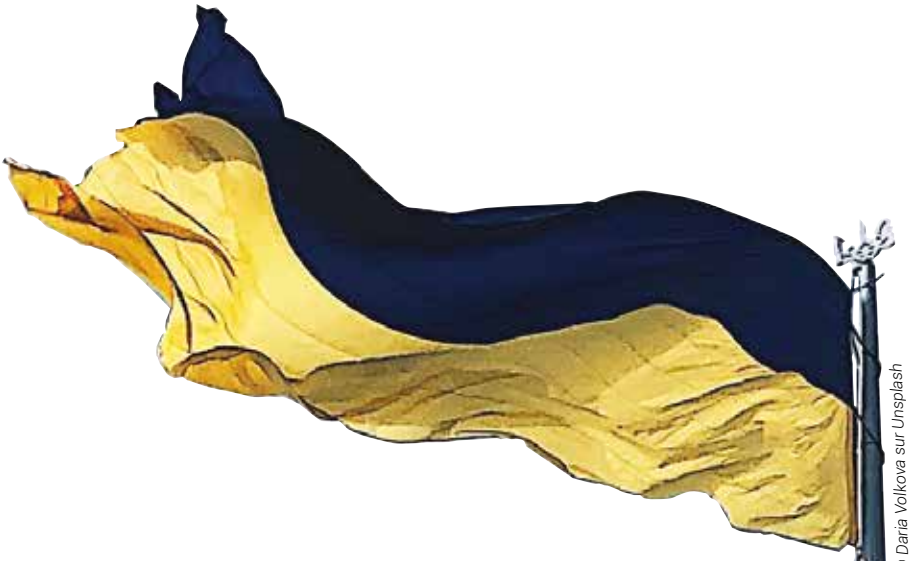
Quels conseils donneriez-vous aux entreprises en temps de crise ?

R. d. V. : Il faut embrasser la réalité avec humilité, essayer de comprendre son environnement, et accepter de faire des paris. Il faut adopter des principes sains et simples si l'on veut pouvoir les sophistiquer au plus près du contexte. À l'inverse, des principes trop précis définis en amont d'une situation ne trouveront aucun écho en temps de crise. Il faut garder une marge de manœuvre et allonger la liste non exhaustive des principes des HRO avec des principes personnels et idiosyncrasiques. ■

Biographie

Group crisis manager de Michelin depuis 2015, Raphaël de Vittoris est aussi enseignant et chercheur en sciences de gestion sur les problématiques de gestion de crise, gestion des risques, communication de crise, négociation de crise et biais cognitifs en situation de crise. Docteur en sciences de gestion et qualifié maître de conférence, diplômé d'un master en physiologie en environnement extrême, d'un master en administration d'entreprise et d'un master en hygiène, sécurité et environnement, il enseigne dans divers masters et il est membre du board de l'Institut d'études des crises et d'intelligence économique et stratégique de Lyon 3 et est l'auteur de Surmonter les crises : idées reçues et vraies pistes pour les entreprises, paru aux Editions Dunod.


ÉTATS
DE
CHOC

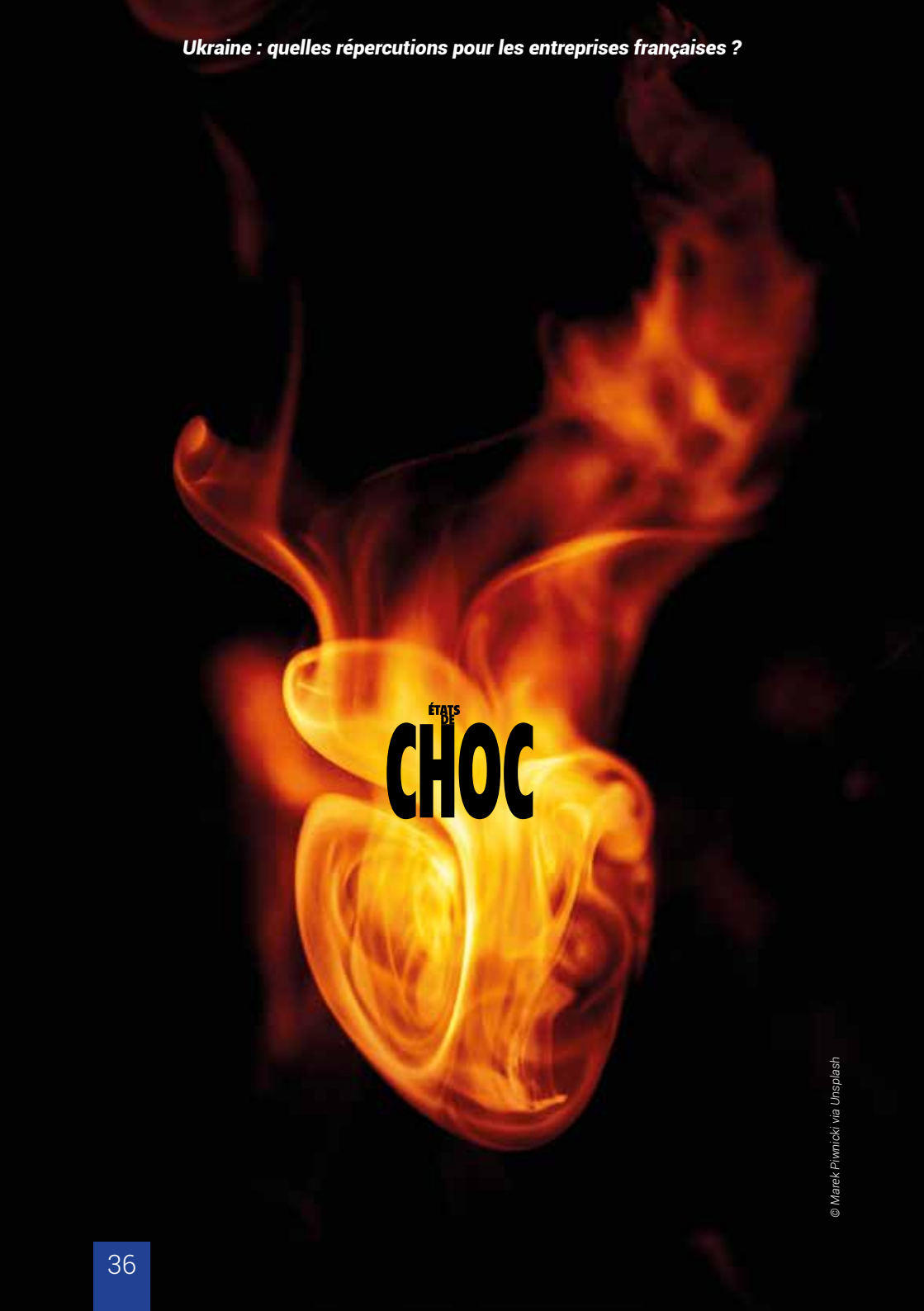


© Daria Volkova sur Unsplash

Ukraine : quelles répercussions sur les entreprises françaises ?

DOSSIER N° 6 ■ 7 mars 2022

La France n'est peut-être pas militairement impliquée dans le conflit qui oppose l'Ukraine à la Russie, mais celui-ci aura des conséquences sur l'économie française. Au-delà des impacts sur les liens diplomatiques entre les différents pays, les entreprises anticipent déjà les retombées. Prix de l'énergie, pénuries des matières premières, cyberattaques… La guerre se joue au-delà des frontières. Le gouvernement se veut rassurant et promet son soutien aux acteurs les plus touchés, mais les organisations vont devoir se protéger et prendre la mesure des risques.



© Marek Piwnicki via Unsplash

© Elysée - YouTube

France-Ukraine : un soutien qui reflète de bonnes relations économiques

Mélanie Roosen ■ 7 mars 2022

Au-delà des liens diplomatiques qui unissent l'Ukraine à la France, les liens économiques se renforcent depuis plusieurs années. Importations, exportations... Focus sur les échanges commerciaux franco-ukrainiens.

Depuis des années, l'Ukraine se tourne vers l'Europe. En 2014, la « Révolution de la dignité » s'accompagnait d'un changement de pouvoir à Kyiv. La situation a mené à la signature d'un accord d'association entre l'Ukraine et l'Union européenne. Celui-ci est entré en vigueur le 1er septembre 2017. Aujourd'hui, l'Union européenne est le premier partenaire commercial de l'Ukraine.

Cette entente économique se traduit par divers dispositifs. Récemment, dans le cadre de la stratégie « Team Europe » annoncée par l'Union européenne, en soutien à ses partenaires pendant la pandémie, l'Ukraine a par exemple bénéficié de 190 millions d'euros d'aide financière.

L'Union européenne soutient aussi les réformes structurelles du pays. Depuis 2017, elle a mis en place des programmes d'assistance macro-financières à hauteur de plusieurs milliards d'euros. Le 1er février 2022, la Commission européenne a, à ce titre, consacré une aide de 1,2 milliard d'euros à l'Ukraine.

FOCUS FRANÇAIS

La France a établi des relations diplomatiques avec l'Ukraine dès son indépendance, en 1992. Depuis, les deux pays ont signé près de 300 traités et accords pour renforcer leurs relations.

En 2021, le total des échanges commerciaux entre la France et l'Ukraine atteignait 2,1 milliards d'euros (contre 1,6 milliard d'euros en 2020).

Au niveau mondial, la France est le 10ème fournisseur de l'Ukraine. Au niveau européen, elle est le 4ème fournisseur (derrière l'Allemagne, la Pologne et l'Italie). Malgré cela, la France enregistrait une part de marché en baisse en 2021 (2,46% contre 2,7% en 2020).

Côté investissements, le gouvernement estime que la France serait le 6ème investisseur étranger et européen en Ukraine, avec 2% du stock d'IDE (Investissements Directs à l'Étranger).

Ce sont les industries chimiques et cosmétiques qui représentaient la majorité des exportations françaises en Ukraine en 2019 (plus d'un tiers), devant le machinisme agricole, l'industrie des transports et l'industrie pharmaceutique. Côté imports, les deux tiers des importations d'Ukraine concernent les produits agricoles et agroalimentaires.

Enfin, avec près de 160 entreprises françaises employant 30 000 personnes, la France est le premier employeur international, rapporte l'OCDE.

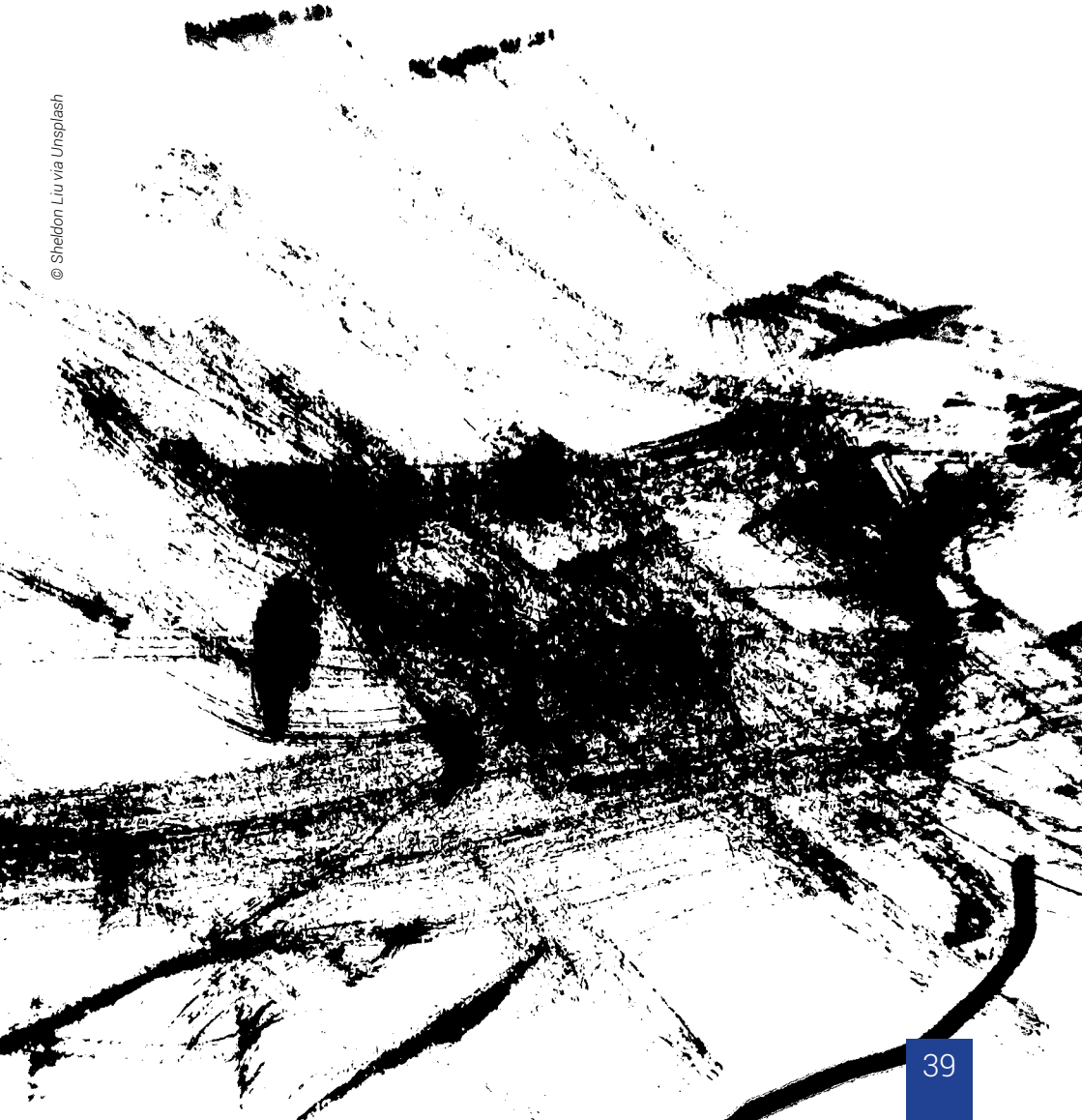
ET CÔTÉ RUSSIE ?

La posture française va-t-elle impacter les relations économiques entre la France et la Russie ? En 2020, la France était le deuxième pourvoyeur de flux d'IDE (avec 19 milliards d'euros de stock d'IDE en 2020) et les entreprises françaises, avec 156 000 salariées, faisaient de la France le premier employeur étranger.

Cependant, malgré une progression des échanges commerciaux en 2017 et 2018, une baisse s'est fait sentir à partir de 2019 (14 Milliards d'euros, -7%). Un phénomène qui s'explique par le recul des importations, notamment d'hydrocarbures (-24%) qui représentent aux côtés des produits pétroliers raffinés l'essentiel des importations.

Du côté des exportations, le gouvernement note une progression légère en 2019 (5,6 milliards d'euros, +6%) liée à l'augmentation des ventes de produits pharmaceutiques, qui représentent le deuxième poste à l'export après l'aéronautique.
Malgré ces chiffres en augmentation, la Russie n'était « que » le 18ème client à l'export de la France en 2020. Les réels risques concernent plutôt les investissements directs. Les grands groupes français entretiennent un dialogue poussé

avec le gouvernement russe via un Conseil économique franco-russe, créé en 2010. À l'occasion de la réunion de ce conseil (qui rassemble, entre autres, les dirigeants d'Air Liquide, Danone, Legrand, Renault, TotalEnergies, Thales, Safran, Saint-Gobain, Sanofi ou encore Vinci) en 2021, Vladimir Poutine avait déclaré souhaiter impliquer les entreprises étrangères voulant investir en Russie dans des projets considérés comme « hautement prioritaires », à l'aide de régimes d'investissement préférentiels. Pour les entreprises déjà impliquées se pose la question du rapatriement des revenus ainsi que de la fragilisation des investissements. ■



© Sheldon Liu via Unsplash

© Mikhail Nilov via Pexels

Guerre en Ukraine : quels impacts sur les entreprises françaises ?

Mélanie Roosen ■ 8 mars 2022

Les entreprises françaises, qu'elles soient implantées ou non en Ukraine, vont subir les effets de la guerre. Après deux ans de pandémie, le choc risque d'être lourd à encaisser. Mais le gouvernement se veut rassurant et promet de venir en aide aux acteurs concernés.

À mesure que les entreprises françaises implantées en Ukraine s'organisent pour protéger leurs salariés, leur stock et leurs locaux, certains craignent que le conflit qui oppose le pays à la Russie ait des répercutions au-delà des frontières.

AUGMENTATION DES PRIX DE L'ÉNERGIE ET RISQUE DE PÉNURIES

Moins de 20% du gaz utilisé en France provient de Russie. Cela ne suffit pas à rassurer François Asselin, président de la Confédération des Petites et Moyennes Entreprises (CPME), qui plaide pour des mesures de soutien aux PME face à une potentielle hausse des prix de l'énergie. Au micro de France Inter, il expliquait le 1er mars 2022 que le prix de l'énergie était une « préoccupation majeure » pour certaines entreprises énergivores, qui craignent de voir leur facture énergétique doubler. Il assure que si le gouvernement ne prend pas de mesures pour amortir les coûts exponentiels, certains entrepreneurs pourraient stopper leur activité.

L'autre crainte, c'est la pénurie de matières premières. Palladium, néon, titane… autant d'éléments qui sont importés de Russie et d'Ukraine et qui, s'ils venaient à manquer, pourraient mettre à mal certaines industries – notamment l'aéronautique.

LE GOUVERNEMENT RÉPOND PRÉSENT

Dès le 1er mars, le ministre du Commerce extérieur Franck Riester promettait que l'État allait accompagner les entreprises françaises subissant les conséquences du conflit. Une promesse appuyée dès le lendemain par Emmanuel Macron lors d'une allocution télévisée. Soulignant que de nombreux secteurs

économiques – « comme l'agriculture et l'industrie » – allaient souffrir, le président de la République a alerté sur les conséquences que le conflit allait avoir sur la croissance française. Il a annoncé la préparation d'un « plan de résilience » par Matignon. « Nous épaulerons les secteurs économiques exposés en recherchant de nouveaux fournisseurs et débouchés commerciaux. Nous apporterons des réponses adaptées à l'augmentation des prix », a-t-il assuré.

De son côté, l'ancienne ministre de l'Industrie Agnès Pannier-Runacher a reçu les représentants des 19 filières industrielles françaises pour analyser les points de difficulté des différents secteurs.

À L'AVENIR, MIEUX PRENDRE EN COMPTE LES RISQUES GÉOPOLITIQUES

Au-delà des aides du gouvernement, le conflit doit aussi être le signe pour les entreprises qu'il est important de se protéger face aux risques géopolitiques.

François Beaume, vice-président de l'Association pour le management des risques et des assurances de l'entreprise (Amrae) regrette dans les colonnes des Echos que si peu d'entreprises soient protégées face à ce type de situation. Il exprime un décalage entre les précautions des grands groupes, qui ont mis en place des outils de veille sur les risques géopolitiques, et les PME qui, même lorsqu'elles sont physiquement implantées sur des territoires « à risque », s'en soucient peu car « couvrir un risque de guerre est onéreux et difficile à mettre en place », précise-t-il. Du côté des entreprises qui entretiennent des relations commerciales avec les pays concernés, il existe aussi des risques – plusieurs patrons évoquent les pertes liées à l'impossibilité d'honorer les contrats avec l'Ukraine – mais elles sont, en général, encore moins protégées.

Le conflit rebattra-t-il les cartes en matière de protection des entreprises ? ■

© str33tcat sur iStock


© Hexatrust

Maxime Alay-Eddine
(Cyberwatch, Hexatrust)
« Le vrai risque, c'est que les incidents cyber aient des répercussions dans le monde physique »

Mélanie Roosen ■ *9 mars 2022*

La guerre en Ukraine nous rapproche d'un état d'urgence cyber. Dans le chaos ambiant, les attaques, plus nombreuses mais pas forcément ciblées, pourraient faire de gros dégâts.

Maxime Alay-Eddine est le vice-président d'Hexatrust. Ce groupement d'entreprises françaises de cybersécurité a pour objectif de couvrir toutes les failles des entreprises, quelles que soient leur taille ou leur secteur d'activité. À l'aune du conflit entre la Russie et l'Ukraine, il alerte les sociétés françaises : les risques cyber pèsent plus lourd en temps de guerre.

Avec la guerre en Ukraine, l'Anssi appelle les entreprises à renforcer leur vigilance cyber. Les menaces sont-elles vraiment plus importantes en temps de conflit ?

Maxime Alay-Eddine : C'est indéniable. Depuis le début de l'invasion militaire, l'Agence nationale de la sécurité des systèmes d'informations (Anssi) recense diverses attaques à l'encontre des institutions et banques ukrainiennes, des défigurations de sites internet, des tentatives d'intrusion sur les messageries électroniques, des cyberattaques… L'entreprise Vade Secure, membre d'Hexatrust, a noté que les tentatives d'attaques via les services de messagerie avaient été multipliées par 10. Celles-ci ne semblent pas spécialement ciblées, mais il ne faut pas se leurrer : elles provoqueront des dégâts collatéraux et ne vont pas se cantonner aux frontières du conflit. À titre de rappel, le virus NotPetya, qui avait touché plusieurs entreprises majeures en Ukraine en 2017, s'était propagé jusqu'à Saint-Gobain, lui coûtant 80 millions d'euros de résultats. On ne peut pas caractériser la menace à 100% mais il est certain que des personnes malveillantes cherchent à bénéficier du chaos ambiant. Dans ce type de situation, on constate ainsi que certains groupes en profitent pour mener des cyberattaques en désignant un autre coupable : un État ou un collectif de hackers va pouvoir agir et blâmer la Russie, par exemple. Cela rend leur identification d'autant plus difficile.

Que risquerait-on, dans un scénario catastrophe ?

M. A.-E. : Nous n'y sommes pas encore, mais le vrai danger, c'est que les incidents cyber aient des répercussions dans le monde physique. C'est ce que l'on appelle des attaques sur les systèmes industriels. Elles peuvent viser, par exemple, les éléments de production énergétique. Il existe des simulations d'attaques sur des centrales électriques, et les dégâts sont terribles : on parle de générateurs qui peuvent exploser. Le risque, c'est bien sûr que les hackers s'attaquent aux fournisseurs des centrales, voire aux fournisseurs des fournisseurs, pour pénaliser ce type de structures. Il y a une vraie probabilité d'attaque par propagation.

Pensez-vous que les alertes du gouvernement soient suffisantes pour pousser les entreprises françaises à se protéger ?

M. A.-E. : Lors de son allocution, le président a évoqué le risque cyber. Mais c'est surtout l'Anssi qui donne le tempo depuis quelques semaines, en émettant des recommandations simples et régulières. La première, qui s'adresse à toutes les entreprises, c'est de mettre à jour son matériel dès que possible. La deuxième est destinée aux sociétés qui sont déjà un peu équipées : il faut surveiller son système d'information et son réseau pour détecter une activité anormale, comme une requête réseau vers des acteurs douteux – des pays avec lesquels on n'a pas l'habitude de commercer, par exemple. Enfin, l'Anssi

rappelle l'importance de diversifier ses systèmes de sauvegarde pour avoir des solutions de secours en cas de vol ou cryptage de données.

Peut-on s'attendre à ce que les entreprises suivent, plus que d'habitude, une liste de recommandations en ligne ?

M. A.-E. : Les recommandations de l'Anssi sont bonnes, la question est en effet de savoir si les entreprises vont les appliquer. C'est toute la difficulté du risque cyber : il est impalpable, immatériel. On dit souvent que les entreprises agissent lorsqu'elles sont victimes d'une attaque, et c'est vrai. Il ne faut pas négliger qu'une bonne stratégie cyber demande du temps et du budget. Peut-être qu'il faudrait une plus grande forme de sensibilisation nationale, mais d'après moi, elle doit passer par les médias. Si la menace est suffisamment relayée dans les médias « mainstream », toutes les entreprises, y compris les plus petites, vont s'intéresser au sujet.

Diriez-vous que la France est bien placée pour réagir à la menace cyber ?

M. A.-E. : La force de la France, c'est une solide industrie au niveau des fournisseurs et des intégrateurs de solutions. Nous avons de très bons ingénieurs capables de les déployer. La faiblesse, c'est la partie commerciale. Nous avons encore énormément de travail à faire pour que les entités françaises consomment des offres françaises. Ce n'est pas pour rien que l'Anssi questionne l'emploi de solutions russes en ce moment : il faut consommer local aussi en matière de produits de sécurité. C'est aussi notre rôle, au sein d'Hexatrust, de soutenir l'économie locale. ■

Biographie

Co-fondateur et président de Cyberwatch, Maxime Alay-Eddine est diplômé de l'Ecole Centrale de Nantes (promotion 2013) et parrain de la promotion 2022. Il a fait ses premiers pas dans la sécurité informatique en 2002, avant de mettre ses compétences au profit des entreprises. En 2015, il a co-créé Cyberwatch, afin d'aider les entreprises et administrations à traiter leurs vulnérabilités informatiques. Il est aussi vice-président d'Hexatrust, le groupement des solutions cyber françaises et cloud de confiance.

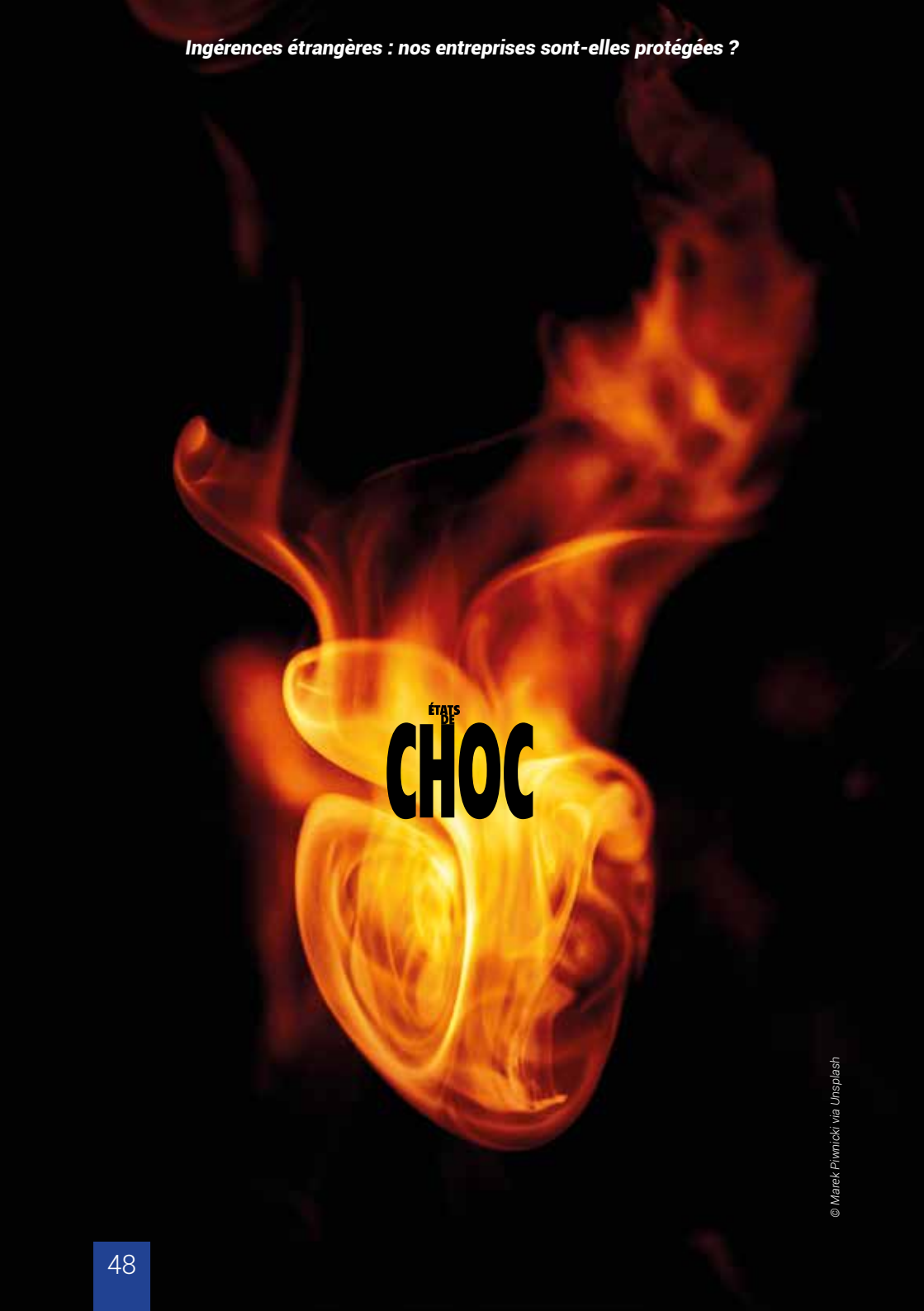
ÉTATS DE CHOC

© Victor sur Unsplash

Ingérences étrangères : nos entreprises sont-elles protégées ?

DOSSIER N° 4 ■ 21 février 2022

Les entreprises françaises ne cessent d'attirer les appétits étrangers. Et certains ne voient pas forcément cela d'un bon œil. Entre les risques liés aux investisseurs déloyaux, les start-up stratégiques qui se font absorber par des entreprises étrangères, et les moyens de déstabilisation informelle comme l'espionnage économique ou la diffusion de fake news, nos (futurs) fleurons ne sont pas à l'abri de perdre le contrôle de leur activité. L'alerte est lancée, maintenant, il s'agit de riposter. Sauf que les moyens déployés – du côté de l'État, notamment – ne sont pas toujours suffisants. Les investissements des fonds d'État ne sont pas à la hauteur des montants étrangers, et ne sont en outre pas toujours les bienvenus au capital des entreprises à cause de leur manque de flexibilité. Dans ce contexte, il devient difficile de rivaliser avec les grandes puissances qui zieutent nos pépites.



© Marek Piwnicki via Unsplash

Prises de contrôle capitalistiques : des risques bien réels

Mélanie Roosen ■ 21 février 2022

© Canva

Les prises de contrôle capitalistiques étrangères au sein des entreprises, start-up et laboratoires stratégiques ne sont pas sans conséquences. Pour les entreprises, c'est risquer de perdre le contrôle de leur activité, et de se soumettre à des orientations stratégiques différentes. Pour l'État, c'est risquer de voir des entreprises stratégiques quitter le territoire, et donc perdre en souveraineté.

« Dès qu'une entreprise est incubée en France, financée en premier tour en France, elle se tourne vers un acteur étranger pour devenir mondiale. » Ce constat, le président de Bpifrance Nicolas Dufourcq le faisait, amer, dès 2013. Depuis, la France se dote de moyens pour protéger ses jeunes pousses stratégiques. Mais ceux-ci ne sont pas toujours suffisants face aux appétits étrangers. La preuve : en 2020, les chiffres qu'il donne sont éloquents. « La tech française est extrêmement attractive, essentiellement pour les grands groupes américains.

Il faut avoir conscience en particulier que dans des mondes comme la medtech ou la biotech, le pourcentage d'entreprises qui, à la fin, sont rachetées par de grands groupes américains est de l'ordre de 80%. »

LES RISQUES LIÉS AUX INVESTISSEMENTS ÉTRANGERS

Dans son flash de janvier 2022 sur l'ingérence économique et les risques liés aux investisseurs étrangers déloyaux, la DGSI met particulièrement en garde les jeunes pousses tricolores : leur potentiel technologique et leur vulnérabilité financière font d'elles des cibles privilégiées des investisseurs étrangers. « En cas de divergences d'intérêts trop importantes, les cadres historiques des sociétés s'efforcent de s'opposer à la stratégie et aux décisions de leur nouvel actionnaire. Dans ce contexte, certains investisseurs peuvent déployer des manœuvres de déstabilisation et de blocage, n'hésitant pas à fragiliser financièrement les sociétés ou à menacer leurs principaux dirigeants. Ils peuvent également tenter d'obtenir les droits de propriété ou d'exploitation de la propriété intellectuelle de ces entreprises », note la DGSI.

Un phénomène que constate l'économiste et professeur en classes préparatoires Laurent Izard. Dans son livre *La France vendue à la découpe* (2019, éditions de L'Artilleur), il explore comment de nombreuses PME sont rachetées par des investisseurs étrangers. « Le processus s'est accéléré à partir de 2015. Il est la corrélation de la libre circulation des capitaux, de la globalisation de l'économie, et d'une volonté d'appropriation d'entreprises étrangères, analyse-t-il. La nouveauté ? C'est que les fonds d'investissement se transforment en fonds activistes. Ils font pression pour faire évoluer les politiques des groupes qu'ils rejoignent. Il n'y a qu'à voir l'exemple de Danone : deux fonds américains ont pris une participation extrêmement minoritaire à son capital, mais ils sont parvenus, par un jeu d'influence, à convaincre les autres actionnaires de changer totalement le cap stratégique du groupe. »

DES FAIBLESSES FRANÇAISES

La première faiblesse française identifiée par Laurent Izard, c'est la frilosité de certaines banques qui ne sont pas prêtes à jouer le jeu des entrepreneurs. « Nos PME ont besoin d'investissements pour croître. Si on ne leur apporte pas, elles seront de facto la proie d'investisseurs étrangers. »

Par ailleurs, il existerait un réel déséquilibre dans le rapport de forces à l'œuvre. « Certains États, comme les États-Unis, exercent une veille stratégique puissante sur les entreprises innovantes, notamment dans le domaine des nouvelles technologies », regrette Laurent Izard en évoquant le cas de Latécoère, passée sous contrôle américain notamment grâce à son avance sur la technologie LiFi. Pour lui, cet exemple comme bien d'autres démontrent une réelle volonté de la part du gouvernement américain. « Les prises de contrôle capitalistiques sont peut-être le fruit d'entreprises privées, mais il n'est pas rare de retrouver des

individus qui travaillent pour la CIA dans les équipes. Cela montre bien que ce n'est pas qu'une question de moyens, mais bien une intention stratégique de la part du gouvernement américain. »

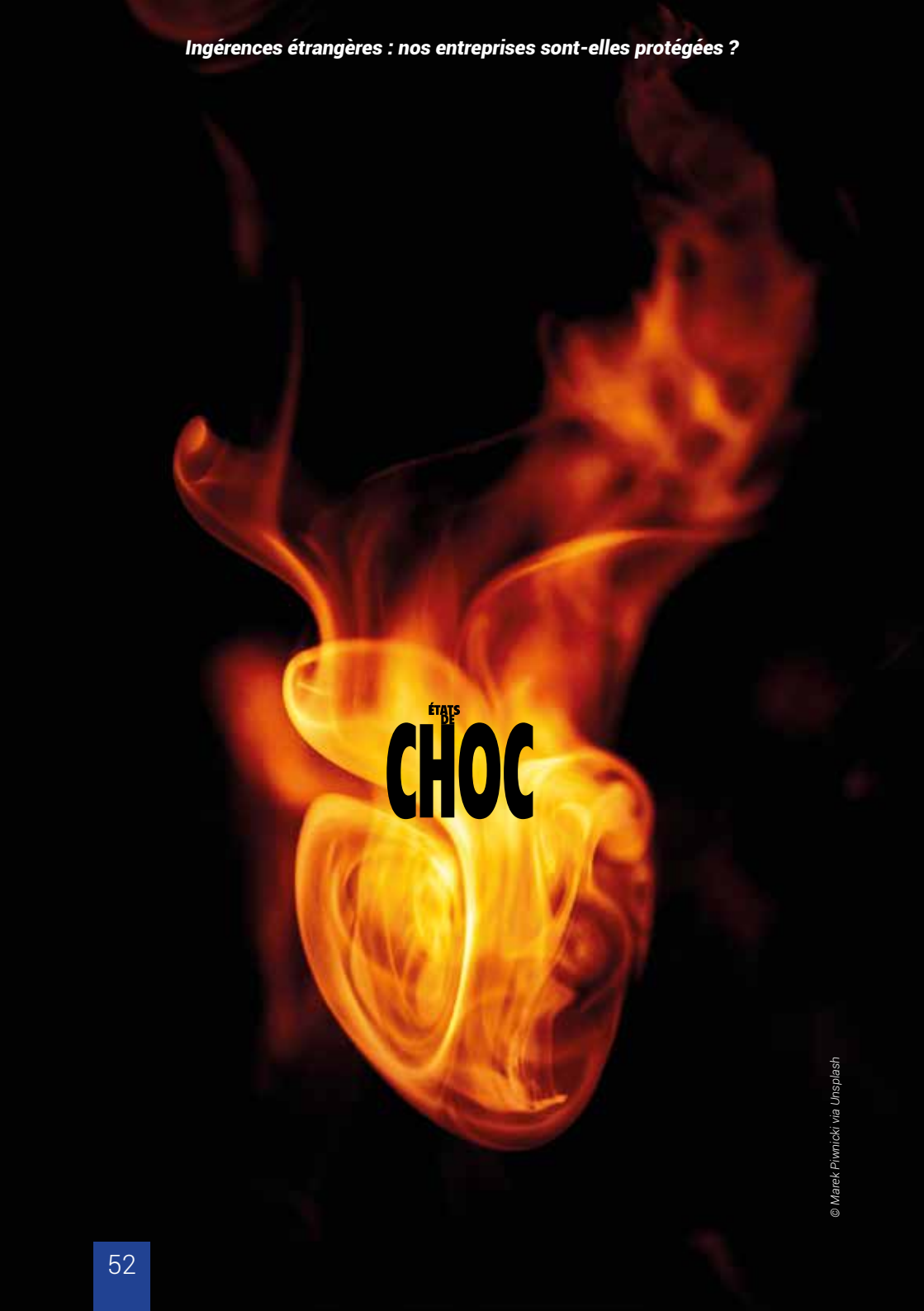
Alexandre Medvedowsky, président du Synfie, souligne aussi l'importance du rôle des banques et des cabinets de conseil qui accompagnent les investisseurs étrangers. « Les équipes connaissent bien les fonds américains. Il n'est pas rare qu'elles les appellent pour leur suggérer certaines pépites dans lesquelles investir. »

Bien sûr, il est aussi des cas où la France rachète des entreprises étrangères. « Ce n'est pas une logique à sens unique, admet Laurent Izard. Mais force est de constater que dans ce vaste marché, nous sommes plutôt cibles que prédateurs. »

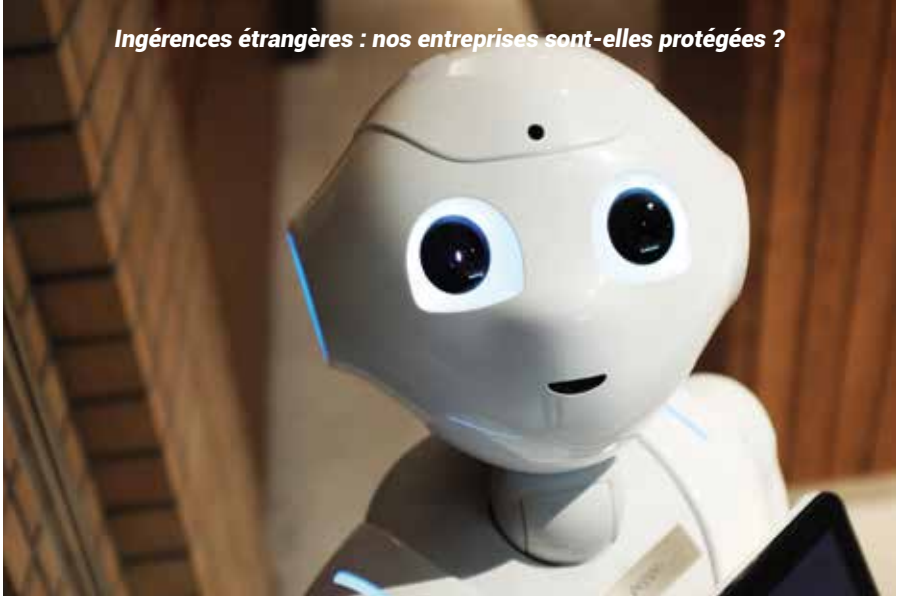
LES RIPOSTES SONT-ELLES SUFFISANTES ?

Le gouvernement français tente de changer la donne, notamment à travers certains fonds souverains, comme Definvest ou Bpifrance. « Le problème, c'est que ces fonds ne jouent pas dans la même catégorie que les fonds étrangers, les montants sont incomparables ! » alerte Laurent Izard. Par ailleurs, même si leurs moyens étaient similaires, Alexandre Medvedowsky rappelle qu'ils ne bénéficient pas toujours d'une bonne image auprès des dirigeants. « Les fonds d'État ne sont pas souvent les bienvenus dans les entreprises françaises. » Exception faite, peut-être, de Bpifrance, qui compte 900 sociétés à son portefeuille, « les start-up, les licornes et les secteurs où les chefs d'entreprise sont jeunes et dynamiques n'ont pas vocation à aller chercher des financements auprès de fonds souverains, qui n'ont pas du tout la même vitesse de développement. Tout est lourd, compliqué, contrôlé… » Il souligne cependant un autre type de démarche : l'État français peut inciter les entreprises qui sont partiellement sous son contrôle – comme Thalès ou Airbus – à investir dans des secteurs ou entreprises clefs. « Mais on peut toujours faire plus, et mieux. »

Laurent Izard regrette le manque de posture offensive du gouvernement, mais admet qu'une logique défensive existe. « Le droit évolue, et permet de disposer d'outils juridiques qui permettent de bloquer certains investissements étrangers », notamment l'article L. 151-3 du code monétaire et financier qui soumet ceux-ci à une procédure d'autorisation préalable dans le cas où ils pourraient nuire aux intérêts du pays. Malgré tout, Laurent Izard estime que la réalité du terrain est différente de celle du papier. « Ces outils de contrôle sont assez peu utilisés, et ils aboutissent rarement à un veto de Bercy. Bercy contrôle et donne parfois son accord sous conditions – notamment en termes de défense de l'emploi ou de maintien des sites industriels, poursuit Laurent Izard. Mais en réalité, il est très compliqué de vérifier que les investisseurs respectent ces conditions », conclut-il. ■



© Marek Piwnicki via Unsplash



© Alex Knight via Unsplash

Tech : 8 start-up stratégiques qui sont passées sous contrôle étranger ces dernières années

Mélanie Roosen ■ 22 février 2022

À l'heure où le gouvernement français essaye de valoriser les pépites tech par tous les moyens, force est de constater qu'une bonne partie de celles qui développent des innovations stratégiques passent sous le joug américain. Tour d'horizon.

Les pépites étrangères qui souhaitent se développer doivent-elles forcément se tourner vers l'étranger ? La liste des licornes françaises de 2021 tend à confirmer le phénomène : les levées de fonds sont, en grande partie, menée par des fonds étrangers. La tendance dure depuis quelques années, et concerne des entreprises issues de secteurs très stratégiques.

ALDEBARAN ROBOTICS, RACHETÉE PAR SOFTBANK (JAPON), 2012

On se rappelle toutes et tous de Pepper, le mignon robot, star des aéroports et des salons en tout genre chargé d'accueillir les visiteurs. À l'origine du projet, une société française, Aldebaran Robotics, véritable pépite en matière de

robotique. En 2012, le groupe japonais Softbank investissait 100 millions d'euros dans Aldebaran Robotics contre 78,6% du capital. À l'époque, Arnaud Montebourg, alors ministre du Redressement productif, mise beaucoup sur la robotique pour redresser le pays. Pour éviter le scandale, la vente est tenue secrète… mais fuite dans le Financial Times et Les Echos avant que les principaux intéressés n'aient le temps de confirmer. Plus tard, en 2015, Softbank monte à 95% sa participation au capital de l'entreprise.

Aujourd'hui, les robots de Softbank robotics sont utilisés dans de nombreux secteurs : le retail, la finance, la santé… Le Covid-19 a même donné de nouvelles fonctions à Pepper, qui se charge de détecter le bon port du masque, ou d'accompagner les entreprises dans de nouveaux dispositifs de téléprésentiel.

CAPSULE TECHNOLOGIE, RACHETÉE PAR QUALCOMM (ÉTATS-UNIS), 2015

La crise du Covid a rappelé l'importance de la santé en matière de souveraineté. En 2015, la société parisienne Capsule Technologie, spécialisée dans les solutions de connectivité des appareils biomédicaux, l'optimisation du suivi et de la prise en charge des patients, était rachetée par Qualcomm Life, la division santé de Qualcomm. Un mouvement pas si surprenant, puisque Capsule Technologie réalisait déjà la majeure partie de ses revenus aux États-Unis. Six ans plus tard, le gouvernement français fait de la santé connectée l'un de ses chevaux de bataille et lance une stratégie d'accélération sur la santé numérique.

MOODSTOCKS, RACHETÉE PAR GOOGLE (ÉTATS-UNIS), 2016

Experte en deep learning et reconnaissance d'images directement depuis la caméra des smartphones, la start-up Moodstocks n'aura pas mis longtemps à taper dans l'œil de Google. Intégrées au centre de R&D parisien du géant américain, les équipes se font plutôt discrètes depuis l'acquisition. Il faut dire que pour certains, la technologie pourrait transformer n'importe quel appareil qui en est équipé en véritable espion…

MEDTECH, RACHETÉE PAR ZIMMER BIOMET (ÉTATS-UNIS), 2016

Les robots d'assistance chirurgicale de Medtech ont séduit Zimmer Biomet, leader mondial dans les soins musculosquelettiques. Une acquisition qui fait suite à un précédent rachat de la part de Zimmer Biomet : celui des brevets du premier robot produit la société montpelliéraine. À l'époque, la directrice de la communication de Medtech Sophie Munoz-Vincent expliquait qu'il s'agissait d'une nécessité. « Même si nous avions réussi à lever des fonds avec notre introduction boursière, l'effort financier pour poursuivre notre croissance à l'export, où nous faisons 80% de l'activité, était colossal et nous a poussés à

privilégier cette option », déclarait-elle. Une opportunité manquée côté française, puisque la robotique figure dans le plan de financement de santé numérique du gouvernement.

EDEVICE, RACHETÉE PAR IHEALTH (ÉTATS-UNIS), 2016

eDevice, entreprise bordelaise pionnière de l'IoT et leader de la santé connectée, a été rachetée par la Californienne iHealth, qui propose une gamme de produits de santé connectée. Le groupe a déboursé près de 94 millions d'euros pour acquérir la pépite française, avec l'objectif de répondre aux conséquences du vieillissement de la population et des solutions de mSanté. Pour les équipes d'eDevice, il s'agissait d'une opportunité pour « conquérir des marchés mondiaux, grâce à une présence géographique plus importante et davantage de ressources », selon les mots de son co-fondateur Stéphane Schinazi. Côté France, le gouvernement ambitionne de s'appuyer entre autres sur l'internet des objets pour dynamiser une médecine 5P (personnalisée, préventive, prédictive, participative, par des preuves).

PROPHESEE, SOUTENUE PAR IN-Q-TEL (ÉTATS-UNIS), 2016

Le cas de Prophesee a fait couler beaucoup d'encre. Il faut dire que l'entrée d'In-Q-Tel au capital de la start-up tricolore n'a rien d'anodin : il s'agit du fonds d'investissement de la CIA. La technologie de Prophesee est capable de reproduire les capacités de l'œil humain en matière de surveillance, de détection d'obstacles ou de ciblage d'individus. Cette prise de capital remonterait à 2016 et n'a été dévoilée qu'en octobre 2021 – tout en n'ayant pas été confirmée ni infirmée par les principaux intéressés. Par ailleurs, depuis l'été 2021, Prophesee compte également de nouveaux actionnaires chinois – Sinovation et Xiaomi. Pour de nombreux analystes, c'est une réelle perte de souveraineté. Le Sénat avait d'ailleurs publié un rapport en juillet 2020, soulignant que les technologies de défense françaises – auxquelles peuvent être rattachées les activités de Prophesee – sont « à la fois une conséquence et un instrument de la souveraineté, un élément indispensable de notre liberté. »

SENTRYO, RACHETÉE PAR CISCO (ÉTATS-UNIS), 2019

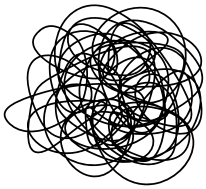
La start-up lyonnaise Sentryo a séduit Cisco avec sa solution de visibilité et de sécurité pour les réseaux de systèmes de contrôle industriels. L'objectif pour le spécialiste américain : renforcer son offre sur le marché de l'IoT industriel. Toujours basées à Lyon, les équipes de Sentryo bénéficient en contrepartie d'une meilleure visibilité à l'international : un an après l'acquisition, la technologie de Sentryo avait séduit des clients en Inde, au Japon ou en Australie

et les effectifs de la start-up avaient doublé. De quoi faire craindre pour la souveraineté française, ou se réjouir ? La Chaire Digital, Gouvernance et Souveraineté de l'École d'affaires publiques de Sciences Po se posaient la question à l'occasion d'une table ronde en présence de Sentryo : comment atteindre un équilibre entre investissements étrangers et souveraineté numérique dans un contexte de féroce compétition technologique entre les États ?

ALSID, RACHETÉE PAR TENABLE (ÉTATS-UNIS), 2021

La cybersécurité est, de l'avis de plusieurs experts, l'un des secteurs à protéger en priorité en matière de souveraineté. Cela n'a pas empêché l'Américain Tenable de racheter la pépite Alsid, qui propose une solution de protection et de sécurisation d'Active Directory, l'annuaire de Microsoft qui permet l'identification et l'authentification sur un réseau d'ordinateurs utilisant un système Windows. La solution permet ainsi d'identifier en temps réel les potentielles attaques. Une lourde perte, alors que la résistance s'organise du côté des fonds français et européens pour faire décoller les pépites cyber.

En-dehors des frontières françaises, les enjeux de protection des start-up stratégiques concernent l'Europe entière. C'est d'ailleurs ce qui a poussé le Parlement européen à adopter le Digital Markets Act en décembre 2021. Le texte contient des mesures pour réguler les pratiques commerciales des grandes entreprises du numérique, afin de protéger de leurs appétits les pépites européennes. Reste à voir si protéger les jeunes pousses pourra leur éviter, à un stade de développement avancé, de passer sous le joug étranger : en 2018, le leader des micro-connecteurs pour cartes à puces Linxens, créé en 1986, s'était fait racheter par le groupe chinois Tsinghua Unigroup. À l'époque, le projet avait été validé par Bercy, qui jugeait que l'activité de Linxens n'était pas stratégique. Qautre ans, une pandémie, et de nombreuses pénuries plus tard cette décision peut prêter à débat. ■



Déstabilisation informelle, l'autre menace qui pèse sur nos entreprises stratégiques

Mélanie Roosen ■ 23 février 2022

Les entreprises sont parfois la cible d'acteurs malveillants. Qu'il s'agisse de concurrents ou d'activistes, tous les moyens sont bons pour déstabiliser une activité : de l'espionnage économique aux fake news, attention aux attaques informelles !

« Comment les États-Unis contribuent-ils à affaiblir l'économie française ? » Cette question, l'École de Guerre Économique la posait lors de la rédaction d'un rapport d'alerte en octobre 2021. Bien entendu, les dynamiques de déstabilisation observées ne se limitent pas aux États-Unis et à la France, mais le rapport vise à montrer que, même « entre pays alliés », les attaques économiques de déstabilisation informelle sont fréquentes. Très proches, méthodiquement parlant, du monde du renseignement, elles sont souvent opérées de façon cachée. Une mise en lumière de ces pratiques permet, sinon de s'en prémunir, de comprendre comment réagir en cas d'attaque.

© Markus Winkler via Unsplash

ESPIONNAGE ÉCONOMIQUE

L'une de ces manœuvres est l'espionnage économique, ou industriel. Régulièrement utilisé comme un moyen pour déployer d'autres actions plus qu'une fin en soi, il permet de collecter des informations pour alimenter et mettre en œuvre une offensive économique. Il peut prendre plusieurs formes, alerte le cabinet PwC. Vol d'ordinateur, attaques informatiques, espionnage à l'occasion d'une visite… Et mauvaise nouvelle pour les PME et ETI : celles-ci représentent 71% des entreprises victimes d'espionnage économique, selon le rapport d'activité 2019/2020 de la DGSI. Souvent moins équipées (et moins méfiantes) que les grands groupes, elles sont visées en tant que « portes d'entrée » vers des entreprises stratégiques. Les risques sont multiples : vols de secrets de fabrication, atteinte réputationnelle, pertes économiques…

En France, l'organe chargé de lutter contre l'espionnage économique est la DRSD (Direction du Renseignement et de la Sécurité de la Défense). À l'occasion d'un discours prononcé le 6 janvier 2022, Florence Parly, alors ministre des Armées, rappelait qu'en « quelques années, les demandes d'enquêtes administratives adressées à la DRSD ont augmenté de près de 150% » pour atteindre 370 000 requêtes par an. Pour faire face à cette « bataille immatérielle », la loi de programmation militaire dédie 295 milliards d'euros entre 2019 et 2025 afin d'augmenter notamment les capacités de renseignement françaises.

Du côté des entreprises, il est impératif de maîtriser ses informations stratégiques, de protéger son savoir-faire et d'assurer la sécurité de sa structure et de ses services pour éviter d'être victime d'espionnage économique.

MANIPULATION DE L'INFORMATION

Une autre tactique de déstabilisation informelle est la manipulation de l'information. Fake news ou contre-vérités : elles sont redoutables sur un temps très limité. Les services de vérification de l'information permettent en général de dévoiler les manipulations, ce qui n'empêchent pas celles-ci de faire de gros dégâts. Elles peuvent d'ailleurs s'appuyer sur des faits réels qui n'ont pas vocation à être diffusés. C'est d'ailleurs lorsque les fausses informations sont mêlées à des faits vérifiables qu'elles sont le plus difficiles à déceler. Dans un communiqué daté du 20 janvier 2022, Wiztrust, solution de certification de l'information des entreprises, analysait que 2021 avait été propice aux fake news financières. À leur origine : des activistes qui veulent dénoncer les comportements de certaines entreprises, des hackers qui veulent s'enrichir… et parfois des agences de communication, mandatées par des entreprises concurrentes.

Fake news peut-être, mais dégâts bien réels : chute du cours de l'action pour les unes, attaques réputationnelles pour les autres, baisse des ventes dans certains cas… En 2016, Vinci était ainsi victime d'un faux communiqué de presse reprenant l'identité graphique du groupe, et indiquant que le directeur financier

avait été licencié à la suite de nombreuses malversations comptables. La diffusion du communiqué de presse par Bloomberg et Dow Jones a fait chuter le cours de bourse de Vinci de 19% pendant une heure.

Pour lutter, plusieurs solutions. La blockchain semble être une piste privilégiée : la Société Générale a par exemple choisi la solution de la start-up KeeX pour certifier ses communiqués, et 20% de l'information du SBF 120 utilise la technologie Wiztrust. Enfin, en cas d'attaque informationnelle, le cabinet Haas Avocats rappelle qu'il existe des moyens juridiques pour redorer son blason et obtenir une compensation financière. Cependant, la réactivité est de mise. La loi de 1881 prévoit un délai de prescription très court : 3 mois seulement à partir de la diffusion de l'information trompeuse. ■

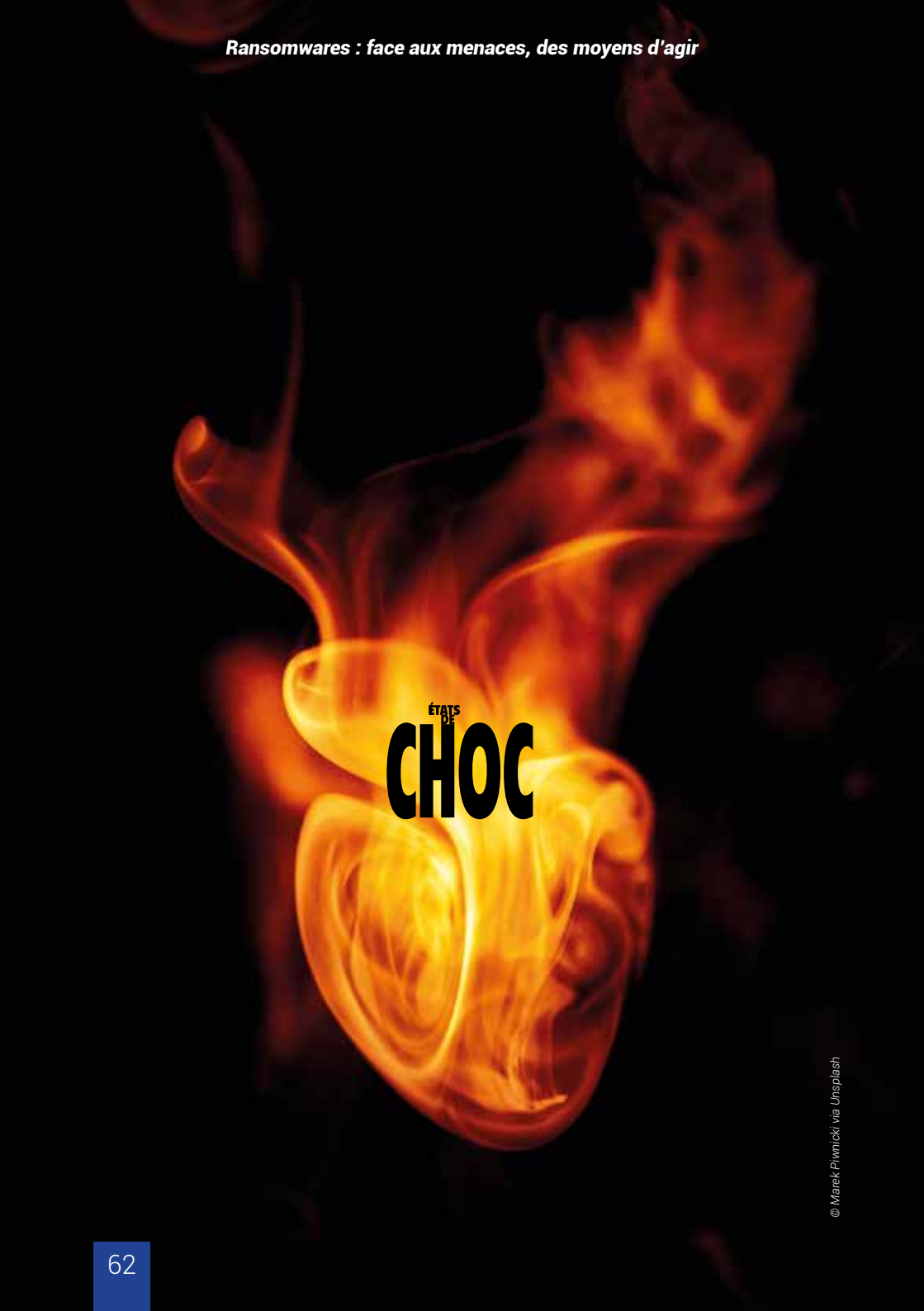
© Sheldon Liu via Unsplash

Ransomwares : face aux menaces, des moyens d'agir

© Jefferson Santos sur Unsplash

DOSSIER N° 2 ■ 7 février 2022

En moyenne, une entreprise française est touchée par un ransomware tous les deux jours. Et pour une entreprise attaquée, ce sont potentiellement 150 entreprises qui sont en danger : les hackers utilisent les données récupérées lors des attaques pour toucher d'autres sociétés. Parmi les victimes, 44% de PME. Les conséquences de ces chiffres qui donnent le tournis ne sont pas toujours malheureuses. Certaines organisations s'en sortent, d'autres choisissent de porter plainte, permettant ainsi aux autorités d'enquêter. Enfin, de plus en plus de jeunes pousses technologiques prometteuses voient le jour. Autant de facteurs qui sont porteurs d'espoir pour les PME et ETI : ce n'est pas parce que l'on n'a pas, en interne, les moyens d'employer un RSSI à temps plein que l'on ne peut pas se prémunir des attaques.



© Marek Piwnicki via Unsplash

Les PME, premières cibles des ransomwares

Mélanie Roosen ■ 7 février 2022

Au moins 20% des entreprises françaises ont subi une attaque par rançongiciel en 2020. À mesure que les attaques se diversifient, les signalements augmentent. État des lieux des menaces actuelles.

« Le ransomware, c'est l'arme du pauvre. C'est ce qui explique son succès, et c'est ce qui rend les PME particulièrement vulnérables », estime Fabrice Epelboin, enseignant à l'IAE de Poitiers et Sciences Po Paris. Cet expert en géopolitique et cybersécurité explique qu'il n'est plus nécessaire d'avoir des compétences techniques ou d'importants moyens financiers pour lancer une attaque de ce type. Il existe désormais des ransomwares « prêts à l'emploi », qui ne coûtent rien (à part le partage des gains avec le développeur du logiciel malveillant), et qui visent large, sans distinction. Quelle est l'ampleur de la situation ?

©Bady Abbas via Unsplash

UNE PROGRESSION DIFFICILE À CHIFFRER

En novembre 2021, le service Interstats du ministère de l'intérieur publiait une étude sur l'état des ransomwares en France. De 2016 à 2020, entre 1 580 et 1 870 plaintes en lien avec des attaques par rançongiciel auraient été enregistrées. Parmi celles-ci, 15% concernent les entreprises et les institutions.

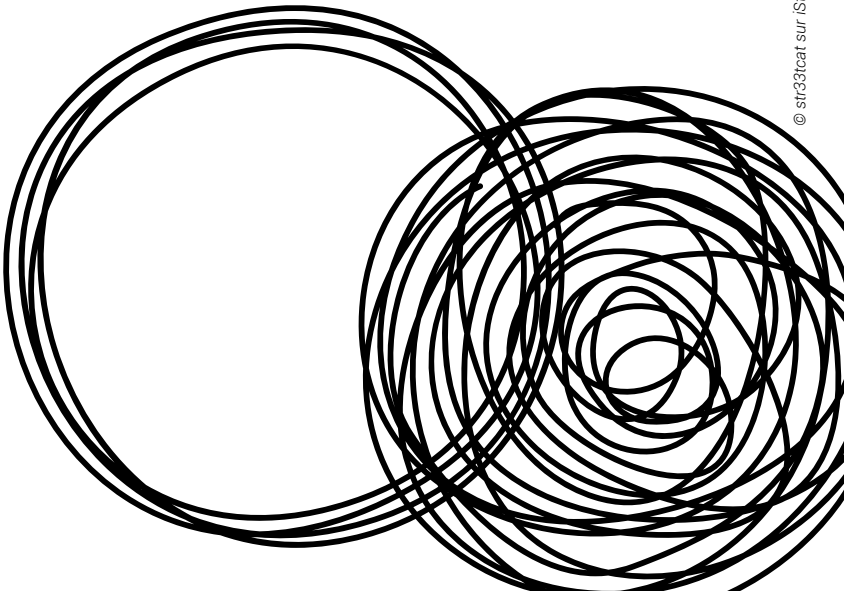
Les chiffres de l'Agence Nationale de la Sécurité des Systèmes d'Information donnent encore plus le vertige : l'Anssi mesure une augmentation de 255% des signalements d'attaques par ransomwares envers des organismes publics ou privés entre 2019 et 2020 – et ceux-ci ne s'accompagnent pas toujours d'une plainte formelle.

Du côté des montants des rançons, ils ne sont renseignés que dans 16% des procédures. Entre 2016 et 2020, seules 7 entreprises ont déclaré des rançons supérieures ou égales à 250 000 euros. La valeur médiane des rançons est passée de 1 350 euros en 2016 à 6 375 euros en 2020, augmentant en moyenne de 50% par an. Bonne nouvelle néanmoins : la tendance au paiement des rançons serait à la baisse (5% en 2021 contre 20% l'année précédente). Selon le cabinet Wavestone, c'est le signe d'une meilleure compréhension des enjeux et d'une plus grande capacité à régler le problème en interne, peut-on lire dans un rapport sur l'état des ransomwares en France réalisé en octobre 2021.

DES ATTAQUES QUI SE DIVERSIFIENT

Dans 80% des attaques, les ransomwares sont le fait de groupes criminels selon l'ONUDC (Office des Nations Unies contre les Drogues et le Crime). Mais les auteurs de ces délits n'ont plus nécessairement besoin de développer de compétences techniques complexes. Les plateformes de « ransomwares as a service » fournissent directement des rançongiciels, moyennant l'obtention d'un pourcentage de la somme rançonnée.

Les chiffres du ministère de l'intérieur confirment qu'une infraction d'atteinte aux systèmes de traitement automatisé des données (STAD) est identifiée dans 82% des attaques par ransomwares, mais il existe d'autres types d'assaut,



© str33tcat sur iStock

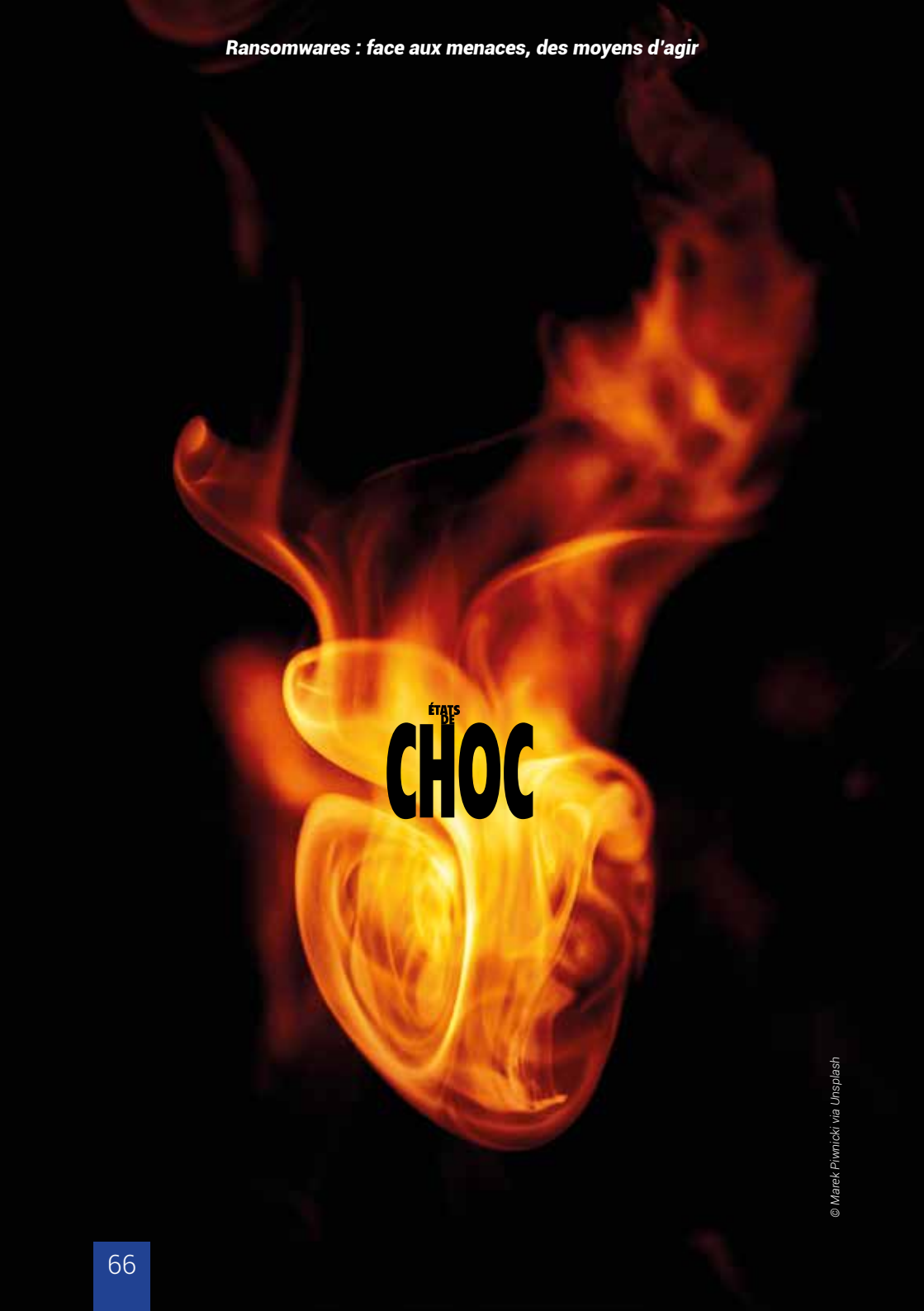
comme le chantage pour extorsion de fonds ou l'abus de confiance. Au-delà du blocage du service informatique, la combinaison avec un vol de données se fait de plus en plus fréquente (30% des cas), rapporte Wavestone.

Dans la majorité des attaques, il s'agit de campagnes non ciblées. E-mails, téléchargements automatiques (« drive by download »), logiciels gratuits ou publicités malveillantes (« malvertising »)… Ces attaques installent des logiciels pirates via une pièce jointe ou une page web. Wavestone analyse que le principal canal d'accès est l'utilisation de comptes valides (23% des attaques), suivi des e-mails frauduleux (20%) et des services d'accès distants grâce à des failles de sécurité ou des défauts de configuration (18%).

Lorsque les attaques sont ciblées, les cybercriminels cherchent à obtenir des listes d'adresses de messagerie professionnelles sur le darknet, avec l'objectif de toucher directement les entreprises dont certaines données sensibles sont stockées sur les ordinateurs des salariés.

COMMENT S'ORGANISER ?

La meilleure des préventions reste la sensibilisation des équipes, notamment grâce à la mise en place d'exercices. Il peut être utile de mettre en place un service de détection d'attaques, actif 24 heures sur 24. Enfin, de nouvelles offres de cyberassurance voient le jour et doivent permettre aux entreprises d'identifier leurs failles en amont, de minimiser la perte des données et de se faire rembourser en cas de paiement d'une rançon. C'est par exemple le cas de Stoïk, première cyber-insurtech française à associer assurance et logiciel de sécurité, qui a annoncé une levée de fonds de 3,8 millions d'euros le 12 janvier 2022. ■



© Marek Piwnicki via Unsplash

Jean-Charles Duquesne *(La Normandise)* « La priorité en cas de cyberattaque, c'est d'assurer la tranquillité du service informatique »

Photo - Par Mélanie Roosen ■ 8 février 2022

Visée par un ransomware, La Normandise s'en est bien sortie : un peu de chance, beaucoup de réactivité et une bonne dose de sang-froid ont permis de limiter les dégâts.

Votre entreprise a été touchée par un ransomware en octobre 2020. Que s'est-il passé ?

Jean-Charles Duquesne : Notre entreprise produit des aliments pour chiens et chats. Notre usine tourne 24 heures sur 24, 7 jours sur 7. L'équipe du lundi matin est arrivée à 5 heures et a remarqué dès 6 heures que les outils nécessitant un accès aux serveurs étaient lents ou buguaient. Une personne de la maintenance informatique a immédiatement éteint tous les serveurs. Le service informatique a été prévenu, et je suis arrivé sur le site aux environs de 8 heures. C'est à ce moment-là que nous avons relancé les machines : tous nos fichiers étaient infectés par un cryptovirus, c'est-à-dire qu'ils étaient cryptés et inaccessibles. Nous n'avions accès qu'à un fichier « .txt », au sein duquel se trouvaient les coordonnées de l'émetteur du cryptovirus – une adresse e-mail russe – pour payer la rançon, dont nous ne connaissions pas le montant. Nous avons relancé les serveurs sans les connecter les uns aux autres pour mesurer l'étendue des dégâts et nous avons utilisé un système d'exploitation alternatif pour identifier les disques durs touchés. Nos sauvegardes étaient en bon état. Nous avons donc choisi de ne pas contacter l'émetteur et de rétablir nos fichiers nous-mêmes. Dans notre malheur, nous avons eu de la chance : la première, c'est d'avoir une usine qui fonctionne en continu, avec quelqu'un capable de réagir vite sur place. La seconde, c'est le cœur de notre activité : nous ne produisons pas à flux tendu, les stocks ne s'écoulent pas du jour au lendemain. La troisième, c'est que nous avions prévu de remplacer notre matériel, et que nous avions donc à disposition de nouveaux serveurs, ce qui nous a permis de ne pas utiliser les serveurs infectés. Tous ces facteurs nous ont permis de nous en sortir indemnes, sans avoir à payer de rançon. Tout le monde n'est pas aussi bien loti : je fais partie du groupement d'entrepreneurs normands N'Way,

et l'un des membres a également été victime d'un ransomware. Il n'a pas eu d'autre choix que de payer. Pour débloquer son premier disque dur, il a dû verser 100 euros. Pour le second, les pirates lui en demandaient 1 000. Si on ajoute un zéro à chaque fois qu'il faut débloquer un disque dur, la note peut être salée.

Comment s'est organisée la journée du service informatique ?

J.-C. D. : Mon frère, qui est également directeur général, et moi-même étions les seuls interlocuteurs du pôle informatique, pour qu'il ne soit pas parasité par les demandes des chefs de services. Nous leur avons mis à disposition des snacks et des boissons. Nous organisions un point toutes les heures, afin de mesurer la progression de la restauration des fichiers. Enfin, nous avons demandé aux équipes de quitter l'entreprise à 18 heures pour qu'elles puissent se reposer et reprendre sereinement le lendemain.

Et comment s'est organisée la journée des autres salariés ?

J.-C. D. : Nous sommes, à l'origine, une entreprise familiale. Même si nous avons grandi, l'esprit de famille subsiste. Résultat, le lundi matin, tout le monde a… fait le ménage ! Cela a permis de garder une ambiance vraiment positive. Vers midi, nous avons demandé à toutes les personnes travaillant aux services généraux de prendre une journée de congé entre le lundi après-midi et le mardi matin. 99% des salariés ont joué le jeu. En termes d'émotions, c'était un peu les montagnes russes. Mais finalement, cela a un peu fait office de team building de l'extrême !

Comment avez-vous priorisé les différents services à rétablir ?

J.-C. D. : En débranchant les serveurs, l'usine était à l'arrêt. Les équipes ont continué à fabriquer « à l'aveugle » les produits récurrents, en laissant de côté les produits hors standard et dès 17 heures, l'usine était de nouveau fonctionnelle. La période d'arrêt nous aura coûté 100 000 euros en non-production. Nous avons très vite remis en place le service RH ainsi que les services de sécurité. Le lendemain, les services de facturation et communication étaient opérationnels. Enfin, le mercredi, l'ensemble des données et l'accès aux e-mails étaient rétablis. En 48 heures, tout était réglé.

Vous n'avez pas contacté l'émetteur du ransomware, mais avez-vous porté plainte ?

J.-C. D. : J'ai été à la gendarmerie du coin, qui m'a très bien reçu, mais j'ai rapidement constaté qu'il n'y avait pas un engouement particulier à mener l'enquête. J'ai dû épeler « ransomware », ça en dit long sur l'état des connaissances de la gendarmerie. J'ai finalement fait un signalement auprès de l'Anssi, et les choses ont alors été très différentes : j'ai dû leur fournir un fichier cryptolocké, un disque dur infecté, et une enquête a été lancée.

© La Normandise

Avez-vous mené certaines actions en interne après l'attaque ?

J.-C. D. : Le premier investissement qui a suivi l'attaque concerne nos outils : notre vitesse de sauvegarde est 100 fois plus rapide aujourd'hui, ce qui coûte une centaine de milliers d'euros. Par ailleurs, l'hypothèse la plus probable, c'est que l'attaque venait d'un e-mail malveillant qui a été ouvert par l'équipe de production. Le second investissement concerne donc la sensibilisation : nous avons mandaté une entreprise, qui envoie régulièrement des e-mails aux équipes pour mesurer le pourcentage de personnes qui les ouvrent puis cliquent sur des liens potentiellement dangereux. De 30% avant la crise, nous sommes passés à 2%. Je le dis avec fierté, d'autant plus que jusqu'à récemment les deux plus mauvais salariés de l'entreprise sur le sujet ont été… mes parents. Ils ont fondé l'entreprise, et pendant très longtemps, ils n'ont eu qu'une seule adresse e-mail qui leur servait pour les sujets pros et persos. Ils cliquaient sur tous les messages qu'ils recevaient ! ■

Biographie de Jean-Charles Duquesne

Diplômé de l'Ecole Vétérinaire de Maisons-Alfort en 2002 avec une spécialisation en diététique canine et féline, Jean-Charles Duquesne rejoint NORMANDISE Pet Food en avril 2004 en tant responsable Qualité et R&D. Son engagement et sa passion des chats et chiens lui ont permis d'évoluer dans l'entreprise. Il en est maintenant Directeur Général avec son frère, assurant ainsi la continuité familiale et la transition générationnelle.

© Pixabay via Pexels

Face aux menaces, comment les solutions cyber se structurent-elles ?

Par Mélanie Roosen ■ 9 février 2022

Les PME n'ont pas toujours les moyens, en interne, de s'équiper pour faire face aux cyberattaques. Entre les fonds, les offres et les services spécialisés, des solutions existent. Tour d'horizon.

Fin août 2021, le fonds d'amorçage dédié à la cybersécurité Cyber Impact était lancé au niveau européen. Son objectif : investir dans les pépites de la cybersécurité françaises et européennes, avec l'ambition de les faire grandir et d'en faire des championnes dans leur secteur. Le tout, avec un soupçon de souveraineté. « Quand nos entreprises atteignent une certaine taille, elles sont systématiquement rachetées par des fonds ou des entreprises étrangères » regrette Jean-Noël de Galzain, co-fondateur de Cyber Impact et entrepreneur.

Celui qui a aussi fondé Wallix, éditeur français de logiciels de sécurité informatique, connaît bien son domaine. « La cybersécurité devient une filière absolument stratégique. C'est aussi pour cela que nous avons réuni autour de nous une soixantaine d'entrepreneurs, d'industriels, de RSI, d'ingénieurs, de financiers et même de militaires. » Au total, ce sont 30 à 50 millions d'euros qui seront investis dans 30 à 40 pépites. « Cela peut paraître faible au regard des levées de fonds israéliennes ou américaines. Mais est-ce que c'est la taille des levées de fonds qui fait le succès des sociétés ? Je n'en suis pas certain. Par ailleurs, nous intervenons très tôt dans la chaîne de financement, avant même la série A. »

ÉVITER LES CYBERATTAQUES ET PROTÉGER SES DONNÉES

Quand on l'interroge sur les grandes tendances en matière de « pépites cyber », Jean-Noël de Galzain identifie « deux grands piliers : d'une part les technologies qui permettent d'éviter les cyberattaques, de l'autre celles qui permettent de protéger les données des entreprises. »

La promotion 2021 de l'accélérateur Hexatrust, qui accompagne les jeunes pousses européennes de la cybersécurité, confirme la tendance. On y retrouve ainsi CryptoNext Security, qui développe des solutions de cryptographie des données résistantes à la menace quantique qui pèse sur les infrastructures : l'arrivée de l'ordinateur quantique va permettre de « casser » les algorithmes de cryptographie qui sécurisent les réseaux internet aujourd'hui, mais aussi ceux des applications de messagerie ou de blockchain. Patrowl, qui permet d'automatiser l'identification des failles de cybersécurité et de les corriger est également dans la liste, ainsi que ProHacktive, qui a vocation à démocratiser les audits de cybersécurité.

Certaines solutions ont pour ambition d'accompagner les entreprises sur le long terme. C'est le cas de Stoïk, première cyber-insurtech à associer couverture d'assurance et logiciel de veille, qui a annoncé une levée de fonds de 3,8 millions d'euros le 12 janvier. Jules Veyrat, co-fondateur, met un point d'honneur à agir en amont pour ses clients. « Notre logiciel évalue les infrastructures des entreprises en temps réel. Notre objectif, c'est d'être efficace en prévention et de minimiser les attaques. C'est dans notre intérêt, bien

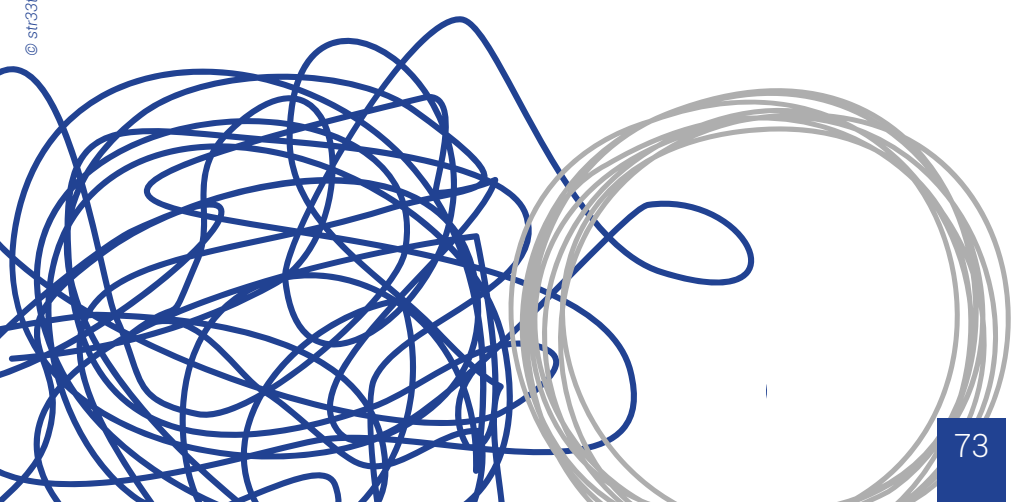
sûr, mais aussi dans celui des clients », promet le patron. Pour relever le défi, une équipe composée pour moitié d'ingénieurs en cybersécurité. « Il faut se mettre dans la peau des pirates. Si nous réussissons à trouver des failles, ils les trouveront aussi. »

SAVOIR S'ENTOURER

La réactivité est primordiale en cas de cyberattaque. C'est pour cela que les entreprises qui ne disposent pas de service informatique à temps plein peuvent choisir de se tourner vers le temps partagé, qui permet d'embaucher un salarié via une structure tierce sur un temps donné. C'est ce que propose Securitrust, par exemple, qui propose d'embaucher DPO (data protection officer) ou RSSI (responsable de la sécurité des systèmes d'information) à raison d'un jour par mois.

Autre solution : se tourner vers un répertoire de prestataires spécialisés. C'est l'une des offres de l'Alliance pour la Confiance Numérique (ACN), qui a mis au point un Répertoire National des Entreprises de la Confiance Numérique. « À terme, nous pourrons par exemple recenser toutes les entreprises disposant d'offres permettant la sécurisation du télétravail », espère Yoann Kassianides, délégué général de l'ACN. Le projet devrait s'étendre en 2022 au reste de l'Europe, porté par l'European Cyber Security Organisation (Ecso), afin de proposer une marketplace capable d'évaluer toutes les entreprises européennes de la cybersécurité.

Pour les PME et ETI, le signal est positif. En investissant sur des solutions externalisées, il est possible de se protéger, tout en dépendant de moins en moins des solutions américaines, russes ou chinoises. Mais plutôt que d'être dans une posture de « réaction », la meilleure solution reste l'anticipation et la sensibilisation. ■



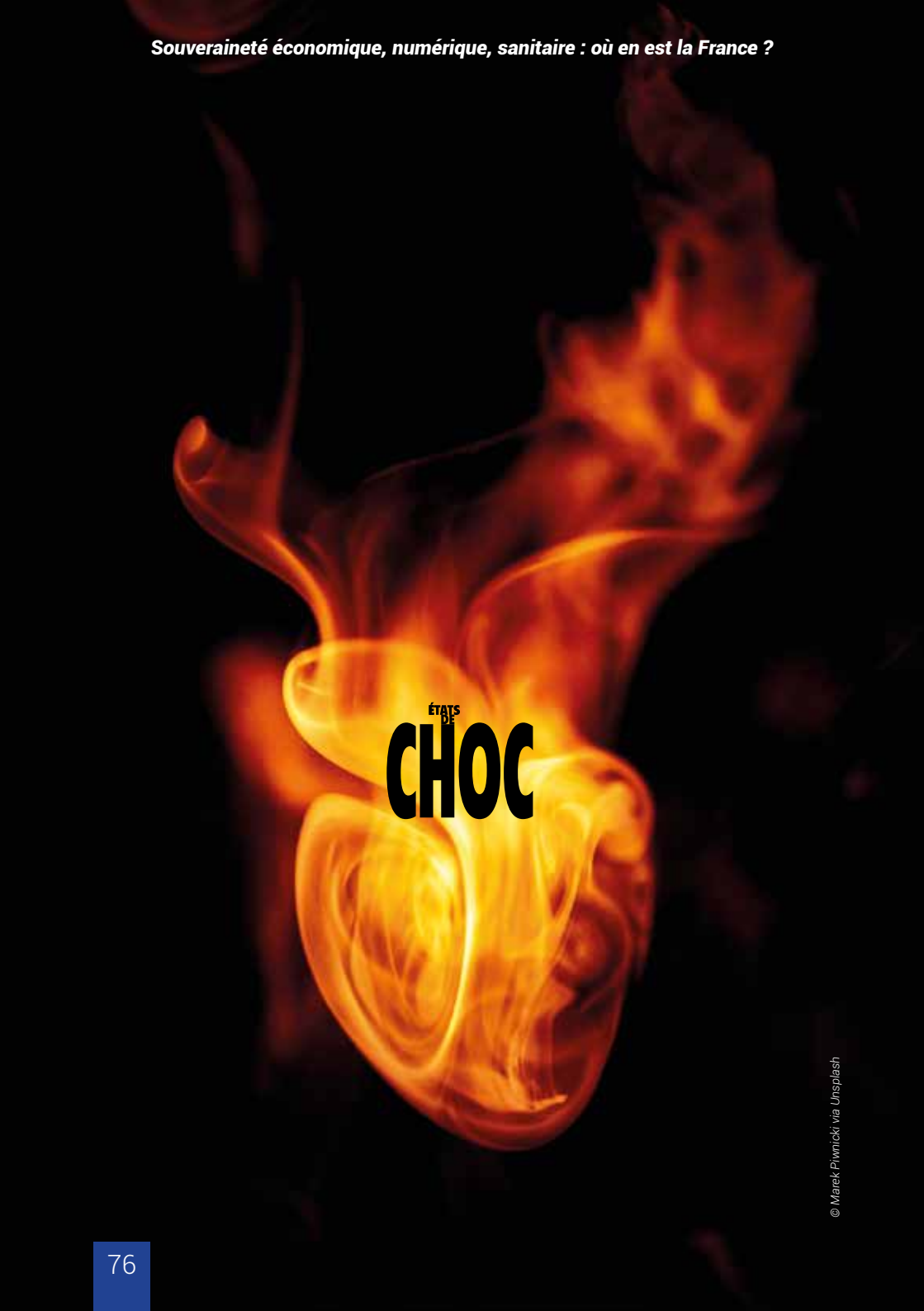
© Popartic via iStock

ÉTATS DE CHOC

Souveraineté économique, numérique, sanitaire : où en est la France ?

DOSSIER N° 1 ■ 1 février 2022

La souveraineté est dans tous les discours – des politiques et des entreprises. Il faut dire que la pandémie a sacrément rebattu les cartes : le moindre couac dans le rouage, pourtant bien huilé, de la globalisation peut paralyser des pans entiers de l'économie, peu importe le secteur. Même ceux que l'on pensait maîtriser, comme l'énergie, viennent à montrer leurs limites en matière d'autonomie. Dans ce contexte, comment remonter la pente ? La solution est-elle à la réindustrialisation ? Aux investissements ? Faut-il jeter l'éponge pour certains secteurs ? Les points de vue divergent, les stratégies aussi. Mais les constats convergent : la souveraineté économique est un enjeu de sécurité nationale, de puissance internationale, et de vision stratégique.



© Marek Piwnicki via Unsplash

Souveraineté : quels secteurs d'activité faut-il protéger en priorité ?

Mélanie Roosen ■ 31 janvier 2022

© Alvaro Reyes via Unsplash

Quand on parle de souveraineté, c'est en général que l'on craint une crise. Une surveillance particulière s'impose pour les secteurs les plus stratégiques, sauf que ceux-si sont aussi mouvants. C'est ce qui rend leur identification et leur protection parfois difficiles.

« Si on parle autant de souveraineté aujourd'hui, c'est parce que nous passons totalement à côté du sujet », s'agace l'économiste Christian Saint-Étienne, titulaire de la chaire d'économie industrielle au conservatoire national des Arts et Métiers. « Depuis 50 ans, l'Europe fait preuve de négligence sur la base que 'tout peut s'acheter' : si on ne fabrique pas, on peut acheter ailleurs. Mais la pandémie a montré les limites de ce raisonnement : les circuits peuvent se retrouver bloqués, et il faut alors faire face aux pénuries. » Une analyse partagée par l'avocat spécialisé en droit des affaires et en intelligence économique

Olivier de Maison Rouge. « Avec la globalisation, nous pensions pouvoir créer des 'entreprises sans usines' », rappelle-t-il en citant le rêve Serge Tchuruk, ancien président d'Alcatel.

SORTIR DE LA LOGIQUE QUI VISE À « ACHETER PLUTÔT QUE PRODUIRE »

La tendance se vérifie en France par étapes dès les années 70, sur fond de désindustrialisation. Une étude de l'Insee révélait que les années 80 ont été la décennie de l'externalisation pour les entreprises, mais que ce sont les années 2000 qui ont vraiment inversé la vapeur en matière de solde extérieur. De +10,5 milliards en 2000, il passe à -10,7 milliards en 2007, puis à -46,5 milliards d'euros en 2020, note l'Insee. Plusieurs causes sont identifiées, notamment le faible investissement en recherche et développement et la taille insuffisante du nombre d'entreprises exportatrices. Cette logique d'acheter ailleurs plutôt que de produire en France s'applique à tous les secteurs. « Prenons l'industrie agro-alimentaire. Nous avons, en France, les ressources pour exploiter la terre. Et pourtant nous produisons de moins en moins, et dépendons d'aliments essentiels venant de l'étranger. Nous pourrions par exemple cultiver du soja en France, mais nous achetons celui qui vient d'Amérique du Sud au nom de l'efficacité économique », constate, amer, l'économiste à l'université d'Angers David Cayla.

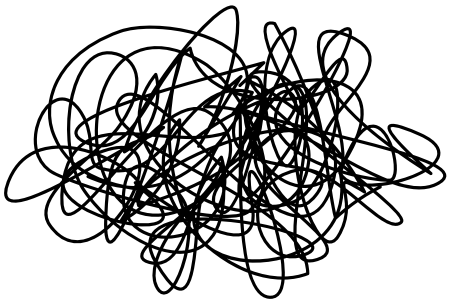
ORGANISER LA SOUVERAINETÉ

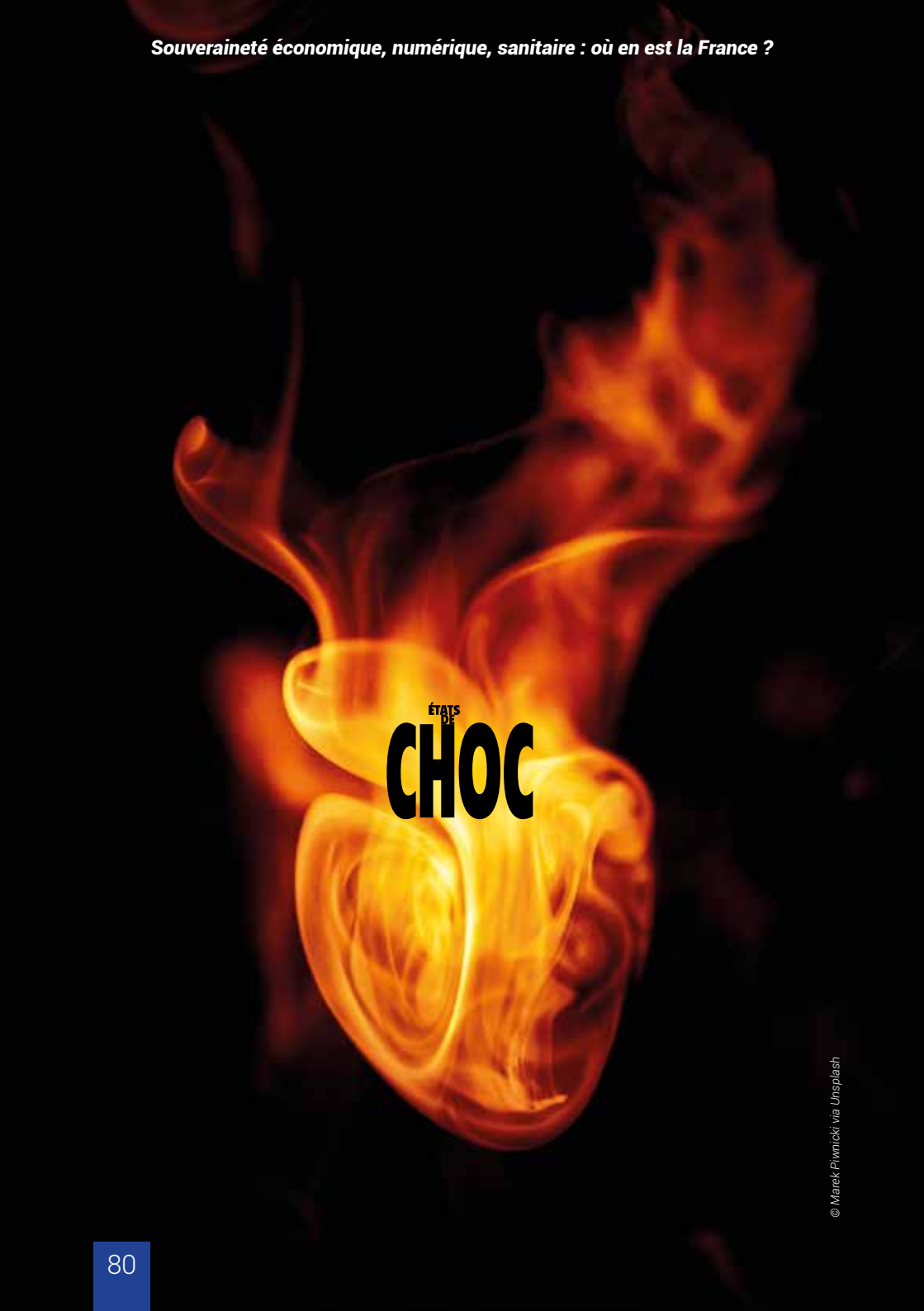
Pour inverser la tendance, la première chose à faire serait de définir les domaines de souveraineté non négociables. Bien sûr, le numérique est à considérer, mais ce n'est pas le seul. Christian Saint-Étienne et Olivier de Maison Rouge ajoutent à la liste la défense, la finance, l'agro-alimentaire, la santé-pharmacie, l'énergie, le transport et l'espace.

« Côté finance, les États-Unis dominent le marché du M&A en Europe. Ce sont les opérations qui génèrent les profits les plus élevés et les liens les plus forts avec la clientèle. Le risque avec la tendance actuelle, c'est que les banques européennes soient cantonnées dans des opérations standards, moins rémunératrices », regrette Christian Saint-Étienne. Un constat confirmé par le fournisseur de données financières Refinitiv, qui consacre les banques américaines au sein du top 10 des opérations de M&A au premier semestre 2021. « Même en matière d'énergie, nous dépendons des importations de gaz et de pétrole venant de Russie ou du Moyen-Orient », poursuit Christian Saint-Étienne. Un rapport du Sénat daté de janvier 2022 note que l'Europe importe environ 3 millions de barils par jour en provenance du Golfe persique, soit 45% de ses importations pétrolières, quand la Russie fournit près de 50% du gaz naturel et 20% du pétrole consommés dans l'Union Européenne.

SOUVERAINETÉ ET SÉCURITÉ NATIONALE

« Ces sujets de souveraineté sont liés à la sécurité nationale », explique Olivier de Maison Rouge. C'est-à-dire qu'il s'agit de secteurs dont dépendent les intérêts stratégiques de la nation : si leur activité venait à être perturbée, cela pourrait bouleverser le fonctionnement du pays. « C'est pour cela qu'ils sont protégés en partie par l'article L. 151-3 du code monétaire et financier, qui soumet les investissements étrangers à une procédure d'autorisation préalable dans le cas où ceux-ci menaceraient les intérêts du pays », explique-t-il, tout en reconnaissant la difficulté de « figer » les secteurs à protéger en priorité. « C'est très mouvant, en fonction des rapports économiques et géopolitiques. Aujourd'hui, on s'intéresse beaucoup à la cybersécurité, mais ça n'était pas du tout le cas il y a 20 ans. » Pour Olivier de Maison Rouge, un bon exercice pour identifier les prochains secteurs stratégiques consiste à surveiller ce qui se passe du côté de la Chine. « En matière d'intelligence économique, la Chine sait tirer son épingle du jeu. Depuis une vingtaine d'années, elle a investi – mais aussi espionné – tous les secteurs qui font aujourd'hui la force des nations au niveau mondial : aéronautique, automobile, construction navale… » Il considère qu'en ce moment, la bataille doit se mener du côté de la cybersécurité en général, mais surtout de la santé numérique. « La Chine s'intéresse à ce sujet depuis plusieurs années déjà. Aujourd'hui, la course s'accélère à cause du Covid-19, il faut faire preuve de vigilance », conclut-il. ■





© Marek Piwnicki via Unsplash

Thomas Fauré *(Whaller)* « Les gouvernements ont tort de privilégier l'efficacité à court terme à notre souveraineté numérique »

Mélanie Roosen ■ 1 février 2022

© Whaller

De plus en plus de dirigeants militent en faveur d'une souveraineté numérique. Pourquoi celle-ci, plus que les autres ? Pour Thomas Fauré, porte-voix des anti-GAFAM, il n'est pas trop tard pour reprendre la main sur un domaine dont dépendent de nombreux secteurs.

Pourquoi parle-t-on autant de souveraineté numérique aujourd'hui ?

Thomas Fauré : La souveraineté, on en parle pour la réaffirmer. Parce qu'elle nous échappe. C'est ce qui se passe avec la souveraineté numérique : nous sommes dans une situation de dépendance aux technologies étrangères. La majorité des États dépendent des États-Unis ou de la Chine – même si certains,

comme la Corée du Sud, Israël ou la Russie s'en sortent mieux. Ce phénomène n'est pas si récent, mais si nous en parlons autant en ce moment, c'est que ses impacts sont enfin perçus : perdre sur le terrain du numérique, c'est perdre sur le terrain de la défense, de l'alimentation, de l'industrie… car la technologie alimente tous les autres domaines. Et aujourd'hui, il n'est plus possible d'appuyer sur un bouton « off » qui nous permettrait de nous couper d'un fournisseur étranger.

Le sujet du moment, c'est le cloud. Peut-on encore reprendre la main ?

T. F. : J'entends souvent dire que « la messe est dite ». Mais je ne suis pas aussi défaitiste : au regard de l'Histoire moderne, l'avènement du numérique dans la technologie est extrêmement récent. Celui du cloud encore plus. Nous n'en sommes qu'à l'âge de pierre, et nous avons les talents et la capacité de créer des solutions qui pourraient rivaliser avec celles des GAFAM. Mais il est vrai que nous partons avec de sérieux handicaps : sans un soutien politique fort et assumé, il n'est pas possible de rivaliser.

Le gouvernement lui-même choisit les solutions des GAFAM : la question, au-delà du soutien aux technologies locales, n'est-elle pas celle de la performance ?

T. F. : Quand le gouvernement choisit Microsoft sans appel d'offre pour mettre sur pieds le Health Data Hub – qui est d'ailleurs en pause puisqu'il n'a pas obtenu l'autorisation de la Cnil pour héberger le SNDS, base principale du système national des données de santé -, il invoque en effet une meilleure efficacité. Mais cette logique nourrit un cercle vicieux. C'est vrai, les GAFAM proposent de meilleures solutions aujourd'hui. Mais on ne peut pas inverser la vapeur si l'on continue à choisir l'efficacité à court terme aux dépens de l'indépendance à long terme : si les politiques se mettaient enfin à choisir les solutions européennes, celles-ci pourraient rattraper leur retard. Par ailleurs, je ne suis pas certain que le fait de favoriser l'efficacité à court terme soit gagnante sur le long terme : cette réflexion ne prend pas en compte le nombre de sociétés rachetées par les États-Unis ou de nos chercheurs qui partent travailler dans la Silicon Valley.

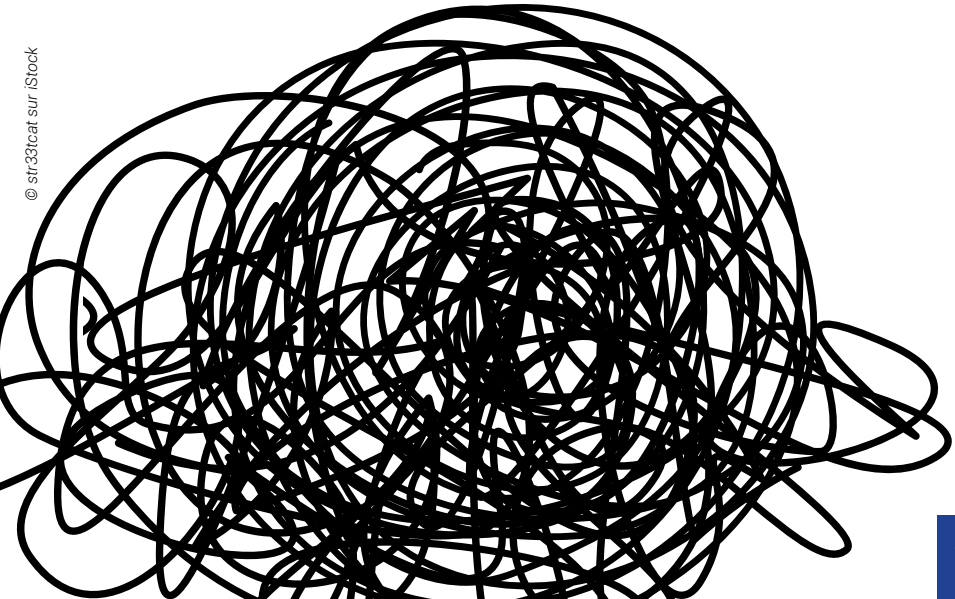
Que risque-t-on, concrètement, à adopter les services numériques américains ?

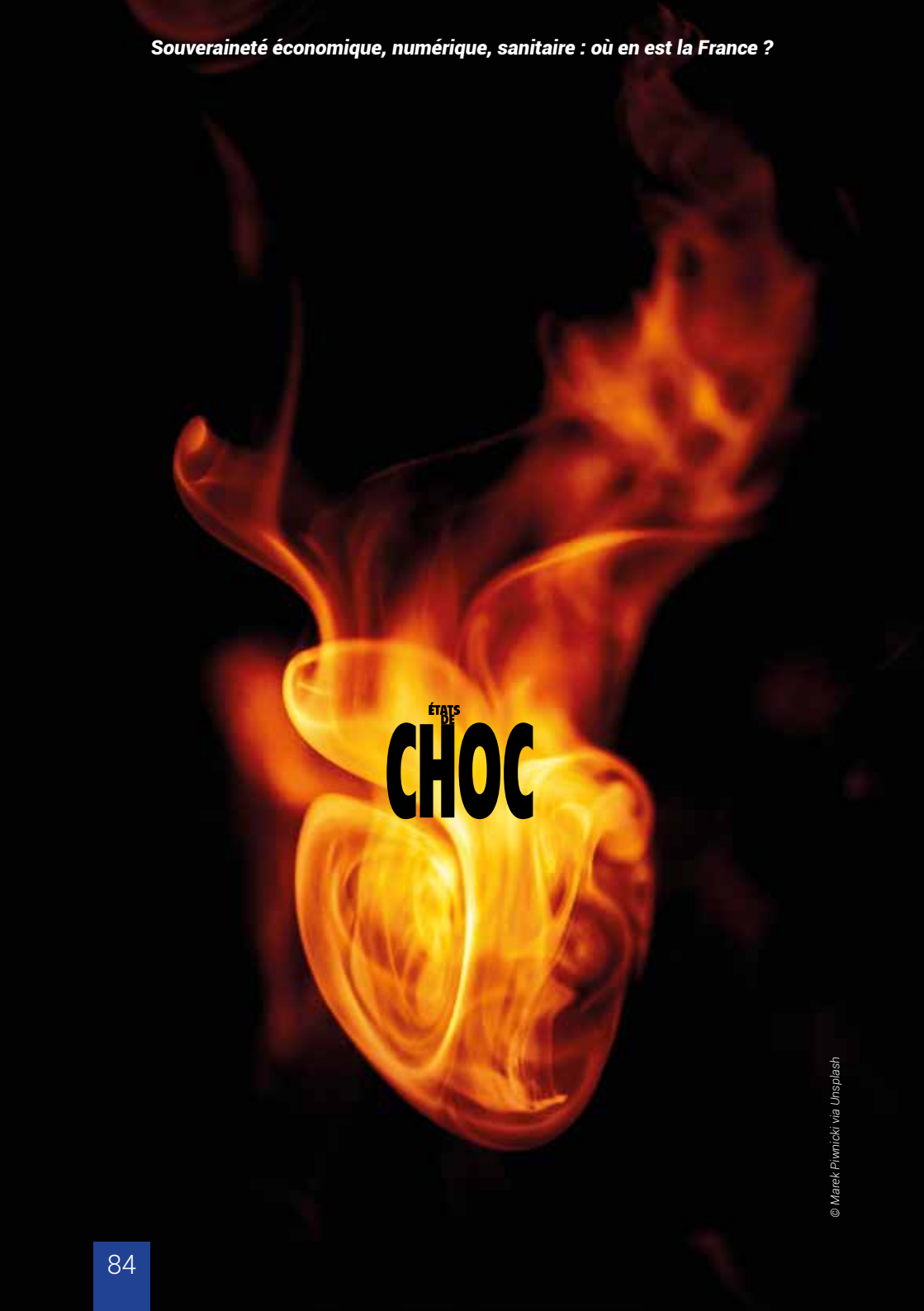
T. F. : L'un des vrais enjeux, c'est le cloud. Aujourd'hui, quand la SNCF choisit les services d'Amazon, Renault et Carrefour ceux de Google… c'est une bonne partie de nos données que nous confions à des tiers. Toutes ces données permettent de nourrir des algorithmes et des programmes d'intelligence artificielle, et donc de les rendre plus performants. Si toutes les données de nos entreprises sont lisibles par les États-Unis, ils seront toujours plus forts

que l'Europe. Dans le contexte actuel, c'est dangereux à plusieurs titres : nous ne sommes pas à l'abri d'une guerre entre les États-Unis et la Chine, ou qu'un gouvernement populiste prenne le pouvoir et décide de couper l'accès aux ressources. Un exemple : de nombreuses entreprises – et particuliers – dépendent des données GPS, autrement dit d'un système de positionnement par satellites américains. Heureusement, nous sommes en train de développer le nôtre en Europe avec Galileo. Il faudrait que nous ayons du recul sur l'ensemble des solutions étrangères et leur utilisation, que nous cartographions leurs implications, pour être capables de mesurer l'ampleur des conséquences qu'elles ont sur nos vies. ■

Biographie

Thomas Fauré est ingénieur (Centrale Lille). Il y a quelques années, alors que son beau-frère lui posait la question de savoir s'il devait ou non laisser son fils s'inscrire sur Facebook, Thomas Fauré se mit en tête d'agir plutôt que de commenter. Il coda et développa Whaller : un réseau qui incarne sa vision des réseaux sociaux. D'abord ingénieur chez Safran, passionné de code et de biométrie, il rejoint Polyconseil (Groupe Bolloré) en 2011, où il évoqua sa passion d'entreprendre et ses projets jusqu'à convaincre Vincent Bolloré d'investir dans Whaller. La start-up est née en 2013. Elle compte déjà plus de 175 000 utilisateurs pour environ 8 000 réseaux hébergés.





© Emin Baycan via Unsplash

Santé : trois pistes pour regagner en souveraineté

Mélanie Roosen ■ 2 février 2022

Au pays de Pasteur, les innovations en matière de santé se sont un peu éclipsées ces dernières années. Les raisons sont multiples : délocalisations, recul de la R&D, manque de confiance dans le numérique… Le seul moyen d'y remédier ? Investir, d'après les experts et le gouvernement.

La pandémie a rebattu les cartes de la souveraineté. Alors que la santé était sortie du scope des secteurs à défendre, les pénuries de masque puis l'absence remarquée de la France dans la course au vaccin contre le Covid ont rappelé qu'il était important de reprendre les devants.

RÉINVESTIR DANS LA SANTÉ MADE IN FRANCE

« Ce qui se passe est dramatique quand on pense que l'industrie pharmaceutique française s'imposait encore il y a une quinzaine d'années », regrette l'économiste Christian Saint-Étienne. Ce constat s'explique par plusieurs dynamiques, notamment une baisse du budget global public de recherche consacré au secteur de la santé (-28% entre 2011 et 2018). Du côté du G5 Santé, cercle de réflexion rassemblant les dirigeants des entreprises françaises de santé bioMérieux, Guerbet, Ipsen, LFB, Pierre Fabre, Sanofi, Servier et Théa, on estime que la perte de puissance de la France en matière de santé est due à la fragilité de l'ensemble de la chaîne de valeur, du fait d'une régulation importante pesant sur les produits de santé. Les groupes expliquent que le prix des médicaments en France étant parmi les plus bas d'Europe, ils préfèrent délocaliser leurs outils industriels dans des régions moins coûteuses, faisant ainsi baisser la production du pays. « L'avantage » de la pandémie, d'après le président du G5 Didier Véron, aura été de permettre une prise de conscience au niveau du gouvernement en matière d'indépendance sanitaire. C'est aussi parce qu'en cas de pénurie d'un seul composant, c'est toute la production médicamenteuse qui peut s'en trouver impactée. Mais selon le groupe Pierre Fabre, membre du G5, pour réduire de 90% les risques liés au sourcing extérieur, il faudrait débloquer un milliard d'euros d'investissements.

Un budget conséquent, qui devra être distribué en fonction des points de faiblesse et des zones de risques du système actuel, afin de relocaliser selon les priorités.

SE TOURNER VERS LA SANTÉ NUMÉRIQUE

En matière d'investissements, le gouvernement se tourne aussi vers la santé numérique. Un plan dédié prévoit l'émergence de solutions innovantes dans le domaine. L'objectif : permettre à la France de « conquérir un marché de l'e-santé en pleine croissance au niveau mondial ». Les prévisions de croissance parlent d'elles-mêmes : le marché de l'e-santé, au niveau international, pourrait croître de 160% entre 2019 et 2023, pour atteindre 253 milliards de dollars. Le gouvernement reconnaît un « retard français », lié, entre autres, au déficit d'investissements dans les infrastructures numériques ainsi qu'un « manque d'acceptabilité et de confiance » dans le numérique de part du public et des professionnels. C'est à ce titre que 2 milliards d'euros ont été débloqués dans le cadre du volet numérique du Ségur de la santé, qui s'est déroulé en juillet 2020. Une partie de cette somme sera dédiée à la formation (81 millions d'euros), aux équipements de recherche (60 millions d'euros), à des appels à projets (20 millions d'euros annuels), à des tiers lieux d'expérimentation (63 millions d'euros d'ici 2025), à l'imagerie (93 millions d'euros) et enfin aux innovations ciblées sur les nouveaux usages numériques en santé (50 millions d'euros).

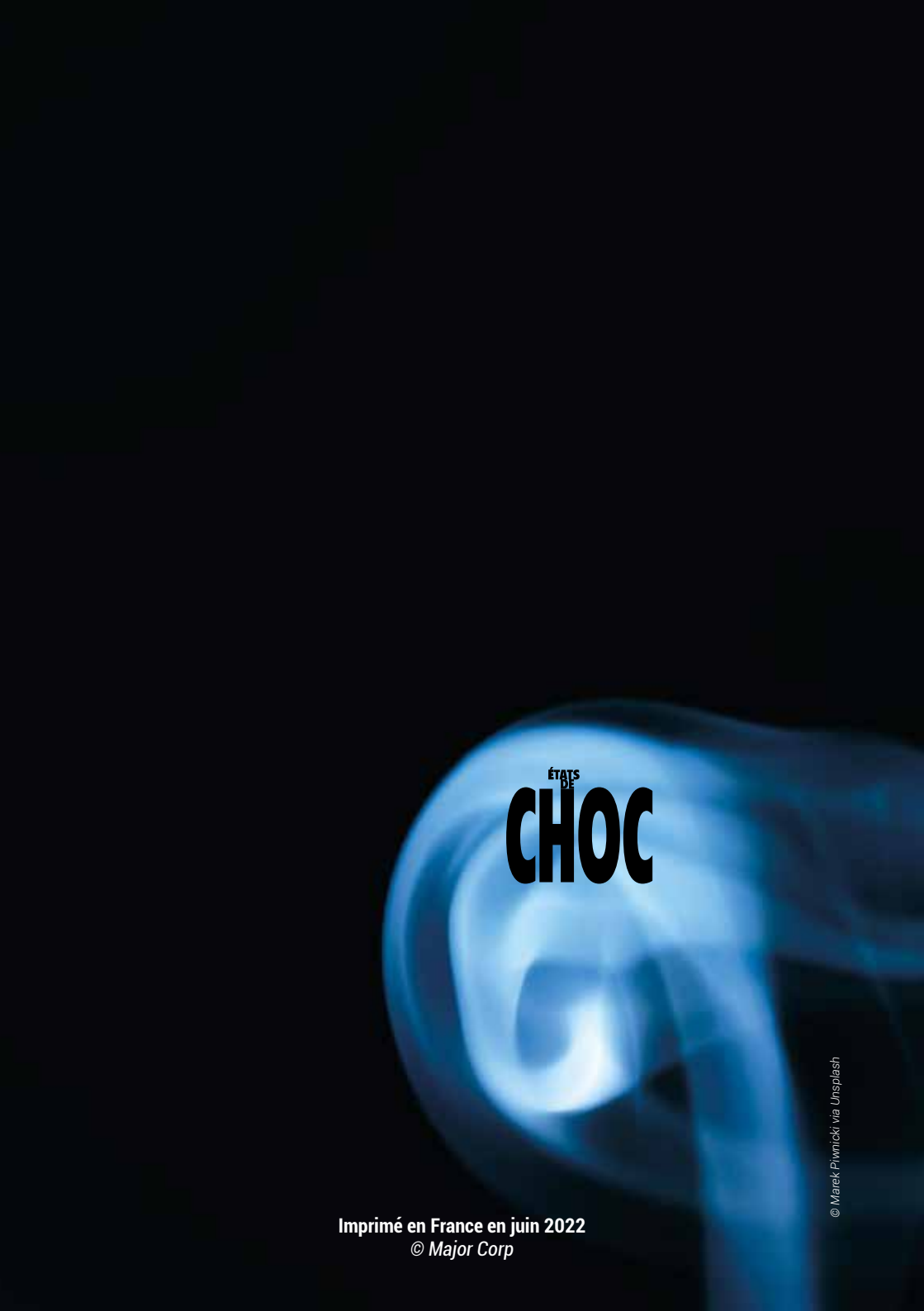
Le secteur de l'e-santé étant particulièrement sensible, notamment en matière de protection des données, le gouvernement promet un « partage fluide et sécurisé des données de santé entre les professionnels de santé et les patients », ainsi qu'un traitement « éthique » de la part d'acteurs soumis à une réglementation plus protectrice des données personnelles.

NE PAS OUBLIER LES BIOTECHS

Enfin, il faudra aussi compter sur les biotechs. Tandis que la CCI promet un écosystème « en pleine croissance » en France, avec 60 nouvelles entreprises chaque année et une troisième place sur le podium européen (derrière l'Allemagne et le Royaume-Uni), les chiffres en matière de financement laissent à désirer. En 2019, les biotechs françaises étaient 72% à chercher des fonds, avec 11% de leur capital provenant des fonds nationaux, qui dépendent de l'État. Aux États-Unis, cette proportion grimpe à 82%. Une tendance qui n'a rien d'anodin au royaume du capitalisme, quand on sait qu'un médicament innovant sur deux provient aujourd'hui des biotechnologies, rappelle l'économiste Frédéric Bizard dans une tribune parue dans Le Monde.

La souveraineté du secteur de la santé française ne pourra donc être assurée qu'en investissant. Dans de nouvelles technologies et innovations… mais également dans les outils existants, oubliés ou délocalisés. ■

© Marek Piwnicki via Unsplash



Imprimé en France en juin 2022

Covid-19, guerre en Ukraine, inflation… Les chocs sont là, s'enchaînent mais ne se ressemblent pas. Au point que l'on se demande presque si le choc est devenu un état de fait, auquel il faut s'habituer.

Pour les organisations, cela demande une sacrée capacité d'adaptation. Car en plus des chocs « macros », elles sont soumises à des défis quotidiens, protéiformes et mouvants. Elles doivent composer avec les risques cyber, les attaques réputationnelles, les assauts étrangers, les défaillances internes. Et trouver le moyen de se relever, choc après choc.

Ce livre blanc n'a pas vocation à être un guide à suivre à la lettre. Il ne fait pas non plus un état des lieux exhaustif des situations de crise auxquelles font face les entreprises. Mais il revient, à travers différents exemples et disciplines, sur les essentiels à maîtriser, les bonnes pratiques à dupliquer et les points de vigilance à garder à l'esprit.

www.major.com

major

Major Corp, Société Anonyme à conseil d'administration au capital de 2 702 000 €
37, rue Dubois-Crancé 69 600 Oullins ■ nous-contacter@major.com
R.C.S. Lyon 894 689 975 ■ SIRET : 89468997500015