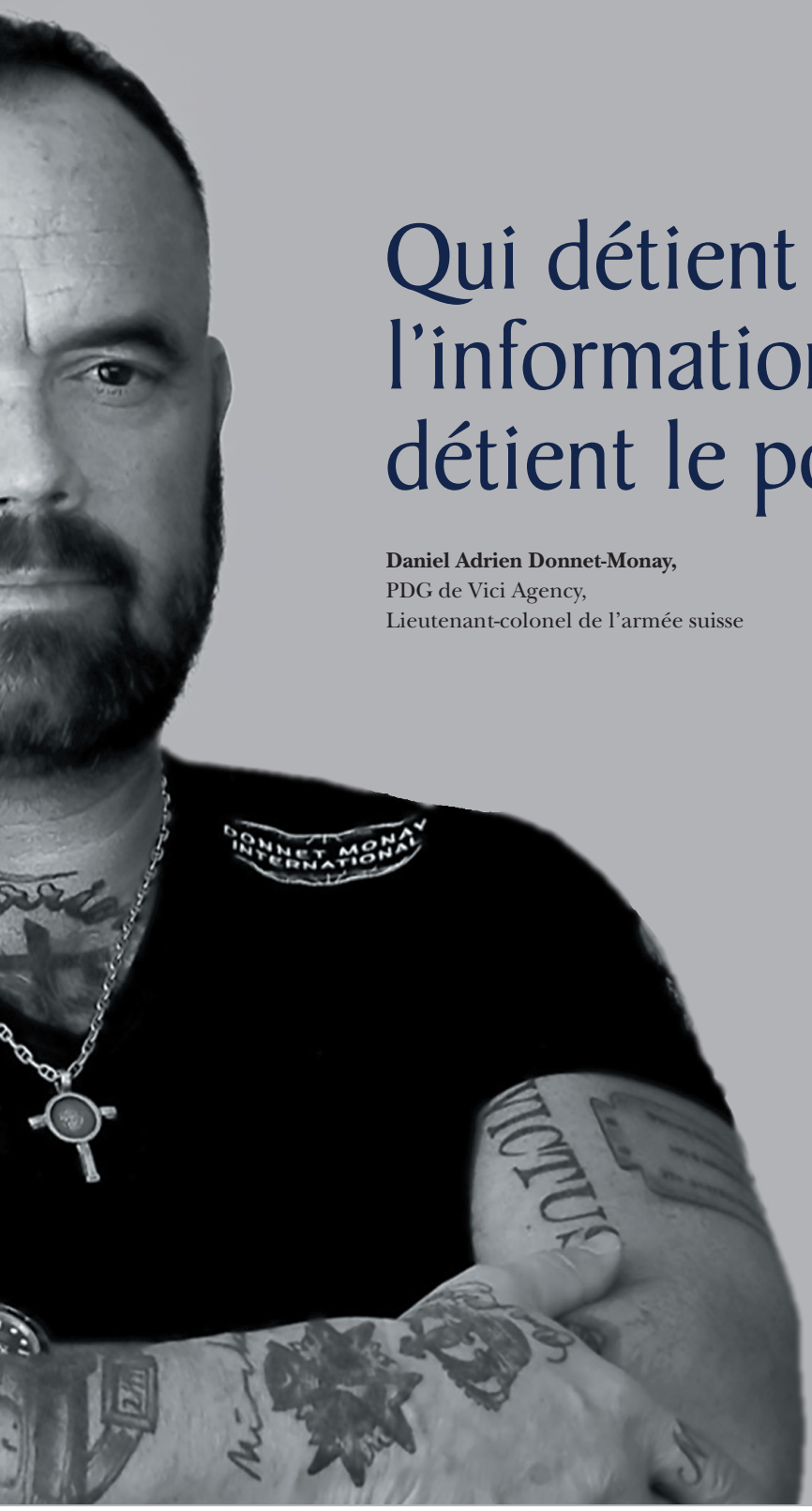


Qui détient l'information détient le pouvoir

Daniel Adrien Donnet-Monay,
PDG de Vici Agency,
Lieutenant-colonel de l'armée suisse

VICI SWISS COMPETITIVE INTELLIGENCE

TABLE DES MATIÈRES

VICI
SWISS COMPETITIVE INTELLIGENCE

INTRODUCTION PAR DANIEL ADRIEN DONNET-MONAY

Les évolutions du monde ont de quoi ébranler les entrepreneurs et les dirigeants d'entreprises. Jamais nos forces vives économiques – celles qui créent de la valeur et des emplois – n'ont été autant malmenées. Conséquences de la mondialisation et expression du libre jeu de la concurrence, direz-vous ? Pas seulement.

Il se trouve que pour de nombreux facteurs sur lesquels nous reviendrons dans cet ouvrage, nos entrepreneurs ne luttent pas nécessairement à armes égales avec leurs concurrents internationaux. Question de « logiciel culturel » notamment, de situation géopolitique aussi. Mais tout autant de changement de comportement dans les affaires.

Depuis un certain temps déjà, nous sommes en guerre économique. Et cela va bien au-delà du conflit commercial sino-américain, abondamment relayé dans les médias : cette guerre est globale.

En raison de mon vécu professionnel et personnel, de mon engagement dans l'armée suisse et des valeurs qui m'ont toujours guidé, je me sens « interpellé » par tout cela. Mais j'ai surtout une grosse envie d'intervenir. Voilà pourquoi j'ai créé Vici Agency, Swiss Competitive Intelligence.

Depuis plus de 20 ans, j'accompagne des dirigeants de PME et d'entreprises en croissance. Avec le recul, je me rends compte que j'avais des prédispositions pour ce faire, même si l'année 2009 s'est révélée décisive dans mon cheminement. Voilà en effet une décennie que j'ai fondé la fiduciaire AAGS, à Martigny.

Au début, je voulais aider des entrepreneurs, majoritairement européens, à venir s'implanter en Suisse. Je trouvais logique qu'ils puissent bénéficier de conditions fiscales plus favorables que dans leur mère patrie, pour y développer leurs affaires tout en préservant des fonds qui seraient précieux pour leur croissance. C'est de bonne guerre...

Ainsi, j'ai développé auprès d'eux un rôle de conseil. Il s'avérera un poste d'observation privilégié de ce que ces patrons vivaient, de ce qu'ils ressentaient et espéraient de leur business. Témoin de leurs préoccupations, j'ai pu partager leurs inquiétudes, parfois leurs souffrances. J'ai pu également mesurer leur sidération suite à de sérieuses déconvenues ou de « coups du sort » qu'ils n'auraient jamais imaginés, mais aussi à la peur de manquer de trésorerie, la honte de devoir expliquer à leurs salariés qu'il faudrait bientôt dégraisser... voire de devoir fermer boutique !

Mais il y a surtout les mauvais coups ! Car En effet, jamais les risques et les menaces pesant sur la vie et l'exploitation de l'entreprise dans toutes ses formes n'ont été aussi nombreux. Je parle d'un niveau de « conflictualité », de manœuvres et d'attaques que l'on pensait réservées au seul champ de bataille. À ceci près que la vie des affaires en est devenue un. Et peut-être le principal, notamment dans le cyberespace.

Il existe un « gap » opérationnel et tactique considérable entre ce que les pouvoirs publics des pays francophones ont voulu mettre en œuvre en matière d'IE et la capacité de réponse effective, donc de résilience et de survie, de notre tissu économique.

Certes, l'intelligence économique (IE) est aujourd'hui un sujet relativement connu du public. Mais connu comment ? Connu jusqu'à quel point ? À l'occasion de la sortie de quelques rapports (Martre, Carayon, Bockel…) ? À travers quelques affaires ayant défrayé la chronique aux actualités ? Ou connu au point de savoir comment faire face à une menace voire à une attaque que l'on aura su clairement identifier ? Vous apprécierez la nuance.

Si certains avaient vu un progrès dans la nomination d'Alain Juillet comme Haut Responsable chargé de l'IE , leurs espoirs se sont trouvés douchés par l'inertie du monde politique français sur le sujet. Il y a comme un tabou, notamment dans les pays francophones. Bien sûr, certains corps intermédiaires comme les chambres de commerce et divers ordres professionnels ont créé des boîtes à outils en matière d'IE, contribuant à vulgariser la thématique. Mais de là à être capable de les utiliser de manière concrète et parfois dans une urgence absolue (l'information électrique se déplace dans les fils de cuivre du cybermonde à 270 000 km/seconde…), c'est une tout autre affaire !

Je me souviens que le plus souvent, mes clients subissant une attaque ou une manœuvre réalisaient à peine ce qui leur arrivait. Quant à savoir d'où les coups pouvaient venir, alors… Ils en restaient au constat qu'un « truc » clochait, ou avait cloché, au point de leur infliger un dommage économique. Mais il leur fallait du temps pour décider des actions à suivre, sans garantie qu'elles soient appropriées.

Comme si le monde était infesté de maladies et de virus sans qu'il n'existe des médecins, des hôpitaux et des traitements – ou alors réservés aux milliardaires… Car on pense volontiers que ces dispositifs de lutte sont réservés aux grands groupes, ceux cotés sur les premiers segments boursiers. Eux seuls disposent en interne d'équipes de sécurité suffisamment professionnelles pour agir, ou ont les moyens de mandater des agences spécialisées pour enquêter, si nécessaire en terrain extérieur et dans le cyberespace.

Pour information, j'ai arrêté l'école assez tôt. À un âge où la priorité est de s'acheter une Mobylette pour épater les copains et plaire aux filles. Si j'ai pu, à un moment, souffrir d'un « handicap académique », je n'ai pas mis longtemps à le compenser en développant d'autres habiletés, fort utiles par la suite. La plus importante d'entre elles : m'informer. J'ai pris l'habitude de me renseigner – formation militaire oblige – avant de décider et d'agir, au point que les rares fois où je ne l'ai pas suffisamment bien fait, j'ai pris des uppercuts dont je me souviens encore.

Bien sûr, j'ai su me « refaire » et gagner très correctement ma vie comme conseil fiduciaire, ou en vendant des produits d'assurance et de prévoyance comme auparavant à la Bâloise. Mais cela ne me suffisait pas : il restait un « bout de code » à écrire dans mon propre programme. Si j'avais acquis ces expériences, c'était pour aller plus loin dans l'accompagnement et le partage : je devais mettre ce capital au service d'une cause qui ait du sens pour le « chevalier 4.0 » qui sommeillait en moi.

Je veux aider leurs fondateurs et leurs dirigeants à sortir de la sidération. Je veux qu'ils soient capables de « divertir des moyens pour contrer la surprise ». Je veux les aider à réveiller la combativité dont ils auront besoin, non seulement pour se défendre mais aussi pour mettre en œuvre les menées offensives qui font aujourd'hui partie de leur jeu concurrentiel. Car il ne s'agit plus simplement de survivre : il s'agit de vaincre, ce que les Chinois appliquent à merveille.

En créant Vici Agency, j'ai voulu donner aux PME et aux entreprises de croissance, amenées à se développer à une échelle internationale pour survivre, des moyens d'investigation digitaux parmi les plus avancés. Cela afin qu'elles s'informent, qu'elles se protègent et puissent influencer positivement leur marché.

C'est ici que le monde militaire est « modélisant » pour les entrepreneurs. Désormais, il ne suffit plus d'organiser un séminaire avec une ancienne gloire du football ou un expert en motivation sportive pour « aller tous ensemble vers la performance… » Non. Ça, c'est une version « bisounours » de ce qui vous attend.

Vous vous autoriserez à aller plus loin, parce que – pour filer la métaphore sportive – vos concurrents sont dopés. Parce qu'ils souhaitent ardemment vous empêcher de jouer la prochaine Coupe du monde. Parce que s'ils le peuvent, ils achèteront votre joueur vedette juste avant la nouvelle saison. Ils vous empêcheront même de prendre l'avion pour assister au tirage au sort de la Champions League… Bref, ils vous intimideront. Ils vous « incapaciteront ».

D'une certaine façon, la mondialisation a mis au grand jour de nouvelles mœurs en affaires. Eh oui, les gentlemen n'ont pas le monopole du business ! En opérant à l'international, mais même pas si loin de chez vous, vous vous exposez à des concurrents prêts à tout pour prospérer. Tant pis si c'est sans ménagement ! Tant pis si c'est à vos dépens !

On parle beaucoup d'algorithmisation des conduites, et même d'une digitalisation du monde… En tout cas, elle n'épargne pas le monde des affaires : bien au contraire, ce dernier en est l'avant-poste. Le Web et ses technologies procurent aujourd'hui des moyens décisifs pour paralyser des concurrents, mais aussi influencer un marché, dans des conditions de retour sur investissement imbattables.

Alors oui, le tableau que j'ai commencé à vous brosser peut vous sembler bien sombre, cynique même. Sans doute une déformation professionnelle. Mais il ne sert à rien de rester dans le déni.

Si « seuls les paranoïaques survivent », la vie reste belle… pour autant qu'on lui en donne les moyens ! La bonne nouvelle, c'est que ces moyens se développent autant que les menaces venant assombrir votre horizon.

Vici Agency porte les moyens de remédier à ces nouvelles problématiques que nul patron ne saurait ignorer.

Alors place à l'action !

Daniel Adrien Donnet-Monay,
PDG de Vici Agency,
Swiss Competitive Intelligence
Lieutenant-colonel de l'armée suisse.

1 . CONTEXTES ET QUESTIONS

1.1 QUELQUES CHOSES À SAVOIR DU MONDE ACTUEL

Le monde actuel n'a « plus rien de sûr ». Il suffit d'observer objectivement certains phénomènes. Et s'il a pu sembler économiquement plus sûr à certains moments de son histoire, cette notion de sûreté demeure très relative.

Après un rappel des facteurs expliquant les différents niveaux des bouleversements actuels, nous ferons une synthèse des principaux risques et menaces qui pèsent aujourd'hui sur les entreprises.

1.1.1. Des facteurs explicatifs à différents niveaux

• Un climat de violence généralisée

Cela fait bientôt trois quarts de siècle que nous n'avons connu de conflit mondial. Pourtant, en dépit d'une certaine idée du progrès et d'une conversion des États à la démocratie, les guerres n'ont jamais cessé, à une échelle plus ou moins locale.

Les inégalités continuent de se creuser et les médias sont de plus en plus présents pour dénoncer toute forme d'anormalité, concourant à aseptiser d'une certaine manière le monde.

Un peu partout, on voit les mœurs en affaires se durcir : une « impatience » peut-être imputable à une économie qui s'est financiarisée et qui prédispose aux frictions.

Dans nos contrées, les bouleversements climatiques à l'œuvre et les catastrophes migratoires promises renforcent un sentiment d'insécurité : les populations devront (ré)apprendre à se protéger même si, sans doute, nos arsenaux judiciaires et une peur du politiquement – comme du médiatiquement – correct, tempéreront les ardeurs.

Si nos actualités relatent une explosion des violences faites aux personnes, celles – notamment digitales et cyber – faites aux entreprises vont tout autant se multiplier : hacking, défacement de sites, phishing, rançonnage, fraude au président… les cyberattaques ne manquent pas.

Il y a une corrélation entre les opportunités offertes par la globalisation, le développement des risques pesant sur le business et la criticité de ces mêmes risques : se développer implique de s'exposer davantage, donc d'apprendre à se protéger proportionnellement aux nouveaux risques encourus.

• Une « prédation » organisée

La guerre pour les ressources est une constante de l'histoire humaine. Il y a eu le pétrole, les métaux précieux puis les terres rares, et demain sans doute l'eau. Mais les entreprises représentent, elles aussi, une classe d'actifs stratégiques en soi :

> Certaines se font racheter : par des groupes américains et japonais hier, et chinois de plus en plus. Ils ont pris des habitudes d'acquisition soit à maturité, soit au berceau lorsque ces entreprises ne sont encore que des start-up. Si la démarche ressemble à du capital développement compte tenu du manque de moyens pour faire émerger des licornes en France et en Europe, n'oublions pas que les GAFAM aiment faire main basse sur les technologies décisives… avant qu'on ne les connaisse comme telles.

> D'autres se font déstabiliser : pour faire baisser leur valeur et obtenir des conditions d'acquisition plus favorables, notamment en Bourse. Ici, tous les coups sont permis et s'appuient sur le bad buzz, la duplicité humaine, la corruption…

> D'autres, enfin, restent non cessibles en raison de leur importance pour la souveraineté nationale. Elles deviennent alors des cibles à abattre : on pense à des menées d'intimidation américaines ou à des cyberattaques russes, chinoises et là encore étasuniennes (Airbus est parfois cité comme le prochain Alstom…). On voit comment de puissants virus peuvent paralyser des entreprises tout comme des États : la première cyberattaque d'un État souverain fut perpétrée en 2007 contre l'Estonie. Autre cas, Stuxnet : ce ver informatique fut conçu en 2009 par les services américains et l'Unité 8200 de Tsahal (l'armée israélienne) pour freiner le développement du programme nucléaire iranien.

Friandes elles aussi d'acquisitions en tous genres, les pétromonarchies voulaient au départ diversifier leurs actifs en achetant des participations minoritaires dans des groupes cotés de premier plan. Mais leurs dirigeants se montrent beaucoup plus volontaristes dans certains secteurs ciblés : hôtellerie de luxe, immobilier ou sport. Et l'on ne peut que s'interroger sur leurs visées finales.

• Une course à la taille critique

Rares sont les secteurs de l'économie qui n'ont plus besoin de se consolider. Avoir une taille critique reste un enjeu majeur, parce que les marchés sont devenus mondiaux et parce que **vous devez vous rendre capables d'opérer là où la croissance se fera demain dans vos secteurs d'activité.**

Même lorsqu'une filière se montre mature au plan stratégique, aucune n'est à l'abri d'une disruption par les technologies numériques. À ce jeu, tout ne se fait pas par fusion-acquisition, même si le cash n'est actuellement pas très cher sur le marché (en même temps, cela dépend pour qui…). Aussi les « manœuvres » font-elles partie des stratégies de croissance externe.

• Des élites toujours aussi timorées

Plusieurs constats se combinent : appauvrissement du niveau général de l'éducation (programmes scolaires décriés, dérégulation cognitive potentielle des enfants par une invasion notamment des tablettes numériques, enseignants sous-payés réduits à faire la police ou du social sur une part significative du temps…), fonctionnements stéréotypés, faillite entre autres du modèle de l'ENA en France… Les élites ayant développé leur légitimité dans un contexte de « guerre de position » se montrent aujourd'hui incapables de se renouveler, rétives à toute prise de risque. Les sociologues des organisations appellent cela l'« homéostasie ».

Même les diplômés de grandes écoles de management et autres MBA se comportent tels des mandarins. Ils vont se fonctionnariser dans de grands groupes : fraîchement diplômés, ils partent faire carrière dans des banques et au sein de « noms qui claquent sur le CV » pour rentabiliser leur investissement, d'ailleurs très conséquent. Dommage qu'ils soient découragés d'avance à entreprendre à la hauteur de leurs atouts intellectuels… Souvenons-nous qu'« apprendre à oser » est la devise d'HEC.

• Des enjeux de résidence et d'imposition

On a beau parler de globalisation, de convergence et d'homogénéisation des modes de vie à de nombreux niveaux, les territoires tiennent à leur pré carré et se livrent à une guerre d'attractivité. Ils le font par la fiscalité et à diverses intensités mais quoi qu'il en soit, les paradis fiscaux et l'évasion subsistent.

En France, nous l'avons bien vu dans l'actualité sociale de l'année écoulée : les Gilets jaunes demandaient à un État notoirement surendetté de commencer par recouvrer ce que les grands groupes évadent depuis trop longtemps… Idem pour les riches patrimoines personnels.

Après les ressources naturelles, la fiscalité est l'une des principales sources de tension du monde économique. C'est donc un levier de compétition majeur : **les entrepreneurs doivent prendre cette réalité à leur compte et penser la localisation de leurs actifs là où les règles du jeu leur sont les plus favorables.** À ce jeu, l'Irlande et la Suisse notamment ont su s'illustrer.

La Confédération helvétique propose depuis longtemps aux entrepreneurs candidats à l'installation une négociation de leur taux d'imposition, les cantons pratiquant entre eux une « saine émulation ». Moins d'impôts, c'est aussi davantage de trésorerie et davantage de fonds à investir dans son développement et dans la création d'emplois. Du bon sens là encore !

Pour autant, les paradis fiscaux n'ont pas disparu : si Barack Obama a mené sa guerre sainte contre eux, c'est ni plus ni moins pour éliminer des rivaux pour les USA. A priori, l'État du Delaware propose toujours des conditions d'immatriculation d'entreprises parmi les plus favorables au monde… Et que nous sachions, Le Luxembourg de Jean-Claude Juncker peut être considéré à la limite du paradis fiscal, bien qu'il ne figure pas sur la liste des ETNC . Nos entrepreneurs doivent sérieusement **réfléchir à de nouvelles options d'investissement, dans des zones qui leur sont peut-être moins familières mais qui recèlent le potentiel nécessaire à leur croissance : les pays d'Europe centrale, la Russie et certains pays d'Asie ou d'Amérique, autrefois considérés comme « secondaires » par les investisseurs.**

• Peut-on encore parler de stratégie d'entreprise ?

Les ruptures technologiques et numériques rendent obsolètes les modèles et scénarios prospectifs. Les progrès réalisés dans les sciences quantiques « ringardisent » les vieux principes de la physique newtonienne et son cortège de certitudes tels que le principe de linéarité et les conditions de prévisibilité qui pouvaient s'y attacher.

Qu'une entreprise ait besoin d'afficher des ambitions chiffrées (plus ou moins réalistes) sur des agrégats financiers afin de rassurer ses actionnaires, d'embarquer ses talents, de donner le change à ses parties prenantes ou d'impressionner ses concurrents, on peut le comprendre. C'est même vital. En revanche, l'élaboration de plans stratégiques pour les atteindre devient illusoire.

Les paramètres sont devenus trop nombreux, trop turbulents et trop complexes à appréhender. Le chaos devient la norme et il est rare que les choses « se passent comme prévu » à un tel niveau de variabilité.

Néanmoins les gestionnaires auront toujours besoin de décider, de préparer l'action et de mesurer des progrès réalisés sur la base d'une « heuristique ». Alors l'entreprise misera plutôt sur son agilité et sa résilience, développées comme des capacités stratégiques à part entière. Mais pour ce qui est de la « prévisibilité », c'est plus complexe. Et nous n'entrerons pas ici dans un débat sur le degré de prédictivité aujourd'hui réellement permis par l'IA et le deep learning.

Vouloir élaborer la stratégie sur la base d'une démarche mécanique ne peut aboutir qu'à des résultats médiocres.

HENRY MINTZBERG

• La « guerre » des talents ?

Le public a une image un peu romancée et, disons-le, darwinienne de la chose : seuls les meilleurs candidats tireraient leur épingle du jeu et auraient le choix du roi, c'est-à-dire l'accès aux entreprises les plus attractives pour leur employabilité. Mais le reste ? Comment sourcer des professionnels qui seraient déjà bien assez compétents pour convenir aux besoins des TPE, des PME voire des ETI ? Ces dernières rencontrent pour leur part de grandes difficultés à recruter, par déficit de notoriété ou tout simplement parce qu'elles n'ont pas leur siège opérationnel à Paris. Sans ce capital humain, impossible pour elles de réaliser le potentiel de croissance qui les attend pourtant lorsqu'elles prennent des risques à l'international.

Alors il y a un risque. Celui que ces entreprises n'aient d'autres choix que de recruter du personnel d'origine étrangère mais autant diplômé que les « nationaux ». Avec un second risque, celui du reverse engineering, qui n'est pas nul : une PME travaillant sur une technologie jugée stratégique ou utile à Pékin, peut être tentée de recruter un ingénieur chinois à d'excellentes conditions… pour le voir s'évaporer dans la nature juste avant la fin de sa période d'essai. Ceci n'est pas de la science-fiction.

• Un management de plus en plus hypothétique

Héritage de mai-68, il est « interdit d'interdire ». Mais par extension malheureuse, il est de plus en plus compliqué de cadrer, de borner les choses. Les cadres faisant traditionnellement autorité ont perdu leur crédit, le rapport aux référents normatifs et de valeur évoluant. **Les technologies Blockchain en sont l'illustration : demain ce ne sont plus des figures instituées qui certifieront, mais une diversité voire une infinité d'observateurs qui donneront un avis, valideront puis accréditeront un produit selon des chaînes décisionnelles complexes mais autrement plus sécurisées.**

Pour les digital natives ainsi, une monnaie aura davantage de sens parce qu'elle proviendra d'une certification, certes privée mais produite sur une base circulaire et communautaire, et non parce qu'elle aura été émise par une institution dépassée à leurs yeux. Et la tendance s'applique à tous les domaines de consommation courante et professionnelle, comme en témoignent les success stories de La Fourchette, TripAdvisor ou Glassdoor.

Enfin, le paysage managérial de ces dernières années s'est trouvé marqué par les théories d'holacratie et d'entreprise libérée. D'origine américaine, elles mettent la récompense au centre du jeu et formulent une promesse d'égalité ou de parité croissante entre le management et les collaborateurs. Pourquoi pas ? Sauf que lorsque « tout le monde la ramène », cela pénalise non seulement la prise de décision, mais encore davantage la mise en application des rares décisions ayant pu atteindre un stade de consensus… À l'heure où les rapports économiques se tendent et où l'on entend des « bruits de bottes », prenons garde à un excès de câlinothérapie qui alimenterait le mercenariat plus qu'autre chose.

• Des logiques de réseau et un esprit communautaire

En matière de consommation d'information, les technologies numériques ont modifié les usages et la manière dont les gens interagissent. Les générations milléniales sont clairement communautaires. Plus encore qu'en réseaux, elles fonctionnent en tribus. Elles partagent et accèdent en permanence à de l'information, et elles n'ont parfois pas le discernement suffisant pour savoir ce qui doit rester dans l'entreprise et ce qui peut éventuellement en sortir : l'important, c'est de partager en communiquant dans l'instantanéité, sur leurs comptes de réseaux sociaux ou dans des forums.

Mais pour l'entreprise, la viralité inhérente à ces usages comporte des risques : divulgation de savoir sensible, bad buzz, etc. On a même pu observer ce phénomène chez des militaires américains qui, pensant donner des nouvelles à leurs proches, parlaient de leur prochaine manœuvre sur le terrain et en indiquaient la localisation… Il fallut alors annuler certaines opérations !

Ces facteurs explicatifs doivent être articulés aux principaux risques et menaces régulièrement rencontrés par les entreprises.

VICI
SWISS COMPETITIVE INTELLIGENCE

Attaque & défense commerciale • Audit stratégique • Autonomisation décisionnelle • Bad buzz • Collecte de renseignement • Conquête de nouveaux marchés • Corruption • Contrefaçon • Croyances erronées • Cyber attaques • Cyber protection • Cyber visibilité • Deep web Intelligence • Défaçage web • Dénigrement de produits • Déstabilisation • Détermination • Détournement • Discernement d'affaires • Dissimulation • Due diligence • Duplicité humaine • Espionnage • Extra-territorialité • Fake news • Fatalisme patriotique • Fraude au dirigeant • Géoéconomie • Guerre cognitive • Guerre économique • Guerre pour les ressources • Hacking • HUMINT • Hyper connectivité • Inféodation économique • Infiltration • Influence • Ingénierie sociale • Intelligence économique • Intoxication • Investigation • Knowledge management • Libération du potentiel offensif • Maliciel • Manipulation • Nouvelles voies comportementales • Offensive • OSINT • Patriotisme économique • Patron d'assaut • Phase introspective • Prédation économique • Pressions commerciales • Protection des données • Ransomware • Remédiation opérationnelle • Renseignement • Résilience • Rétro-ingénierie • Surveillance • Systémique décisionnelle • TECHINT • Trahison • Traitement de l'information stratégique • Veille stratégique • VUCA • War room •

1.1.2. Une liste des risques et menaces aux entreprises qui tend à s'allonger

Pour un chef d'entreprise, il est vital de connaître les différentes typologies de risques pesant sur la sécurité de son exploitation. En raison des phénomènes précédemment retracés, cette liste ne cesse de s'allonger. Voici quelques « incontournables » qui n'arrivent pas qu'aux autres :

Familles de risques et de menaces	Exemples et illustrations
géopolitiques	> terrorisme > changement de politique étrangère > risque « pays » > catastrophe naturelle
humains	> corruptibilité, duplicité humaine : un personnel indélicat, par exemple démissionnant pour rejoindre un concurrent et exploitant sa connaissance de la clientèle pour la détourner au bénéfice de son nouvel employeur > exploitation d'un bad buzz pour nuire à la marque employeur > sociaux et psychosociaux : personne clé, turnover, licenciement, démission, accidents, exposition dangereuse… > sur le personnel clé, lors de voyages d'affaires (exploitation de situations compromettantes) > sur le personnel expatrié, dans des pays à risques, dans des cas d'enlèvement avec demandes de rançons, mais aussi des pressions
technologiques	> espionnage humain et écoutes > informatiques et menaces de cybersécurité : intrusions dans les systèmes, envoi de malwares pouvant entraîner par exemple un DDOS (ou « Déni distribué de service »), de ransomwares, mais aussi des risques de maintenance, de confidentialité, et toutes les attaques visant les appareils dits d'extrémité et terminaux (voir en Annexe 3 nos repères infographiques relatifs à la cybersécurité) > contrefaçon > reverse engineering
économiques et financiers	> concurrence plus ou moins déloyale > risque de refinancement > indisponibilité des matières premières > nouvelles contraintes légales > crise économique globale comme localisée > taux d'intérêt, liquidités, risque de change, de crédit, impôt, pricing… > fraude et usurpation de l'identité d'un dirigeant ou collaborateur signataire > exploitation d'un bad buzz pour nuire à la réputation et aux relations bancaires > exploitation d'un événement négatif visant à orienter le cours de Bourse
commerciaux	> vol de recettes, de formules, de protocoles… > divulgation de coûts de production, de coûts d'achat, de tarifs commerciaux > exploitation d'un bad buzz pour biaiser les conditions de réponse à un appel d'offres, ou pour affaiblir la confiance des partenaires, voire de tout un écosystème
réputationnels et d'intégrité	> fabrication de fake news > alimentation de bad buzz (notamment depuis les réseaux sociaux ou les sites d'avis) > exploitation d'un moment de crise, lancement de rumeurs ou fabrication d'un scandale (lié à l'entreprise, à ses produits ou à ses dirigeants) pour nuire commercialement ou à la marque employeur… > défacement d'un site web, d'un blog, d'un compte sur un réseau social pour y poster du faux contenu > besoin de respect des lois et de la réglementation en vigueur > besoin de respect de l'éthique et des valeurs de l'entreprise
opérationnels et logistiques	> vol > dégradations > intrusion dans les locaux et les sites d'exploitation (domestiques comme à l'étranger) > approvisionnement en énergie et risques naturels associés > dommage aux tiers > qualité du produit ou du service > intégrité de la chaîne logistique
légaux et réglementaires	> utilisation des lois sur l'extraterritorialité (notamment américaine) > déploiement d'un arsenal de sanctions économiques > blocage des avoirs de sociétés comme d'individus > contraintes inhérentes à la protection des données suite à l'adoption de réglementations contraignantes, comme le RGPD > qualité du produit ou du service > intégrité de la chaîne logistique

On note au passage qu'un bad buzz est un risque transverse, c'est-à-dire ayant des répercussions dans de nombreuses catégories.

1.2. NOS ENTREPRISES RESTENT TRÈS VULNÉRABLES

1.2.1. Une combinaison de nombreux facteurs

Face à cet ensemble de menaces et à la complexité qui en découle, l'organisation et la mobilisation des entreprises françaises sont toutes relatives.

Non pas qu'elles soient démunies, du moins sur le papier. Depuis le coup de semonce que fut le rapport Martre, l'Intelligence économique fait l'objet d'une activité et d'une communication régulières. De même pour la cyberstratégie française, issue d'une tradition du chiffre et de la cryptographie remontant à la Seconde Guerre mondiale (voir Annexe 2), ou pour le modèle cyberstratégique suisse prévu par Jean-Philippe Gaudin au sein de la Confédération helvétique.

Non pas davantage que les médias passent ce sujet sous silence. Les exemples sont légion, qu'il s'agisse d'espionnage d'entreprise, de hacking (parfois purement lucratif, parfois hacktiviste), d'attaques en tous genres via des maliciels, ou encore de prédation organisée, voire étatisée. Ils ont été souvent repris et abondamment commentés, même si sur le moment les protestations officielles ont pu « manquer de souffle » (nous savons maintenant pourquoi).

Les lacunes, voire une certaine candeur de nos entreprises vis-à-vis de menaces qu'une politique efficace d'intelligence économique pourrait traiter, proviennent là encore de nombreux facteurs bien souvent imbriqués.

• Des facteurs technologiques

Une « siliconisation du monde » (Éric Sadin). L'algorithmisation de la vie, la datafication des comportements à partir notamment des technologies web, l'omniprésence et la « pervasivité » de la data et ses conséquences (IA, transhumanisme, quantified self, objets connectés)... abolissent les distances et procurent désormais la puissance. Qui sait collecter, analyser, exploiter et diffuser les bonnes données possède une grammaire universelle, devient une sorte de généticien numérique.

Une montée en puissance du cyberespace. Il s'agit d'un espace lisse , c'est-à-dire sans obstacles ni points de friction, totalement dégagé comme le désert, la steppe ou l'océan. Il est également non contigu : la distance n'y compte plus et la notion de voisinage y est annihilée. La proximité n'est plus un critère de choix des alliances.

Une convergence croissante – globalisation oblige – des normes, standards et protocoles technologiques et informatiques. Les systèmes ayant besoin d'être « interopérables », le développement massif d'API facilite dans un même temps les attaques potentielles, puisque les fonctionnements se normalisent, s'alignent et ont gagné en prévisibilité.

Une multiplication de la puissance de stockage et de la miniaturisation. Aujourd'hui, vos actifs peuvent être stockés en d'immenses quantités sur des espaces de plus en plus confidentiels. Et de nouveaux seuils significatifs devraient être franchis dans les années à venir, compte tenu des progrès de l'informatique quantique.

• Des facteurs culturels et psychologiques

Une exception culturelle bien cruelle. L'histoire française, par exemple, est jalonnée de nombreuses guerres et d'une période de décolonisation qui aura laissé beaucoup de traces. Contraintes par de nombreux traités et conventions de paix multilatérales, nos sociétés occidentales ont fini par dévaluer l'utilité même du conflit. La « non-létalité » est devenue la règle, puisqu'il ne reste plus vraiment de territoires à conquérir (si ce n'est le Groenland que ce vieil Oncle Sam rêve de racheter au Danemark !). Le peu de guerres qui restent sont là pour chasser d'odieux dictateurs et restaurer la démocratie. Alors pour le monde de l'entreprise, longtemps pensé comme « sanctuarisé » par rapport à la vie civile et militaire, il y a encore un fossé.

Nous sommes restés sur un paradigme au fond bien commode : la guerre n'est pas bonne pour les affaires. Ce qui a plongé de facto nos entreprises dans un niveau de déni inespéré pour leurs prédateurs. « Il n'y a pas pire aveugle que celui qui ne veut pas voir. » Alors rien d'étonnant à ce que l'espionnage économique soit resté un parent pauvre du renseignement dans les pays européens .

Trop de confort tue l'effort. Si les gens ne veulent plus se battre, c'est aussi parce qu'ils n'en ont plus autant besoin, indépendamment même du droit qu'ils auraient à le faire. Dans nos sociétés industrialisées, le confort et la facilité ont fini par s'imposer. Mais ce n'est pas le cas pour tout le monde sur la planète : si de nombreux concurrents étrangers ont conservé un caractère plus grégaire que le nôtre, c'est peut-être aussi parce que leur peuple se bat continuellement pour s'extraire des étages inférieurs de la pyramide de Maslow.

Une culpabilité post-coloniale. Ex-puissance colonisatrice, la France n'échappe pas à une certaine recherche de repentance vis-à-vis des pays dits en développement, ce qui se conçoit. Mais pendant ce temps les États-Unis, la Chine et dans une autre mesure la Russie échappent à ce passif. Après, on peut toujours considérer que la colonisation revêt de multiples formes ;

Une pénible fascination pour l'Oncle Sam. Nous avons été « biberonnés » dans une gratitude éternelle envers les USA. Elle remonte à la Libération, au Plan Marshall et, depuis, elle a savamment été entretenue par une ingénierie culturelle hollywoodienne.

C'est un fait : les États-Unis d'Amérique sont le grand frère qui doit veiller sur nos intérêts et derrière lequel il est généralement préférable de se ranger. Même s'il nous est arrivé de mettre quelques coups de canif dans le contrat (notamment lors du discours de Villepin à l'ONU sur l'Irak) ou si la solidarité de fait est sérieusement malmenée par l'unilatéralisme obsessionnel du président Trump. D'ailleurs nos élites politiques ne sont pas en reste, à en juger par le nombre de nos dirigeants passés par les programmes des Young Leaders. Donc rien d'étonnant à ce que ces responsables, une fois aux commandes, gardent la fâcheuse habitude de penser aux intérêts étasuniens au moins autant qu'à ceux de leur mère patrie. Pourtant, il ne faut jamais être dupe du jeu outre-Atlantique vis-à-vis des intérêts de ses alliés : ne perdons pas de vue comment les affaires Echelon, puis en 2013 l'affaire PRISM (devenue Snowden) ont pu révéler au monde la duplicité américaine lorsqu'il il s'agit d'intercepter les télécommunications de ses populations alliées afin d'en tirer profit.

Des facteurs macro

La souveraineté, c'est has been. Il est vrai que depuis la mort du général de Gaulle, elle n'a plus bonne presse. Synonyme de marginalisation vis-à-vis du monde et de scores électoraux maigrichons, elle s'assimile aujourd'hui à un combat d'arrière-garde et à l'engagement d'une poignée de nostalgiques et de réfractaires incapables de se projeter dans le monde tel qu'il sera de toute façon, que cela leur plaise ou non. Alors il n'est pas étonnant que la souveraineté économique souffre d'un déficit d'intérêt et de conscience, même si des boucliers anti-OPA ont pu être mis en place pour protéger certains fleurons nationaux ;

La mondialisation et la société ouverte comme horizon indépassable ? La Silicon Valley et ses émanations, les GAFAM, ont créé des technologies qui ont pu soutenir cette idéologie, synonyme aujourd'hui de bien et de progrès indiscutables. On a aussi pu parler de « post-westphalisme » . Mais le phénomène reste partiel, tant les États-nations ont la peau dure : les BRICS et les monarchies du Golfe tirent leur épingle du jeu en termes de croissance, et il demeure des incertitudes liées aux relations avec des États moins démocratiques (Chine, Russie, Iran, Turquie, Arabie saoudite) mais détenteurs de ressources clés comme le pétrole ou les terres rares...

Le contexte géopolitique impacte de plus en plus concrètement les dirigeants d'entreprises, même moyennes. Pression fiscale, « tectonique monétaire », bataille des ressources naturelles, conséquences du changement climatique, tendances migratoires, coût du travail... Tout va les amener, comme leurs concurrents, à élaborer une stratégie d'implantation ou de relocation optimisée plutôt que de continuer à subir. Ce n'est d'ailleurs rien d'autre que ce que font spontanément les animaux et les individus.

Le fardeau de l'UE. L'environnement réglementaire européen, droit de la concurrence en tête, et ses méandres procéduraux n'aident pas, la peur de la sanction étant permanente. Pendant ce temps-là des blocs impériaux (USA, Chine et Russie) pensent de manière décomplexée, décident et agissent d'une seule voix sur une échelle comparable – même s'ils ont eux aussi leurs propres failles et leurs contradictions.

• Des facteurs humains

Pour jouer, il faut être deux. Si toute action malveillante a nécessairement un commanditaire (gouvernement étranger, lobby, concurrent ou fournisseur indélicat), celui-ci s'appuie souvent sur un agent de l'intérieur. Or ne mésestimons jamais la duplicité humaine : la loyauté, le respect de valeurs cardinales et le sens de la parole s'effacent parfois devant l'appât du gain. Et face à d'immenses enjeux concurrentiels, la corruption d'un dirigeant ou d'un cadre peut s'avérer peu coûteuse. Bien que majeur, ce facteur est largement sous-évalué.

Les générations Y et Z n'ont pas le sens de la loyauté d'antan et entretiennent un rapport clivant à l'argent. D'un côté leurs représentants disent s'accommoder de la décroissance et veulent donner du sens à leur action ; mais d'un autre ils sont impatients, veulent « tout et tout de suite », et savent aussi que l'argent est un moyen de vivre ou d'atteindre plus rapidement leurs rêves.

Certains n'auront aucun problème à l'idée de « faire un coup », ou bien auront le souci de financer une retraite qu'ils savent plus ou moins hypothétique.

Nous voyons tout l'arrière-fond et l'écheveau culturel, politique, juridique et économique qui rend aujourd'hui les entreprises et leurs dirigeants vulnérables aux nombreuses problématiques que l'Intelligence économique pourrait justement adresser.

Imbriquées et souvent inconscientes, ces considérations ne sont pas pour rien dans l'absence d'une véritable politique d'intelligence économique pour les entreprises françaises. Mais il ne manque pas que la politique : c'est un véritable arsenal opérationnel, mobilisable en cas de menace, qui reste à concevoir. **Car lorsqu'elles se retrouvent au pied du mur, les entreprises ont besoin de répondre vite et de manière appropriée.** Nul besoin alors de littérature ni de groupes de travail : place à la décision et à la recherche de remédiation sous quelques heures, quand ce n'est pas moins.

En cas de menaces, d'une survenance d'attaques ou de manœuvres de déstabilisation, des modes opératoires efficients, rodés, informatiquement appuyés et préalablement définis doivent être déployés au plus vite. Les dirigeants connaîtront à l'avance non seulement leur existence, mais aussi leurs protagonistes ainsi que leurs conditions matérielles, opérationnelles et financières.

Et pour les raisons qui viennent d'être présentées, n'attendons pas de miracle des pouvoirs publics s'agissant des aspects opérationnels : c'est bel et bien à des opérateurs privés, à des sociétés commerciales, agences et autres cabinets de se mobiliser pour mettre sur le marché les bons outils et les améliorer sans cesse. C'est précisément la mission de Vici Agency.

1.2.2. Ne soyons pas dupes

Lorsque vous avez créé votre entreprise, lorsque vous l'avez reprise de vos parents, ou bien quand vous l'avez reçue en management sur mandat de ses actionnaires, vous étiez avant tout soucieux des conditions de son exploitation afin de générer le niveau de profit attendu. En fait, la plupart des entrepreneurs et des dirigeants **concentrent leur attention sur des cas, des situations ou des scénarios de normalité :** pour eux, le jeu de la concurrence s'exerce par l'efficience opérationnelle, par un certain montant de capitaux et de trésorerie, et s'il reste un peu de temps, pourquoi pas par un soupçon d'audace stratégique. C'est dans cette approche que les business schools ont pu produire pendant des décennies les légions de cadres efficaces dont les grandes organisations avaient alors besoin.

Aujourd'hui, pour reprendre l'expression chère à Alain Minc , nous semblons revenus à un « nouveau Moyen Âge ». Les opérations se déroulent avec davantage de brusquerie, occasionnant de la casse sociale – financiarisation et raccourcissement du reporting obligent. Les entreprises changent de main de plus en plus vite, les actifs doivent se valoriser au mieux pour être revendus avec le taux de rendement interne promis aux investisseurs.

Aujourd'hui, des start-up mettent les technologies numériques au service de promesses de désintermédiation. Si cela part d'une bonne intention (le bon plaisir du consommateur), ces leviers digitaux peuvent aller jusqu'à recomposer en quelques années la totalité d'un secteur ou d'une filière, non sans avoir invité des dizaines de milliers de travailleurs à se reconvertir du mieux qu'ils le peuvent.

PUBLICITAS NE DEVRAIT PAS LAISSER UN GRAND VIDE (TRÈS LONGTEMPS) !

Le 11 mai 2018, coup de tonnerre : la firme helvétique Publicitas annonce sa faillite. Pourtant, ce n'est pas le premier mastodonte du secteur à quitter prématurément la scène. Eberhard von Kuenheim, de BMW, ne disait-il pas « Ce ne sont pas les gros qui mangent les petits mais les rapides qui mangent les lents » ?

Certes, en dix ans le marché suisse de la publicité avait chuté en volume de 50%, la consolidation de la presse s'accentuant et complexifiant les métiers d'intermédiaire. Mais on pensait que Publicitas, à l'instar de nombreux opérateurs historiques, avait les reins pour tenir. Du moins en théorie.

Nous ne sommes pas là pour juger de la qualité d'une gestion, mais plutôt pour souligner le caractère révélateur d'un tel phénomène. Selon Vici, derrière toute faillite se cache une forme nécessaire de prédation. Nombreux sont les rentiers de leur filière à n'avoir pas su anticiper leur avenir, ou à n'avoir pas pu décrypter leurs signaux faibles. La plupart d'entre nous se souviennent de Kodak, quand les plus jeunes auront en tête ce qu'Airbnb ou Uber sont venus suppléer.

Nous allons le dire et le répéter : ne pas vous tenir au courant d'une manière proactive de ce qui se passe sur vos marchés relève de la faute professionnelle ! Cela ne veut pas dire « espionner » la concurrence, d'autant que vos compétiteurs directs regardent le monde avec les mêmes lunettes ou du moins la même correction optique que vous-même…

Attendez-vous à ce que d'ici quelques mois seulement, une start-up (américaine jusqu'ici et demain chinoise, est-européenne, israélienne, russe ou indienne) annonce avoir repensé votre business model, et clamer à toute la twittosphère être en mesure de satisfaire beaucoup mieux votre clientèle pour moins cher que vous. Et plus vous êtes un acteur installé, plus votre nom viendra en top of mind de vos accusateurs ! Mais comment n'avez-vous pas pu y penser, voir le truc venir ?

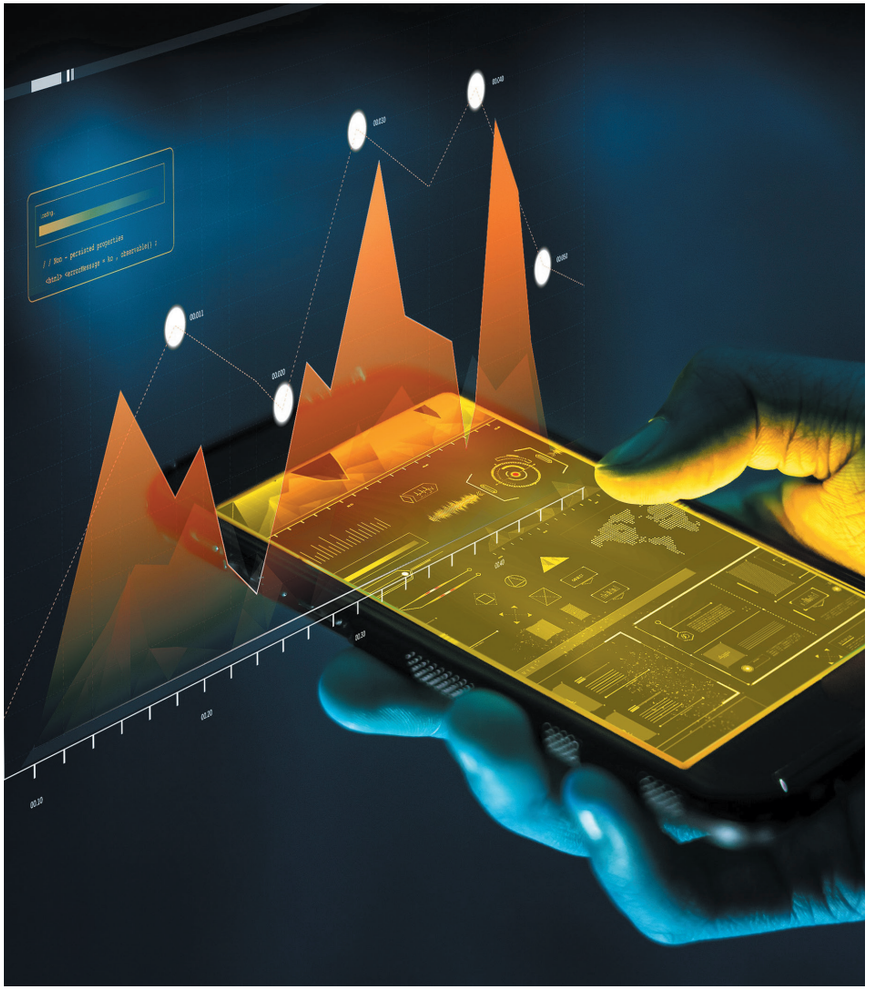
Il y va de votre responsabilité de leader. Et en l'espèce, prendre le virage du numérique va au-delà de votre responsabilité : c'est devenu la première des politesses vis-à-vis de vos clients. Ce n'est pas le nombre de consultants en transformation digitale sur le marché qui dira le contraire.

Ne finissez pas comme la grenouille dans la casserole d'eau, ne terminez pas « bouillis » faute d'avoir vu que vous barbotiez sur une plaque à induction… Activer vos antennes ne veut pas dire dépenser des sommes folles. Les asymétries se réduisent, et vous disposez aujourd'hui des mêmes moyens (digitaux) que ceux mis en œuvre par vos concurrents ou disrupteurs potentiels. Il vous faut simplement reconnaître cette réalité et décider d'entrer sur le terrain, pour vous battre à armes égales.

Vici Agency a conçu une panoplie de solutions dédiées aux entreprises en croissance, pour qu'elles puissent continuer de croître dans la sérénité, en des temps complexes et troublés. Visibilité et protection digitale en sont la partie émergée, mais c'est aussi d'investigation digitale avancée et de renseignement prédictif que nous parlons. Si Publicitas avait déployé un dispositif d'observation de son marché (largement dans ses moyens, faut-il le rappeler), elle n'aurait pas été contrainte de jeter piteusement l'éponge. Notre solution data predictor propose précisément ce type de services:

- Apprenez à détecter les marchés qui vont vous sauver la mise (veille stratégique) !
- Découvrez des opportunités de distribution à l'international que vous ne soupçonniez pas !
- Faites déjà connaissance avec vos futurs clients avant même de décrocher votre téléphone !
- Sachez-en davantage sur vos futurs partenaires d'affaires (fournisseurs, distributeurs, cibles de croissance externe) afin de piloter vos négociations et d'éviter de vous engager à mauvais escient.

Le jeu de la concurrence ne se déroule pas toujours « à la loyale », loin s'en faut. Les États-Unis ont beau être les chantres de l'ultralibéralisme, ils savent inviter la force publique lorsque c'est nécessaire et, sans crier gare, contourner des règles du jeu qu'ils ont eux-mêmes fixées. Des pratiques économiques particulièrement choquantes telles que l'extraterritorialité du droit américain sont désormais monnaie courante (en témoigne par exemple l'épisode de scandales au sein de la FIFA, révélés en 2015 et qui mèneront à la décapitation de l'organisation ainsi qu'à la mise en cause de son président Sepp Blatter), sans qu'aucun gouvernement européen ne soit en mesure de broncher. Et ne parlons même pas d'une quelconque réciprocité…



Jamais l'agressivité n'avait été aussi décomplexée, et jamais autant qu'aujourd'hui la loi du plus fort n'avait semblé la meilleure. Bienvenue dans cette jungle 4.0 où l'économique, le juridique et le politique s'articulent au service de la puissance, qu'il s'agisse de conserver ses bastions face à l'avancée du « nouveau monde » ou de s'y tailler la part du lion. À telle enseigne tous les coups sont permis !

Mais revenons au monde du renseignement. Chacun a lu des romans ou vu des films d'espionnage. En outre, tout le monde espionne tout le monde, certes dans la mesure de ses moyens. Affrontement Est-Ouest, japonais, coréens, chinois, israéliens et iraniens, tout le monde envoie des pions mais abrite aussi chez soi des indésirables. Lorsqu'un agent est « découvert », il n'est pas nécessairement exécuté : des tractations sont menées et il fait l'objet d'un échange. Et surtout, que cela reste sous le tapis puisqu'en la matière, nul ne saurait être irréprochable…

Tout au plus entend-on parfois parler d'expulsions sèches de personnes indésirables, accompagnées de protestations plus ou moins inspirées. Mais les dégâts sont limités, l'épisode ne fâche pas plus qu'auparavant des protagonistes déjà méfiants les uns envers les autres, ou même tout simplement… lucides. The show must go on, car il s'agit d'un jeu à somme plus ou moins nulle : le tout est que le grand public et la presse n'aient surtout pas l'occasion d'en connaître.

Or c'est exactement ce qui se passe dans le monde économique : les coups tordus deviennent monnaie courante dans le monde des banques, des cabinets, des fleurons industriels et… même des PME. Nier cette réalité reviendrait à perdre du temps. Sauf que si les États et les administrations diplomatiques sont rompus à ces pratiques, s'ils ont su investir et former des générations d'agents efficaces et capables d'opérer jusqu'en territoire hostile, 99,9% de nos entreprises en sont tout bonnement incapables.

Parce que nous continuons à **nous bercer d'illusions avec le libre jeu de la concurrence.** Si celui-ci a toujours une raison d'être à un niveau dirons-nous opératif (il faut bien un code de la route, des feux rouges, des giratoires et des agents de circulation…) afin de sécuriser a minima les échanges économiques, le fait du prince revient dans le jeu dès que cela redevient « sérieux ».

Nous l'avons dit et nous le répéterons : il n'y a, du moins dans les pays occidentaux, aucune politique de formation des cadres d'entreprise à ces questions tant elles sont complexes, multiformes, encore récentes et culturellement conditionnées. Quand bien même il existe des réponses privées, une littérature et un cadre théorique, et même quelques formations méritoires et qualitatives (EGE, IHEDN), tout cela ne constitue pas pour autant une capacité de défense, et encore moins d'offensive stratégique pour nos entreprises. **Ce manque d'arsenal a empêché nos cadres et nos dirigeants de cultiver des attitudes efficaces ou gagnantes face à ces menaces.**

Vu d'en haut, et notamment sous la focale de la souveraineté économique nationale, il n'y a pas encore de corrélation entre les enjeux et les moyens. Il y a comme un chaînon manquant.

1.3. IL EST TEMPS D'AGIR

Anticipez, quelles que soient les circonstances, surtout si elles sont critiques. Esquissez, dessinez l'après avec ambition, quelle que soit votre raison d'être.

JEAN DE COUDRIE

1.3.1. Une feuille de route « étagée »

Les précédents constats doivent aider entrepreneurs et dirigeants à envisager sereinement des modes d'action. Ils peuvent s'inscrire dans plusieurs horizons :

Court terme : La priorité, si ce n'est l'urgence, est d'informer les entreprises de l'existence même de solutions à des menaces identifiées. Ici prime la pédagogie, notamment quant aux différentes étapes d'intervention (identification, analyse/traitement, remédiation, suivi/veille…) et dont Vici Agency possède la maîtrise.

Moyen terme : Ces mêmes entrepreneurs doivent être convaincus de pouvoir bâtir des stratégies préventives et offensives pour protéger, développer et garantir leurs actifs. Ici également, Vici propose des réponses ad hoc.

Long terme : Une culture de l'intelligence économique pourra s'implanter en aidant les cadres et les dirigeants de petites et moyennes entreprises francophones à développer les bonnes attitudes pour demain. Il y a toute une filière de professionnels de haut niveau à créer, et qui seraient entraînés à avoir les bons réflexes pour protéger et valoriser le patrimoine économique de nos PME. Vici souhaite s'inscrire dans un projet éducatif poursuivant une telle finalité.

1.3.2. Des situations à distinguer

On peut distinguer trois natures de situations : défensives, préventives, et offensives.

Situations défensives Vous avez subi ou subissez une attaque	**Scénario 1 :** Vous êtes en mesure de qualifier ce qui vous arrive et éventuellement d'en apprécier un dommage, ne serait-ce que la portée ou les conséquences pour votre patrimoine. Vous organisez plus facilement la remédiation, si vous le pouvez par vos propres moyens, sinon en recourant à des prestataires. **Scénario 2 :** Vous êtes perplexe, dans une situation de sidération : la surprise, des choses inhabituelles se produisent et vous ne saisissez pas encore. Vous voulez mettre fin à l'anormalité en répondant le plus vite possible, mais avant cela vous devez comprendre de quoi il retourne.
Situations préventives Vous n'avez pas encore subi de dommages	**Scénario 1 :** Vous disposez d'éléments précis qui vous mettent la puce à l'oreille quant à un risque d'attaque, de menace d'intrusion, etc. Pour éviter que cela arrive, vous souhaitez mettre en place une organisation ou un processus. **Scénario 2 :** Vous n'êtes pas en mesure de saisir les risques auxquels vous êtes exposé, tandis qu'un œil exercé (voir encadré infra) le permettrait. Vous êtes dans une « incompétence inconsciente », tout à fait logique mais qui vous place dans la plus grande vulnérabilité. **Scénario 3 :** Vous mesurez la potentialité de la menace et vous décidez de prendre les devants. Deux variantes à distinguer selon le degré de probabilité ou d'imminence : > **l'attaque préemptive :** pour anticiper une attaque adverse sûre et imminente ; > **l'attaque préventive :** elle peut être lancée sans preuve d'une quelconque attaque à venir, mais dans le but de contenir un adversaire qui aurait à un moment donné l'intention de nuire (ou dont vous avez de bonnes raisons de le penser).
Situations offensives Vous êtes à la manœuvre	**Scénario 1 :** « La meilleure défense, c'est l'attaque. » Ici, rien d'anormal à constater, mais vous souhaitez comprendre pour pouvoir, le moment venu, « imprimer votre tempo stratégique ». Votre environnement est riche de dangers potentiels et vous souhaitez vous forger une idée précise, en effectuant une veille (un renseignement plutôt passif, mais qui n'empêche pas la précision). **Scénario 2 :** Vous avez déjà une idée précise de qui pourrait déclencher un prochain mouvement contre vous, et vous souhaitez tuer la menace dans l'œuf. Vous montez une opération de renseignement plus actif visant, cette fois-ci, à connaître les intentions de vos partenaires de jeu (concurrents, fournisseurs, etc.). **Scénario 3 :** Vous n'avez pas besoin de vous faire une idée de la situation, vous avez votre propre feuille de route stratégique et vous souhaitez balayer les obstacles sur votre route. C'est dans cette dernière catégorie qu'évoluent, totalement décomplexés, les prédateurs économiques. Ici, vous décidez de la manœuvre à mener et des différentes séquences qui viendront la jalonner. **N'ayez pas peur de « finir le boulot » et de méditer au passage cette phrase de von Clausewitz : « Tant que je n'ai pas terrassé mon adversaire, je dois craindre qu'il ne me terrasse et je ne suis pas maître de mes actions, puisqu'il est tout aussi en mesure de m'imposer sa loi que je le suis de lui imposer la mienne. »** Enfin, privilégiez la fugacité dans votre offensive : soit l'attaque l'emporte rapidement parce que le point de faille ou de rupture était avéré, soit elle cesse. Car la réaction tarde rarement (« La rapidité est l'essence même de la guerre. » - Sun Tzu).

Une fois ce constat posé, comment être attentif à ce qui se passe ? À quoi reconnaît-on les symptômes d'une situation à risque si une attaque n'est pas d'ores et déjà réalisée ou bien en cours ? Quels signaux faibles ou indices devez-vous identifier ? Enfin, quelles sont les questions à vous poser ?

PEUT-ON APPRENDRE À « EXERCER » SON ŒIL ?

Il y a une part de votre savoir-faire mais aussi de votre sens de l'observation : ce qui vous semble être des symptômes ou des indices sont autant de signes avant-coureurs ou de signaux faibles d'une situation potentiellement grave et en cours de survenance. Vous avez l'expérience de votre métier, de votre secteur et savez ce qui peut « clocher ». Mais parfois, des événements, anodins pour des profanes en matière de sécurité, portent les germes d'un dommage futur.

Le vrai problème est bien le moment de la prise de conscience : si vous arrivez suffisamment tôt par chance, alors vous aurez « eu chaud » mais vous aurez aussi le loisir d'organiser une réparation et éventuellement une réponse. Mais si vous arrivez trop tard, eh bien tant pis ! ***Souvenez-vous bien des cas précis dans lesquels vous-mêmes ne pouvez absolument pas vous permettre d'arriver trop tard, et ne serait-ce qu'une seule fois*** *(par exemple, le piratage de votre serveur détenant des données ultrasensibles sur votre prochaine technologie).*

En réalité, c'est une logique « assurantielle » : dans certains domaines particulièrement sensibles pour votre entreprise, vous ne pouvez pas vous permettre le moindre risque. Vous devez mettre sur pied des « routines » comprenant certains points de vigilance qui correspondront aux points de faiblesse ou de rupture de votre modèle. Tout écart sur un ou plusieurs de ces points devra automatiquement vous alerter, pour déclencher la mise en place d'une réponse.

Ère digitale oblige, beaucoup de ces sujets sont automatisables dans votre système d'information, notamment par la programmation d'algorithmes. De plus en plus de sujets… mais heureusement pas tous les sujets… !

1.3.3. Rappels utiles pour votre approche de l'information

Dans un monde chaque jour plus chargé en données et plus riche en analyses, les entreprises ont pris l'habitude de s'informer en temps réel. Mais en raison d'un déluge informationnel et d'un risque de saturation, elles se heurtent rapidement à une problématique de discernement.

La qualité du rapport à l'information devient une capacité stratégique car le besoin de décision ne disparaîtra jamais, lui. Au contraire il s'intensifie et devient de plus en plus gourmand en data. Si des technologies donnent (ou promettent) des effets de leviers vertigineux en la matière, en bout de course l'humain garde encore toute sa place.

Cette capacité d'approche de l'information se comprend en plusieurs moments et doit se développer en autant de niveaux :

• La capacité de collecte

Tout commence par la récupération d'informations intéressant directement vos activités. Un travail de veille active doit être mené :

En OSINT : Ou Open Source INTelligence, c'est-à-dire l'ensemble des activités et des méthodes de collecte et d'analyse de l'information de sources dites ouvertes. Des informations en somme accessibles au grand public qui incluent les journaux, Internet dont les réseaux sociaux, les livres, les magazines scientifiques, les diffusions radio, télévision, etc. (Wikipedia). Un peu au-delà de ces sources, on trouve la capacité à opérer en deep web (ou « web profond ») : ce n'est pas à la portée du grand public mais il n'existe pas d'impossibilité technologique à aller y chercher des informations, à condition de disposer du savoir-faire nécessaire.

En HUMINT : Ou HUman INTelligence, renseignement dont la source est un ou plusieurs individus. Par extension, le renseignement humain désigne l'ensemble des activités de traitement de ce type d'information (collecte, évaluation, analyse, diffusion). Il se distingue du renseignement technique (renseignement d'origine électromagnétique, renseignement d'origine image), et du renseignement d'origine source ouverte (Wikipedia). Ce renseignement devra parfois se faire en territoire hostile, « derrière les lignes ennemies ». Le secret réside dans le fait de disposer de sources, voire d'« indics » suffisamment précis, fiables et loyaux.

Ces moyens sont orchestrés pour collecter et entretenir tout le patrimoine d'informations utiles à la conduite des activités de l'entreprise. Mais devant la masse, il est important – et l'effet d'expérience joue alors beaucoup – de discerner ce qui est critique et différenciant de ce qui reste plutôt commun (notamment côté OSINT) et moins décisif. Progressivement, des processus de soutien de cette collecte sont à mettre en place, puis à améliorer en continu.

Aujourd'hui, les actifs informationnels d'une organisation prennent de nombreuses formes. Big data oblige, on parle beaucoup de datalakes, ces gigantesques bases de données cependant marquées par des enjeux de mise à jour et de maintenance réels : lutte contre leur obsolescence naturelle ; et conservation de leur contextuation pour, après traitements appropriés, en générer des produits d'information pertinents (croisements, agrégats pertinents et corroborés) pour les différents interlocuteurs et publics concernés.

• La capacité de traitement et d'analyse

Par construction, cette capacité doit être proportionnée à la masse de l'information recueillie. D'où l'importance de savoir prioriser le matériau collecté car le traitement de l'information, qu'il soit humain ou technologique, représente du temps et un coût. Il faut donc allouer la capacité « algorithmique » par ordre de priorité, car rappelons que les capacités de traitement ont gagné en puissance grâce aux progrès de ces dernières années.

Pour autant, l'intervention humaine ou automatisée (développement de logiciels, de scripts) représente un coût et des inconvénients : c'est au management d'arbitrer où et pourquoi il décide d'allouer du coût humain ou bien du coût machine. En conséquence, des « routines informationnelles » appropriées pourront être définies pour l'organisation, sans oublier que rares sont les situations d'investigation pouvant se passer au final d'une analyse humaine, a fortiori si l'entreprise dispose d'experts chevronnés.

Enfin, il faut rester attentif au coût et à l'empreinte de stockage de l'information de second plan, même si les vulnérabilités inhérentes à sa détention sont moins dommageables que pour une information réputée stratégique.

• La capacité de diffusion

Des packages d'information exploitables sont en principe définis par public-cible ou « persona », au sein de l'organisation. Ce qui implique de bien les connaître et de respecter leurs habitudes de consommation d'information pour pouvoir les leur adresser par le bon canal, dans le bon format et, surtout, au bon moment :

Le bon canal : Espace privatif dans l'intranet, mailing list spécifique, e-mail personnalisé, messagerie sécurisée, call, Skype, présentiel, etc. Vous devez connaître les canaux suffisamment usités et sécurisés pour ne pas créer de gêne et générer suffisamment de confiance à leur usage.

Le bon format : Intrinsèquement lié au bon canal, le bon format permet de toucher les cibles dans des volumes et des modalités de présentation de l'information qui respectent notamment leurs préoccupations quotidiennes et leurs impératifs de mobilité. Privilégiez les formats courts lorsqu'ils sont en déplacement, et les formats plus délayés et illustrés lorsqu'ils peuvent consulter l'information « à tête reposée ».

Le bon moment : Dernier paramètre mais non le moindre. Pouvoir adresser une information au moment critique produit un effet d'interpellation, de réflexion et d'engagement approprié des collaborateurs concernés. Là encore, l'effet d'expérience et la connaissance des bons moments dans les cycles d'activité permettent de programmer l'envoi des produits d'information désignés lorsque c'est pertinent, et pérennisent d'autant le processus.

Enfin, ne sous-estimez pas le besoin en mobiquité de vos usagers, c'est-à-dire leur capacité – en situation de mobilité – à se connecter à un réseau sans contrainte de temps, ni de localisation, ni de terminal.

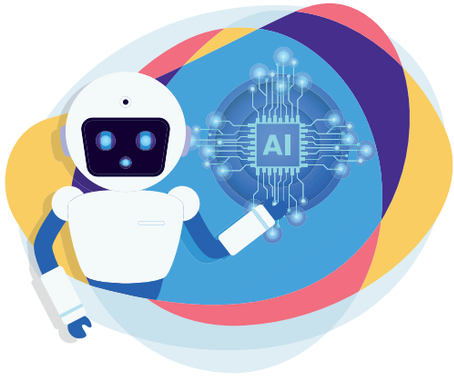
1.3.4. Nos contrées ont besoin de patrons d'assaut !

Le patron d'assaut n'est ni plus ni moins qu'une projection nécessaire de l'entrepreneur et du dirigeant de PME ou de belles structures familiales désirant survivre et, demain, gagner, dans un environnement hautement complexe et continuellement évolutif.

Derrière cette appellation se cache une figure singulière, néo-chevalière, presque archétypale. Nous l'espérons modélisante pour des dirigeants en attente de réponses opérantes et « raisonnablement offensives », en tout cas toujours dans la proportionnalité et la déontologie requises par notre système de valeurs.

Promouvoir cette figure suppose un fort enjeu d'éducation, car les cartes mentales de nombreux dirigeants se sont périmées. Et ce n'est pas une question générationnelle ni de digital litteracy : même les plus jeunes n'auront pas reçu dans leur éducation les réflexes de défense suffisants pour un monde aussi violent et décomplexé.

Petit détour par les neurosciences : les chercheurs constatent une inadéquation croissante entre les impératifs de l'économie et un phénomène d'appauvrissement des capacités sémantiques des enfants. Celles-ci nécessitent l'activation de 3 circuits pour une mémoire à long terme, alors qu'ils se développent aujourd'hui essentiellement sur le plan procédural (qui lui-même privilégie seulement 2 circuits) ou mémoire à court terme. Nos enfants sont devenus très efficaces dans la collecte superficielle d'information pour pouvoir la « recracher » plus tard, chose que l'x est partie pour faire infiniment mieux qu'eux… **Or c'est surtout leur intelligence sémantique, celle qui donne du sens (qui est également la troisième couche du cyberespace) qu'ils auront besoin de développer.**



Vous avez déjà vécu une ou plusieurs de ces situations ?

Consultez-nous
+41 213 11 29 42
daniel@vici-agency.com

COMMENT RECONNAÎTRE UN PATRON D'ASSAUT ?

√ ***Il a une capacité de raisonnement élargie :*** *Doté d'une grande culture générale, il n'a pas de problème pour raisonner sur une échelle globale. Pour lui, les facteurs géopolitiques et géostratégiques entrent en considération dans le choix de ses marchés, de ses investissements et de ses implantations. Il balaie chaque sujet « en 360° » des problématiques et des risques susceptibles d'impacter son business (cf. infra).*

√ ***Il aime la résolution de problèmes et apprend de ses erreurs :*** *Un patron est censé être le plus apte à résoudre les problèmes, car c'est lui qui décide en dernier ressort. C'est pourquoi il excelle dans ce domaine en variant les techniques, les points de vue, les temporalités… Son expérience l'amène non pas à refouler ses échecs mais à savoir en tirer parti.*

√ ***Il est doté d'une bonne dose de jugeote et d'intuition :*** *S'il sait que les capacités analytiques et la culture générale sont un atout, le patron d'assaut voit dans le bon sens et l'intuition un concentré d'intelligence pratique en situation. Il leur réserve un bon accueil et il n'a pas honte de se fier à eux, y compris dans des situations à enjeu – tout en sachant que cela ne fonde jamais 100% de sa décision.*

√ ***Il a une capacité d'influence personnelle :*** *Pas besoin d'un charisme débordant, un patron d'assaut est conscient que l'image globale de son entreprise repose sur l'empreinte médiatique et interrelationnelle qu'il laisse. Il voit l'organisation qu'il dirige comme un prolongement de lui-même et il se montre soucieux de ses prises de parole comme des convictions qu'il défend.*

√ ***Il sait se montrer persuasif :*** *Il prend les choses à son compte, comme s'il était en négociation permanente. Il ne veut pas subir mais plutôt convaincre ses parties prenantes du bien-fondé de ses vues. Il sait faire adhérer autrui en rendant clairs les bénéfices pour chacun, quitte à orienter les sentiments et les représentations de ses interlocuteurs.*

> *La politique et la stratégie de la guerre ne sont qu'une perpétuelle concurrence entre le bon sens et l'erreur.*
>
> CHARLES DE GAULLE

√ ***Il sait faire preuve de résilience et d'agilité :*** *Il reste focalisé sur ses objectifs. Et si jamais les circonstances de ses affaires lui disent non, il ne s'effondre pas. Il ne dévie pas de son but et verra derrière tout problème une opportunité. Il essaiera de trouver une solution de rebond, quitte à jouer avec le temps, et il s'appuiera sur toutes ses forces vives pour embarquer tout le monde autour d'un pivotement devenu nécessaire.*

√ ***Il sait « aller au fight » si nécessaire :*** *Il n'a jamais pensé que le monde des affaires était un sanctuaire. S'il ne surréagit pas inutilement, il est conscient de la duplicité de ses congénères. Il s'attend à des coups tordus et ne porte pas de jugement dessus. Pour lui, « c'est ainsi ». Il n'a pas non plus de problème à envisager des actions offensives pour obtenir ce qu'il recherche, mais toujours dans la limite de la légalité puisqu'il est un chevalier.*

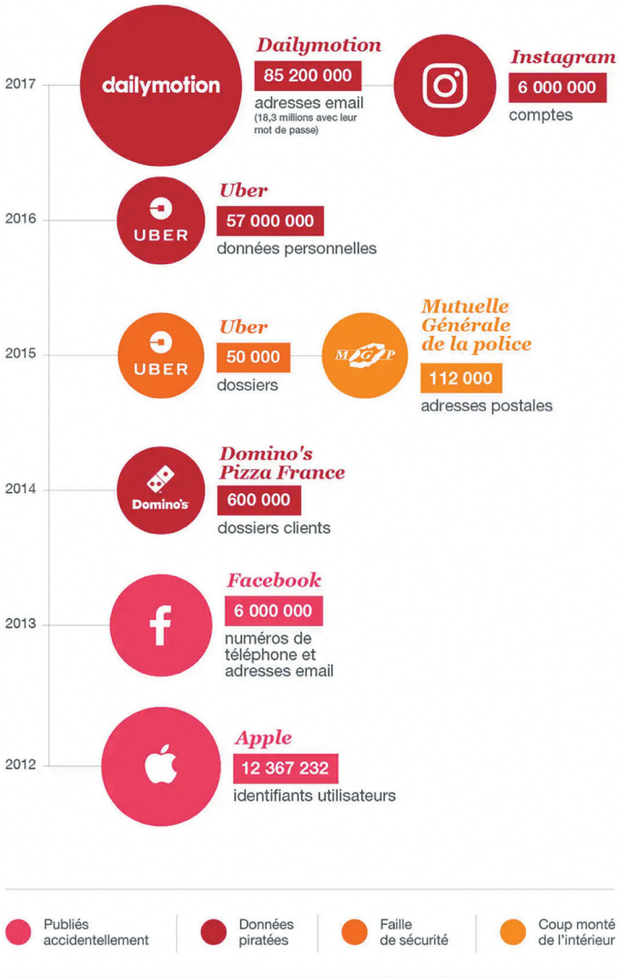
√ ***Il dispose d'un fort esprit critique :*** *En cette ère d'ultra-information, il s'agit d'une qualité cruciale. Il est animé d'un doute constructif permanent. Il ne prend rien pour acquis, il connaît ses biais perceptuels et sait s'en affranchir. Il veut être capable de voir au-delà des apparences pour résoudre les problèmes et trouver la meilleure solution qui soit.*

√ ***Il sait gérer son ego :*** *Il en connaît l'utilité et les limites. Il n'a plus de choses à prouver aux autres et ne plie pas dès la première contrariété. Mais il sait en utiliser la force pour poursuivre ses objectifs, balayer les obstacles qui ont besoin de l'être, et qui ne sauraient justement l'être sans son ego…*

√ ***Il est connecté à une finalité :*** *Il n'a pas choisi d'entreprendre pour faire des coups financiers et se mettre à l'abri, le temps de réaliser son business plan. Il croit en sa mission et sait vouloir mettre ses talents au service d'une « causalité » qu'il voudra découvrir tout au long de sa vie. Pour lui, un tel projet est « incarné », sinon rien.*

Piratage de données, tous concernés !

Hackers, employés, erreur, les causes de divulgation de données des entreprises sont nombreuses et le phénomène touche plus d'entreprises qu'on pourrait le croire. La preuve avec cette sélection de fuites recensées depuis 2012 en France et à l'international.



World's Biggest Data Breaches, www.informationisbeautiful.net

ESPIONNAGE INDUSTRIEL : LES PIÈGES AUXQUELS VOUS NE PENSEZ JAMAIS

Parachutiste de l'Armée de Terre puis Officier de renseignement, **Chems Akrouf** a occupé différentes fonctions au sein du Bureau de lutte anti-terroriste, où il a notamment été en charge du recrutement des agents de renseignement. Il quitte l'armée fin 2011 pour créer RensForm International, avec l'objectif de transposer le savoir-faire du renseignement au profit des entreprises, en matière de formation, de recrutement ou d'intelligence économique.

Et si vous étiez la cible d'agents secrets ? Un scénario fantasque pour la majorité des DRH et des DSI, qui sous-estiment largement les risques liés à l'espionnage industriel. Et pourtant, selon Chems Akrouf, Fondateur de RensForm International et ex-officier des services de renseignements, beaucoup d'entreprises sont espionnées sans le savoir.

La poubelle, l'imprimante, le post-it…
A l'occasion d'un audit de sécurité, Chems Akrouf a envoyé une personne de son équipe en tenue de technicien de surface dans les locaux d'une entreprise qui suspectait un de ses concurrents d'accéder à ses données stratégiques. « Il n'a eu aucun problème pour passer le contrôle de sécurité à l'entrée, il a ramassé le contenu de toutes les poubelles remplies de documents sensibles. Il a imprimé des fichiers qui étaient dans la mémoire des imprimantes. Il a accédé aux sessions des PC des collaborateurs dont les codes étaient inscrits sur des post-it. Nous avons laissé des clés USB infectées sur les bureaux des salariés : au bout de 2 semaines, on recensait 40 connexions » raconte l'expert. Effrayant.

L'offre d'emploi
Si vous recrutez un chef de marché qui parle portugais et justifie d'une expérience opérationnelle en Amérique latine dans le secteur pharmaceutique, par exemple, vous risquez de mettre immédiatement la puce à l'oreille de vos concurrents sur votre projet de développement au Brésil. « Les descriptions de poste contiennent souvent des informations clés. Attention à ne pas trop en dire » conseille Chems Akrouf.

Le wifi public
Dans les hôtels, sur les salons, dans les aéroports : se connecter à un réseau wifi public est devenu une pratique quasi-quotidienne. Or « il est très facile, pour ceux qui savent le faire, d'accéder aux données présentes sur vos ordinateurs portables, smartphones ou tablettes. Il ne faut jamais se balader avec des documents sensibles lorsqu'on est en mobilité » suggère Chems Akrouf.

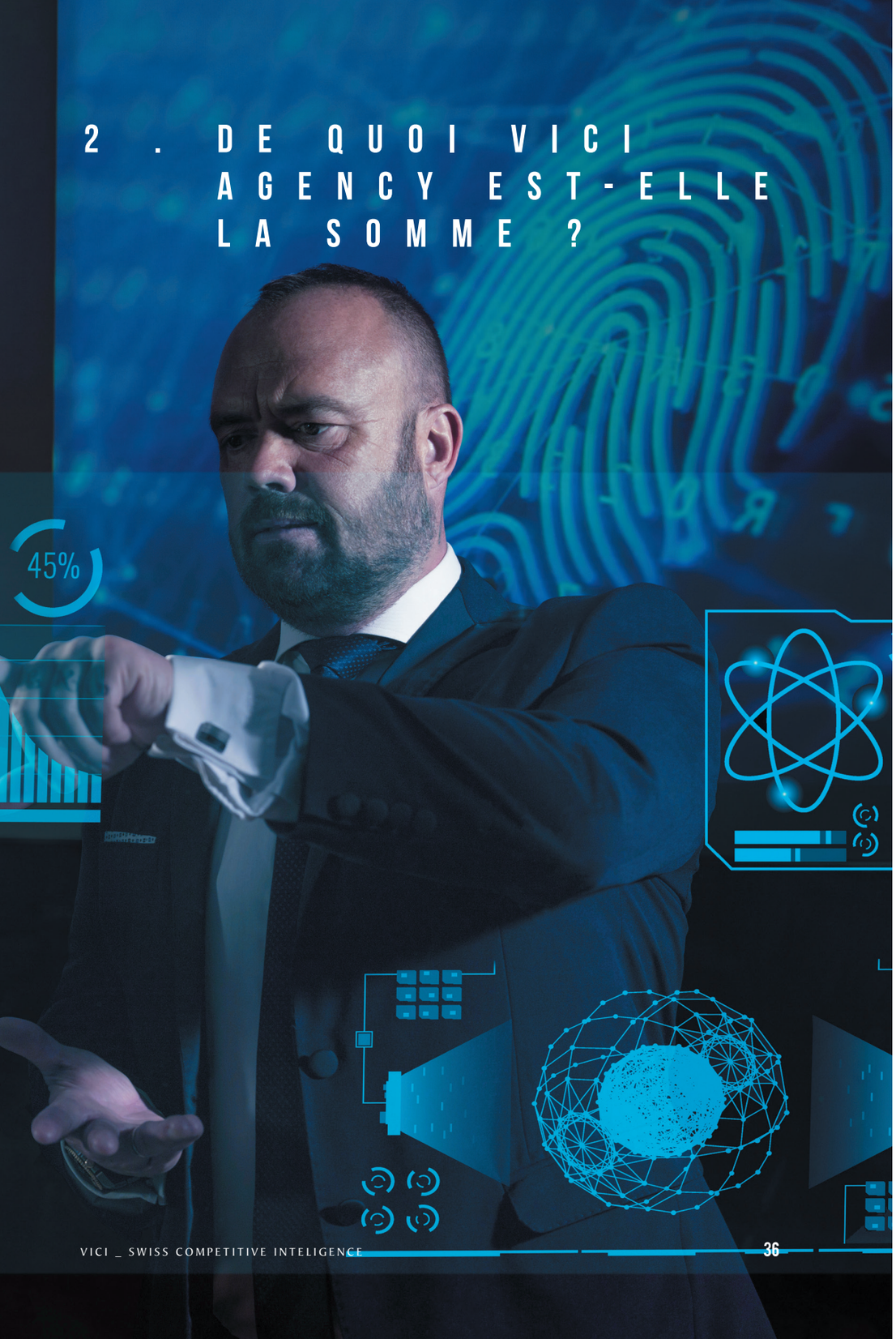
Les rapports de stage
Il n'est pas rare que les jeunes diplômés utilisent leur rapport de stage comme une pièce à part entière de leur dossier de candidature à un poste. « Les entreprises mal intentionnées convoquent d'ex-stagiaires en entretien pour mettre la main sur des infos clés sur leurs concurrents » assure l'expert. Seul rempart à envisager : faire viser les mémoires et rapports de stage par la DRH avant validation.

Les fournisseurs
Parfois, vos sous-traitants travaillent également pour vos concurrents. Quand ils ont accès aux données depuis des années, via les collaborateurs ou des messageries communes, ils peuvent être des espions de luxe pour la concurrence. « Partagez avec eux uniquement ce qui est utile. Quand on ne sait pas, on ne peut pas répéter » insiste l'ex-officier des renseignements.

Les logiciels gratuits de traduction
Qui n'a pas déjà copié-collé un document rédigé en langue étrangère dans Google Translate ? « La majorité des logiciels de traduction en ligne sont gratuits car ils revendent les données. De plus, certains mots-clés sont automatiquement transmis à la NSA aux Etats-Unis. Mieux vaut opter pour un programme payant mais sécurisé » conclut Chems Akrouf.

Source : http://exclusiverh.com:30080/articles/conseil-sirh/espionnage-industriel-les-pieges-auxquels-vous-ne-pensez-jamais.htm

2 . DE QUOI VICI AGENCY EST-ELLE LA SOMME ?



VICI AGENCY COMBINE PLUSIEURS INGRÉDIENTS :

L'histoire de son fondateur

L'intégration de changements

Des ressources uniques

2.1. UNE HISTOIRE SINGULIÈRE

Daniel Adrien Donnet-Monay est né en 1968 à Troistorrents (Valais, Suisse). Après une scolarité écourtée, il entre en apprentissage professionnel avant d'entamer sa carrière comme artisan plâtrier-peintre.

À 20 ans, il s'engage comme grenadier de chars dans l'armée suisse, jusqu'à atteindre le grade de lieutenant-colonel – engagement qu'il poursuivra tout au long de son parcours professionnel. Il opérera également comme officier des forces spéciales.

Passionné de sport depuis l'enfance, il s'illustre en hockey sur glace jusqu'au niveau professionnel. Il prendra également part à plusieurs éditions de la célèbre Patrouille des Glaciers.

Daniel entame sa vie professionnelle en lançant son propre business dans le secteur de l'étanchéité, avant de se découvrir un talent pour les métiers de contact : il y enregistrera de beaux succès comme cadre commercial, notamment dans les secteurs de l'intérim (Manpower, dont il sera le directeur pour le Valais Romand) et des assurances (La Bâloise Assurances).

> *Le hockey sur glace est un savant mélange de glisse acrobatique et de Seconde Guerre mondiale.*
>
> ALFRED HITCHCOCK

Mais la perspective d'une carrière salariée l'ennuie. Entrepreneur intuitif et spontané, il sera tour à tour artisan à son compte, patron de bar, importateur pour la Suisse du karaoké ou encore des dartboards (jeux de fléchettes électroniques), tout en poursuivant son parcours militaire.

Daniel cumule alors des expériences variées pour apprendre, tester ses limites et élargir sa zone de confort. Sans qu'il le sache, la résilience va devenir le fil rouge de ses nombreuses séquences de vie :

- *Une mission de réorganisation et de redressement d'entreprise en Afrique, où d'ailleurs il contractera la malaria.*
- *Un investissement malheureux qui lui fera perdre sa maison au début de la décennie, et qui l'amènera à vivre de manière spartiate pendant deux ans, avant de se remettre à flot.*
- *Un grave accident de la route et divers pépins de santé, qui mettront à rude épreuve sa résistance physique et psychologique.*

2009 marque un tournant dans sa trajectoire professionnelle. II s'associe à un ami genevois pour créer AAGS SA, une structure fiduciaire qu'il préside toujours. Celle-ci propose à des entrepreneurs étrangers des services d'intelligence patrimoniale et de family office. En une décennie, les deux associés accompagneront près de 500 entreprises souvent familiales, d'une dizaine de nationalités et de tous secteurs, à optimiser leur empreinte fiscale.

Au contact de ces dirigeants, à l'écoute du monde et fort de son expérience militaro-entrepreneuriale Daniel connaît deux prises de conscience :

- *Une empreinte fiscale optimisée est un moyen pour les entreprises de préserver leur capacité d'investissement.*
- *Cette capacité est devenue d'autant plus nécessaire que l'environnement des affaires s'est considérablement durci et que la concurrence se fait de moins en moins loyale. Les entrepreneurs en croissance préserveront d'autant mieux leurs capacités de développement qu'ils auront une vision proactive de leur business, qu'ils accepteront de s'acculturer à de nouveaux domaines, qu'ils développeront leur leadership, qu'ils élargiront leur niveau de lecture du monde, et surtout qu'ils sauront activer de véritables réflexes de survie.*

Désireux de mettre en œuvre ces prises de conscience, Daniel s'associe en 2017 à Jean-Jacques Martin, un expert en neurosciences reconnu des milieux scientifiques, et à Jean-Louis Marx, un entrepreneur à succès dans le milieu du logiciel. Tous trois créeront Vici Agency, une agence privée d'intelligence et de renseignements économiques.

Celle-ci réunit des chercheurs qui développeront data predictor, un outil d'analyse prédictive d'avant-garde permettant aux entrepreneurs de tirer parti des signaux faibles de leur marché. Cela doit les aider à identifier et à concrétiser leurs opportunités de business à l'international, mais tout autant à repérer, à traiter et à prévenir les menaces pesant sur leur patrimoine informationnel, technologique et réputationnel.

D'une certaine manière, Daniel Adrien Donnet-Monay est lui-même l'assemblage de caractéristiques surprenantes tant il s'est illustré dans des environnements divers.

2.1.1. Le Valaisan : le bon sens terrien et le caractère

Troistorrents est une terre typiquement valaisanne. Le rapport à la nature y est quotidien, son terroir est exceptionnel mais ses rudesses, notamment hivernales, forgent chez ses habitants un caractère tout reconnaissable : « Nous sommes un peu les Corses de la Suisse », s'amuse l'intéressé.

Cet état d'esprit prédispose Daniel à l'effort, au sens de l'entreprise et de l'initiative pour « survivre », en restant connecté avec bon sens à la terre et à l'essentiel.

2.1.2. Le sportif de haut niveau

Daniel est un sportif dans l'âme. Féru depuis l'enfance de hockey sur glace, il a évolué dans plusieurs équipes locales avant d'œuvrer en ligue nationale helvétique. Il aurait pu poursuivre sa carrière sportive professionnelle, mais il a privilégié ses aventures entrepreneuriales et militaires. Il reconnaît lui-même que la pratique du hockey, et les relations exceptionnelles qu'il a entretenues, notamment avec ses entraîneurs et présidents de clubs, l'ont construit.

Sans doute une préfiguration de ce qu'il connaîtra à l'occasion de la Patrouille de Glaciers qu'il accomplira d'ailleurs à trois reprises ! Pour ceux qui ne connaissent pas, cette course militaire historique, nationale et internationale rallie Zermatt à Verbier dans les Alpes. Créée lors de la Seconde Guerre mondiale, elle est ouverte aux concurrents civils, élites et populaires, et fait partie de « La Grande Course », qui réunit six épreuves de ski-alpinisme de longue distance.

Soucieux de rester en « condition opérationnelle », Daniel continue de se rendre tous les jours à la salle de sport.

2.1.3. Le Chevalier 4.0

Daniel a été membre de nombreuses associations sportives et caritatives, par passion autant que par esprit de service. Sensible aux vicissitudes et aux épreuves de la vie, qu'il a lui-même connues à de nombreuses reprises, il aime aider son prochain sous différentes formes et à différentes occasions.

Aujourd'hui membre de l'Ordre des chevaliers de Saint-Martin, la dimension « chevaleresque » comptera beaucoup dans la formulation qu'il donnera à l'aventure Vici.

> *On devient l'homme de son uniforme.*
>
> NAPOLÉON BONAPARTE

2.1.4. L'officier supérieur

Entré comme simple soldat à l'âge de 20 ans, Daniel choisit une spécialité parmi les plus difficiles : les grenadiers de chars . Nommé caporal un an après, il fait l'École d'officiers l'année suivante pour franchir successivement les grades qui l'amèneront à obtenir ses deux commandements.

À 36 ans, il est nommé commandant de sept compagnies (dont trois compagnies de chars et une d'artillerie), soit un périmètre de 980 personnes pour un budget annuel de fonctionnement équivalent à 100 millions d'euros. Quelques années plus tard, il obtiendra le grade de lieutenant-colonel et complétera son expérience comme officier au sein des forces spéciales.

Daniel est conscient que cette expérience fut décisive à plus d'un titre dans la genèse de Vici Agency. Elle lui a procuré notamment :

- un regard militaire, qui rend conscient des risques et des menaces ;
- une habitude à l'endurance, tirée des situations de manœuvre ;
- une logique décisionnelle, privilégiant l'efficacité.

2.1.5. Le serial entrepreneur

Après quelques années d'apprentissage en boulangerie et comme artisan plâtrier-peintre, Daniel compense une entrée dans la vie professionnelle précoce (13 ans) par un besoin d'expérimentation, un sens de l'audace et un goût prononcé pour les défis. L'entrepreneuriat lui en donnera toutes les occasions.

Sorti de l'armée à 22 ans (mais pas de l'expérience militaire, qui reste continue) et hormis des expériences salariées qui lui apporteront beaucoup – notamment en termes d'aptitudes commerciales – il créera de nombreuses sociétés (cf. supra). Il connaîtra certains échecs qui le marqueront dans sa chair et seront, à chaque fois, un électrochoc et l'occasion d'une prise de conscience.

La faute est dans les moyens bien plus que dans les principes.

NAPOLÉON BONAPARTE

Bien que jalonné de défis et de projets choisis par instinct, le parcours de Daniel trouve une nouvelle cohérence au début des années 2010 : ses activités chez AAGS SA vont lui servir de formidable poste d'observation, et lui apporteront un concentré d'expérience irremplaçable : celle de ses clients. Il développera une acuité et un discernement en matière d'affaires, que l'on retrouve dans les principes d'intervention des équipes Vici ainsi que dans la philosophie de développement de l'outil data predictor.

Ce capital d'expériences et cette capacité de rebond, voire de dépassement des circonstances, forgeront chez Daniel **la conviction de devoir accompagner les dirigeants d'entreprise à ne pas subir leur condition et à refuser le fatalisme de la globalisation, pour au contraire en tirer de belles opportunités.**

2.2. LA PRISE DE CONSCIENCE D'UN MONDE QUI CHANGE ET LA NÉCESSITÉ D'Y APPORTER SA PIERRE

C'est au contact et à l'écoute de ses clients, que Daniel comprend qu'il faut aller plus loin aux côtés des entrepreneurs de croissance. Nous l'avons dit, mais il est important de le répéter : « Ces derniers préserveront d'autant mieux leurs capacités de développement qu'ils auront une vision proactive de leur business, qu'ils accepteront de s'acculturer dans certains domaines, de développer leur leadership, d'élargir leur niveau de lecture du monde, et surtout d'activer les bons réflexes de survie. » Cette conviction forte, issue de sa double expérience militaro-entrepreneuriale, ne le quittera plus.

Il est regrettable que des patrons qui investissent et prennent des risques puissent rencontrer des difficultés au plan économique, fiscal ou réputationnel, faute de s'être suffisamment informés. C'est pour Daniel un « crève-cœur » que de les voir aller à l'échec, lorsqu'on sait à quel point notre culture tolère mal l'insuccès.

Nous savons que pour se projeter sur de nouveaux marchés à l'international, nos entrepreneurs ont besoin d'être accompagnés. C'est parfois loin de leur environnement domestique qu'ils trouveront les relais de croissance utiles à la suite de leur aventure. Or les dispositifs prévus par nos pouvoirs publics – bien qu'ils relèvent d'une bonne intention et d'une conscience déjà prise en la matière – ne sont pas assez opérants. Parce qu'ils sont pensés dans des termes administratifs, parce qu'ils s'appuient sur des dispositifs parfois lourds, et parce qu'ils n'ont pas suffisamment pris la mesure du rôle du renseignement.

Ce que Daniel sait. Mais il sait tout autant que les outils ne sont rien sans les individus pour les utiliser. Si la collecte des données est cruciale, encore faut-il savoir leur donner du sens pour prédire et gagner.

2.2.1. Des changements

Désormais, il faut prendre des décisions de plus en plus rapidement et sur la base d'un nombre toujours croissant de paramètres et de sources d'informations. Afin de saisir de nouvelles opportunités de marché, entrepreneurs et dirigeants disposent d'outils de prédiction à base statistique. Ils peuvent les aider à anticiper les évolutions qui les percutent, pour réaliser au bon moment les arbitrages nécessaires.

2.2.2. Une prise de conscience et des convictions

Le rythme des changements abordés va non seulement se poursuivre, mais sans doute s'accélérer. En contexte de guerre économique globale, et surtout sur le terrain « cyber », les frontières entre le défensif, le préventif et l'offensif tendent à s'estomper.

Les dirigeants seront tenus de conduire leurs affaires en « intelligence de situation », sans s'affranchir d'une vue globale tenant compte de la transformation digitale et du changement dans le rapport à l'information.

Celle-ci se révèle autant une mine d'or qu'une menace. Devenue entropique et « plastique », l'information nécessite des actions spécifiques pour savoir œuvrer sur le web, comme s'y protéger durablement (réputation, cybermenaces). Néanmoins, la digitalisation croissante des organisations leur commande de **développer un niveau de résilience proportionné.**

EXTRAIT D'INTERVIEW DE DANIEL ADRIEN DONNET-MONAY

Daniel, vous posez un diagnostic singulier et sans concession sur la situation actuelle des PME des pays d'Europe occidentale, notamment françaises, helvétiques ou encore italiennes. Pouvez-vous nous en dire plus ?

Depuis le début des années 1990 et l'entrée dans l'ère de l'information, le monde n'est que « changement continu ». Ce qu'on appelle l'hyperconnectivité, conjuguée à une lecture du monde probabiliste, a sans doute produit le plus grand bouleversement que l'humanité ait connu !

Auparavant newtonien et déterministe, notre monde est tout d'abord devenu quantique et « probabiliste ». Les trajectoires deviennent moins prévisibles, et le fait de ne plus savoir avec précision requiert de nouvelles approches, parfois déconcertantes.

Le monde est par ailleurs devenu « infotropique ». Avec Internet les graines de l'hyperconnectivité sont semées et une révolution s'enclenche, cette fois centrée sur l'information et l'entropie comme nouveau modèle. L'émergence des technologies digitales a provoqué un déluge d'informations, rapidement devenu un désordre mondial : en effet, l'information s'enrichit continuellement à mesure qu'on l'observe et qu'on la commente.

« Heureusement », le soleil californien a donné naissance à des start-up qui ont investi suffisamment tôt et massivement dans de nouvelles technologies de tri et d'analyse de l'information pour asseoir leur suprématie sur le marché de l'information du monde occidental.

En outre, les distances s'abolissent : le principe d'intrication quantique veut que l'on puisse passer instantanément d'un point A à un point B en se jouant des distances physiques, du temps et de la vitesse. Et ce principe « réinforme » en permanence les marchés. Le monde est devenu un écosystème infini et hyperconnecté, mais dont les modalités relationnelles ont besoin d'être réapprises.

Le Web, enfin, est porté par ce qu'on peut appeler des « vecteurs mutagènes ». Ils se chiffrent en des termes énergétiques. Chaque acteur sur le marché doit disposer d'un « scoring économico-énergétique » qui est une combinaison d'un volume d'information et d'une puissance de calcul et d'analyse suffisants pour leur permettre de prévoir leur positionnement à moyen terme. Et pour le déterminer, l'entreprise doit mener une analyse introspective :

- *Mon indice énergétique me permet-il de suffisamment bien interagir avec l'écosystème actuel ?*
- *Mon organisation compte-t-elle suffisamment de cerveaux capables de libérer le potentiel d'action et d'innovation que le marché attend ?*
- *Sommes-nous suffisamment protégés des attaques externes ? etc.*

Quoi qu'il en soit, il ne vous aura pas échappé que nous sommes en guerre économique généralisée ! Qu'il s'agisse d'une start-up, d'un groupe de hackers ou de la diplomatie d'affaires, des super-prédateurs sont à l'affût. Ils combinent de brillants cerveaux humains à la puissance prédictive des machines pour disrupter, cyberattaquer ou déstabiliser les actifs économiques et les entreprises ciblés de pays occidentaux. Quel qu'en soit le visage, cette prédation produit toujours des effets prémédités !

Alors face à l'ampleur de la transformation et des menaces, j'ai voulu « passer aux manœuvres ».

*Je l'ai aussi fait par convictions personnelles. Cela me désole que des patrons qui investissent et prennent des risques souffrent. Qu'ils souffrent économiquement, que la fiscalité ne les aide pas, mais qu'ils pèchent **également dans leur capacité à traiter l'information stratégique pour leur entreprise – alors que celle-ci reste pour elles un formidable gisement de résilience!** Ils sont perdus, ils n'ont pas nécessairement conscience d'aller mal et ne se réveillent qu'au moment de mettre la clé sous la porte ou de devoir se vendre à un concurrent étranger. C'est un comble et c'est surtout un énorme gâchis !*

En plus, ces patrons n'ont souvent personne à qui confier leurs états d'âme. Pourtant, ce sont eux les « premiers de cordée » : leur boulot est de résoudre les problèmes complexes de leur entreprise en éclairant les autres, jour après jour. Et ces problèmes sont devenus d'une complexité suprahumaine ! Le tout dans une culture qui ne tolère pas l'échec ni même le doute ! Vous voyez le chemin qui reste à parcourir… ?

Sans doute, mais n'existe-t-il pas aujourd'hui de nombreux dispositifs publics ou parapublics pour aider les entreprises et leurs dirigeants ?

*Lorsque ces dirigeants s'adressent aux organismes publics censés les aider, ils manquent cruellement de réponses **opérantes**. Ce ne sont pas les instances, les groupes de travail, les observatoires ni les inévitables rapports parlementaires qui manquent… bien au contraire ! Mais ils ont besoin de solutions*

pragmatiques, outillées et produisant des résultats mesurables… C'est autre chose. À mon sens, il y a inadéquation entre l'offre et la demande !

Contrairement aux Américains ou aux Chinois, les patrons français, suisses ou italiens par exemple ne sont pas suffisamment convaincus que leur salut passe par le fait d'aller « arracher » leur croissance à l'international. Je parle bien d'arrachement, oui. On est sur une démarche volontariste, agressive même. Dans le même temps, qui nierait que la diplomatie de nos compétiteurs américains et chinois est économiquement orientée et décomplexée ?

Nos patrons de PME doivent envisager des marchés qu'ils ne connaissent pas encore, par définition. Parce qu'ils ont tardé à s'y pencher. Et parce qu'ils n'ont pas été en mesure d'y investir pour les comprendre et pour les prospecter.

Oui, et ils n'ont pas su voir certains signaux faibles ?

Absolument. Ces dirigeants ont perdu du terrain ***en ne se donnant pas l'occasion de détecter les signaux faibles qu'ils auraient pu convertir en opportunités.*** *Bien sûr, ils ne bénéficient pas des réseaux d'informateurs des grandes banques ou des groupes cotés à l'UBS 100 ou au CAC 40. Leur connaissance du fonctionnement du monde d'aujourd'hui, et a fortiori de demain, n'est pas à la hauteur des enjeux. Pensons par exemple aux facteurs géostratégiques, dont l'impact pour eux s'avère plus concret qu'ils ne l'imaginent… Quand ils n'élaborent pas leurs scénarios sur des croyances erronées ! Ce qui se passe d'important pour eux n'est aujourd'hui pas dans leur radar, quand bien même ce ne sont pas les moyens de s'informer ni la quantité d'information disponible qui manquent.*

Très bien, mais que manque-t-il alors selon vous ?

- *Primo, de la détermination*
- *Secundo, de la méthode et de la discipline*
- *Tertio, les outils adéquats notamment de traitement de l'information stratégique pour produire de la prédictivité et éclairer la décision offensive*
- *Enfin, un pilotage serré des actions et des progrès réalisés.*

Cela doit reposer sur un cadre pédagogique adapté. Ce que je décris, les patrons de PME ne le tiendront d'aucune business school, si renommée soit-elle. Et ce ne sont pas non plus leurs aînés qui auraient pu le leur apprendre – si je devais être un peu cynique, eux qui ont eu la chance de leur transmettre le flambeau au bon moment. Et c'est surtout que le monde a évolué trop vite : ce monde ne ressemble à rien de ce que nous avons connu : il est « VUCA » et de plus en plus insaisissable.

C'est bien la somme de ces facteurs et de cet état d'esprit qui a généré cet immobilisme, qui compromet depuis trop longtemps la croissance et demain la pérennité du poumon économique de la France, de la Suisse et de l'Italie, pour m'appuyer sur mon cadre de référence.

Pour autant, de formidables opportunités sont au bout. Car je ne crois pas en la fatalité. Donc j'aimerais conclure en lançant un appel, un peu comme le général de Gaulle le 18 juin 1940 : Ce n'est qu'en revêtant leur uniforme de « patrons d'assaut » que les entrepreneurs seront en mesure d'aller chercher une croissance rentable. Si le sujet n'est pas d'entrer en résistance au sens littéral, il s'agit quand même de s'ouvrir aux changements déjà à l'œuvre et qui n'attendront pas, ça je peux vous le garantir, l'assentiment des retardataires ou des déclassés !

Daniel, votre diagnostic est sans concessions, mais il repose aussi sur une lucidité et des convictions ancrées. J'imagine que vous avez réfléchi à une solution pouvant aider les dirigeants que vous ciblez à sortir de cette fatalité ?

Vici Agency veut aider les entrepreneurs à développer leur degré de résilience économique et à apprendre à s'adapter plutôt qu'à continuer d'apprendre pour le plaisir. Car les besoins sont considérables et il y a urgence !

Nous voulons permettre aux chefs d'entreprise de définir une stratégie d'attaque et de défense commerciale sur les nouveaux marchés actuels. Nous allons les aider à développer une nouvelle vision, à intégrer les nouvelles techniques d'analyse ainsi que les outils dédiés à l'accomplissement de cette vision.
Il y a urgence aussi à les rendre les plus autonomes possibles face aux GAFAM et consorts, qui ont fait du traitement de l'information une nouvelle donne de la guerre économique désormais menée dans le sillage de la globalisation.

Ce qui implique de s'approprier davantage des enjeux d'Intelligence économique, et d'apprendre à utiliser ses outils dits offensifs. Voilà pourquoi Vici leur dédie des moyens d'investigation d'avant-garde, et à des conditions de marché adaptées.

Une IE offensive nécessitera une approche complexe liant la stratégie militaire de l'attaque à une approche analytique de niveau scientifique. Cette interaction subtile remet en cause les fondamentaux du management moderne, et les comportements doivent s'adapter et façonner des réflexes calibrés pour aider à relever des challenges sans cesse plus exigeants.

Diversification, développement partenarial, arbitrages entre investissement et fiscalité, internationalisation : nous pensons que **les patrons d'entreprises moyennes et familiales ne sont pas assez préparés au type de discernement que la conduite de leurs affaires requiert à une échelle globale.** Rien à voir avec une insulte à leur intelligence ! C'est juste qu'à l'ère des « datanomics », ce que l'on qualifiait jadis de rationalité limitée ou d'asymétries risque d'avoir des conséquences plus lourdes qu'auparavant.

Il importe aux patrons de ces entreprises de développer un « **discernement d'affaire**s », une « **business acuity** » d'un nouveau genre, en revisitant certaines pratiques d'affaires par un triple effet :

- une meilleure prise en compte de l'**environnement macro** de l'entreprise ;
- une mise en place d'une **Intelligence économique défensive comme offensive ;**
- un déploiement de solutions de **Business Intelligence** et de **datamining**. Une fois son contexte appréhendé et sa stratégie de défense définie, on déploie les protocoles et les outils « permettant de collecter, consolider, modéliser et restituer les données, matérielles ou immatérielles, d'une entreprise en vue d'offrir une aide à la décision et de permettre à un décideur d'avoir une vue d'ensemble de l'activité traitée » (d'après Wikipedia).

Par ailleurs, le monde de demain est quantique. Cela rejaillit concrètement dans la compréhension du temps, de l'espace et de l'information, qui sont des paramètres clés dans la définition des stratégies entrepreneuriales et de différenciation concurrentielle. En particulier, **les dirigeants ne peuvent se désintéresser du rendez-vous posé par les data sciences**. Il leur faut tirer parti de la préparation des données, des statistiques, du machine learning et d'une intelligence artificielle capable d'apprentissages autonomes, lorsque toutes ces approches présentent des avantages concurrentiels dans leurs activités. S'ils ne le font pas, leurs concurrents, eux, ne s'en priveront pas : ils ont d'ailleurs déjà commencé.

Autre exigence : les comportements doivent s'adapter et façonner des réflexes calibrés à la hauteur des challenges rencontrés. Sur ce terrain, les dirigeants ont d'abord à comprendre quels sont leurs possibles inhibiteurs décisionnels : certains sont culturels, nous l'avons vu, tandis que d'autres sont aussi liés aux traits de caractère et à la personnalité. Or, **fort des épreuves qu'il a eu la douleur de vivre mais aussi la chance de surmonter, Daniel a voulu transmettre son capital d'expériences (dépasser ses limites, élargir son horizon, se réinventer sans cesse…) à des dirigeants, car il sait maintenant que leur formation et leur parcours les préparent insuffisamment à faire face à ce qui se trame.**

BON À RETENIR

Les entrepreneurs comme les dirigeants gagneront :

À **INTÉGRER À LEUR RÉFLEXION** LA SITUATION GÉOPOLITIQUE MONDIALE, CAR IN FINE ILS N'Y ÉCHAPPERONT PAS.

À **DÉVELOPPER UNE CONSCIENCE** AIGUË DU PATRIMOINE DONT ILS ONT LA CHARGE : COMMERCIAL, TECHNOLOGIQUE, RÉPUTATIONNEL.

À **APPRÉHENDER LES NOUVELLES APPROCHES TECHNOLOGIQUES** (NOTAMMENT L'IA) ET À SAVOIR LES PILOTER DANS UNE STRATÉGIE DE GUERRE ÉCONOMIQUE.

À **CULTIVER LEUR DÉTERMINATION**.

À **DÉVELOPPER UN DISCERNEMENT** D'AFFAIRES DANS UN MONDE COMPLEXE À DE NOMBREUX TITRES : VUCA, MONDIALISÉ, INFOTROPIQUE, HYPERCONNECTÉ… ET DE PLUS EN PLUS HOSTILE.

À NE PAS FAIRE DE COMPLEXES, MAIS À **ÊTRE RÉSOLUS À SE BATTRE** CONTRE LES SUPER-PRÉDATEURS (HACKERS, START-UP, CONCURRENTS, OFFICINES GOUVERNEMENTALES…).

À **DÉFINIR UNE STRATÉGIE OFFENSIVE COMME DÉFENSIVE** SUR LEURS NOUVEAUX MARCHÉS, INTÉGRANT LES OUTILS D'IE À LEUR DISPOSITION ;

À **DÉVELOPPER NON SEULEMENT DES CAPACITÉS D'APPRENTISSAGE, MAIS SURTOUT D'ADAPTATION.**

À **ÊTRE CONSCIENTS DE LEURS CROYANCES ERRONÉES ET LIMITANTES** (COMME LE DÉFAITISME PATRIOTIQUE) ;

À **DÉVELOPPER LEUR RÉSILIENCE**, ET NOTAMMENT DE NOUVEAUX RÉFLEXES DE CONDUITE.

2.2.3. Un besoin de réponses

Être un patron d'assaut, c'est bien. Disposer de son équipement et de la logistique qui l'accompagne, c'est mieux. Dans la mesure où les patrons s'occupent au quotidien d'innombrables processus et procédures, mobiliser des réponses à finalité d'Intelligence économique – qui plus est en contexte d'urgence ou tendu – doit être le moins pesant et inconfortable pour eux.

Il y a des actions qu'ils peuvent directement prendre à leur charge, et d'autres dont l'expérience recommande la sous-traitance à un tiers de confiance :

Actions internalisables	Actions externalisables
> formuler une vision à l'aune de ces nouveaux impératifs ; > définir les objectifs ; > élaborer une stratégie en vue de les remplir ; > réaliser un suivi des réalisations ; > cultiver les attitudes favorables à l'excellence décisionnelle et à la survie.	**Renseignement** > audit pour disposer d'un constat objectif sur leur situation ; > éclairage informationnel de leur prise de décision stratégique, notamment à l'international ; > opérations de marketing digital (stratégie, référencement, analyses de marché, positionnement de marque…) ; **Protection** > veille/protection de marque, incluant des actions de remédiation ; **Influence** > actions de remédiation en cas de crise / atteinte à leur e-réputation (défacement de site, déréférencement de contenus) ; > actions d'influence en ligne : écoute du marché via les réseaux sociaux, forums et communautés ; cartographie des comportements en ligne ; > actions de légitimation de marque ;

BON À SAVOIR

L'« inattribution » dans le cyberespace

En cyberstratégie, il reste très difficile de remonter au véritable commanditaire d'une offensive. Cette opacité arrange tout le monde, et elle est le pendant de la nécessaire exposition qu'un conflit conventionnel, lui, entraîne. Ce principe d'inattribution technique est commode, tant il empêche l'imputation politique et pénale.

Nos moyens d'investigation figurent parmi les plus avancés du marché privé. Nous les avons voulus totalement adaptés au monde actuel : à échelle mondiale, décomplexés et astucieux, digitaux lorsqu'il s'agit de procurer un effet de levier décisif pour nos clients, et jamais déconnectés du « flair de l'enquêteur ». Le tout toujours dans les limites de la légalité !

DANIEL ADRIEN DONNET-MONAY

2.3. DES RESSOURCES

2.3.1. Une technologie

Algorithmisation de la vie oblige : nous avons vu que les data sciences résidaient dorénavant au cœur de la performance. Lorsqu'il s'associe à Jean-Jacques Martin en 2017, Daniel Adrien Donnet-Monay souhaite **réunir sous un même toit des chercheurs** capables de comprendre la systémique énergétique du Web en expansion, et d'en tirer parti :

- pour collecter, analyser et traiter de la donnée de tous formats, à une très grande échelle ;
- pour modéliser de nouveaux algorithmes prédictifs ;
- pour créer des outils capables d'assister les stratèges d'entreprise dans leur prise de décision.

C'est ainsi que naîtra data predictor : il s'agit d'aider des dirigeants à tirer parti d'un maximum de signaux faibles disponibles. Ce qui est décisif lorsqu'il s'agit d'identifier et de concrétiser leurs opportunités à l'international (nouveaux produits, conquête de marchés, réseaux de distribution, alliances stratégiques…) ; et qui l'est tout autant quand il faut repérer, traiter voire prévenir les menaces pesant sur le patrimoine informationnel, technologique et réputationnel de leur entreprise.

Paramétrable à l'infini, selon les contextes et les problématiques posés par les clients de Vici Agency, data predictor est une boîte à outils singulière, un socle technologique d'appui de nos consultants dans le cadre de leurs interventions (collecte, analyse, traitement et diffusion notamment). Nous nous mettons à l'avant-garde du conseil augmenté et au service de la sécurité économique pour faire de Vici l'Agence de renseignement digital des PME.

2.3.2. Une équipe

Vici rassemble une équipe experte, multigénérationnelle et multi-référentielle aguerrie à des formats d'intervention impactants, comptant :

- des entrepreneurs ;
- des cadres militaires ;
- des chercheurs en neurosciences ;
- des experts en programmation informatique ;
- des marketeurs et des communicants.

2.3.3. Un savoir-faire

Notre ADN prend sa source dans trois domaines : militaire, neuroscientifique, et informatique.

Notre culture professionnelle favorise non seulement la rigueur et la discipline mais aussi la précision, l'art de la synthèse, la créativité et l'effet de surprise.

De par la variété des profils et le niveau d'expérience de ses consultants, Vici Agency dispose d'une palette complète de compétences. L'agence adresse tous les moments du cycle de renseignement, OSINT comme HUMINT, nécessaire aux entreprises et à leurs dirigeants dans une logique d'information, de protection et d'influence.

Les méthodologies utilisées par Vici s'appuient sur le capital d'expérience de ses professionnels, mais bénéficient également d'une innovation et d'un apprentissage continus grâce aux nombreuses interventions menées continuellement.

2.3.4. UN ÉCOSYSTÈME RICHE

Vici Agency a su nouer puis cultiver des relations privilégiées non seulement dans le monde militaire mais aussi des neurosciences et de l'informatique de pointe.

Nous participons à des conférences en Europe, notamment sur la veille stratégique, le cyberrenseignement et la cyberprotection.

Cet écosystème professionnel est vital pour développer notre vision et renouveler sans cesse notre engagement, car **Vici n'est pas qu'une aventure commerciale : c'est surtout un combat pour les valeurs que nous développons dans le présent ouvrage.**

3 . NOS RÉPONSES

3.1. DOMAINES DE COMPÉTENCE

Est-ce que des informations erronées sont diffusées et nuisent à mes intérêts ?

Est-ce que des alliances se créent dans l'objectif de me déstabiliser ?

Quelle est la position de mes concurrents et de leurs produits ?

Qui sont les clients qui se renseignent sur ma catégorie de produits ?

Suis-je la cible de cyberattaques ?

Est-ce que de nouveaux produits arrivent sur le marché ?

Suis-je plagié et copié ? Si oui, par qui ?

Sur quels nouveaux territoires étendre mes activités ?

Sur quels nouveaux territoires étendre mes activités ?

Où sont mes débiteurs indélicats et ont-ils des actifs cachés ?

Quelles sont les attentes des consommateurs et les meilleures zones de chalandise ?

Est-ce que mes partenaires sont loyaux et axés sur nos intérêts communs ?

...

De nombreuses années d'accompagnement des entrepreneurs donnent aux consultants de Vici Agency un poste d'observation privilégié de la vie des affaires. Ils ont été et demeurent les témoins de nombreuses et légitimes interrogations des dirigeants et des cadres d'entreprises moyennes et de croissance. Cette expérience nous permet même d'affirmer que le diable se dissimule dans les situations d'affaires parfois les plus courantes !

Spécialiste de la collecte massive de données et des enquêtes ciblées de toutes natures, Vici organise ses interventions autour de trois domaines de besoins critiques des entrepreneurs : se renseigner, se protéger, et influencer.

3.1.1. Se renseigner

Les bons renseignements enrichissent votre prise de décision. Vici collecte toutes les natures d'informations qui viendront soutenir votre développement :

• **Étude 360° des acteurs du marché :** Ne vous lancez pas sans savoir où vous mettez les pieds. Nous collectons des données brutes ou structurées sur les différentes dimensions de votre marché, qu'il s'agisse de structures ou de personnes physiques :

Concurrents : Sachez précisément qui vous « attend », quelles en sont les forces et les faiblesses mais aussi la dangerosité.

Clients : Ne vous engagez pas avant de savoir à qui vous avez affaire. Mieux vaut parfois s'abstenir que de conclure avec un mauvais payeur... ou quelqu'un qui fera du reverse engineering...

Fournisseurs : Sachez à qui vous confiez les clés de vos approvisionnements stratégiques et ayez une vision réaliste de votre potentiel de négociation.

Partenaires : Identifiez ceux qui vous aideront à booster votre notoriété, à développer de nouveaux produits, et à prescrire vos solutions auprès de vos cibles.

• **Enquêtes de moralité :** Sachez à qui vous vous adressez pour vous engager en connaissance de cause, notamment dans des contextes réglementés (due diligence d'acquisition, KYC, compliance) et sécurisez vos engagements contractuels.

• **Appui aux campagnes marketing :** Vos campagnes se multiplient et se digitalisent mais vous peinez à en mesurer le retour ? Rentabilisez votre processus de lead acquisition en mettant en place un tracking de l'expérience utilisateur de vos opérations, sur vos indicateurs référents.

• **Enquêtes d'investigation :** La vie des affaires demande de constituer de nombreux dossiers administratifs et juridiques. Renforcez-les d'informations décisives et donnez à vos conseils juridiques la matière qui fera la différence lors de contentieux, en défense comme en demande.

• **Listings et mappings qualifiés :** Établir des listings commerciaux opérationnels, et en assurer la maintenance peut s'avérer lourd et coûteux, même lorsqu'on dispose d'un outil de CRM. Nous pouvons les établir sur demande, à l'échelle du monde entier, dans tout secteur économique, et pour un nombre de champs d'information surprenant. Nous reconstituons des organigrammes complexes et générons des mappings relationnels pour vous aider à préparer votre théâtre d'opérations.

• **Audit de la solidité économique** : Assurez-vous de la solvabilité économique de vos partenaires, de la solidité de leurs infrastructures (notamment informatiques), et de leur potentiel commercial.

3.1.2. Se protéger

Ne pas réagir à la rumeur peut s'avérer fatal. Vici Agency met en œuvre des dispositifs de protection sur mesure à vos enjeux, proportionnés aux menaces que vous subissez :

• **Fake news :** Incontournables autant qu'indésirables, les fausses nouvelles lancées par des concurrents malveillants peuvent être fatales à votre business faute d'avoir été démenties à temps. Nous réalisons des veilles de réputation périodiques que votre community manager n'aura pas nécessairement le temps ni les moyens de mener. Cela lui permet de se concentrer davantage sur l'accroissement et la rentabilisation de vos audiences.

• **Protection de vos marques :** Celles-ci sont l'un de vos principaux actifs. Nos moyens de surveillance poussés sur le Web vous offrent davantage de sérénité en identifiant des tentatives de plagiat et de contrefaçons que seul un réseau de renseignement structuré est en mesure de signaler.

• **Cyberattaques :** Moyen économique et efficace de nuisance envers votre exploitation, elles connaissent un accroissement exponentiel, qu'il s'agisse de saturer vos serveurs, de discréditer la sécurité de vos infrastructures, ou simplement de vous extorquer de l'argent. Nos consultants auditent votre dispositif de sécurité, vous accompagnent dans sa mise à niveau, et réalisent tous les tests nécessaires.

3.1.3. Influencer

L'influence est devenue déterminante dans le déploiement de votre notoriété, car elle est un vecteur d'engagement de vos communautés d'affaires. Vici vous conseille dans le choix de l'approche la plus appropriée à vos objectifs :

• **Légitimation de marques :** Le faire-savoir est crucial pour le développement des entreprises, même s'il est complexe et coûteux à orchestrer, notamment à l'international. Nos outils et nos méthodologies d'investigation permettent de dégager des signaux faibles, des tendances de consommation mais aussi les bons publics sur lesquels concentrer vos moyens et auxquels dédier vos actions de communication.

• **Développement de popularité :** Coutumiers des logiques et autres algorithmes d'indexation web, nos consultants vous aident à optimiser le référencement naturel de votre site web, à définir des stratégies de développement de son trafic, et également à optimiser vos budgets publicitaires et de SEA (Search Engine Advertising).

• **Identification de prospects :** Constituer des listings est une chose, générer de véritables prospects en est une autre. Nous vous donnons les moyens de mieux comprendre le comportement de vos cibles (tracking digital, expérience utilisateur) afin de nourrir votre sales funnel en continu et d'améliorer vos scores de conversion client.

• **Community management :** Nous mettons la création et la gestion de communautés à la portée des structures de taille modeste, par des formules d'externalisation adaptées.

3.2. CAS CLIENTS

CAS #1 - « PATRON, ON A COMME UN PROBLÈME D'E-RÉPUTATION… »

LES FAITS

Notre client est le distributeur d'une grande marque automobile, leader sur son marché. Il souffre cependant d'une mauvaise réputation chronique sur les réseaux sociaux.

Il ne comprend pas pourquoi : cela ne provient pas d'une mauvaise gestion technique de son community management, ni de défauts de service de la part de ses techniciens ou de ses commerciaux, qui auraient pu entraîner des mécontentements répétés ou des contentieux en cascade. Il y a un curieux décalage entre la réalité du business perçue par notre client et sa réputation sociale, extérieurement observable.

Il sent que la situation lui échappe, alors qu'il est absolument dépendant du capital confiance construit depuis tant d'années avec son constructeur automobile. **Craignant que son fonds de commerce ne finisse par se déprécier, il sollicite Vici Agency pour comprendre l'origine de cette situation et prendre toutes les mesures correctives qui s'avéreraient nécessaires.**

Après leurs premières analyses, nos enquêteurs constatent qu'un grand nombre des commentaires désobligeants envers notre client sont en réalité postés par des avatars actifs. Ce premier fait établi, ils concentrent leurs efforts pour découvrir leur identité. Or ils se rendent compte que ceux-ci ne relèvent en fait que d'une seule adresse IP : il n'y aurait donc qu'un seul protagoniste derrière cette opération relevant clairement du sabotage.

En remontant la piste de cette adresse IP, nos experts parviennent à trouver l'identité de son propriétaire : il s'agit d'un jeune homme de 19 ans. Mais alors **quel est le mobile du délit ?** On imagine mal qu'un adolescent ait un quelconque intérêt à nuire à un distributeur automobile. Nos consultants approfondissent leurs recherches sur cet individu. En dressant un mapping de son écosystème relationnel, ils découvrent un proche lien de parenté avec le CEO d'un grand distributeur d'une autre marque automobile.

Cette dernière est connue pour être une rivale, en segment de marché comme en produits, de celle que distribue notre client. En outre, ce deuxième distributeur se trouve implanté dans une zone de chalandise similaire à celle de notre client… Il est tout simplement son concurrent frontal.

Vici formalise un rapport complet comprenant l'ensemble de ces éléments puis le transmet, conformément à sa demande, à la Direction juridique de son client afin qu'il décide des mesures à prendre et des éventuelles poursuites à engager.

LE DÉCRYPTAGE

Dans cette affaire, notre client est alerté par un décalage flagrant entre la perception que ses propres clients peuvent avoir de lui au quotidien et ce qui circule à son propos sur les réseaux sociaux. **L'anormalité doit être votre premier signe d'interpellation,** alors soyez continuellement attentifs à votre e-réputation. Confiez à votre community manager, si vous en avez un, ou à votre webmaster, le soin de la surveiller et de vous signaler tout buzz négatif : car tout écart significatif ou récurrence indue doit être un signal faible à prendre en compte au plus tôt.

Le second point important est lié à son business model : en tant que distributeur exclusif d'une grande marque automobile, il est par nature vulnérable. En effet, son activité est 100% liée aux véhicules confiés par son mandant constructeur, sur la base de ses performances commerciales mais aussi et en sous-jacent, du degré de confiance qu'il lui accorde. Or la digitalisation des usages et l'omnicanalité faisant, **quel constructeur pourrait durablement maintenir sa confiance à un distributeur dont la cote est très mauvaise sur les réseaux sociaux, ainsi que sur les sites d'avis de clients ?** Quand bien même une « bulle de médisance » serait montée de toutes pièces (ce qui est le cas ici), c'est au distributeur qu'il appartient de rechercher pourquoi et d'y remédier. Pas au constructeur. Notre client a donc eu un bon réflexe en sollicitant Vici Agency, puisqu'à moyen terme (peut-on parler de long terme quand on connaît la viralité du Web ?), il en allait de la valeur même de son patrimoine.

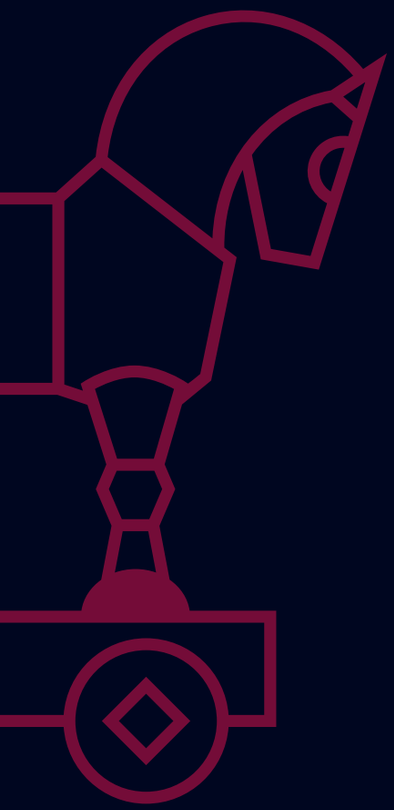
Autre point intéressant : les avatars. On sait le cybermonde régi notamment par un principe dit d'« inattribution » : les gens qui y mènent des activités, notamment malveillantes, se cachent derrière des avatars préservant leur anonymat. Mais ce qui en l'espèce a permis à nos experts d'y voir plus clair, c'est **l'unicité de signature numérique entre eux, à savoir une seule et même adresse IP. Pour rappel, une adresse IP** [pour Internet Protocol] est le numéro identifiant chaque ordinateur connecté à Internet, ou plus généralement et précisément l'interface avec le réseau de tout matériel informatique (routeur, imprimante…) connecté à un réseau informatique utilisant l'Internet Protocol .

Après l'IP, il fallait s'intéresser au mobile de la manœuvre, qui n'était pas flagrant au premier abord. Et c'est d'ailleurs **une incongruité apparente** (un jeune de 19 ans s'acharnant sur un distributeur automobile) qui a mené nos consultants à décortiquer l'identité et l'écosystème relationnel du propriétaire de l'adresse IP. Certes nous avons déjà vu de plus jeunes assaillants encore, surdoués de l'informatique, « hacker » des sites gouvernementaux ou dits « sensibles ». Mais c'était « pour le sport ». Dans notre affaire, rien d'aussi exaltant ou méritoire au sens où les crypto-communautés l'entendent. Donc le mobile était peu clair.

Et c'est ce flou qui nous a amenés à **établir un mapping relationnel de l'individu.** Celui-ci dévoilerait finalement un lien de parenté insoupçonné avec le dirigeant d'une firme directement concurrente. À ce stade, le mobile devient nettement plus clair : un concurrent désireux d'affaiblir notre client met sur pied une campagne de déstabilisation par dénigrement continuel contre lui sur Internet, et en s'appuyant sur un seul assaillant.

Sans des **moyens avancés d'investigation**, il aurait été impossible de remonter à l'existence d'une adresse IP unique ainsi qu'à l'identité réelle de l'assaillant. Si parfois de grandes banques, des compagnies d'assurances ou des leaders industriels disposent de « limiers » dans leurs équipes IT, ce genre d'enquêtes est généralement confié à un cabinet spécialisé. Ici, le commanditaire a pensé qu'il suffirait de « bricoler » en chargeant un proche de cette manœuvre. **Il aurait dû passer par des professionnels ou de vrais tiers qu'aucune cartographie n'aurait permis de lui rattacher, et qui en outre auraient usé de plusieurs adresses IP afin de brouiller les pistes et de rendre ainsi le buzz plus réaliste.**

L'identité du vrai commanditaire permet en outre de valider son intérêt à agir : une similarité de marché et de produits à ceux de notre client. Enfin, Vici s'est bornée – conformément à la demande du client – à la remise d'un rapport. Celui-ci est **suffisamment documenté et précis pour servir de base opposable lors d'un contentieux** devant une juridiction civile ou criminelle. Mais parfois, certains commanditaires nous demandent d'aller plus loin et de leur suggérer, voire d'opérer nous-mêmes après leur validation, des actions résolutoires. Bien évidemment, nous **restons toujours dans les limites permises par la réglementation d'affaires qui leur est applicable.**



3.2. CAS CLIENTS

CAS #2 - « MES PARTENAIRES S'ENTENDRAIENT-ILS DANS MON DOS ? »

LES FAITS

Notre client est un acteur de premier plan mondial du secteur du luxe. Il s'approvisionne en denrées et en matières premières de haute qualité auprès d'un panel diversifié de fournisseurs, implantés dans plusieurs pays de l'UE. Depuis des années, il est habitué à mener avec eux des négociations dures mais justes, et toujours dans la confiance.

Pourtant depuis quelques mois, il s'étonne que trois d'entre eux adoptent systématiquement à son endroit une politique de négociation tarifaire étonnamment alignée. **Craignant de leur part une entente sur les prix, il sollicite Vici Agency pour confirmer son intuition et voir comment y remédier.**

Nous optons pour une **investigation croisée** entre notre client et ses trois fournisseurs. Celle-ci débouche rapidement sur l'identification d'un « point de convergence ». Une enquête approfondie sur ce point met au jour son identité : il s'agit ni plus ni moins d'un Senior Advisor de notre client, rôle ô combien influent dans son organisation.

Après accord de notre client, nous mettons en place un **dispositif de surveillance** de cet individu. Cette période, combinée à différentes analyses, permet de **caractériser un comportement suspect.** Le Senior Advisor mettrait à profit son statut et le niveau d'information dont il bénéficie à ce titre, pour s'octroyer certaines libertés dans les négociations menées au nom de son entreprise mandataire, à savoir notre client. Quel est son mobile ? A priori pécuniaire puisqu'il encaisse à plusieurs reprises des commissions indues de la part chacun de ces trois fournisseurs, **quand bien même son mandat ne le lui permet pas.**

Non seulement notre client ignore que son Senior Advisor agissait de la sorte, mais de même pour chacun des trois fournisseurs : après **un contrôle global**, nos experts établiront que ces mêmes partenaires se sont en réalité fait manipuler par l'individu, qui **a fait état de sa qualité pour obtenir des faveurs** de chacun d'entre eux, mais de manière séparée et sans qu'il n'ait organisé de concertation entre eux.

Nos investigations auront permis à notre client de **caractériser le comportement indélicat de son conseiller, et surtout de se rassurer quant à la fiabilité et à la loyauté de ses fournisseurs.**

LE DÉCRYPTAGE

Ce second cas est révélateur du **décalage pouvant exister entre l'intuition d'un dirigeant et la réalité des manœuvres jouées à son encontre.**

En l'espèce, notre client est **interpellé par un alignement devenu systématique** des positions tarifaires des trois mêmes fournisseurs, dans des négociations. Ces faits lui font penser à une possible entente concurrentielle à son encontre, en quelque sorte un délit d'initié – même si nous ne sommes pas dans un contexte boursier.

Il cherche à savoir **comment ces fournisseurs parviennent à se mettre d'accord, et comment à chaque fois ils réussissent à être informés.** Par qui : un espion, une taupe ? Et surtout derrière cela : **ses partenaires sont-ils fiables ou doit-il s'en méfier, voire en changer ?**

Dans ce type de situation, des investigations croisées et approfondies entre les protagonistes aident à **mettre au jour des liens a priori peu visibles ou insoupçonnés.** En l'occurrence, les recherches aboutissent à un dénominateur commun, ou « point de convergence ». Nos consultants établissent avec certitude qu'un individu opérant depuis des années comme Senior Advisor du client entretient des liens nourris avec chacun de ces fournisseurs. Une situation plutôt troublante.

Pour rappel, un Senior Advisor est généralement un professionnel très expérimenté, dont un dirigeant ou un Comité exécutif s'adjoint les services en échange d'une rémunération. Ses prestations doivent soutenir son business : cela peut aller d'un apport de conseil, de coaching, à l'ouverture d'un carnet d'adresses, et autres entremises, en fonction du pedigree professionnel de ce conseiller. C'est quelqu'un qui est proche du pouvoir et qui intervient au plus haut niveau stratégique d'une organisation.

Sa position et son expérience lui donnent une forme d'influence, parfois d'ascendant sur son client, qui lui accorde sa confiance et lui donne accès à un niveau d'information confidentiel pour mener à bien le mandat qu'il lui confie. Or comment se fait-il qu'il soit en lien actif avec des fournisseurs alors que son rôle est de se borner, sauf mandat spécifique, à conseiller son mandant ? Et surtout, comment se fait-il que ce dernier ne soit pas au courant de ces relations directes ?

Le **mobile de la manœuvre** réside dans le statut même de ce conseiller, dans le niveau d'information élevé dont il dispose sur le client, et aussi dans l'établissement de liens financiers avec ces fournisseurs : en l'occurrence un versement répété de commissions de leur part et à son seul bénéfice. Une fois le mobile éclairci, il restait à caractériser l'entente. En effet, il n'était **pas question d'accuser les fournisseurs si ceux-ci n'entretenaient pas de relations entre eux et n'agissaient pas réellement de concert au détriment de notre client.**

Or la relation entre notre client et ses fournisseurs est ancienne. Elle porte sur des flux d'affaires significatifs, génère des emplois et une production haut de gamme. Nous sommes dans le secteur du luxe où des PME très spécialisées, artisanales et parfois dépositaires d'un savoir-faire ancestral, sont intimement connectées au sein de filières d'excellence : **s'il y a un incontestable « effet de place », il y a aussi un risque de place corrélatif à toute accusation qui s'avérerait infondée. Notre client aurait risqué gros en termes de réputation, s'il s'était laissé aller à accuser sans fondement.**

C'est ce facteur de risque qui amènera Vici Agency à opérer un contrôle global avant de fournir sa réponse à son client. Contrôle qui clôturera finalement l'hypothèse de l'entente. En effet le Senior Advisor a bel et bien **opéré de son propre chef et à seule fin d'enrichissement personnel,** en monnayant sa position et les informations en sa possession, **auprès de chacun des fournisseurs pris isolément.**

3.2. CAS CLIENTS

CAS #3 - « CASH INVESTIGATION »

LES FAITS

Notre client est une société cotée en Bourse. Un jour, son directeur financier lui donne son congé sans l'avoir prévenu, ceci juste avant la publication des résultats annuels de son employeur. **Compte tenu des enjeux et de sa situation financière, notre client souhaite savoir s'il doit s'inquiéter de ce départ soudain et quelles pourraient en être les conséquences.**

Nos enquêteurs lancent une investigation complète sur cet individu. Le recours à des **outils de recherches web avancés** permet de découvrir qu'il utilise certains réseaux sociaux sous couvert d'activités à caractère commercial dans le secteur immobilier. Un **secteur sans lien apparent avec celui de notre client.**

Des recherches accentuées sur ces activités immobilières amènent notre équipe à découvrir que des biens sont effectivement loués, et des loyers réellement encaissés par l'ancien directeur financier. Fait troublant cependant : il n'y a **aucun vrai locataire derrière.** Soit les noms figurant sur les contrats de bail indiquent des personnes décédées, soit il s'agit de personnes ayant fait l'objet d'une expulsion du pays d'exécution desdits contrats. Nous sommes en présence de faux contrats de bail mais avec un réel encaissement de loyers. Mais pourquoi ?

Nos consultants décident de **concentrer leurs recherches sur ces sommes d'argent.** Quelle peut bien en être la provenance ? Il s'agit en réalité de sommes réglées par une entreprise chinoise. Des recherches complémentaires établissent que cette entreprise est connue pour être active en matière de fusions-acquisitions ciblées.

À ce stade des investigations, nos experts comprennent que ces « loyers » sont en réalité **des commissions payées par ce commanditaire au directeur financier de notre client, afin de disposer d'informations privilégiées sur son entreprise,** qui s'avère être sa cible en vue d'une opération prochaine. Opération qui ne serait rien d'autre qu'une OPA inamicale lancée par ce groupe chinois, sur la base d'un cours d'actions qui aurait chuté une fois annoncée la démission du directeur financier. **Le mobile de la collaboration frauduleuse est enfin établi.**

L'intervention de Vici dénouera les fils d'une **opération d'infiltration par une entité étrangère et prédatrice, prenant appui sur la duplicité humaine au sein d'une entreprise figurant dans son agenda stratégique** (neutralisation d'un concurrent dans un secteur jugé prioritaire, acquisition à bas prix d'une technologie clé, etc.).

LE DÉCRYPTAGE

Il s'agit ici d'un véritable cas d'école, sans doute l'un des plus intéressants et des plus complexes qui aient été résolus par nos équipes.

Précisons tout d'abord que notre client opère **dans un environnement coté.** Les processus d'information du public et des investisseurs y sont très réglementés, et l'activité des entreprises inscrites est fortement scrutée par les analystes financiers. Spécialisés et très fins connaisseurs de leur secteur, l'opinion de ces analystes est autant respectée que redoutée. Très au fait de ce qui se passe, ils bénéficient d'un benchmark en temps réel des meilleures pratiques des acteurs de la filière qu'ils surveillent, et ils peuvent servir de caisse de résonance à la communication d'une information ou à un événement particulier survenu dans une entreprise.

Résonance qui se traduira par un infléchissement à la hausse ou à la baisse du cours de la société concernée, surtout si les interprétations de plusieurs analystes reconnus vont dans le sens d'un consensus. Et **dans ce contexte, la publication des résultats annuels au marché est un véritable *momentum.***

Si tout événement en marge de ce moment particulier est sujet à interprétation, alors que dire de la décision totalement inattendue du DAF de notre client de démissionner… la veille de la communication des résultats ? **Le cœur de l'intrigue se noue ici : comment interpréter le choix de la date de cette démission ?** Faut-il y voir un acte de défiance ? Une forme de lancement d'alerte ? Le fait de ne pas assumer la réalité des résultats ? Le fait de vouloir attirer l'attention sur la sincérité des comptes ? Etc. Toutes les interprétations sont permises mais en l'espèce, **il y a de quoi rompre la confiance des investisseurs dans le titre** et voir sa valeur temporairement compromise.

Quoi qu'il en soit, l'enquête démarre en décortiquant les activités du DAF pour trouver des indices. Nos consultants dévoilent des intérêts dans une structure immobilière, sans aucun rapport avec son métier d'origine. Cela aurait pu en rester là, car il arrive que certains dirigeants à fort patrimoine personnel créent une SCI ou une structure foncière pour gérer les biens immobiliers dans lesquels ils ont décidé d'investir et les loyers qu'ils génèrent.

Cependant, **trois éléments vont interpeller :**

- **l'absence de vrais locataires,** puisqu'il s'agit de personnes décédées ou expulsées du territoire, et le fait que les contrats de bail puissent être de complaisance ;
- **l'encaissement par le directeur financier de sommes d'argent,** ce qui, compte tenu du premier point, caractériserait une fraude ;
- enfin, **le règlement de ces sommes par une société chinoise,** qui n'a rien d'un locataire mais est plutôt connue, après investigations, pour se montrer active sur le terrain de fusions-acquisitions ciblées.

Les **cas de prédation économique** de la part d'entreprises chinoises se multipliant et se sophistiquant, en France comme d'ailleurs dans d'autres pays, il convient de rester très vigilant à leurs menées sur notre territoire.

Or l'analyse établira que les sommes versées par l'entrepreneur chinois sont en réalité des commissions venant rétribuer, d'une part une information économique de première main fournie par le directeur financier, et d'autre part sa promesse de démissionner la veille de la publication des résultats annuels de son employeur. **Les loyers ne sont ainsi qu'un habillage frauduleux**.

La démission survient comme prévu. Elle stupéfie le PDG et **produit les effets escomptés.** Le cours de Bourse dévisse et permet peu après à cette même entreprise chinoise d'envisager le lancement d'une OPA inamicale. Avec un cours de Bourse très favorable, l'opération se serait faite à un prix d'achat potentiellement bien inférieur à la valeur de marché. Fort heureusement, elle n'aboutira pas.

On sait pourtant que les OPA inamicales sont monnaie courante, notamment dans les secteurs en consolidation. Mais il y a fort à parier que **cette entreprise représentait un enjeu stratégique pour l'assaillant :** besoin de tuer un concurrent dans un secteur jugé prioritaire, besoin d'acquérir une technologie clé à un moment où elle n'est pas encore trop chère, etc.

Ce cas est d'une collaboration frauduleuse ayant permis l'infiltration d'une cible jugée prioritaire par une entité étrangère à des fins de prédation économique. **Si la manœuvre est machiavélique et repose sur un enchaînement de séquences bien huilé, elle n'a pu être tentée qu'en s'appuyant sur la duplicité humaine.**

Or **la corruption est un risque avéré pour nos entreprises :** loin des clichés des fonctionnaires corrompus dans les pays en développement, des cadres bien payés et exerçant de hautes responsabilités peuvent être tentés, à tout moment, de céder aux approches de prédateurs. **Ceux-ci disposent de moyens financiers sans commune mesure avec les préoccupations patrimoniales d'un individu, fût-il gourmand.**

C'est une leçon à méditer et il existe en réalité assez peu de moyens de détection, si ce n'est de **rester vigilant à tout élément qui pourrait trahir un changement de train de vie ou un niveau d'endettement excessif** chez des cadres exposés et ayant accès à certaines informations critiques de votre organisation.

L'ENTREPRISE
SON PATRIMOINE
SES INTÉRÊTS

RENSEIGNER

ETUDE 360° DES ACTEURS DU MARCHÉ
Concurrence, partenaires, clients et fournisseurs

ENQUÊTES DE MORALITÉ
Due Diligence, KYC, compliance

APPUI AUX CAMPAGNES MARKETING
Tracking de l'expérience utilisateur

ENQUÊTES D'INVESTIGATION
Assistance à la création de dossiers juridiques, contentieux

LISTINGS ET MAPPINGS QUALIFIÉS
Dans le monde entier et dans tous les secteurs économiques

AUDIT DE LA SOLIDITÉ ÉCONOMIQUE
Sécurité informatique, solvabilité économique, évolution commerciale

PROTÉGER

FAKE NEWS
Veille de réputation, de fake news et des conséquences sur vos intérêts

PROTECTION DE MARQUES
Veille contre les plagiats et les contrefaçons

CYBER-ATTAQUES
Protection et tests de sécurité

INFLUENCER

LÉGITIMATION DE MARQUES
Valorisation de votre marque et de vos produits au sein de publics-cibles

DÉVELOPPEMENT DE LA POPULARITÉ
Optimisation de référencement, hausse de popularité, augmentation du potentiel de trafic sur le web

IDENTIFICATION DE PROSPECTS
Génération de leads qualifiés, tracking digital et expériences utilisateurs

COMMUNITY MANAGEMENT
Création et gestion de communautés spécifiques, valorisation de votre marque et de vos produits

Pourquoi Vici Agency ?

UN **SAVOIR-FAIRE UNIQUE** DANS LA COLLECTE MASSIVE, L'ANALYSE ET L'EXPLOITATION DE DONNÉES ;

UNE **INNOVATION 100% PROPRIÉTAIRE** ;

UNE **TECHNOLOGIE UNIQUE** À L'ORIGINE D'OUTILS PERFORMANTS ;

UNE TRAÇABILITÉ ET UNE **INTÉGRITÉ DES DONNÉES CLIENT** ;

UN RENSEIGNEMENT EN **OSINT** ET EN **HUMINT** ;

DES **PROFESSIONNELS HAUTEMENT QUALIFIÉS** (ENTREPRENEURS, CADRES MILITAIRES, CHERCHEURS EN NEUROSCIENCES, EXPERTS EN PROGRAMMATION INFORMATIQUE, CONSEILS EN RELATIONS PUBLIQUES...) ;

DES SYNERGIES MÉTIER (NEUROSCIENCES + INFORMATIQUE + STRATÉGIE) QUI **DÉCUPLENT NOS CAPACITÉS D'INVESTIGATION ;**

INDÉPENDANCE - DISCRÉTION - EFFICACITÉ ;

UNE **CONFIDENTIALITÉ** ET UNE PROTECTION GARANTIES ;

UNE CAPACITÉ D'INTERVENTION DANS LA **PLUPART DES LANGUES EUROPÉENNES.**

POUR CONCLURE

La guerre est la seule véritable école du chirurgien.

NAPOLÉON BONAPARTE

Ce livre, qui est aussi notre manifeste, est là pour vous aider à faire le point sur un certain nombre de risques et de menaces pesant sur vos activités.

Mais ce « nouveau monde », que nous avons essayé de vous dépeindre par différents phénomènes et facteurs, vous réserve tout autant de bonnes nouvelles et de clés de réussite potentielles.

À condition de vous maintenir en veille et de faire évoluer votre état d'esprit.

Le parcours de Daniel Adrien Donnet-Monay en témoigne. Nous l'avons sommairement présenté pour illustrer certaines des caractéristiques et des attitudes – la résilience en tête – dorénavant indispensables pour avancer.

Non pas pour rester sidéré ou stupéfait, mais pour faire que des séquences brutales et déstabilisantes s'avèrent des opportunités et autant d'occasions de croissance personnelle.

Car il y en aura, immanquablement !

Bien sûr, nous avons longuement insisté sur les conduites défensives comme offensives à mener en cas d'attaque ou de déstabilisation. Nos cas clients en témoignent.

Pour autant, ceci n'est qu'une première étape. Car nous avons foi tout autant et sans doute davantage encore dans l'éducation, dans l'autonomisation et dans les vertus des conduites préventives.

À l'image de nombreux patrons qui commettent un jour un faux pas pouvant leur coûter leur entreprise, voire

leur patrimoine personnel, Daniel aurait sans doute aimé bénéficier des informations et surtout des moyens d'analyse suffisants pour éviter de s'engager dans certains projets. Si certaines erreurs lui ont permis d'ancrer de nouvelles convictions que ce livre donne l'occasion de vous partager aujourd'hui, elles lui auront coûté cher. Et pas seulement sur un plan financier. Mais il aura appris. Tellement appris !

L'heure est à la « datafication » du monde, qu'on le veuille ou non. Un nombre exponentiel de phénomènes et de comportements peuvent être transcrits en données, et être rendus sans cesse plus intelligibles et prévisibles. Le pouvoir appartiendra à ceux qui maîtriseront le cycle complet de la data (collecte, traitement, diffusion, exploitation…), qu'ils en soient propriétaires grâce à leurs moyens financiers et technologiques, ou qu'ils puissent a minima louer ces capacités à des tiers de confiance.

Vici Agency se positionne précisément en tiers de confiance et accompagne les entreprises dans leurs choix comme dans leurs renoncements nécessaires. Mais nous pensons aussi à demain et voulons, par les moyens technologiques et méthodologiques de l'agence, aider les entrepreneurs en herbe. Non pas pour qu'ils lèvent des fonds auxquels l'inexpérience de leurs fondateurs ferait courir un risque. Plutôt en leur procurant une information de haut niveau afin de valider le potentiel de marché de leur concept, et aller plus vite à la rencontre de leur croissance.

Et dans ce domaine, data predictor et l'expérience de nos consultants offrent des réponses particulièrement éclairantes, voire inspirantes.

Vous êtes convaincu.e de devoir mettre en application une ou plusieurs de nos recommandations ?

Alors ne perdez plus de temps
et demandez votre RDV de diagnostic gratuit
+41 213 11 29 42
daniel@vici-agency.com

LES DIX COMMANDEMENTS VICI

1 **N'AYEZ PAS PEUR DE RAISONNER « LARGE » :** Le monde est votre jardin. Alors allez chercher la croissance là où elle se trouve et prenez en compte les facteurs géopolitiques, même s'ils vous semblent lointains. Cherchez à comprendre comment ils peuvent vous aider.

2 **FAITES BON ACCUEIL À VOTRE BON SENS ET À VOTRE INTUITION :** Ils vous feront gagner un temps précieux.

3 **INVESTISSEZ DANS VOTRE CAPACITÉ D'INFLUENCE :** Qu'elle soit personnelle ou corporate, elle nécessite des moyens aujourd'hui accessibles à une PME, grâce à la digitalisation.

4 **N'AYEZ PAS PEUR DU CONFLIT :** Étant donné la marche du monde et la lutte pour les ressources, les mouvements de concentration à venir vont privilégier les réflexes de prédation.

5 **GÉREZ VOTRE EGO :** Faites-en un facteur de rebond face aux attaques et de saine agressivité pour accomplir vos objectifs, et ne lui confiez jamais le pilotage automatique.

6 **RESTEZ CONNECTÉ À VOTRE FINALITÉ :** Une certaine dose de transcendance et d'utilité ne fait de mal à personne et vous aide à remettre votre œuvre en accord avec vos valeurs.

7 **N'AYEZ PAS PEUR DE DOUTER :** Dans un monde hautement complexifié, le doute fait partie du jeu. N'ajoutez pas de culpabilité au fait de ne pas savoir, mais acceptez cette donnée sans jugement.

8 **NE SOYEZ JAMAIS DUPE :** Ni de vos concurrents, ni de vos partenaires, ni surtout de vos collaborateurs. La duplicité humaine est un facteur de corruption trop souvent insoupçonné.

9 **INFORMEZ-VOUS TOUJOURS AVANT DE DÉCIDER ET D'AGIR :** On n'est jamais assez informé et, dans certaines circonstances, ne pas l'être assez peut vous coûter très cher.

10 **ENFIN ET SURTOUT SOYEZ RÉ-SI-LIENTS !** C'est votre assurance-survie mais aussi votre assurance-plaisir, à faire ce que vous faites au service de votre mission.

ANNEXE 1

Cybersécurité : Les chiffres clés dans le monde (FIC 2019)

LE FIC 2019 s'est déroulé les 22 et 23 février 2019 à Lille Grand Palais. Le Forum International de la Cybersécurité rassemble les professionnels internationaux du secteur.

Voici une photographie du marché datée de janvier 2019 proposée par Hexatrust (Jean-Noël de Galzain, Président du groupement HEXATRUST) et Systematic (Jean-Pierre Tual, Président du Groupe Thématique Confiance Numérique & Sécurité).

Marché mondial

Selon Gartner, le marché mondial de la cybersécurité a cru de 3.1 Mds € en 2004 à 67 Mds € en 2015 et devrait atteindre 152 Mds € en 2020. Le déploiement généralisé des mobiles, du Cloud, des réseaux sociaux et du Business Intelligence dans les marchés verticaux sont les moteurs principaux du développement de nouveaux services et technologies de cybersécurité.

Un exemple caractéristique en est le marché de la cybersécurité automobile qui, selon IHS2, va croître de manière quasi-exponentielle pour atteindre la valeur de 759 millions de dollars en 2023 avec des croissances variables selon les segments concernés.

Les constructeurs et équipementiers automobiles prennent désormais au sérieux les enjeux de cybersécurité et examinent avec intérêt les différentes manières de développer et d'implémenter des solutions de cybersécurité. Le partenariat mondial pluriannuel entre RENAULT-NISSAN et MICROSOFT autour de la voiture connectée qui a été annoncé en septembre 2016 confirme cette situation.

Les objets connectés représentent une autre tendance structurante. D'une part l'explosion des objets connectés: – 3,5 milliards en 2016, potentiellement 50 milliards d'objets en 2020 – augmente d'autant les enjeux liés à la sécurité de ces derniers.

D'autre part, les objets connectés intègrent et structurent progressivement nos sociétés modernes, que ce soit dans le domaine civil, industriel, ou militaire, ce qui rend la sécurité de ces derniers impérative. Le marché de la sécurité des objets connectés devrait atteindre 36,95 Mds $ en 2021 selon Markets and Markets.

Marchés nationaux

Le marché US représente à lui seul plus de 40 % du marché mondial, l'Europe environ 25 %, c'est-à-dire 17 Mds €, sans inclure la Russie.

Les taux de croissance les plus élevés sont ceux de l'Inde et de la Chine qui témoignent d'un niveau de maturité encore faible en matière de cybersécurité et d'un potentiel de marché important pour la filière industrielle. L'Allemagne, le Royaume-Uni et la France sont les trois premiers marchés de l'Union Européenne (UE). Avec une croissance annuelle moyenne de plus de 6 %, le marché de l'UE dépassera les 22 Mds € en 2020.

Menaces et impacts de la cybercriminalité

En matière de cybercriminalité, Cybersecurity Ventures prévoit un doublement des coûts mondiaux d'impacts de 2015 à 2021, soit de 3 trillions € à 6 trillions €, incluant la corruption et la destruction de données, l'argent volé, la productivité perdue, le vol de propriété intellectuelle, le vol de données personnelles et financières, le détournement, la fraude, la perturbation du cours des affaires suite aux attaques, les analyses post-attaques, la restauration des données et des systèmes attaqués et les atteintes à l'image.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) note dans son rapport d'activité 2016 la forte croissance de la cybercriminalité : 4 000 signalements d'attaques ont été reçus en 2015, soit 50 % de plus qu'en 2014. À noter que plus de 60 % des attaques visent la défiguration de sites Internet et plus de 10 % la compromission de systèmes d'information.

Sur les 228 industriels interrogés à la fin de l'année 2015 par "L'Usine Nouvelle", près de la moitié reconnaissait avoir été victime d'une cyberattaque causant un impact financier (pour 34 %) et écornant l'image de l'entreprise (pour 19 %).

La même enquête fait apparaître que la sécurisation des environnements industriels reste une « course d'obstacles » en raison des nombreux freins rencontrés (comme le manque de budget déployé pour la cybersécurité, le manque de prise de conscience du risque, l'absence de concertation entre les services concernés ...).

Enjeux de la cybersécurité – Vision stratégique

Les enjeux de la cybersécurité peuvent être vus sous plusieurs aspects :

du point de vue de la souveraineté, le manque évident de frontières dans le cyberespace rend les Etats de plus en plus vulnérables face à l'apparition des nouvelles menaces informatiques. De ce point de vue, la cybersécurité est appelée à jouer un rôle de plus en plus fondamental dans la protection des ressources stratégiques de la nation, y compris vis-à-vis d'attaques menées par des acteurs gouvernementaux (cf. par exemple les déclarations du président Obama, en marge du sommet du G20 tenu à Hangzhou (Chine) en septembre 2016, plaidant pour un code de « bonnes pratiques » entre Etats plutôt que pour une course aux « cyber-armements »).

du point de vue économique, les enjeux de la cybersécurité sont également fondamentaux puisque de plus en plus les cyberattaques informatiques sont massives et menées par des groupes extrêmement bien organisés et compétents. Les conséquences de telles attaques peuvent être particulièrement critiques au niveau financier (exemple de la récente attaque du réseau interbancaire SWIFT entre avril et mai 2016, ayant conduit à des détournements frauduleux de plusieurs dizaines de millions de dollars US, ou encore de l'attaque de type DDoS du 21 octobre 2016 contre les serveurs Dyn et ayant paralysé pendant plusieurs heures une partie du réseau Internet aux US et gravement perturbé les activités économiques touchées).

du point de vue industriel, la cybersécurité constitue un enjeu majeur à la fois en matière de protection du patrimoine des entreprises (et particulièrement de nos PME, encore trop peu sensibilisées à la protection de leur système d'information) comme en matière de création de valeur, aussi bien en termes de revenus que d'emplois à très forte valeur ajoutée, portée par de grands groupes capables d'influencer les standards et par les nombreuses PME innovantes du secteur.

en termes sociaux ou sociétaux enfin, les enjeux associés à la cybersécurité imposent de manière essentielle la recherche des meilleurs compromis entre la protection de la vie privée de tout un chacun et la nécessité de vivre dans des sociétés sûres où le concept de confiance numérique parvient à s'imposer face à une vision beaucoup plus négative du type « big brother is watching you ». De ce point de vue, de nouvelles approches holistiques sont requises, basées sur une meilleure intégration des technologies, de la règlementation et des sciences humaines et sociales, conduisant à des politiques de sécurité contextualisées, fluides et efficaces mettant les utilisateurs (cybercitoyen, consommateur ou acteur) au centre des préoccupations.

ANNEXE 2

Cybersécurité : Les dates clés de la politique française

1943 : Création de la Direction technique du Chiffre à Alger, devenue en 2001 la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) ;

2000 : Interconnexion généralisée des réseaux faisant passer la France du chiffrement au cyberespace ;

2006 : Publication à la demande du Premier Ministre d'un Rapport par le Député Pierre Lasbordes « La sécurité des systèmes d'information : un enjeu majeur pour la France » ;

2008 : Rapport du Sénateur R. Romani sur la cyberdéfense, premier document officiel suite au séisme provoqué par les cyberattaques contre l'état Estonien l'année précédente ;

Juin 2008 : Livre blanc sur la Défense Nationale définissant le cyberespace, et proposant un cadre d'emploi à des outils spécialisés ainsi qu'une doctrine d'emploi pour des capacités de lutte informatique offensive ;

Juillet 2009 : Création par décret de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et nomination d'un officier général de la cyberdéfense ou « OG cyber » ;

Février 2011 : Publication d'un document de présentation de la stratégie de la France en matière de « Défense et sécurité des systèmes d'information » ;

Automne 2011 : Développement d'une doctrine militaire de cyberdéfense sous la direction du Centre Interarmées de Concept, Doctrines et Expérimentations (CICDE) ;

Janvier 2012 : Publication d'une doctrine interarmées de cyberdéfense ;

2012 : Rapport du Sénateur Jean-Marie Bockel, proposant de « faire de la cyberdéfense une priorité nationale », et au passage de rester vigilants quant à certaines entreprises chinoises (Huawei et ZTE) ;

2013 : Livre blanc sur la défense et la sécurité nationale, décrivant notamment une chaîne opérationnelle de cyberdéfense « centralisée à partir du centre de planification et de conduite des opérations de l'état-major des armées » ;

Juin 2013 : Discours de Jean-Yves le Drian, dont la parole politique appuiera les conclusions du livre blanc paru la même année, et qui viendra en détailler certains aspects ;

2013 : Adoption de la Loi de Programmation Militaire 2014-2019, apportant des précisions en matière de cyberdéfense et sécurité. C'est surtout son article 20 qui fera polémique, en autorisant un grand nombre d'administrations à se faire communiquer par tous les opérateurs, les documents qu'ils auraient transmis ou stockés, sous réserve de la recherche de renseignements intéressant par exemple la sécurité nationale, la prévention du terrorisme, la criminalité, la délinquance.

ANNEXE 3

Cybersécurité : repères infographiques sur les pratiques des entreprises françaises

LES CYBERATTAQUES ET LEUR IMPACT DE PLUS EN PLUS DÉCISIF

41 % des entreprises interrogées de 0 à 9 salariés et **44 %** des entreprises de 9 à 49 salariés ont déjà subi une ou plusieurs attaques ou tentatives d'attaques informatiques : hameçonnage (**24 %**) ; malware (**20 %**) ; rançongiciel (**16 %**) ; fraude au président (**6 %**)

Si le nombre des cyber-attaques constatées tend à se stabiliser, huit entreprises sur dix continuent d'être impactées, avec pour **59 %** d'entre elles des conséquences sur le business (arrêt de la production, indisponibilité significative du site internet, perte de chiffre d'affaire...) soit 10 points d'augmentation par rapport à l'année dernière.

Le Phishing est le mode d'attaque le plus fréquent, **73 %** en ont été victimes, étonnamment l'arnaque au Président que l'on croyait en extinction touche encore une entreprise sur deux en 2018. Le Ransomware est au troisième rang avec **44 %** d'entreprises touchées, suivi par le social engineering (**40 %**).

Le Shadow IT est le risque cyber le plus répandu, mentionné par **64 %** des répondants comme étant une menace à traiter.

En effet, l'usage notoire des applications et services cloud le plus souvent gratuits, s'est banalisé et échappe au contrôle de la DSI. Cela accroît significativement les risques, comme les fuites de données via les outils de transfert d'information ou de partage de fichiers volumineux. D'autant que l'utilisation même anecdotique d'un service Cloud, peut suffire à compromettre l'intégrité et la sécurité des données de l'entreprise.

LES PROTECTIONS MISES EN PLACE

36 % des entreprises changent les mots de passe de leurs ordinateurs de bureau au moins une fois tous les 6 mois. **33 %** des entreprises interrogées changent leurs mots de passe de leurs ordinateurs de bureau peu régulièrement, soit entre tous les 6 et 12 mois.

39 % des entreprises disposent d'une triple protection (antivirus, firewall, solution, anti-spam) pour leurs ordinateurs de bureau.
La solution anti-spam demeure peu utilisée par les entreprises. **55 %** des entreprises interrogées en disposent pour leurs ordinateurs de bureau et **42 %** pour leur réseau.

LA REPRISE D'ACTIVITÉ POST-ATTAQUE

98 % des entreprises disposent d'au moins un outil de sauvegarde.

17 % des entreprises seulement sont assurées contre les attaques informatiques.

Le principal outil de sauvegarde utilisé par les entreprises est le support externe (clé USB, disque dur externe...) à **68 %,** suite d'une solution cloud (**49 %**) et du serveur de stockage interne (**45 %**).

CYBERSÉCURITÉ, SALARIÉS ET RÉFÉRENT INFORMATIQUE

71 % des entreprises de 0 à 9 salariés et **85 %** des entreprises de 10 à 49 salariés sensibilisent leurs collaborateurs aux risques informatiques, dont **44 %** au moins tous les ans.

47 % des entreprises de 0 à 9 salariés et **61 %** des entreprises de 10 à 49 salariés ont un référent informatique (salarié ou prestataire).

CLOUD ET IOT

98 % des entreprises estiment que la transformation numérique a une incidence sur la sécurité des systèmes d'information des données. En tête des enjeux : le recours massif au Cloud, utilisé par **87 %** des entreprises, dont **52 %** dans des clouds publics. Un mode de stockage qui pose des problèmes de non-maîtrise ; que ce soit par rapport à l'accès aux données de l'entreprise par les hébergeurs (via les administrateurs ou autres) ou par rapport à la chaîne de sous-traitance pratiquée par le fournisseur. Pour **89 %** des RSSI interrogés ces enjeux impliquent le recours à des outils de sécurisation supplémentaires à ceux proposés par le prestataire.

Dans un même temps, les objets connectés se sont progressivement installés dans le paysage et la course à l'innovation ne va pas de pair avec l'implémentation de la sécurité, faisant apparaître de nouvelles typologies de menaces. Les nombreux cas de piratage témoignent d'une progression de la cybercriminalité via les objets connectés. Pour l'IoT, la caractéristique la plus marquante reste les failles de sécurité présentes dans ces équipements. On notera souvent l'absence de chiffrement pouvant porter atteinte à la confidentialité, ou l'absence d'authentification avec des accès non protégés

FACE AUX CYBER-RISQUES, UNE CYBER-RÉSILIENCE À DÉVELOPPER

Pour contrer ces cyber-risques, les RSSI déploient une panoplie de solutions techniques, globalement jugées adaptées à leurs besoins (**75 %**), même si des progrès restent à faire dans leur adaptation à la transformation numérique. À noter l'enjeu de l'IA : **56 %** des répondants ont mis en place des solutions basées sur l'IA ou envisagent de le faire ; toutefois **55 %** estiment que l'IA ne se substituera pas à l'expertise humaine en matière de sécurité.

Pour autant, les entreprises françaises sont-elles en capacité de défendre leurs infrastructures ? Les RSSI se disent moins confiants que l'année dernière quant à la capacité de leur entreprise à faire face aux cyber-risques. **51 %** sont confiants, soit une baisse de 12 points ; et moins d'un sur deux considère que son entreprise est préparée à gérer une cyber-attaque de grande ampleur. **50 %** ont désormais souscrit à une cyber-assurance, soit une hausse de 10 points, mais seule une entreprise sur dix a mis en place un véritable programme de cyber-résilience. Si ce n'est pas en projet pour **21 %**, c'est une tendance avec **33 %** en cours et **34 %** qui l'envisagent.

LES ENJEUX D'AVENIR

D'après les RSSI, l'enjeu principal pour l'avenir de la cybersécurité est celui de la formation et de la sensibilisation des utilisateurs (**61 %**). Les usages des salariés apportent en effet leur lot de risques, notamment via le shadow IT. Et si les salariés sont sensibilisés, ils restent peu impliqués en ne suivant pas forcément les recommandations. Un important travail de pédagogie reste à faire.

La gouvernance de la cybersécurité doit également être placée au bon niveau pour **60 %** des RSSI. Malgré un impact positif de la mise en conformité RGPD sur la gouvernance des entreprises (**59 %**), la confiance en la capacité des COMEX à prendre en compte les enjeux de la cybersécurité est très inégale en fonction des secteurs d'activité.

En France comme dans le reste du monde, la pénurie de ressources humaines en cybersécurité est un défi majeur pour les organisations, constatée par **91 %** des RSSI... À l'heure où **50 %** d'entre eux prévoient d'augmenter les effectifs alloués à la protection contre les cyber-risques.

Sources :
Enquête 2019 de la CPME sur les risques numériques pour les entreprises
4ème édition du Baromètre annuel Cesin et Opinion Way de la Sécurité de l'Information et du Numérique

RESSOURCES

Organismes publics
ANSSI : http://www.ssi.gouv.fr/
SISSE : sisse.entreprises.gouv.fr

Rapports et documentation publique
Pour découvrir les principaux acteurs de l'IE en Île-de-France : http://idf.direccte.gouv.fr/sites/idf.direccte.gouv.fr/IMG/pdf/depliant_intelligence_economique_vok_web2.pdf

Rapport Martre :
https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/rapport-martre.pdf

Rapport Carayon :
https://sisse.entreprises.gouv.fr/sites/sisse.entreprises.gouv.fr/files/files/outils/rapports/a-armes-egales.pdf

Rapport Romani :
https://www.senat.fr/rap/r07-449/r07-4491.pdf

Rapport Bockel :
https://www.senat.fr/rap/r11-681/r11-681_mono.html

Rapport d'activité 2018 de l'ANSSI :
https://www.ssi.gouv.fr/uploads/2019/04/anssi_rapport_annuel_2018.pdf

Pour aller plus loin sur les rapports :
https://sisse.entreprises.gouv.fr/fr/documentation

Associations professionnelles
www.scip.org
www.synfie.fr
www.cesin.fr

AFDIE
D'autres d'associations sur : http://acrie.com/associations.htm

Formations
www.ege.fr
www.ihedn.fr
https://www.union-ihedn.org/
http://www.cyberstrategie.org/
https://inhesj.fr/sites/default/files/inhesj_files/telechargements/presentation_ise_2018-2019.pdf
http://formations.univ-poitiers.fr/fr/index/master-XB/master-XB/master-intelligence-economique-JBI326XJ.html

Sites, blogs, portails et annuaires spécialisés
Portail-ie.fr
www.ie-lobbying.info

https://fr.wikipedia.org/wiki/Intelligence_economique
www.veillemag.com
www.archimag.com
infoguerre.fr
http://jacques.breillat.fr/

Groupes et communautés LinkedIn (> 1 000 membres)
Cesin : https://www.linkedin.com/company/cesin-club/
Intelligence économique pour PME : https://www.linkedin.com/groups/1789456/
Intelligence économique : https://www.linkedin.com/groups/80707/
Revue internationale d'IE : https://www.linkedin.com/groups/4722593/
AEGE – EGE (École de guerre économique) : https://www.linkedin.com/groups/988187/

Éditeurs spécialisés
https://www.vapress.fr/
Collections : Cybersécurité et risques numériques, Guerre de l'information, Indiscipliné

www.economica.fr
Collection cyberstratégie

Guides et publications diverses
Intelligence économique – références et notions clés :
https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/d2ie_reference_et_notion-cle-juillet.pdf

Le Guide du routard de l'Intelligence économique :
https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/routard-guide-intelligence-economique.pdf

Guide de l'Intelligence économique pour la recherche :
https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/guide-intelligence-economique.pdf

Manifeste Medef pour la promotion de l'Intelligence économique :
https://www.innover-en-france.com/file/91088/

Enquête 2019 de la CPME sur les risques numériques pour les entreprises :
https://www.francenum.gouv.fr/comprendre-le-numerique/cybersecurite-et-pme-en-2019-16-chiffres-cles-sur-la-securite-numerique-des

Chiffres clés de la cybersécurité par le Forum International de la Cybersécurité :
https://misskonfidentielle.com/2019/01/26/fic-2019-les-chiffres-cles-de-la-cybersecurite/

4e édition du Baromètre annuel Cesin et OpinionWay de la sécurité de l'information et du numérique :
https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html

VICI
SWISS COMPETITIVE
INTELLIGENCE

Active dans toute l'Europe, Vici Agency est une agence suisse de renseignement ayant installé son siège à Lausanne.

Vici fédère des professionnels hautement qualifiés issus de domaines complémentaires :

> des entrepreneurs aguerris ;

> des cadres militaires suisses (dont un ancien général de corps d'armée) ;

> des chercheurs en neurosciences ;

> des experts en programmation informatique ;

> des professionnels de la communication (relations publiques, conseil éditorial et community management).

Nos experts contribuent activement à la croissance de nos clients en collectant massivement des données utiles à leur expansion, en protégeant leurs intérêts, et en influençant leurs marchés de manière proactive.

> **Renseignement** : étude 360° des acteurs du marché, enquêtes de moralité, appui aux campagnes marketing, enquêtes d'investigation, listings et mappings qualifiés, audit de la solidité économique ;

> **Protection** : fake news, protection de marques, cyberattaques ;

> **Influence** : légitimation de marques, développement de popularité, identification de prospects, community management.

Des synergies entre experts en neurosciences, informaticiens et stratèges ont permis à Vici Agency de développer une technologie spécifique, unique sur le marché. Elle est à l'origine de différents outils garantissant sa totale indépendance, une discrétion totale ainsi qu'une très grande efficacité de ses équipes et interventions.

Notre agence développe et exploite ses propres innovations en matière d'intelligence économique afin de garantir la traçabilité et l'intégrité des données de sa clientèle.

Vici garantit un très haut degré de confidentialité et de protection (protection numérique, physique, et légale) dans le traitement de ses données.

Nous traitons des dossiers internationaux, complexes et stratégiques pour le compte de nos clients et partenaires principalement en OSINT et en HUMINT.

Enfin, nous sommes dotés de capacités d'investigation digitale dans les principales langues européennes : anglais, français, allemand, espagnol, russe et langues slaves, italien, portugais, polonais, roumain, bulgare et hongrois.

CONTACT

Retrouvez Vici Agency,
Swiss Competitive Intelligence

À Lausanne
Direction Générale
Avenue de la Gare 17
CH-1003 Lausanne
+41 213 11 29 42
daniel@vici-agency.com

À Barcelone
Oficina de Barcelona
Calle Àvila 48 1 B
E-08005 Barcelona
+34 605 61 29 41
agency@vici-agency.com

Sur le Web :
www.vici-agency.com

Sur LinkedIn :
www.linkedin.com/company/vici-swiss-competitive-intelligence/

NOTES

Ce n'est pas parce que le monde est devenu chaotique, que nous devons le laisser nous surprendre.

De l'individu lambda à la PME et PMI, chacun détient la responsabilité de se faire sa propre idée d'internet et de sa puissance.

L'arrivée des Fake News ayant modifié le paysage social, économique et politique, collecter le renseignement et la donnée est devenu primordial pour rester dans la course.

Fruit d'expériences entrepreneuriales et militaires, ce livre vous permet de comprendre ce qui est de votre ressort, dans votre plus grand intérêt.

VICI SWISS COMPETITIVE INTELLIGENCE