# LES RANCONS

## lors d'attaques informatiques

« – As-tu lu Jean-Jacques Rousseau ?

– Oui.

– Te souviens-tu de ce passage où **il demande à son lecteur ce qu'il ferait au cas où il pourrait s'enrichir en tuant par sa seule volonté un vieux mandarin en Chine, sans bouger de Paris.** »

*Balzac, Le père Goriot*

… Demande à un informaticien ce qu'il ferait au cas où il pourrait s'enrichir en tuant à distance une entreprise, sans bouger de son siège.

… Demande à un informaticien ce qu'il ferait au cas où il pourrait à distance inoculer un poison lentement mortel, puis s'enrichir en vendant l'antidote contre rançon, sans bouger de son siège.

… Demande au vieux mandarin ce qu'il ferait au cas où il pourrait sauver sa vie en achetant l'antidote par paiement de la rançon (accordera-t-il davantage de valeur aux années qui lui restent, qu'à l'argent exigé ? Privilégiera-t-il le refus du dictat ou son acceptation ?).

… Demande au vieux mandarin s'il paierait au cas où il soit assuré pour le remboursement de la rançon exigée.

… Demande à l'informaticien ce qu'il ferait au cas où il apprend que certaines cibles sont assurées pour le paiement de rançon.

Au final, l'intérêt de la collectivité est-il que la victime soit assurée ou non sur le paiement de rançon ? Préalablement, l'intérêt collectif est-il qu'une rançon soit versée ?

**Chaque jour, près de 500 entreprises françaises sont victimes d'un cryptovirus qui chiffre leurs données, accompagné généralement d'une demande de rançon. Quotidiennement 500 dirigeants sont ainsi confrontés au choix, au quasi pari, de payer ou non, sous la menace parfois de voir détruire leur entreprise.**
**Quel comportement adopter ?**


POUR TOUT RENSEIGNEMENT, VOUS POUVEZ CONTACTER L'IRT SYSTEMX

8, avenue de la Vauve
91127 Palaiseau

www.irt-systemx.fr

gilles.desoblin@irt-systemx.fr - Directeur du Programme « Internet de Confiance »
philippe.wolf@irt-systemx.fr et philippe.laurier@irt-systemx.fr


SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE | Accélérateur de la transformation numérique


# LES CYBERATTAQUES

## ET LEURS PRÉJUDICES

### dans les entreprises

Les Rançons
lors d'attaques informatiques

Coût individuel contre coût collectif

**Essor du nombre d'attaques par rançongiciels ≈ 2015**
**Essor de la propension à payer des rançons ≈ 2018**
**Essor du montant des rançons ≈ 2020 ?**

# LES CYBERATTAQUES ET LEURS PRÉJUDICES DANS LES ENTREPRISES

## Les rançons lors d'attaques informatiques

QUANTIFICATION ET QUALIFICATION

**Essor du nombre d'attaques par rançongiciels ≈ 2015**

**Essor de la propension à payer des rançons ≈ 2018**

**Essor du montant des rançons ≈ 2020 ?**

# Sommaire

# PRÉFACE

Le risque cyber est devenu en quelques années un sujet de décideurs d'entreprise. Par nature, la cyber est un milieu d'experts techniques et de « jargon », mais il impacte d'abord les hommes et les femmes, quelles que soient leurs fonctions dans l'entreprise, et a des conséquences financières significatives.

Le manque d'étude de terrain fiable permettant de mieux appréhender son risque cyber est criant en la matière. L'approche par échantillonnage puis recensement de Philippe Laurier, complétée par de multiples entretiens avec des dirigeants d'entreprises victimes, nous fournit un éclairage novateur. Ses résultats, parfois contre intuitifs, conduisent à considérer avec recul nombre de publications anxiogènes et autres statistiques déclaratives. Les modèles, les prescriptions, les recommandations issues de cette étude sont de véritables outils au service des décideurs publics et privés en matière de gestion du risque cyber.

**Stéphane Lenco**
Airbus Chief Information Security Office

**Eric Ravello**
Airbus Security Transformation Officer

# CADRE DE L'ÉTUDE

Le projet EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité) développe une plateforme expérimentale et technique en cybersécurité appelée CHESS (Cybersecurity Hardening Environment for Systems of Systems) qui permet d'évaluer le couplage de technologies de cybersécurité à travers des cas d'usage innovants dans le domaine des SmartGrids, de l'Usine du Futur, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets. CHESS construite avec l'aide de l'Agence nationale de la sécurité des systèmes d'information dans le cadre de la « Nouvelle France industrielle », permet de traiter de la donnée massive, de modéliser et simuler les attaques, de visualiser les menaces, et d'expérimenter et développer des technologies innovantes. Elle offre un environnement ouvert versatile et complet pour répondre aux défis que rencontrent les industriels dans les phases de conception, de modélisation, de simulation et d'expérimentation des innovations futures pour la sécurité du numérique. Elle est labellisée par le Comité de la Filière Industrielle de la Sécurité (CoFIS).

EIC mène également, en complément de ces tâches techniques, une recherche concertée et cohérente dans les domaines économiques et juridiques. Les commanditaires et les financeurs de ces recherches sont, pour Airbus, le Security office, et l'ANSSI. La présente étude se concentre sur le calcul du coût économique d'une attaque cyber et sa compréhension pour une organisation portant sur sa chaîne de valeur en lien avec la problématique de la gestion du risque d'entreprise d'un point de vue financier et le transfert vers le marché du risque résiduel. Cette étude est à mettre en regard des travaux conduits au sein de la seconde tache de recherche qui vise à quantifier financièrement l'exposition cyber d'une organisation du point de vue du Risk Manager qui opère ensuite le transfert d'une partie du

risque vers le marché de l'assurance1. Le calcul du coût économique du risque cyber i.e. du coût d'une attaque cyber pose la question de la quantification. C'est une question difficile à laquelle les analyses techniques du risque cyber n'apportent pas de réponse en termes de finance d'entreprise. La prise en compte de ce risque sous l'angle de la compliance (respect des normes ISO, etc…) a atteint ses limites. La problématique de la traduction du risque technique cyber en termes de finance d'entreprise (actif, passif, comptabilité, coût de la sécurité, retour sur investissement) est aujourd'hui une question ouverte à laquelle il faut rapidement trouver une réponse dans un contexte d'accélération numérique. Ce sujet a fait l'objet d'une étude en 2017 dans le cadre de la seconde tache de recherche pré citée.

L'Industrie 4.0, l'internet des objets, l'entreprise étendue, la digitalisation de l'ensemble des activités sont une opportunité mais provoquent un changement de paradigme dans la compréhension et la connaissance de l'exposition au risque cyber en démultipliant la surface de vulnérabilité de l'organisation… L'ensemble de la chaîne de valeur est affectée.

Un autre facteur déterminant est constitué par l'évolution de la réglementation concernant le risque cyber aux États-Unis et en Europe. Celles-ci imposent de nouvelles responsabilités pour l'entreprise en tant que personne morale, mais aussi, individuellement, pour certains de ses managers vis-à-vis des actions menées au sein de l'organisation et plus généralement, dans le cadre élargi à son écosystème, à sa supply chain, envers ses tiers, ses clients… Aux fins de construire sa stratégie, une organisation publique ou privée, de grande, moyenne ou de petite taille doit pouvoir comprendre en interne son exposition au risque numérique, ainsi que le recommandent les rapports de recherche EIC – transfert du risque et le rapport FERMA EIICA2 publié en juin 2017. Pour prendre ses décisions d'investissements, en toute connaissance de cause, elle a besoin de métriques, d'indicateurs, de seuils d'acceptation etc. Or ces éléments qui valorisent les biens intangibles numériques ne sont pas encore disponibles.

Une enquête de terrain a donc été lancée en juin 2016 dont un premier rapport d'étape publié en 2019 a détaillé les premiers enseignements.

---

1 Philippe Cotelle, Philippe Wolf, Bénédicte Suzan. *Cyber Risk and Insurance Cyber Risk Governance throughout the value chain and its transfer to the Insurance*. [Research Report] IRT SystemX. 2016. hal-02413904

2- http://www.ferma.eu/ferma-eciia-cyber-risk-governance-report

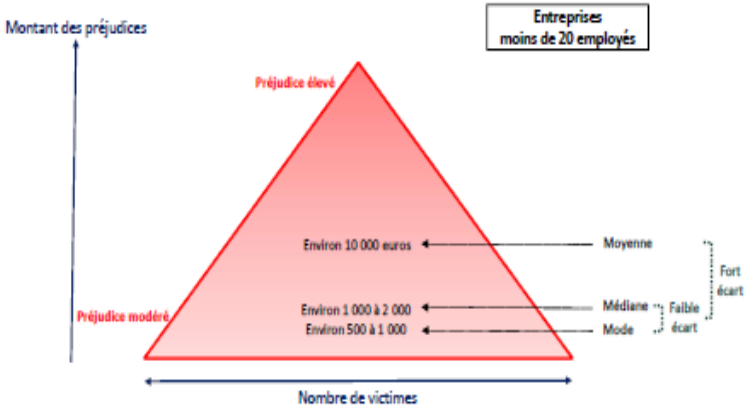
Ce second rapport affine ces enseignements sur les attaques par cryptovirus qui connaissent un fort développement en trois phases :

- Essor du nombre d'attaques par rançongiciels ≈ 2015
- Essor de la propension à payer des rançons ≈ 2018
- Essor du montant des rançons ≈ 2020 ?

Il aborde, en particulier, les questions relatives aux rançons autour du dilemne « coût individuel contre coût collectif ».

# UNE ÉTUDE DE TERRAIN

Une étude de terrain a été menée entre 2015 et 2020 par Philippe Laurier, chercheur à l'IRT SystemX[3] auprès de plus de soixante TPE/PME victimes de cyber attaques (principalement rançongiciels et « fraudes au président »), dans le cadre de son Projet EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité) lancé en coopération avec lancé en coopération avec Airbus -Pascal Andrei, *Chief Security Officier*-. Cette enquête inédite en France, qui est allée au contact d'entreprises victimes, remet en cause les chiffrages habituels, notamment sur le nombre d'attaques antérieurement très sous-estimé, et sur les coûts moyens ou médians quant à eux surestimés car se référant jusqu'à lors préférentiellement aux seules attaques les plus marquantes (voir notre précédent livret « Les cyberattaques et leurs préjudices dans les entreprises », paru en 2018).




Au-delà de ce travail de mesure et de formalisation des préjudices sous toutes leurs formes (matériels ou immatériels, directs ou collatéraux, immédiats ou à long terme …), un objectif est d'aider à repenser les modes de sécurisation au sein des entreprises ou des chaînes logistiques, afin de les mettre en concordance avec cette réalité des menaces observées.

3 L'institut de recherche technologique SystemX installé à Palaiseau a été fondé en 2012 https://www.irt-systemx.fr/

La population ciblée par l'étude s'est constituée d'entreprises de moins de 50 employés, avec pour première surprise une homogénéité forte des résultats recueillis, mais pour seconde surprise des différences énormes avec les observations parallèlement menables sur les grandes entreprises. Au point de devoir isoler ces deux profils très distincts de victimes que sont les grandes et petites entreprises, en vue de mener à bien les travaux statistiques ou d'analyse des comportements.

L'étude de terrain déroulée sur plusieurs années s'est particularisée par l'absence de recours aux traditionnels envois massifs de questionnaires ou autre méthode trop dépendante de réponses rares et difficilement vérifiables, pour privilégier le contact direct par la rencontre avec des victimes, souvent sur site dans leur entreprise.

Cette approche a permis un recueil de témoignages plus fiables, circonstanciés, capables de reconstituer la chronologie des faits. Les chiffrages qui en résultent attestent donc de réalités observées, ou tout au moins observables ; à ce titre, ils sont souvent à considérer comme des minimas qui n'excluent pas quelquefois des niveaux réels plus élevés sur les préjudices financiers ou les nombres d'attaques. Ceci concernera en particulier l'estimation des préjudices sur l'ensemble des entreprises (deux milliards d'euros par an pour les cryptovirus, à interpréter comme un plancher) et les probabilités d'occurrence (au moins entre 4 et 5 % par an pour une petite entreprise).

# AVERTISSEMENT

## Un souci de ne pas porter de jugement sur les entreprises qui versent une rançon

> Les piratés sont victimes d'outils d'attaques efficaces mais souvent aussi d'outils de défense insuffisamment efficaces

Quoique la présente étude soulignera plusieurs effets négatifs des paiements de rançon en matière économique ou judiciaire, aucune appréciation à caractère moral n'en découle à propos des personnes frappées et conduites à opter entre payer ou non. La plupart opèrent ces choix dans l'urgence, sous tension, sans expérience antérieure ni soutien pour les guider. L'enjeu du moment, notamment patrimonial pour la victime, concoure à ne pas vouloir porter un jugement, surtout lorsque selon l'adage le conseiller n'est pas le payeur.

Loin d'ignorer cette dimension humaine dans son évaluation des coûts économiques, l'analyse mettra face à face l'impact social de ne pas payer et celui de payer, en reconnaissant leurs rationalités respectives. Elle suggérera des voies pour réconcilier ces intérêts antagonistes, et surmonter leur opposition.

Un second argument d'ordre moral souvent entendu se focalise sur la faute initialement commise par une victime coupable d'avoir sous-investi en équipement de sécurité, ou par un de ses employés ayant ouvert une pièce jointe sans vérification suffisante. Pareille critique est justifiée dans bien des affaires de fraudes au président ou de fraudes aux sentiments sur les réseaux sociaux, où se détecte une fréquente naïveté. Or la majorité des récentes affaires de cryptovirus ne dévoile rien de très différent d'un comportement standard, usuel chez la plupart des internautes, avec un degré de vigilance modéré mais en phase avec les rythmes du travail quotidien. Autant la sensibilisation des personnes aux dangers informatiques péchait il y a quelques années encore par ses retards, autant il n'est guère de petit patron qui aujourd'hui les méconnaisse, par le bouche à oreille ou par le vécu ; notre observation faite auprès d'entreprises de moins de 50 employés se voit corroborée par une enquête Bessé-PwC parmi les ETI, dont « les dirigeants sont désormais très réceptifs en raison des

attaques Cyber qui affectent leurs organisations »[4]. Beaucoup parmi les victimes rencontrées avaient un niveau en sécurité qualifiable de convenable au regard de leur capacité d'investissement ou d'apprentissage de l'informatique, qui n'est pas élastique, en s'étant équipées de sauvegardes, d'antivirus, souvent de pare-feu, et d'une politique au moins minimale de mise à jour des logiciels. En conscience, elles se croyaient à l'abri d'accidents basiques, et leur première bévue a été paradoxalement de s'en remettre à l'état de l'art -entendez, aux réseaux de communication déployés pour eux et aux logiciels informatiques qu'ils achètent sur étagère, au sujet desquels le nombre élevé de correctifs diffusés (les fameux « patchs ») sert de démenti presque quotidien aux promesses publicitaires de bonne finition de ces produits. Un nombre élevé de témoignages recueillis contiennent dorénavant pour phrase symptomatique un « **je me croyais protégé** ». Bien des fois leur surprise du Jour d'après provenait de la découverte douloureuse que leur dispositif, dûment réglé sur factures d'un fournisseur ou d'un éditeur de logiciel, n'avait pas fonctionné comme explicité dans le mode d'emploi (De même à nouveau chez les ETI, dont les dirigeants « ont la vision d'un risque très technique dont ils délèguent souvent la gestion et la prévention à leurs seules équipes informatiques et leurs sous-traitants »[5]). La responsabilité des victimes se voit diluée dès lors qu'elle est partagée avec un univers numérique insuffisamment protecteur, mais sur-vendeur de ses prouesses affichées en sécurité.

-> Constat de mauvaise qualité de l'information sur la partie protection.

L'ancienne époque où l'entrepreneur sous-estimait la menace, a en partie fait place à un temps où il surestime sa protection, sur la foi des discours de ses prestataires et fournisseurs de logiciels, dont une partie partage cette imprudente confiance dans les dispositifs qu'ils commercialisent ou dans leur propre savoir-faire. La qualité invérifiable de l'information sur la sécurité – le prospect ne peut vérifier si elle est fiable, complète et neutre, elle manque de transparence-, apparaît être un frein actuel à l'acte d'achat d'outils de sécurité (physique, assurantielle …). Une part de la frilosité des demandeurs de protection informatique ne vient pas d'un dédain envers le danger mais d'une défiance envers la dite sécurité qui leur est vendue, dont ils ressentent intuitivement qu'elle manque doublement de crédibili-

4 « Les dirigeants d'ETI face à la menace Cyber ». Mars 2018.

5 Ibid.

té : fiabilité de la sécurité, et fiabilité de l'information sur la sécurité. Le problème n'est donc pas seulement sécuritaire mais aussi informationnel.

En matière d'information précisément, les petites sociétés font face à des pirates plus professionnels qu'elles et dont le métier peu créatif consiste en particulier à s'informer des nouvelles vulnérabilités mises à jour -les « jours zéro » (*zero day*)- pour lancer promptement des vagues d'attaques avant que l'entrepreneur moyen puisse accéder à la même alerte. Hors cas flagrant de légèreté blâmable, la notion de faute s'estompe lorsque l'inégalité d'information biaise l'équilibre entre le bouclier et l'épée.

-> Constat d'asymétrie d'information avec la partie assaillante.

Trop simplificateur, avec une césure unique qui en un instant opèrerait une bascule d'un avant ignare vers un après où tous seraient en mesure d'être informés, comme au coup de départ d'une course, ce concept de *J zéro* déforme une réalité parfois tronçonnée en plusieurs étapes. En réalité existe-t-il des failles connues d'abord de quelques initiés sur des périodes parfois longues, mises à leur service, mises en vente, ou mises en réserve pour une variante d'équilibre de la terreur entre grandes puissances géopolitiques. Ainsi, NotPetya apparaît avoir exploité une faille nommée EternalBlue dans un produit Microsoft, originellement connue voire élaborée par l'équipe d'informaticiens Equation Group liée à l'agence de renseignement américaine NSA, en 2012 d'après l'estimation de F-Secure, bien avant d'être exploitée semble-t-il en mars 2016 par le gang de cyberattaquants chinois Buckeye, puis contenue dans des révélations commencées en août 2016 pour culminer en avril 2017 et faites par le groupe de hackers nommé Shadow Brockers, corrigée à partir de mars 2017 par Microsoft sauf sur Windows XP, réutilisée en mai pour les attaques WannaCry et NotPetya et alors découverte par le grand public ; lequel porte avec justesse ce nom de public, découvrant sur le tard au jour de la Générale un spectacle écrit et répété par ceux admis via l'entrée des artistes. Le dernier informé sera premier à payer.

Sur qui faire peser la culpabilité quand votre comportement était celui de monsieur tout-le-monde, et dès lors que la malchance est deve-

nue un discriminateur majeur pour départager celui qui sera frappé, de son voisin qui ne le sera pas, ou lorsqu'un banal état de fatigue mène untel à cliquer sur un courrier piégé vendredi, alors qu'il se serait méfié jeudi ? En attestent quelques confessions récoltées auprès de professionnels de la sécurité eux aussi victimes, dont l'expérience acquise a été mise en défaut sur un bref moment d'inattention ou à cause d'une masse de travail qui empêche de toujours déployer des procédures d'école, et qui ont souffert d'un évènement dont la probabilité d'occurrence était si faible qu'on se trouve tenté de jouer sa chance.

Les assurances se trouvent en théorie sur un terrain presque idéal pour elles, quand leur rôle dépasse celui de trier les bons et les mauvais quidams assurables, pour inciter à relever un faible niveau collectif de prévention, et lorsque la malchance devenue cause explicative se confond harmonieusement avec les calculs statistiques. D'ailleurs le caractère robotisé de bien des vagues d'attaques est-elle la marque que l'assaillant lui aussi s'en remet aux probabilités.

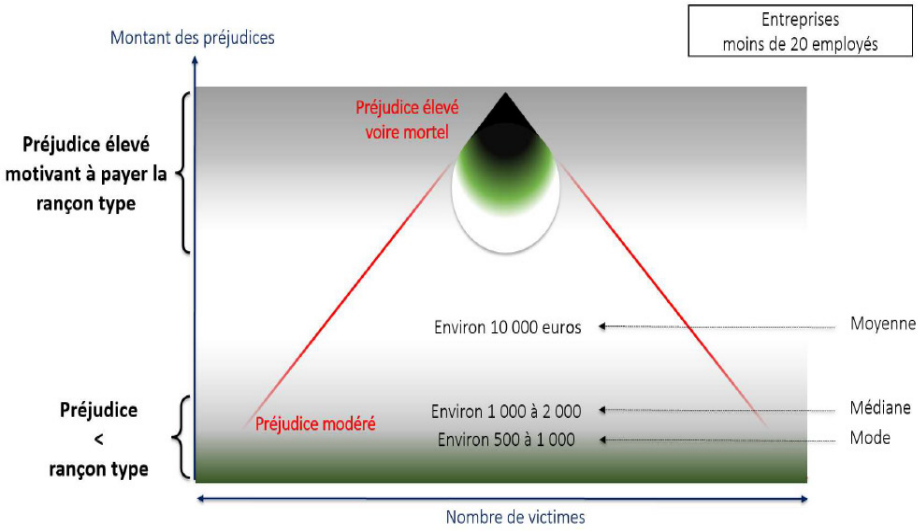
La question des rançons se situe là, au point de confrontation des mathématiques et du facteur humain, au cœur d'une malchance qui s'industrialise puis exige des choix solitaires.

**********

# Introduction

## « Par pertes et profits » : combien de préjudices pour combien de revenus ?

Chaque jour, 500 entreprises françaises environ sont victimes d'un cryptovirus[6] qui leur occasionne des torts économiques mais aussi humains. Pourtant peu d'entre elles iront jusqu'à la faillite, car une proportion élevée des entreprises confrontées à la perspectives d'un dépôt de bilan imminent se résignent alors à payer une rançon pour tenter d'obtenir les clés de déchiffrement (Inversement ci-dessous, la majorité des préjudices dans les entreprises sont inférieurs ou voisins du montant de rançon exigée par les pirates –quelques milliers d'euros également-, dès lors inintéressante à acquitter. Le coût moyen d'une attaque est resté relativement supportable, tout au moins jusqu'à aujourd'hui mais avec une tendance à l'aggravation). La donne est technique mais aussi commerciale et sociale, elle place la rançon au centre de notre questionnement.




6 Notre précédente brochure en 2018 retenait une fourchette large allant de 2 % à 4,5 % de victimes par an au sein des petites entreprises, en soulignant la probabilité que le haut de la fourchette soit le plus vraisemblable. Depuis lors, confirmation est venue de cette option haute, à proximité de 5 %. Soit de l'ordre de 180 000 victimes par an / 365 jours ≈ 500 entreprises touchées par jour.

Quel est le coût des attaques informatiques, et qui le supportera au final ou plus justement qui devrait légitimement le supporter ? Quel est le gain des pirates, à travers quel modèle économique ? Faut-il ou non verser des rançons en cas de chiffrement de données –a fortiori lorsque la victime est publique, et puisera dans les caisses du service public- (le Sénat de l'Etat de New-York débat d'une loi proscrivant le recours à l'argent public, suivant en cela des décisions similaires en Floride notamment), et comment s'opère la fragilisation des victimes par les pirates informatiques, pour les amener à céder ? Quelle est la « proposition de valeur » transmise par le pirate rançonneur à sa victime, et est-elle plus « compétitive » que l'offre assurantielle ? Sur un sujet complémentaire mais sensible, l'assurabilité des paiements de rançons a-t-elle une utilité économique ?

Et de manière terre-à-terre, les conditions sont-elles réunies pour qu'un marché pérenne de la cyber-assurance se développe ? Répondre nécessite d'apporter un éclairage préalable sur l'économie du piratage, qui se structure autour de trois grandeurs principales, à savoir :

- son coût pour les victimes, c'est-à-dire leur préjudice ou encore la destruction de valeur subie, une sorte de destruction intérieure brute (« DIB », ou PIB négatif. D'autant que s'incorpore la cessation de création de valeur, en cas de blocage d'une entreprise) ;

- son revenu brut c'est-à-dire les rentrées d'argent pour les pirates, autrement dit leur chiffre d'affaires ;

- son revenu net, frais déduits, à partager entre leur rémunération et le bénéfice distribuable qu'ils en retireront.

Une déclinaison de la troisième de ces grandeurs fait intervenir le revenu net par tête -par pirate ou complice-, qui oblige à tenir compte de leur organisation et des clés de répartition des gains entre membres. Tenir compte donc du nombre de membres, exercice qui conduit à dépasser les descriptions fantasmées du petit génie de l'informatique solitaire -pour les cryptovirus- ou de l'escroc au beau parler -pour les fraudes au président-. En réalité, et malgré l'automatisation de diverses tâches, « l'industrie du piratage » est pour partie une industrie de main-d'œuvre, avec sa division du travail, ses hiérarchies et ses sous-traitances, ses petites mains et les donneurs d'ordre.

## Jean qui rit et Jean qui pleure

Cette cascade de chiffres allant du préjudice pour le piraté au bénéfice dépensable par le pirate fait intervenir deux couples de protagonistes :

Le premier couple se constitue d'une part de pirates opportunistes d'une porosité constatable sur les équipements ou logiciels informatiques et de télécommunications, ou permis par leur mode d'usage courant. Avec d'autre part et en vis-à-vis, des équipementiers et développeurs de ces dispositifs, qui mettent sur le marché des produits et logiciels dont certains sont conçus sans priorité suffisante accordée à la sécurité, ou dont la maintenance et la mise à niveau ultérieures pèche parfois (l'ensemble des éditeurs de logiciel se trouve interpellé par cette interrogation, à moins qu'ils considèrent leurs produits comme livrés sans sécurité. Les lois américaines, qui donnent le ton dans beaucoup d'autres pays, ainsi que la formulation des licences d'exploitation, rendent très difficiles la condamnation des éditeurs lorsque des défectuosités sont constatées dans leurs logiciels. En 2002, plusieurs experts de la *National Academy of Sciences* avaient enjoint le législateur de modifier les lois pour davantage les responsabiliser7). Il en résulte un environnement technologique aléatoire au sens le plus littéral –présence de risque + de hasard-. Où se dévoile une aberration de ces piratages, qui à la fois attestent de l'imperfection de notre environnement numérique, mais procurent parfois des revenus à certains acteurs de cet environnement lorsqu'ils vendent ensuite de la sécurité ; ou lorsqu'au lieu de leur faire perdre un client victime, l'insécurité a tendance à le fidéliser à certains prestataires devenus indispensables à la maintenance interrompue de son système d'information. Le monde des informaticiens, éditeurs de logiciels compris, ne souffre guère directement des failles dont il est l'auteur.

Le second couple se positionne sur cet existant, avec pour mission d'en limiter les conséquences négatives. Binôme souvent considéré complémentaire (protection technique et protection assurantielle) :

Le premier rassemble les *réducteurs de préjudice* que sont les prestataires de sécurité informatique, dont le rôle attendu est d'empêcher

7 Computer Science and Telecommunications Board de la NAS : *« Cybersecurity Today and Tomorrow: Pay Now or Pay Later »*.

ou de réduire le précédent DIB. L'ambiguïté comptable vient de ce qu'ils contribuent également au PIB apparent, en ce que telle dépense de sécurisation ou de restauration d'un système d'information sera facturée à la victime d'une cyber-attaque. De manière neutre serait à calculer combien une unité de monnaie dépensée auprès de ces prestataires -enregistrée dans le PIB quant à la valeur ajoutée- économisera d'argent sous forme de préjudice évité -dégât enregistrable dans le DIB-, avec pour réponse usuelle une rentabilité marginale décroissante mais dont le seuil de rentabilité reste peu identifiable au niveau de chaque petite entreprise[8]. Notre étude de teraain a mis en relief que la moitié environ des préjudices étudiés auraient été évitables à coût quasi-nul par des mesures organisationnelles au sein des entreprises victimes –savoir notamment compenser par le maillon humain, l'imperfection des équipements techniques, et réciproquement-, puis à nouveau que la moitié environ du reliquat était évitable par des outils de sécurité peu onéreux déjà disponibles pour le grand public.

Le second rassemble les protagonistes de l'assurance –courtiers, assureurs et réassureurs- dont le rôle n'est pas directement d'atténuer le DIB, mais d'en répartir la charge sur une collectivité (voire sur eux-mêmes s'ils ont mal évalué le risque et les primes d'assurances) de manière à la rendre plus supportable ; et plus prévisible pour chacun, dans un rôle de réducteur d'incertitude. Au regard de ce que nous constatons être un préjudice annuel cumulé de près d'un milliard d'euros pour les entreprises de moins de 50 personnes[9], dû aux seuls cryptovirus, avec une évaluation plus délicate mais d'un plancher probable à deux milliards d'euros pour l'ensemble des entreprises, imaginer que toute la collectivité soit assurée reviendra à faire assumer ce ≥ deux milliards par elle (+ frais généraux, assistance, audits de sécurité préalables puis a posteriori, mais en défalquant les franchises, la partie capée des dédommagements, les victimes qui n'activent pas de demande de prise en charge, celles considérées fautives lors de l'attaque...).

Dans une dissymétrie flagrante, le maillon amont des prestataires d'équipements informatiques et de télécommunications dégage une marge bénéficiaire sans guère partager pécuniairement les risques encourus par sa clientèle ; tandis que le maillon aval des prestataires

8 Voir notre précédente étude *« Les cyberattaques et leurs préjudices dans les entreprises »*, 2018

9 Ibid.

d'assurances partage ces dangers au plus haut point, jusqu'à mettre en jeu toute marge bénéficiaire et au-delà. L'injustice économique qui transparaît ici se double d'une inefficacité économique, lorsque parmi deux acteurs au chevet d'un même besoin, l'un n'est pas assez impliqué par les conséquences, tandis que l'autre l'est à l'excès.

*Nous reviendrons dans la troisième partie sur ce déséquilibre du mode de répartition des coûts, qui surexpose l'assureur et l'assuré.*

## Un marché qui souffre d'incertitudes

Ajouter au coût des cryptovirus celui des autres types d'attaques –par déni de service, défacement, *phreaking* –piratage téléphonique-, hameçonnage, fraude au président ou fraude aux sentiments ….- positionne aujourd'hui le choc économique global du piratage très au-dessus de ces deux premiers milliards d'euros par an. Montant global qui, rapporté au nombre total d'entreprises françaises –près de 4 millions-, fait se demander si le seuil annuel de mille euros par entreprise n'a pas été atteint –ce que chacune paierait si le préjudice était réparti uniformément sur toutes, indépendamment de leur taille-. Les sources disponibles restent trop approximatives pour être affirmatif, mais cette barre du millier d'euros est désormais crédible, peut-être même dépassée déjà, et sa puissance évocatrice donne enfin une image concrète à ce fléau (une perception d'ensemble y accolerait les dépenses de sécurité, qui n'ont pas d'utilité productive et n'existent que par la présence d'une insécurité diffuse. Ce sont des frais induits).

Quelques-uns trouveront ce montant faible, à tort car il ne se jauge pas à l'aune du chiffre d'affaires mais notamment du bénéfice des sociétés, au détriment duquel l'amputation se révèle cette fois conséquente.

Ce ratio rançon/bénéfice dévoile en partie ce que nous verrons être une césure entre grandes et petites entreprises, qui sont en positions inégales face à des chocs, des pertes économiques et le paiement de rançons. Les grandes entreprises cotées en bourse sont d'abord structurées pour générer une rentabilité forte (Elles « ont restauré leur niveau de rentabilité préalable à la crise finan-

cière avec des bénéfices qui ont augmenté de plus de 60 % depuis 2009 »[10] et pour beaucoup activent « un recours accru aux paradis fiscaux et aux niches fiscales »), tandis qu'un grand nombre de PME et TPE dégagent des rentabilités plus modestes, qui les laissent exsangues en cas d'attaques majeures. Une autre différence sera il est vrai l'attractivité de ces deux types de cibles, au détriment cette fois des grandes. Attractivité à son tour modulée par la meilleure capacité des grandes à se protéger, etc.

En recentrant l'analyse sur les seuls cryptovirus –composante mieux explorée à ce jour-, la répartition uniforme des préjudices par entreprise correspondrait, toujours en ordre de grandeur général, à 500 euros pour chacune. Mais, hors peréquation, à bien davantage pour une multinationale, et un peu moins **pour une TPE –de l'ordre de 300 à 400 euros par an**, selon nos projections-.

## 1ère cause d'incertitude : l'imprévisibilité des changements d'échelle sur les préjudices (faut-il trouver 2 milliards par an ou davantage ?)

Le plancher actuel de deux milliards d'euros pour les cryptovirus, observable en situation devenue habituelle, laisse entrevoir l'ordre de grandeur des déboursements additionnels à subir par les entreprises ou leurs assureurs en cas par exemple de brusque pandémie frappant le tissu économique : a minima en centaines de millions –ce fut le cas en 2017 avec WannaCry et NotPetya- mais possiblement en milliards d'euros ou davantage, sur la France.

### Plausibilité ou probabilité

Nous nommons plausibilité, le fait que rien n'invaliderait la réalisabilité d'un scénario de destruction. Elle se distingue de la probabilité d'occurrence, que la présente étude s'est contentée d'observer d'après les faits. La plausibilité demande si tel évènement de telle ampleur peut ou non survenir, et facilement ou non ; elle ne s'in-

10 Rapport Oxfam France et le BASIC (Bureau d'Analyse Sociétale pour une Information Citoyenne), 2018. Etude menée à partir des bilans de 31 entreprises présentes au CAC 40 depuis 2009.

terroge pas directement sur le pourcentage de chances qu'il survienne, lequel dépend aussi de facteurs humains et sociaux tels que le nombre de pirates, le nombre de vulnérabilités, etc.

- Plausibilité économique (les grandeurs évoquées sont-elles atteignables ?)

  • en nous basant non plus seulement sur les quantifications issues de l'enquête de terrain, donc sur ce qui est arrivé, mais sur ce qui aurait pu arriver et que les dialogues avec les victimes ont fait surgir. Ces entretiens ont été l'opportunité de faire s'exprimer des entrepreneurs autour de telles hypothèses du pire, dans le cadre de leur société ou celui plus étendu qui englobe leurs partenaires, clients et fournisseurs. Avec des résultats inquiétants, puisque nombreux sont ceux estimant a posteriori qu'ils ont « eu de la chance » et que leur préjudice aurait pu être beaucoup plus élevé, en cas de performance légèrement accrue de l'attaque. La plausibilité d'une hausse accentuée des préjudices apparaît forte.

  • Un motif supplémentaire de redouter une capacité des coûts à atteindre des niveaux plus élevés découle de la tendance accélérée des entreprises à connecter davantage de leurs équipements ou à numériser leurs tâches ; tendance qui revêt quelques parentés avec un *effet-club* ou *effet de réseau* (i.e. une progression arithmétique d'une cause, qui engendre par exemple une progression géométrique des effets) mais cette fois, au service d'une propagation ou d'un gonflement des préjudices.

  Ces deux items ci-avant ont pour commun dénominateur que des petites variations d'amplitude des attaques seraient génératrices d+e grandes variations des impacts, du fait des fragilités latentes ou en germe dans les entreprises (l'importance de leur patrimoine numérique destructible notamment).

- Plausibilité matérielle. Par exemple en matière d'accident domestique, la plausibilité que de l'eau pure s'enflamme est nulle, celle que de l'alcool s'enflamme dans l'air est complète (hors schéma comme ici binaire, la plausibilité peut se graduer en proportion des difficultés techniques de réalisation).

Le présent cocktail unit une plausibilité assez élevée avec une probabilité d'occurrence difficile à cerner, constitutives ensemble d'un

contexte d'incertitude forte. Incertitude à regarder comme un mistigri dont le poids sera supporté par certains protagonistes plus que d'autres ; l'époque actuelle où se conviennent des clés de répartition des coûts entre acteurs impliqués –fabricants d'équipements, utilisateurs, assureurs …-, est aussi celle où cette incertitude commence à se répartir de manière assez inégalitaire entre eux. Les futurs gagnants et perdants se départagent aujourd'hui.

## Une échelle des surcroîts de préjudices

Surcroîts venant en ajout sur le coût déjà existant de ≥ deux milliards d'euros par an. L'échelle se décomposerait sommairement en quatre stades, chacun décuplant les masses d'argent du précédent :

- Le 1er, avec un surcroît à payer en centaines de millions, déjà éprouvé en 2017 avec WannaCry et NotPetya mais dont chacun a perçu le potentiel nuisible sous-utilisé, dans ce qui serait qualifiable d'attaque avortée ou mal orchestrée par les pirates.

A signaler, l'intéressant travail mené en 2018 de scénario d'attaque catastrophe intitulé Skyfleet-Dobycha, qui aide à anticiper les coûts envisageables lors de réplication de telles attaques, à plus grande échelle (aide aussi à mieux sonder ce que serait la portée du soutien ou les limites des assureurs et des réassureurs). Dobycha, imagine le blocage de plusieurs progiciels de gestion intégrée –PGI- chez des fournisseurs de la filière aéronautique par un cryptovirus de type NotPetya, sans latitude d'obtenir une clé de déchiffrement. Pour une population touchée, directement ou non, de 1800 entreprises membres de la chaîne logistique aéronautique, l'estimation finale de préjudice s'est hissée à 720 millions d'euros[11].

- Le 2ème -décuple de la 1ère, en milliards d'euros-, à plausibilité forte puisqu'une de ses matérialisations triviales serait une attaque de niveau WannaCry et NotPetya cette fois non avortée. Par exemple correspondrait-elle à un doublement du niveau usuel de dégâts (≥ deux milliards d'euros) sur une année

11 Philippe Cotelle, Philippe Wolf, Bénédicte Suzan, Jean-Laurent Santoni, Laurence Lemerle, et al..*Maîtrise du Risque Cyber et Assurance : Scénario cyber s'appliquant à la filière aéronautique Réponse du marché.* [Rapport de recherche] IRT SystemX. 2019. hal-02416407

; variation couramment éprouvée par les assurances sur les catastrophes naturelles, affectées d'un caractère erratique et qui d'une année sur l'autre peut occasionner là un doublement, ici une réduction de moitié.

NB : des entretiens menés lors de notre étude avec des victimes collatérales de WannaCry et NotPetya mènent à penser que les coûts globaux de ces attaques ont été sous-estimés. Il s'agit non pas nécessairement d'une minoration des coûts internes aux entreprises les plus touchées –les plus grandes souvent-, dont plusieurs ont effectué un travail approfondi d'évaluation, mais d'un recensement incomplet des coûts externes, au sein des petites entreprises partenaires en amont ou aval. Ce point, qui se rattache aux supply chains –les chaînes de sous traitance- et aux propagations d'impacts susceptibles de s'y produire, rappelle que la modélisation de cette propagation depuis les petites entreprises telles que des sous-traitants vers de gros donneurs d'ordre, ne sera pas nécessairement le symétrique d'une propagation depuis des grandes entreprises vers des petites. Assurément les coûts collatéraux ont-ils été moins remarqués au niveau de ces dernières, lors de ces récentes attaques. Deux cas illustratifs méritent citation :

- L'un, d'une petite entreprise de distribution située en aval d'une des multinationales frappées par NotPetya, et qui a subi à ses frais la désorganisation des systèmes d'information et de passation de commandes de la grande entreprise, sur une durée plus longue et dans des proportions plus douloureuses que ce qui en est ressorti publiquement. Des dysfonctionnements nombreux ont eu lieu dans la circulation de l'information commerciale pendant et post-crise, entre la grande entreprise et son distributeur, y compris après que les systèmes informatiques aient été remis en fonctionnement dans l'opinion de la grande entreprise (toutes deux n'ont donc pas la même perception de la vraie date de fin-de-crise). Cette situation de cacophonie prolongée, où la petite entreprise s'est sentie mal ou sous-informée, traitée comme tiers négligeable et mise en porte-à-faux avec ses propres clients, a contribué à renforcer les coûts cachés.

- Pour parallèle, dans une autre affaire qui ne concernait pas cette vague d'attaques, un autre sous-traitant d'une grande entreprise du numérique a été impacté lui aussi par une gestion

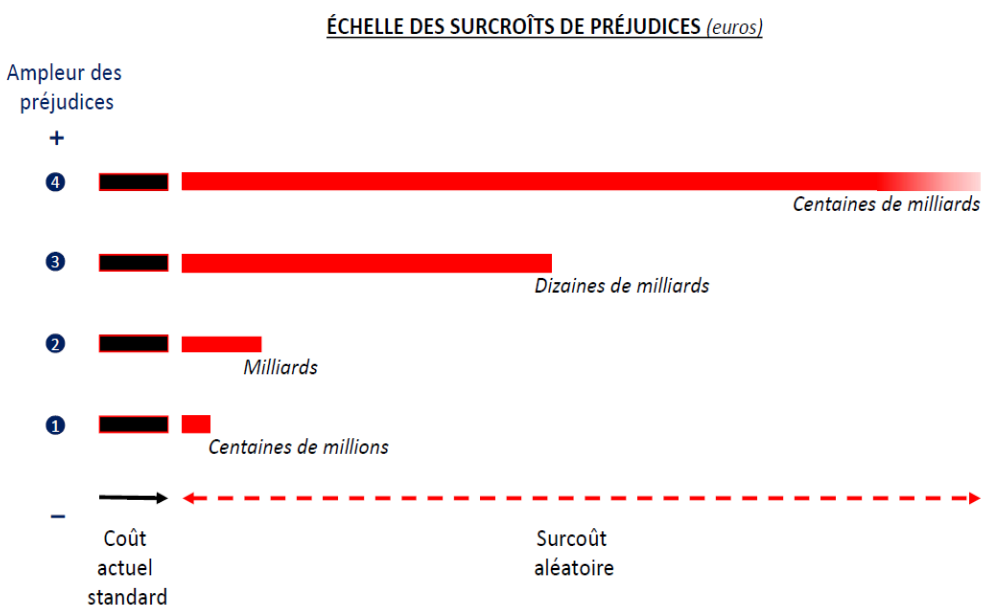
de crise qualifiable d'égocentré de la part de son grand donneur d'ordre. Lequel a méconnu les intérêts vitaux de ce petit fournisseur de services, et a défini sa politique de communication et de relation amont-aval en fonction de sa préoccupation de notoriété propre.

Ces deux cas ont en commune de recéler des coûts invisibles élevés. Ou plus exactement non-vus, du fait qu'aucun pointage ne semble avoir été lancé à leur propos. Au manque de visibilité s'ajoute l'évitabilité, car une meilleure méthode de gestion de crise les aurait grandement réduits.

- Le 3ème -centuple de la 1ère, en dizaines de milliards-, à plausibilité moyenne, qualifiable de systémique et frappant l'économie profondément, gênant ou bloquant non plus seulement des entreprises avec leurs alentours immédiats mais certaines fonctions collectives de production, de transport, de coordination, du tertiaire, etc.

- Le 4ème -milluple de la 1ère-, en centaines de milliards d'euros ; masse colossale mais qui cesse de paraître inenvisageable une fois rapportée au PIB de la France, de 2 353 milliards en 2018 (100 milliards en équivaut 4,2 %. Lors du krach financier, sur l'année 2009, le PIB de la zone euro avait chuté de 4 %, tout comme aux USA, tandis que celui du Japon avait plongé de 9 %[12]). Crise informatique ardue à concevoir et à scénariser, qu'on suppose souvent plus étendue ou plus durable : étendue jusqu'à une paralysie plus généralisée des fonctions socio-économiques, ou durable voire définitive en empêchant de manière radicale un retour à la normale. Sa plausibilité n'est pas très inférieure à celle du 3ème, puisque l'irréversibilité des effets sur les données est déjà latente dans un chiffrement robuste, si aucune clé n'est livrée et si les données mais aussi les logiciels infectés ne sont pas reconstituables pour redevenir fonctionnels.

12 Pour rappel, les présents préjudices globaux d'attaques informatiques sont des compilations de préjudices individuels d'entreprises, mais qui ne sont en fait pas strictement additionnables. En effet, les arrêts de production de l'une (perte) font fréquemment le bonheur d'une rivale (gain), ce qui relativise l'impact final. Inversement, n'est pas encore intégré l'effet diffus d'une grande attaque sur la consommation d'une population, sur l'investissement général, la confiance, etc.




*Pour comparaison, en 2018 le coût des incendies de forêts en Californie a été chiffré à près de 13 milliards de dollars[13] ; ceci le situant à un équivalent entre ② et ③ (Californie et France ont un PIB quasi équivalent). Sur la France en 2018 également, les assurances de biens et de responsabilité ont versé 39 milliards d'euros en prestations[14], dont 17 pour l'automobile. Une meilleure analogie se décèle entre l'effet des cryptovirus dans les entreprises, et les assurances de biens des professionnels et agricoles qui ont enregistré 4,9 milliards de charge de prestations ; ou encore avec les catastrophes naturelles à 1,6 milliard (Source FFA).*

Concrètement se demande quel(s) acteur(s) économique(s) aurait la surface financière suffisante pour fournir un surcroît de liquidités nécessaire à des crises de stade ① ou ② dans un délai court (Les stades ③ et ④ se réfléchissent en termes aussi de risques de mor-

13 Voir la faillite consécutive de l'assureur Merced Property & Casualty Company. 2018 *Annual report of the Insurance commissioner.* California Department of Insurance, page 33.

14 Au niveau européen, « Les assureurs européens ont versé en 2018 (...) 407 milliards pour l'assurance non vie (principalement pour les contrats d'assurance auto et habitation) » (FFA).

talité du payeur, s'il s'agit d'entreprises ou d'assureurs. Pour spéculatifs qu'ils soient, de tels multiples nous rappellent l'existence d'un seuil de rupture du système assurantiel).

- Désigner l'Etat signifierait l'activation d'abord de l'impôt donc du contribuable :

Dans la même fourchette que les milliards de cyber-préjudices redoutés en ② se trouve le récent IFI, Impôt sur la fortune immobilière, ayant collecté 1,3 milliard d'euros en 2018 (Son prédécesseur l'ISF -Impôt de solidarité sur la fortune- s'était élevé à 4,2 milliards d'euros en 2017). Ces montants avoisinants soulignent le poids social qu'aurait une telle ponction, la résonnance politique qu'elle trouverait. Les ≥ deux milliards actuels de préjudice équivalent à une cinquantaine d'euros pour chacun des 38 millions de foyers fiscaux français, mais prendre aussi en charge des surcoûts élevés démultiplierait cette première facture.

Envisager que l'Etat pourrait financer une crise de stade ③ équivaudrait à se rapprocher de ce que rapporte l'impôt sur le revenu (80 milliards par an). En 1976, le financement de « l'impôt sécheresse », par une hausse prévue de 10 % de l'impôt sur le revenu, avait contribué à la démission du premier ministre (l'aide de 2,2 milliards de francs octroyée à l'époque aux agriculteurs, équivaudrait aujourd'hui avec l'inflation à 1,5 milliard d'euros).

La dette publique, en particulier pour le stade ④, apparaîtraient à tort comme une solution miracle. Un tel endettement se hisserait à hauteur des récents assouplissements quantitatifs –injections de monnaie par la planche à billets- des banques centrales. Cependant celles-ci sont déjà mobilisées jusqu'à leurs limites de prudence par leurs récentes émissions pour atténuer les seules crises financières ; y ajouter des injections de volumes aussi astronomiques pour motifs informatiques (après également les injections de la Banque de Chine pour motifs économiques d'origine sanitaire suite au coronavirus), quoique matériellement réalisable, renforcerait néanmoins le risque de crise financière systémique ou même d'effondrement monétaire. Ces injections dérogent à la philosophie originelle d'être pourvoyeuses provisoires de cette monnaie (les q*uantitative easing* ou leur ancêtre de l'*open market* consistent de la part des banques centrales à acheter des titres tels que des

obligations ou des bons d'Etat avec la monnaie créée, donc à récupérer in fine cet argent lors de la revente future de ces titres) pour devenir pourvoyeuses définitives, donc à dilater la masse monétaire sans véritable manette de marche arrière : une grande partie des injections depuis une dizaine d'années ont rencontré des difficultés à enclencher un *tapering* –réduction progressive du montant des émissions- puis à récupérer l'argent émis -réduction de la taille du bilan d'une banque centrale- -> La présente solution se résumerait à financer les conséquences d'un risque informatique advenu, en renforçant un risque monétaire plus grave encore.

- les entreprises victimes sont aujourd'hui l'acteur payeur à plus de 95 %, puisqu'une faible minorité est assurée.

L'incertitude quant aux probabilités vaut en particulier pour les 3ème et 4ème stades, puisque des attaques de grande taille sont susceptibles de résulter de circonstances géopolitiques autant que techniques. Avec en arrière-plan un nombre croissant d'Etats qui participent actuellement à une « course aux armements informatiques » les faisant accumuler des moyens d'agression –virus, portes dérobées, vulnérabilités recensées chez l'adversaire …-, et exposant le tissu économique à la moindre activation ou fuite d'une partie de cet arsenal dormant (NotPetya constitue une illustration de ces stocks de moyens d'agression émanant ou connus de structures étatiques, puis capables de fuiter vers des sphères plus ou moins criminelles).

L'évaluation des probabilités est ainsi compliquée d'une part par la présence de ces facteurs humains et politiques, d'autre part par la présence en arsenal d'une capacité de destruction inactivée mais précisément soumise à des bons-vouloirs géopolitiques ou des collusions mafieuses (l'incertitude n'est pas de type météorologique pour deviner s'il y aura la grêle, puisqu'elle est là en attente, mais si quelqu'un l'activera et contre qui). La probabilité d'occurrence n'est plus seulement affaire de statistiques dès lors que les jeux d'acteurs nous renvoient vers la théorie des jeux, les modèles de prédation économique, la concurrence déloyale ou l'art de la guerre. De surcroît, l'existence d'outils d'attaque s'aggrave d'une pré-existence de nombreuses failles logicielles. Les armes comme les opportunités sont à la fois futures mais déjà présentes, qui

conservent aux statistiques leur efficacité pour refléter le passé, mais limitent celle de prédire l'avenir.

## 2ème cause d'incertitude : le décalage temporel entre la prévision du risque et la vérification du risque

Un point clé n'est pas le montant des primes et des remboursements dans l'absolu, tant que ces deux volumes restent avoisinants, mais le taux de sinistralité -ratio entre le montant des sinistres à dédommager et celui des primes encaissées- c'est-à-dire l'écart comptable entre eux deux permis par l'écart temporel qui sépare la date de fixation de la prime et les dates couvertes : l'assureur propose un montant à t-1, contractualisé à t, pour couvrir un éventuel évènement à t+1.

Au vu des variations concevables sur l'axe de l'amplitude des préjudices, la question se pose de savoir s'il existe une prévisibilité suffisante de ces variations sur l'axe temporel (concernant des horizons supérieurs à un an, ou autre échéance de reconduction ou révision des contrats et du montant des primes).

Avec pour précédent inquiétant à propos de tels rythmes de fluctuation, la rapide hausse des fraudes au président à partir de 2010, puis quelques années plus tard la même soudaineté sur celle des rançongiciels[15] (une rupture moins souvent identifiée a été l'apparition du bitcoin, par lequel le rançonnage s'est vu facilité). Jusqu'où les assurances peuvent-elles remplir leur rôle de répartir un risque, si celui-ci semble appelé à grossir de manière non linéaire (l'imprévisibilité n'est pas qu'il grandisse mais par à-coups), donc pas reportable a posteriori sur les primes déjà versées par les assurés ? Les assureurs se trouvent face aux pirates dans la même situation qu'un négociant en matières premières exerçant sur un marché influencé par les spéculateurs.

## Des primes parfois trop faibles pour garantir l'équilibre des assurances mais paradoxalement souvent dissuasives pour les

15 « Les attaques de cryptovirus perçues visant nos sondés sont en hausse, de 37 % à 45 % par rapport à l'année passée. » Kaspersky : *Enquête sur les risques informatiques mondiaux 2015*, menée auprès de 5 564 entreprises interrogées dans 38 pays, d'avril 2014 à mai 2015.

**petites entreprises**

> « Le montant des primes affectées au risque cyber semble donc encore insuffisant pour répondre à des évènements d'ampleur. » [16]

En imaginant que toutes les entreprises souscrivent une cyberassurance –sans franchise ni remboursement plafonné …- ce premier repère ≥ deux milliards pour les cryptovirus servirait à fixer les primes à collecter, desquelles retrancher diverses exclusions de garantie mais auxquelles ajouter les frais et la marge de l'assureur. Marge essentielle puisqu'elle est le moyen de constituer une cagnotte de précaution, un matelas pour les mauvaises années. Dans un cas d'école presque insoluble, quelle marge de rentabilité en année normale faudrait-il appliquer afin de se constituer un matelas de précaution, lorsque vous ignorez triplement la date, la taille et la probabilité de survenance d'une future vague d'attaques ? « Pharaon rêva de sept vaches grasses *puis* de Sept vaches maigres », Genèse – 41 : quelle position adopter lorsque vous n'êtes pas certain du puis ?

Dans l'hypothèse où le préjudice double sur un an, ce bas de laine devra s'être auparavant garni de ≥ deux milliards d'euros. La rentabilité usuelle de cette profession permet-elle de la couvrir contre une telle vague submersive ? Sachant que l'agressivité commerciale de certains assureurs étrangers, qui ont concocté des grilles tarifaires à faible marge afin de pénétrer le marché français, pèse négativement sur la capacité des acteurs de ce secteur à constituer un tel matelas (faible marge & forte incertitude).

Plutôt que de marge faible, serait-il judicieux de parler d'une marge inconnue à terme, car le recul acquis à propos de ce type de risque est faible encore. Hormis pour les marchés anglo-saxons plus développés puisque le seul marché nord-américain représentait près de

16 Philippe Cotelle, Philippe Wolf, Bénédicte Suzan, Jean-Laurent Santoni, Laurence Lemerle, Christophe Delcamp, Virginie Wyka, Sébastien Héon : *« Maîtrise du Risque Cyber et Assurance : Scénario cyber s'appliquant à la filière aéronautique. Réponse du marché* ». IRT SystemX. 2019. hal-02416407. Page 11.

90 % du marché mondial en 2015[17]. Selon la société de courtage d'assurance londonien Aon, le taux de sinistralité sur les cyber-assurances aux Etats-Unis serait de 35 %[18], témoignant d'une profitabilité là-bas très honorable, mais à assortir de deux réserves :

- la première est le recours fréquent des victimes et assureurs américains à verser des rançons pour éviter des préjudices supplémentaires. La rentabilité du marché assuranciel n'y est pas dissociable de ce « joker » dont l'activation n'est pas anodine.

  Une question clé voudra comprendre comment convertir le marché français à des habitudes de s'assurer sur les risques informatiques, en visant de semblables taux de rentabilité, sans importer la recette du paiement de rançon qui contribue à ce rendement hors norme. Le risque n'est-il pas encouru que les professionnels anglo-saxons de l'assurance transposent en France un modèle assuranciel intégrant un modèle comportemental laxiste envers les rançonneurs ?

- la seconde est que la rentabilité affichée par le marché américain sur ce segment, en année relativement normale, ne nous livre qu'une photographie provisoire. Tout équilibrage issu d'un court passé apparente les tarifs d'aujourd'hui à des paris pour demain ; L'agence de notation A.M. Best résumait en 2019 la situation en notant que « les cyber-assureurs sont rentables aujourd'hui, mais restent circonspects quant aux risques futurs ». Un symbole de ce souci provient de l'Autorité de régulation prudentielle britannique, qui a incité dès 2017 les assureurs à renforcer la surveillance des risques cyber, et à mettre en œuvre des *stress tests*. Une même tonalité imprègne un communiqué de l'ACPR française -Autorité de contrôle prudentiel et de résolution- : « Si les contrats dédiés au cyber risque sont pour le moment peu développés, les organismes (d'assurance) ne mesurent pas encore suffisamment leur exposition, notamment

17 Parti de 2,5 milliards au niveau mondial en 2014, il est estimé à 4,3 milliards de dollars pour les USA en 2018 par Grand View Research, et à 7,3 milliards mondialement en 2019 par Mordor Intelligence. Il avait été anticipé à 14 milliards pour 2022 par Allied Market Research (*Global Opportunity Analysis and Industry Forecasts, 2014-2022*), et à 19 milliards pour 2025 par Grand View Research, quoique d'autres études récentes envisagent plus de 20 milliards à cette échéance (près de 28 milliards en 2025 selon le *Global Cybersecurity Insurance Market - Growth, Trends, Forecast (2020-2025)* de Mordor Intelligence).

18 Aon : « *US cyber Market Update. 2018 US cyber insurance profits and performance* », juin 2019, page 4.

à travers les garanties implicites contenues dans les contrats en cours. (..) Peu disposent d'une cartographie exhaustive des contrats et portefeuilles concernés. Ils ne peuvent par conséquent pas évaluer correctement leur exposition au risque cyber. »[19]).

Un autre talon d'Achille vient de l'incomplétude des vérifications techniques menables par les assureurs, quant au niveau réel de sécurité déployée chez chaque nouveau client (il est exact qu'un audit coûterait plus cher que la prime d'assurance annuelle chez bien des petites entreprises) ; se contenter d'une procédure déclarative et de questionnaires simplifiés insuffisants pour reconstituer chaque contexte d'entreprise, avec son exposition et ses besoins particuliers, est une démarche qui accroît le précédent pari (les organisations mettent trop peu en œuvre encore par exemple la méthode EBIOS Risk Manager de gestion du risque numérique, ou certaines recommandations du rapport « Maîtrise du risque numérique » publié par l'ANSSI et l'AMRAE[20]).

## Piètre connaissance de la qualité du risque au niveau individuel

A cette première incertitude au niveau individuel s'ajoute une seconde au niveau collectif :

## Piètre connaissance quantitative du niveau de risque futur au niveau collectif

Face à cette double incertitude, qualitative et quantitative, à propos de l'argent susceptible de devoir sortir, et faute de pouvoir aisément accroître les primes -l'argent qui rentre-, la tentation ou la prudence devient de s'exonérer du risque mortel qui s'y attache. Trois évacuateurs s'offrent, en cas de vague d'attaques réussies :

---

19 Communiqué : « La distribution des garanties contre les risques cyber par les assureurs », 12 nov. 2019

20 Ce rapport rappelle l'utilité de mener en parallèle plusieurs actions qui se complètent, de cartographie des risques et des faiblesses, de recensement de l'existant dans chaque entreprise, et de scénarisation d'évènements (« L'élaboration de scénarios de cyberattaque permet de mettre en évidence des systèmes d'information qui, dans un premier temps, n'avaient pas été identifiés comme critiques. »), etc.

- retransmettre le risque vers la collectivité ou l'Etat qui en est un intermédiaire.

- Le transmettre vers l'amont, vers les prestataires informatiques défaillants sur la qualité et la sécurité intrinsèque de leurs produits, option pertinente mais que nous avons vue inactivée à ce jour.

- Le retransmettre vers l'aval, le client, en diminuant le volume contractuellement remboursable en cas de préjudice. Réflexe à l'œuvre désormais, fait de garanties diminuées et plafonnées. L'AMRAE –Association pour le management des risques et des assurances de l'entreprise- a exprimé sa crainte que « s'il y a un choc, ce sont les entreprises qui devront le porter sur leur bilan. »[21]

Le système, qualifiable presque de demi-assurantiel, tendrait à se concentrer sur des garanties pour des préjudices de niveau intermédiaire, excluant ceux à coût faible par la franchise, et ceux à coût très élevé par le plafonnement, sans d'ailleurs apporter une sécurité complète à l'assureur puisqu'il demeure exposé à une multiplication brusque des dossiers à coût intermédiaire.

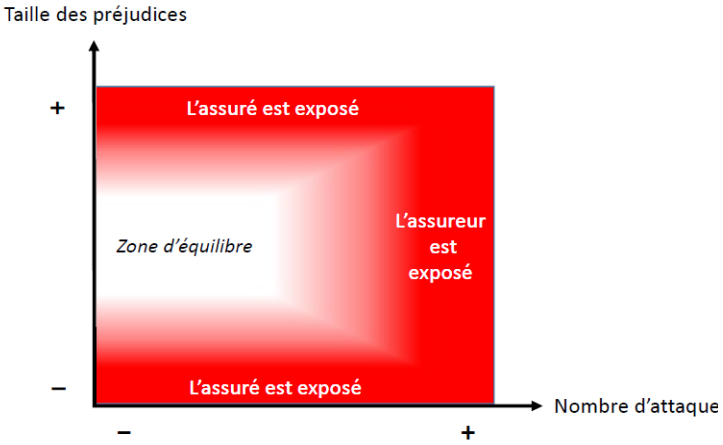
Il n'y a pas de repère certain quant à un plafond maximal de préjudice d'une attaque réussie

Il n'y a pas de repère certain quant à un nombre maximum d'attaques réussies

Ce trop-plein d'incertitudes dérive en flou contractuel où l'assuré comme l'assureur ont peine à savoir jusqu'où ils sont couverts ou engagés. Il s'ensuit une défiance paralysante, notamment pour le segment des petites entreprises où l'un hésite à s'assurer, et l'autre à assurer (En matière de prime souscrite sur 2016, « l'Europe représente (…) un montant maximum de 255 millions d'euros de primes, sur lesquels la France ne représente que 40 millions d'euros »[22]. D'autres sources retiennent 50 millions pour 2016, montant doublé à 80 millions en 2019). Le marché français de la cyber assurance représente une modeste fraction des préjudices observés, et le problème de la répartition des risques reste quasi entier.

21 Brigitte Bouquot, présidente de l'Amrae, janvier 2020.

22 Rapport du club des juristes « Assurer le risque cyber », janvier 2018.




*Le tableau d'ensemble ainsi brossé délimite une zone –ici en blanc- qualifiable « d'équilibre » (équilibre des efforts entre assureur et assuré), où le cyber-assuré sera convenablement couvert sans que l'assureur s'expose pour autant à une insolvabilité, zone centrée sur des montants intermédiaires et peu fréquents : sur l'ordonnée qui reflète la taille des préjudices, ceux très élevés sont souvent exclus par plafonnement, ou tarifés à prix assez dissuasifs (sont aussi exclus les préjudices bas, par la franchise). Sur l'abscisse du nombre d'attaques réussies, l'assureur se trouve mis en danger si ce nombre est élevé (par multiplication du nombre de victimes différentes ou récurrence des impacts sur une même victime). Les zones « de déséquilibre » -en rouge- pointent les situations où l'un des membres du couple assureur-assuré assume à lui seul l'essentiel des conséquences.*

## Le rôle limitateur de coûts endossé par les rançons

Dans le métier de l'assurance où les statistiques sont tournées vers le passé, mais sur une cyber-assurance qui a peu de passé –les rançongiciels sous une forme ou une autre datent à peine d'une génération-, ce savoir embryonnaire n'a pas encore circonscrit de limite maximale au volume et au périmètre du préjudice possible. Pour parallèle, nul jusqu'alors hormis pour bâtir des modèles, ne s'est soucié de l'hypothèse que sur une année toutes les régions du monde connaissent une catastrophe climatique, qui un cyclone, qui des inondations. Guère plus ne s'étaient pris à imaginer que toutes les voitures de la planète souffrent simultanément d'une panne ou d'un accident -le marché traditionnel de l'assurance d'accident routier reflète et exprime avant tout les limites humaines de millions de conducteurs et de leurs comportements qui ne sont pas uniformes- ; questionnement jusqu'à lors inutile tant l'improbabilité était immense, mais désormais plausible dès lors que toutes les voitures seront communicantes et potentielle-

ment exposées à une même fragilité informatique.

Le phénomène numérique, par sa quasi ubiquité, peut ramener des évènements en nombre inconnaissable par avance, à une seule origine au demeurant minuscule, par le truchement d'un virus ou de virus souvent apparentés.

A la capacité déclencheuse répond une seconde particularité elle aussi ubiquitaire, de pouvoir depuis tout lieu faire cesser les préjudices de cryptovirus, par la rançon. En cela, la cyber-assurance dépend d'un nombre réduit d'acteurs que sont des pirates capables d'activer le deus ex machina du déchiffrement, comme un auteur dramatique en mesure d'apporter un épilogue heureux à sa pièce de théâtre, un dénouement qui annule les frais supplémentaires.

> Face à l'absence de limite fournie par les statistiques du passé ou les projections pour l'avenir, la rançon devient une limite de substitution, fixée par des protagonistes.

La rançon octroie à un marché de masse des caractéristiques jusqu'à lors réservées à quelques créneaux spécifiques du secteur de l'assurance, et comportant une phase possible de négociation –enlèvement de voyageurs à l'étranger, vols de tableau de maître puis transaction pour sa restitution-. Jusqu'où ira la résistance sociale au paiement de rançon s'il s'agit demain d'éviter ces milliards ou dizaines de milliards d'euros de préjudices ? L'interrogation initiale bifurque vers celle de l'inéluctabilité sociale ou non du rançonnage, et sa banalisation comme en territoire mafieux. La rapide habituation actuelle des victimes à envisager et parfois acquitter la rançon dessine un état social pré-mafieux, qui impose un tribut sur une portion grandissante de la population, dont chaque membre lorsqu'il accepte de payer participe à l'établissement d'une norme comportementale larvée. Une lente prise en otage de l'économie s'institue, permanente et assujettissante à terme.

Ce tribut, qui doit se lire comme un dilemme à la fois individuel et collectif, laisse le choix entre un préjudice parfois mortel ou une spoliation, entre se retrouver mort ou nu.

## Non plus les préjudices mais le vol d'argent proprement dit

## Le train de vie des pirates

En matière de revenus bruts pour les pirates, notre estimation faite pour les petites entreprises de moins de 50 personnes touchées par des cryptovirus aboutit à une trentaine de millions d'euros versés sous forme de rançons, par an et sur la France, souvent par la collecte de petites sommes, typiquement de l'ordre de 3 000 euros (Ces chiffrages concernent essentiellement les années 2017 et 2018, et sont révisables à la hausse depuis lors, probablement plus proches de 40 à 50 millions en 2020 ; notamment du fait de l'augmentation forte de la propension à payer des rançons, de la part des victimes. De même en 2020, le frémissement de hausse sur les montants exigés laisse craindre une nouvelle élévation de ces chiffrages).

La mesure des versements effectués par les grandes entreprises est plus ardue, qui se heurte à un mur de silence du fait notamment d'enjeux de réputation. Avec les réserves inhérentes à ces rétentions d'information, il est envisageable que le total des rançons approche la centaine de millions.

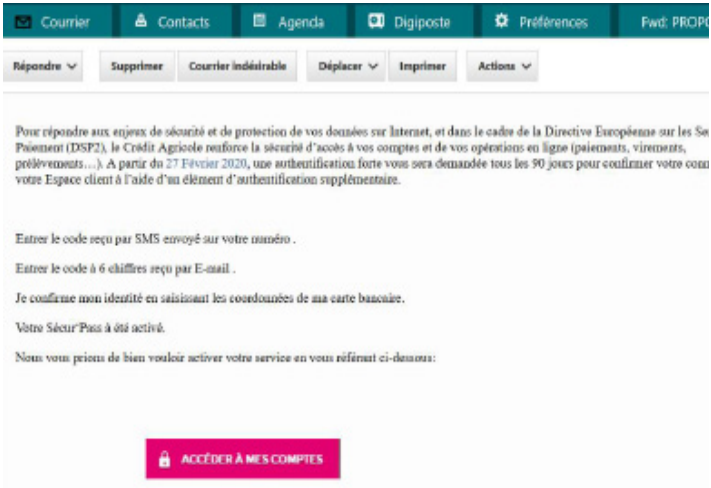
*(A partir de la répartition de la valeur ajoutée produite en France par catégories d'entreprises -Grandes entreprises, ETI, PME, microentreprises-, et sachant que celles de < 50 personnes y contribuent pour près du tiers, le montant estimé pour ces dernières triplerait pour l'ensemble des entreprises, soit de l'ordre de 120 millions. Toutefois la valeur ajoutée est un point de repère imparfait)*

Une extrapolation à l'échelle internationale serait hasardeuse –le ciblage effectué par les pirates n'est pas homogène planétairement –Symantec estimait à près du quart la proportion de victimes situées aux USA, mais ceci doit y tenir compte d'une moindre omerta locale-, la culture de protection diffère selon les pays, la tolérance au paiement de rançon semble par exemple plus installée aux Etats-Unis qu'en Grande Bretagne …- mais un ordre de grandeur en centaines de millions d'euros serait vraisemblable pour l'Europe, et en milliard(s) mondialement. Ce montant paraît en phase avec l'estimation publiée par le FBI, d'un milliard de dollars de rançon en 2016[23]).

S'y ajoutent les saisies effectuées par les fraudes au président –que nous verrons être entre 100 et 200 millions- et celles d'un ordre de grandeur vraisemblablement voisin occasionnées par les fraudes aux sentiments actives sur les réseaux sociaux au détriment des per-

23 Interview du FBI par CNN. « *Cyber-extortion losses skyrocket, says FBI* » par David Fitzpatrick et Drew Griffin CNNTech 15 avril 2016.

sonnes seules, âgées ou influençables. Une réalité surprenante se découvre, qui hisse le revenu brut des diverses formes de piratage en centaines de millions d'euros par an, probablement voisin de 500 millions si l'on y incorpore les autres formes de prédation que sont le hameçonnage ou encore la fraude dite nigériane[24], laquelle sollicite de l'argent via des courriels trompeurs (mais sans inclure l'ensemble des fraudes aux cartes bancaires ou autres moyens de paiement, domaine qui n'a été couvert que sur des hameçonnages par notre étude de terrain, et se trouve déjà bien exploré par ailleurs avec 439 millions d'euros de fraude via les cartes de paiement françaises recensés en 2017 sur les transactions de paiement et de retrait[25]).




*Exemple de tentative de hameçonnage, d'assez bonne facture malgré quelques coquilles et qui s'ornait du logo de la banque. L'expéditeur diffuse par envoi massif son message à une liste d'adresses sans s'être préoccupé de la nettoyer pour ne conserver que des destinataires possédant effectivement un compte dans l'établissement. Mais sachant que la banque revendique 21 millions de clients particuliers et une entreprise sur trois, il peut espérer un malentendu favorable chez cette sous-population.*

Concernant ces agrégats, le revenu brut de ces diverses criminalités informatiques est divisable en trois postes : frais humains (plus importants qu'imaginés et que l'on peut supposer être en dizaines de millions d'euros au moins), bénéfice final (incluant son partage avec des protecteurs mafieux ou plus institutionnels. Le total pouvant être envisagé supérieur à 50 % des gains bruts), enfin frais techniques qui correspondent croit-on souvent au seul « investissement » informatique. Or cette composante matérielle est modeste -ordinateurs, serveurs …-, surtout une fois rapportée au préjudice occasionné chez les victimes, de quelques millions d'euros pour l'un et quelques milliards pour l'autre, soit un ratio symbolique d'un millième. Au contraire, les pirates recourent de manière importante aux télécommunications, en utilisant les réseaux mondiaux comme vecteur, comme écran, ou pour accéder à des places de marché noir numériques et autres plateformes de location de rançongiciels (RaaS) … Utilisation quasi-gratuite, qui fait d'eux des profiteurs d'investissements collectifs, détournant leur finalité comme un pirate de l'air détournerait un gros avion quand il souhaite se rendre vers telle destination personnelle. Que le coût soit assez négligeable sur le versant matériel informatique fait ressortir deux autres sous-postes d'investissement quant

à eux immatériels et plus conséquents, d'une part des achats d'informations sensibles facilitatrices d'attaques (identifications permettant l'accès à un système, ou encore information sur des vulnérabilités logicielles), d'autre part des achats clé-en-main de rançongiciels (d'autres modèles économiques que l'achat sont possibles, depuis le troc jusqu'à un abonnement pour disposer d'un tel cryptovirus, ou sa mise à disposition gratuite par son concepteur contre rémunération –au pourcentage ou avec un fixe …-. Variété de modèles révélant que ce qui apparaît comme un poste de dépense pour un premier pirate, est un poste de recette pour un autre situé plus en amont, donc qui contribue aux bénéfices de ce dernier).

*Montant des rançons ou extorsions = montant des revenus bruts criminels = capacité d'investissement en piratage informatique (une fois les frais défalqués)*

L'opulence du bénéfice net probable laisse penser que les pirates pourraient investir davantage dans de l'équipement matériel, qu'ils en possèdent comptablement la force, sans en ressentir l'utilité, l'envie ou l'opportunité ; ce qui les bride n'a pas une cause financière. Inversement pour les forces de l'ordre, leur limite première apparaît bien être financière, subie et non pas choisie, du fait de moyens budgétaires insuffisants pour traiter les plaintes sur l'ensemble du territoire et pousser les enquêtes plus avant (une crainte veut que le sentiment diffus d'inutilité à porter plainte, entendu de la part de nombreuses victimes lors de la présente étude, soit contributeur au réflexe palliatif de verser une rançon). Certainement serait-il peu rassérénant de comparer les capacités d'investissement des pirates pour attaquer, et des forces de police ou gendarmerie pour contrer les cryptovirus. Mais ceci serait aussi peu instructif, car un équilibre financier attaquant-défenseur, bien que symbolique, n'aurait pas de portée dans le présent type de conflit teinté de guerre asymétrique et de doctrine « du faible au fort », au sens où il suffit statistiquement de peu de victoires au bénéfice d'un camp, pour faire subir un grand choc au détriment de l'autre camp : face aux défenses en place, un pirate n'a pas besoin de réussir toutes ses innombrables tentative d'attaques, et une petite minorité de réussites suffira à créer un climat d'insécurité ; face aux attaquants en action, le judiciaire n'aurait pas besoin de tous les interpeller, et une petite minorité d'arrestations suffirait à rétablir une peur du gendarme. Reconnaissons que seul le premier de ces deux défis –imposer l'insécurité- a rempli sa mission.

Parmi les exceptions, une double arrestation présente une dimension pédagogique en ce qu'elle dépeint la division du travail qui prévaut dans cette délinquance, avec les coopérations planétaires qui en découlent ; mais aussi l'imbrication entre vie sociale intégrée et activités illégales. D'une part, vivant en Grande-Bretagne, l'étudiant en informatique Zain Qaiser, pirate et maître chanteur pour un total estimé à un minimum de 900 000 dollars, qui piégeait des sites internet avec un programme malveillant développé semble-t-il par un comparse d'un gang russophone, afin d'infecter leurs visiteurs (sans recours au chiffrement de données). D'autre part son blanchisseur d'argent Raymond Uadiale, d'origine nigériane puis installé dans la région de Seattle ; clin d'œil de l'histoire, ce dernier était après une courte activité d'enseignant en mathématiques devenu ingénieur réseau employé chez Microsoft, et propriétaire d'une maison valant 390 000 dollars. Il conservait 30 % de l'argent blanchi et reversait le solde à son complice via une plateforme sur internet[26].

## Un vol d'argent, d'ordre à la fois individuel et collectif

Une quatrième grandeur s'est intégrée au tableau en ce que, au regard de l'origine géographique supposable des attaques, ces montants sont autant de sorties de capitaux du territoire français vers l'étranger, alors que notre Compte de transactions courantes national est d'ores et déjà en déficit chronique, à hauteur dernièrement d'une quinzaine de milliards par an (Quand bien même certains pirates seraient français, contrairement au dossier judiciaire ci-avant, il est peu vraisemblable, dès lors qu'ils ont réussi à dépayser ces millions provisoirement devenus des cryptomonnaies, qu'ils aient pour réflexe d'en rapatrier la majeure partie en France et en euros, où la manœuvre de blanchiment constituerait un aléa superflu, et la principale prise de risque comparativement à celle des étapes antérieures de l'attaque).

Ces flux constituent une sortie d'argent sans contrepartie. En quelque sorte, nous « achetons » des escroqueries, intégrables à nos importations dans la balance des échanges. Une comparaison instructive sera fournie par les vins de Bourgogne, dont le volume d'exportation oscille lui aussi entre 500 et 900 millions d'euros selon les années ; avec pour distinguo que ce revenu brut des viticulteurs est amputé

26 Department of Justice. Office of Public Affairs. https://www.justice.gov/opa/pr/washington-state-man-sentenced-prison-role-connection-reveton-ransomware

par des coûts de production conséquents, alors que celui des pirates l'est dans une ampleur moindre.

**Montant des rançons ou extorsions ≈ Sorties de capitaux hors du territoire**

Economiquement, le territoire français se voit vidé d'une somme qui ne participe plus à la construction de notre PIB, ni à la taxe sur le PIB qu'est la TVA, et fait défaut pour les rentrées fiscales. Prenons conscience qu'à l'échelle d'une décennie, plusieurs milliards d'euros seront ainsi exfiltrés de l'espace national ; or ces milliards, une fois la vitesse de circulation de la monnaie prise en compte, généreraient un chiffre d'affaires bien supérieur dans l'économie. Facteur de paupérisation d'autant plus néfaste que cette confiscation se fait au sein des entreprises, alors tentées de compenser ce choc par une réduction de leurs projets d'avenir et des investissements (postes budgétaires faisant aisément office de variable d'ajustement lors de coups du sort).

Inversement, les pays de transit ou de destination de cette manne accroissent leur masse monétaire. Gilbert Chikli, condamné en 2015 par le tribunal correctionnel de Paris pour 7,9 millions d'euros de fraudes au président mais à l'époque installé à Ashdod en Israël, déclara l'année suivante que 90 % de ces revenus passaient par la Chine ou Hong Kong, qualifiés par lui de « plaque tournante universelle pour toute forme de fraudes »[27]. De tels montants irriguent leur économie et concourent à la croissance économique, favorisant à la fois les rentrées fiscales et la corruption du tissu social local.

A l'image de la spécialisation sur les fraudes aux sentiments existante sur telle ville -Bouaké- d'une région -celle de Gbèkè- d'un pays -la Côte-d'Ivoire-, le piratage affiche dès lors un autre visage, multiniveaux, où l'échelon individuel s'interpénètre avec l'échelon local qui procure un écosystème de soutien, avec l'échelon national de protection diplomatique, et avec l'échelon international d'appui au blanchiment. En cela, le piratage est devenu un système (L'expression « économie des vulnérabilités » à propos de leur marchandisation, est représentatif également de cette réalité). Par opposition, de notre diplomatie indulgente envers plusieurs pays en phase de spécialisation au sein d'une sorte de division internationale du travail cyber-délin-

27 Entretien avec Erika Kinetz : "*AP Investigation: How con man used China to launder millions"*, Associated Press News, 28 mars 2016.

quant jusqu'à notre appareil policier en carence de moyens, le volet défensif n'a pas atteint le stade d'être un système, complet, cohérent et coordonné.

L'objectif de cet ouvrage est précisément d'adopter une analyse multi-niveaux, pour raccorder l'échelon individuel, essentiel pour mener des observations sur le terrain auprès de sources fiables, à une réflexion globale capable de replacer ces évènements, ces masses d'argent et ces flux, dans une compréhension de la confrontation entre un système de prédation (détruire ou le menacer, pour en tirer un revenu) et notre système économique mû par une logique de création de valeur (produire pour en tirer un revenu).

# ETAT DES LIEUX ET BILAN GENERAL

***Nota : ce chapitre à la fois résume les constats développés ultérieurement dans les trois parties de l'ouvrage, et apporte des compléments d'information nécessaires à leur compréhension.***

Le bilan dressé dans ce document est descriptif des actuelles pratiques dominantes de cyber-rançonnages, mais il laisse entrevoir la menace de changement, de saut à la fois qualitatif + quantitatif + tarifaire, déployé sur deux axes principaux :

Changement d'échelle, pour manipuler davantage de cibles, d'argent …

- si les montants des rançons exigées viennent à s'envoler, tendance qui s'est esquissée en 2019 et apparait à l'œuvre plus nettement en 2020. Venant de collectivités locales ou d'entreprises –notamment des prestataires informatiques auprès de TPE et PME-, l'écho de rançons désormais en centaines de milliers d'euros s'est accru[28], là où les montants entendus il y a deux ou trois ans encore se standardisaient autour de prix en milliers d'euros, plus rarement en dizaines de milliers (pour des petites entreprises). Il sera vu [dans l**a deuxième partie**] que les pirates disposent aujourd'hui d'une marge de hausse potentielle très conséquente, qu'ils n'ont pas exploitée initialement pour des raisons probablement tactiques mais peut-être provisoires. Une étape préparatoire semble avoir été la hausse de la propension à accepter de payer des rançons de la part des victimes, qui nous est parue palpable depuis deux ans environ ; comme si un verrou psychologique ou éthique avait soudain été forcé chez les victimes, désormais plus enclines à considérer d'abord la rentabilité individuelle et à court terme du geste ;

- Si le champ d'action mord sur de nouveaux publics. Après une phase initiale d'assauts indiscriminés contre le monde des entreprises, s'est opéré une meilleure segmentation où « Les attaquants sont plus réfléchis dans leurs modes opératoires : ils savent différencier leurs attaques pour aller à la chasse aux gros gibiers »[29]. La focalisation a gagné en subtilité, comme aux Etats-Unis où a été remarquée une concentration de ten-

29 Loïc Guézo, secrétaire général adjoint du Clusif.

tatives contre les entreprises de taille intermédiaire, jugées assez grosses pour détenir une trésorerie attractive, mais trop petites pour s'être dotées de moyens conséquents de protection informatique. Après les entreprises, le sentiment s'impose désormais d'une extension au secteur médical, en particulier hospitalier, ainsi qu'aux collectivités locales. Peut-être cet élargissement est-il le signe d'une amélioration des défenses érigées par les entreprises, qui déporterait l'action des agresseurs vers des proies moins préparées donc rentables. Dans leur course à la croissance, ils planifient leur entrée sur des marchés complémentaires et diversifient leur portefeuilles en s'ouvrant de nouveaux « créneaux commerciaux ». Stratégie qui laisse augurer le ciblage de milieux jusqu'à lors épargnés, tels que les particuliers, les étudiants inséparables de leurs ordinateurs, et tous ceux qui dématérialisent leurs fiches de paye ou mille autres documents[30]. En cela, la référence faite au tissu économique s'élargit au tissu social. Enième front ouvrable à tout moment, qui étendrait le théâtre du conflit.

Cette scalabilité, ce changement dimensionnel vers des tailles plus grandes, s'entend aussi dans le passage depuis une échelle individuelle (une entité telle qu'une personne ou une entreprise) vers un format collectif, jusqu'à la ville intelligente où vit cette personne, la chaîne logistique dont cette entreprise est sous-traitante.

Ceci impose de ne plus réfléchir cible par cible, isolément ou par simple contagion de proximité, comme l'ont fait de nombreux modèles d'analyse des préjudices, mais selon un modèle dorénavant en poupées gigognes dont chacune sera visable : ma maison intelligente fait partie d'un quartier intelligent dans une ville intelligente reliée à des transports interurbains connectés. Il en ira de même pour mon usine intelligente ou dite 4.0.

La scalabilité est aussi une adaptation aux tailles inférieures, vers l'intérieur cette fois car ces maisons –tout comme nos voitures

30 54 % de citoyens américains interrogés ont répondu être prêts, sur le principe, à payer une rançon pour récupérer leurs données bancaires numérisées. 55 % des parents interrogés ont donné la même réponse pour des photos de famille numérisées. Etude IBM X-Force, « *Ransomware: How Consumers and Businesses Value Their Data* ». 2016. A la même époque, « 24% des Français étaient prêts à consacrer entre 20 € et 50 € par an à une cyber-assurance ». Etude PwC, « Le marché de la cyber-assurance : la révolution commence maintenant ».

communicantes- contiennent des objets qui rivalisent à qui sera le plus connectés, tels que nos compteurs d'électricité.

Un tel regard multidimensionnel révèle une facilitation prochaine des pénétrations, avec des préjudices en bouquets, en grappes, par le seul effet de telles superpositions qui ouvre des brèches inter-niveaux.

Mutation des modes opératoires, en particulier

- Si le chiffrement de données se double de leur exfiltration, pratique en voie d'extension actuellement : vous, victime, avez perdu la jouissance de données, mais dont moi, pirate, je détiens une copie bonne pour usage ou revente à vos concurrents ou mise en ligne préjudiciable auprès du grand public (un tel chantage affecterait également les particuliers et leur vie privée).

- si les attaques gagnent en *intelligence* -capacité d'adaptation partielle à chaque cible- pour cumuler les avantages du prêt à porter et du sur-mesure. En s'inspirant aussi de la patience et de la discrétion des APT -menace persistante avancée, par intrusion prolongée dans le temps- pour gangrener plus en profondeur les systèmes visés avant de laisser se déclarer les premiers symptômes (L'opération « est réalisée sur plusieurs semaines voire plusieurs mois après la compromission effective de la cible. Une étude approfondie de la cible et de son infrastructure est donc fortement probable » - Anssi). Une professionnalisation est effectivement ressentie aujourd'hui, rompant avec une phase plateau qui, durant plusieurs années à partir du milieu de la décennie 2010, avait recours aux mêmes méthodes éprouvées, lancées de manière fortement automatisées, puis dont les pénétrations étaient exploitées rudimentairement, souvent sur l'instant. La confiance installée d'avoir non pas éradiqué mais endigué ces nuisances en volume se voit désormais mise en doute.

Ceci impose de rompre avec une attitude qualifiable de suiviste. Le répit de quelques années, offert par cette relative stagnation des méthodes d'attaque, a été utilisé pour mettre les défenses à leur hauteur mais plus rarement pour les préparer contre celles de demain. Le bouclier se veut réactif, mais omet d'être anticipatif.

- si des attaques de grande envergure frappent l'économie, mais après lesquelles les attaquants ne se manifestent pas et ne proposent aucune clé de déchiffrement. Nous constaterons que la porosité des entreprises aux attaques, déjà très coûteuse pour la victime même lorsqu'il y a rançon finale, serait sinon paralysante à des degrés élevés et cette fois pour la collectivité aussi. Le fait que çà et là quelques victimes soient -sciemment ou non- abandonnées sans clé à leur destin par les pirates, offre un avant-goût des impacts potentiels si le « jeu » cessait soudainement pour devenir guerre, et politique de la terre brûlée.

## Vers une addiction aux rançons

Cet inventaire froid souligne à quel point de vulnérabilité est parvenue notre société face à ce péril, puisqu'elle est exposée au bon vouloir d'agresseurs en capacité de modifier leur règle du jeu, voire d'arrêter d'en faire un jeu. Ce *kriegsspiel* consigne que notre panoplie défensive est en perpétuel risque de se trouver en retard d'une guerre. Un cap insidieux est en cours de franchissement, où nous devenons économiquement dépendants du bon déroulement des rançonnages avec leurs fournitures de clés de déchiffrement qui s'ensuivent ; nous ne sommes plus tout à fait libres, et le débat glisse depuis la question de savoir si l'on doit les payer … vers celle de savoir si l'on peut se passer de les payer. De surcroît, verser aujourd'hui des rançons ne pourra qu'aggraver demain cette addiction et son coût [la **troisième partie** étudiera l'opposition d'intérêt entre court et long terme, le dilemme qui nous tiraille entre privilégier aujourd'hui ou demain].

Une telle épée de Damoclès ne fait que reconnaître l'exposition à une menace qui n'a pas donné sa pleine puissance. Le statu quo contemporain tient par un modèle économique d'attaquant dont on ne peut prédire la perduration, et par un équilibre technologique entre l'épée et le bouclier dont le devenir est tout aussi imprévisible ; il serait plus expressif de parler de déséquilibre technologique, de filet troué qui laisse réussir un nombre d'attaques socialement supporté par la collectivité. Laquelle prie pour qu'il s'agisse d'un *déséquilibre technologie* stable, alors que beaucoup de signes annonciateurs penchent au contraire vers son aggravation tendancielle.

La médiocre espérance que rien ne s'aggravera, à propos d'un état des lieux déjà insatisfaisant, atteste d'une position où la collectivité est sur la défensive et plus exactement sur le reculoir. Nous sommes de plus en plus *dépendants aux rançons*, faute pour les plus fragiles

mais indirectement aussi pour la collectivité de parvenir à s'en passer ou s'en prémunir.

## Vers une sophistication des rançons

La fusion de deux menaces -devenir plus chère & plus mortelle- est à prendre au sérieux, sur les cas où le chiffrement de données paralyse irrémédiablement l'entreprise : un scénario plausible consisterait à ce que brutalement les pirates adoptent un autre modèle économique tolérant par exemple une mortalité de 50 % parmi ces entreprises gravement crypto-virussées, après avoir exigé de celles-ci des sommes décuplées afin d'être admis dans le cercle privilégié des 50 % survivants [La **première partie** de l'ouvrage détaillera les deux principaux modèles économiques mis actuellement en œuvre par les pirates, qui restent moins mortifères]. A l'extrême, quel péage Noé aurait-il pu imposer aux rares couples admis dans son arche ? A l'évidence trouverait-on au sein de toute population nombreuse une minorité de candidats prêts à abandonner l'entièreté de leur bas de laine afin d'avoir la vie sauve. Qui céans renoncerait à tout l'argent qu'il a économisé par le passé pour se préserver un avenir, et échangerait ainsi du passé contre du futur afin de maintenir en fonctionnement, là l'usine, ici le magasin, qui ainsi continuera à lui verser un revenu dans le futur ? [Dans une approche inspirée de la théorie des jeux, la **deuxième partie** décomposera le processus de coercition déployé, à la fois psychologique et de raisonnement comptable, qui retourne l'instinct de survie des petits entrepreneurs au profit de l'attaquant]. « Mon royaume pour un cheval » fait dire Shakespeare au roi Richard III devant l'imminence d'une débâcle qu'il tente en ultime recours de conjurer. Utiliser les plus fragilisés pour fixer la mise à prix standard puis obliger les autres à s'aligner sur ces tarifs, faire préférer le chacun pour soi au tous pour un [Où apparaît la relation entre l'individu et la collectivité, source tantôt de faiblesse tantôt de force face aux crypto-pirates, que nous explorerons dans la **troisième partie** de l'ouvrage].

Intermédiaires naturels entre cet individu et cette collectivité, les dispositifs de mutualisation du coût des préjudices insèrent un interlocuteur doté lui aussi d'un modèle économique en quête de viabilité. Or la présente insécurité sera-t-elle amortissable par un système assurantiel ? En d'autres termes, la fragilité technique de nos systèmes d'information sera-t-elle compensable par une solution non technique. Faute de quoi la survie des victimes grâce à leurs assureurs risque de s'avérer onéreuse au point d'attenter à la survie de ceux-ci.

Un renversement de pensée s'effectue lorsqu'on passe de cette précédente assurance couvrant les préjudices, à une assurance qui éviterait les préjudices en couvrant le paiement de rançon. Au point de demander s'il s'agit encore du même métier, sous l'excuse qu'il y a toujours prise en charge d'un débours.

A propos plus spécifiquement de ces assurances-rançon –venant rembourser l'argent versé par la victime-, la **première partie** de l'ouvrage montrera que la précédente question vaut dans les deux sens : les assurés sur le paiement de rançon risque-t-ils au final d'être coûteux au point d'être nuisibles à leurs assureurs. …Mais tout autant ces assureurs qui proposent d'indemniser les paiements de rançon ne risquent-ils pas d'être au final nuisibles aux assurés ? Car est-on certain qu'une assurance sur les rançons sera sans conséquences sur le montant desdites rançons que s'autorisent à réclamer les pirates ?

Trois acteurs sont ainsi en présence, le pirate, le piraté (et derrière lui l'ensemble de la population ciblée), l'assureur (mais derrière lui aussi une partie de la même population), dont les comportements ou les intérêts ne se contentent pas de s'affronter ou se coaliser mais qui interagissent l'un sur l'autre : un premier regard sur ce jeu laisse supposer qu'il est à somme nulle et que ce que l'un capte fera défaut à l'autre ; en réalité ce jeu, bien qu'à somme nulle effectivement sur les seules rançons qui transitent d'une poche à une autre, ne l'est pas sur les patrimoines mis en jeu par chacun, car la mise peut augmenter ou diminuer selon les postures puis les réactions des uns et des autres. Nul ne peut prétendre être tout à fait neutre, et la compréhension de ces faits économiques nécessite de les étudier dans leur dynamique, qui déroule une partie à trois joueurs.

# A - CONTEXTE ET REPERES

« Parce qu'il est possible de polluer des sites ou de les paralyser voire de les détruire (..) la tentation du chantage est inévitable. »

*Marketing et cybercriminalité* [31]

L'envolée du nombre des attaques par cryptovirus à partir du milieu de la décennie 2010, quoiqu'elle ait été suivie par une période de moindre croissance, a soulevé deux questions, celle du paiement ou non des rançons, puis celle de l'assurabilité des rançons versées çà et là par des victimes. Pratiquée dans quelques pays étrangers, cette prestation d'indemnisation s'expose à deux critiques, d'une part un risque -qui sera évalué dans le présent fascicule- d'influer sur les évènements par le seul fait de les couvrir, d'autre part plus prosaïquement un danger concurrentiel que cette garantie rançon soit utilisée par certains assureurs ou courtiers étrangers en tant que produit d'appel pour démarcher des clientèles d'entreprises françaises, profitant alors du vide laissé sur ce créneau par des acteurs français de l'assurance. Ceux-ci pour beaucoup n'ont pas développé d'offre correspondante, sur un sujet sensible où historiquement les autorités policières et judiciaires mettent en garde contre de telles pratiques jugées ambiguës et pousse-au-crime.

De fait, parmi les trois statistiques clés que sont le nombre d'attaques réussies, le montant des rançons et la propension des victimes à en verser, un souci croissant concerne la troisième, sur laquelle la tendance comportementale va vers l'acceptation de paiement. Cette observation, en germe les précédentes années mais remarquable depuis 2019, est corroborée par un récent questionnaire international qui évalue la proportion de victimes acquittant une rançon à 39,

31 Yannick Chatelain et Loïck Roche, Hermes Science Publications, 2000, page 79.

% contre 14 % l'année précédente[32]. Une seconde étude conforte ce glissement, avec cette fois un quadruplement des paiements de rançons qui passe de 4 % en 2018 à 16 % en 2019[33] ((le second chiffre apparaît très crédible, tandis que le premier semble avoir été en-deçà de la réalité. Probablement existe-t-il parallèlement une baisse de la répulsion à avouer qu'on paye une rançon, qui biaise la statistique finale). A tout le moins et pour la France seulement, un doublement des acceptations de payer apparaît vraisemblable, sur une période de deux à trois ans (nous indiquions dans notre précédent fascicule en 2018 un ordre de grandeur approximatif tendant vers 10 % des victimes, seuil qu'on peut désormais craindre être dépassé. Sur un échantillon un peu différent puisque retenant les victimes ayant déposé plainte, la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces évaluait à la même époque que « 5 % des victimes auraient décidé malgré tout de payer une rançon, en moyenne 5 000 euros »[34]. De manière plus fine, ce pourcentage de payeur est bien sûr insignifiant chez les victimes de petits préjudices –rapportés à leur taille- mais entre dans les mœurs pour devenir majoritaire dès lors que ce coût ébranle l'entreprise jusqu'à remettre en cause sa destinée -sa feuille de route ou son existence-).

D'après nos observations toujours, le nombre d'attaques réussies augmente pour sa part plus modérément (Accenture estimait la hausse des maliciels à 11 % entre 2017 et 2018 . Depuis lors, d'autres sources sont divergentes, certaines voyant une légère baisse mais compensée par des dégâts plus élevés, ou inversement), tandis qu'une hausse du montant des rançons demandées se dessine depuis 2019, difficile encore à chiffrer mais lui conférant le rang de problème numéro deux.

---

32 *CrowdStrike Global Security Attitude Survey 2019*. Publiée par le prestataire de solutions de sécurité californien *CrowdStrike*, fondé par des anciens de *McAfee* avec l'appui du fonds d'investissement *Warburg Pincus LLC* dont l'actuel président est Timothy Geithner, ancien Secrétaire au Trésor de Barack Obama. Etude réalisée par le cabinet *Vanson Bourne* spécialisé dans les études de marché liées aux technologies numériques, en interrogeant près de 2 000 responsables dans la sécurité des TIC, sur le continent américain -États-Unis, Canada, Mexique-, au Moyen-Orient et en Asie -Australie, Japon, Inde et Singapour- et en Europe -Allemagne, Royaume-Uni, France-.

33 Etude *Dark reading*, de septembre 2019, menée auprès de professionnels de la sécurité des TIC dans des entreprises de plus de 100 personnes. Parallèlement, les sondés font part d'une baisse des attaques subies, passant de 12 % à 10 % de réponses positives (cette baisse est de près de 20 %, mais éclipsée par la hausse sur les paiements).

34 « Etat de la menace liée au numérique en 2019 ». Rapport n° 3 Mai 2019.

A l'instar du monde des assureurs, les instances judiciaires n'adoptent pas une conduite uniforme d'un pays à l'autre, par-delà leurs positions officielles quant à elles plus convergentes ; de la sorte en 2015, une gazette rapportant un aparté d'un représentant local du FBI devant un petit comité d'entrepreneurs du Massachussetts a provoqué une onde de choc parmi les publics de la sécurité : « Pour être franc, nous conseillons souvent aux gens de simplement payer la rançon »[35]. Echo qui a d'autant plus nourri la polémique que ce propos s'avère à double détente : un policier reste-t-il dans son rôle lorsqu'il donne un tel conseil hors micro, mezza voce, de personne à personne ? Mais surtout, la police en tant qu'institution est-elle dans son rôle lorsqu'elle le conseille au micro et devant un parterre de chefs d'entreprises, de par son effet incitatif dès lors que cette option se voit adoubée par une autorité morale. Plus fondamentalement la présence d'un « souvent » donne à ce conseil l'allure d'une ligne de conduite récurrente qui ne peut qu'avoir un impact normalisateur chez les décideurs présents, renforcé par le « simplement » (« *just to pay* ») qui assimile ce geste -faire au plus simple- à une solution de facilité portant l'estampille fédérale. D'abord éthique (avec pour détail cocasse, la présence en anglais de ce « *to be honest* … » où l'honnêteté est d'avouer apporter une aide à la malhonnêteté), la question devient pratique, puisque si le conseil individuel de payer, transmis de policier à victime par un réflexe d'empathie, survient après chiffrement des données, donc une fois dans l'impasse et acculée à des expédients, le présent conseil public de payer l'a été quant à lui devant un auditoire d'entreprises qui ne sont pas encore victimes et qui entretemps réfléchiront à investir ou non dans leur sécurité ; que devient, à ce stade antérieur, l'incitation inoculée ? La solution de facilité, qui se cantonnait *a posteriori* à acheter son salut, ne devient-elle pas *a priori* celle de renoncer à bien se protéger puisqu'on achètera -au futur- ce salut à moindre frais par un paiement « de la main à la main » ? Combien me coûtera mon pare-feu dernier cri versus combien me coûterait -au conditionnel- ma rançon ?

Le dilemme est plus global que ce premier prisme micro-économique

35 « The ransomware is that good. To be honest, we often advise people just to pay the ransom. » La position officielle du FBI reste louvoyante, en ce qu'il « ne recommande pas le paiement de rançon, d'une part car elle ne garantit pas que le payeur retrouvera l'accès à ses données (..) » Il ajoute que « le paiement risque d'encourager d'autres attaques (..) Toutefois le FBI comprend que lorsque les entreprises sont en situation de blocage, leurs dirigeants évalueront les différentes options pour protéger leurs actionnaires, leurs employés et leurs clients. » https://www.ic3.gov/media/2019/191002.aspx

observateur de comportements individuels et d'arbitrages comptables ; car nous sommes collectivement tous démunis face à un mal qu'aucun outil de sécurité ne peut garantir bloquer, au sens aussi où notre technologie ne sait pas davantage réparer ce qu'un pirate aura chiffré, que la médecine médiévale ne savait soigner un pestiféré une fois les symptômes déjà présents. Les commentaires ayant suivi cette déclaration du FBI ont souligné son statut de pis-aller, faute de la solution alternative qu'aurait été la mise sous les verrous des agressseurs informatiques … Quand il devient plus simple de payer (« *just to pay* ») un coupable que de l'arrêter. L'habituel débat entre tenants des deux discours -payer ou non- ne fait qu'acter l'impuissance matérielle de l'Autorité -police, justice mais aussi les chercheurs en informatique[36]- à résoudre le problème en amont : en l'absence de solution définitive, payer est-il une solution provisoire ? Si nos impôts légaux ne parviennent plus à nous protéger et donner force à la loi, faut-il s'en remettre à l'impôt illégal qu'est une rançon ?

Il sera signalé dans la **troisième partie** que des améliorations substantielles du niveau de sécurité seraient atteignables, mais qui demanderaient un volontarisme pour retoucher quelques pans précis du droit des contrats et de la responsabilité du fait des choses (touchant à la commercialisation de logiciels mis en vente malgré leur état d'inachèvement, et d'imperfection sue du vendeur mais tue par lui à sa clientèle) ainsi que pour faire évoluer quelques protocoles de communication dépassés par la montée de l'insécurité numérique. Juridiquement comme techniquement, l'impuissance découle d'abord d'un immobilisme.

En France la mise en garde publique est double, à la fois contre le principe de verser une rançon, et contre celui de proposer des contrats d'assurance pour rembourser cette rançon versée. Cependant une telle recommandation d'ordre moral et déontologique s'émousse

36 Un commerce douteux est récemment apparu, où des prestataires informatiques prétendent aux victimes paniquées être en mesure de casser en quelques heures le code chiffrant utilisé par le pirate (à ne pas confondre avec les cas où par exemple un pirate amateur utilise un code dont la clé de déchiffrement est déjà répertoriée, du fait de précédentes rançons versées. Quoique minoritaire, ce cas de figure mérite vérification. https://www.nomoreransom.org/). Philippe Wolf rappelait le paradoxe contemporain où ce meilleur de nos outils de sécurité qu'est le chiffrement, est devenu la pire arme contre nous.

tant qu'elle ne s'appuie pas sur des considérations plus terre-à-terre, comptablement audibles par les entrepreneurs : existerait-il une rentabilité sociale, ou une rentabilité économique, à ces pratiques d'assurance rançon ? Ou au contraire auraient-elles un rendement global négatif à l'échelle de la collectivité, qui les assimile à une nuisance ?

**Afin de comparer des rentabilités, d'abord comparer deux grandeurs :**

ce que coûtent les dégâts dans les entreprises et ce que coûtent les rançons destinées à éviter ces dégâts

### ◊ Préjudice total

Prise entre 2016 et 2019, la photographie de cette période dévoile un **montant de préjudices internes pour les entreprises françaises ayant moins de 50 employées et victimes d'un cryptovirus**, de l'ordre de 700 millions à **1 milliard d'euros par an** (La tendance à l'aggravation nous a rapproché année après année du niveau haut de cette fourchette, que nous retenons désormais). Chiffrage à considérer comme un plancher minimum, et auquel ajouter ceux sur les entreprises > 50 personnes, sur les administrations –dont les universités, laboratoires, hôpitaux …- et collectivités territoriales ainsi que sur le tissu associatif et les simples particuliers. Le total se compte ainsi en milliards d'euros, au pluriel, avec un minimum estimé à **au moins deux milliards d'euros pour l'ensemble des entreprises françaises**, y compris les exploitations agricoles.

*(Quoique se référer à la valeur ajoutée ne fournisse qu'un résultat imparfait, sur la base de la répartition de cette valeur ajoutée produite en France par catégories d'entreprises -Grandes entreprises, ETI, PME, microentreprises-, et sachant que celles de < 50 personnes y contribuent pour près du tiers, le montant estimé pour ces dernières triplerait vers 3 milliards d'euros pour l'ensemble. L'estimation minimale ici retenue à deux milliards est plus basse, car notre étude a constaté que le ratio préjudice moyen/taille des entreprises diminuait à mesure du grandissement de leur taille. En d'autres termes, une petite entreprise supporte un impact (rapporté à chaque employé ou chaque euro de valeur ajoutée par elle) proportionnellement plus élevé qu'une grande. Une des causes avancées pour expliquer cette courbure est que les entreprises, à mesure de leur taille, se dotent de DSI puis de RSSI, et de dispositifs plus protecteurs face à des attaques standards. Ceci est un des motifs nous ayant conduit, en matière de coût des préjudices, à retenir prudemment un doublement du préju-*

*dice de celles de < 50 personnes plutôt qu'un triplement, comme plus proche de la réalité pour l'ensemble des entreprises. Doublement à considérer comme un plancher.*

Seraient à étudier plus complètement certains coûts externes cachés, indirectement provoqués chez autrui –au sein par exemple d'une chaîne logistique, ou chez la Sécurité sociale puisque le coût humain constaté sur le terrain s'avère non négligeable avec son lot de dépressions nerveuses et d'arrêts de travail chez certains employés ou cadres déstabilisés-. Enfin mériteraient d'être intégrés quelques coûts immatériels difficilement valorisables, par exemple sur la confiance des personnes envers l'outil informatique, capable de modifier les comportements (toutefois, face à une numérisation effrénée de nos environnements de travail, toute circonspection ou même attentisme ne sont pas obligatoirement négatifs. Le bilan du tout-numérique reste complexe à dresser, en ce qu'il revendique des gains de productivité à court terme mais prépare une invasibilité à plus long terme).

### ◊ Total annuel des rançons

Sur la même période 2016 à 2019 il a été calculé être d'une vingtaine de millions d'euros environ –mais glissant à l'époque vers une trentaine- sur notre secteur d'étude que sont les entreprises de moins de 50 employés. Le sentiment d'un doublement récent de la propension à acquitter des rançons aboutit en 2020 à redouter un plancher désormais de 40 millions d'euros.

Nous ne nous trouvons pas en capacité d'estimer le montant des rançons glanées auprès de plus grandes entreprises, où une opacité et même une omerta règnent plus fortement. La barre du million de dollars est attestée franchie pour divers dossiers à l'international, dont celui de la compagnie coréenne Nayana en 2017 ; la mutuelle d'assurance américaine FM Global parle à l'encontre des grandes entreprises d'une rançon moyenne de deux millions de dollars pour le rançongiciel Ryuk. Cependant, au vu de certaines exigences médiatisées par les protagonistes eux-mêmes et des importantes disponibilités financières de bien des multinationales, il suffirait qu'une seule grande entreprise ou institution consente sans publicité un gros versement –en dizaines de millions d'euros-, pour dépasser à elle seule l'addition de toutes les modestes rançons payées par les TPE-PME.

> Un tabou fait éviter d'évoquer les caisses noires de certaines entreprises, particulièrement utilisées pour gagner des contrats lors-

qu'elles sont actives sur les marchés internationaux, et que leur habituelle confidentialité érigerait en outil adéquat pour régler des rançons sans alarmer ni la presse ni les actionnaires. A titre d'étalon, une grande entreprise allemande a suite à un procès en 2007 reconnu l'existence d'un fonds secret s'élevant à 1,3 milliard d'euros. A l'aune d'une telle masse silencieuse, la vingtaine ou désormais quarantaine de millions versée en rançons par les petites entreprises françaises équivaut à … 3 % de la caisse noire de cette seule multinationale, qui ne serait qu'écornée par sa soustraction. Il y a tout lieu de penser que le rançonnage se subdivise en deux segments, l'un à demi-caché lorsqu'une entreprise ayant pignon sur rue verse une somme depuis sa caisse officielle vers un pirate hors-la-loi (via l'achat de cryptomonnaie), et qui pratique ainsi un noircissement d'argent[37] ; l'autre totalement en dehors de la loi lorsqu'un versement se fait depuis des caisses noires qui n'ont pas d'existence officielle vers un pirate également acteur de l'ombre ; l'argent est déjà noirci par avance, et il s'agit d'un transfert qui le maintient dans le noir[38]. Le volume du second segment est inconnaissable, sans qu'on puisse de manière péremptoire le qualifier de marginal.

Reste, pour minimum, sur la base de notre estimation actualisée de 40 millions par an pour les petites entreprises, que les sociétés françaises dans leur totalité transfèrent par rançon une masse monétaire considérée proche du seuil symbolique de la centaine de millions, sans exclure son franchissement.

37 Opération inverse au blanchiment d'argent : typiquement quand on fait disparaître une somme de toute comptabilité d'entreprise ; elle n'est plus enregistrée nulle part, hormis dans des paradis fiscaux ou thésaurisée dans des bas de laine. A ce titre, une cryptomonnaie n'est pas tout à fait une disparition d'argent en soi, c'est du « troc » de monnaie officielle telle que le dollar contre un cryptoactif visible par tous sur une blockchain –bloc de pages numériques immodifiables et consultables par des internautes- mais dont chaque détenteur est anonyme. Ici donc, qualifier de noircissement d'argent le versement de rançon est un raccourci mais partiellement impropre car on se contente d'échanger de la monnaie de jure (ayant cours légal ou cours forcé) contre de la monnaie de facto, puis d'échanger cette dernière contre une clé de déchiffrement, au profit d'un ou plusieurs tiers successifs qui tôt ou tard opéreront la manœuvre inverse, à moins que des biens et services soient directement achetables avec cette cryptomonnaie.

38 Un autre procès à la même époque, contre une multinationale de l'automobile à propos de sa caisse noire située en Suisse, rappelle que ces sommes se trouvent fréquemment hors du pays où l'entreprise a son siège.

La hausse récente des montants exigés par les pirates sera intéressante à scruter, pour comprendre si elle diminuera la propension à payer une rançon et peut-être le total versé, ou si elle augmentera ce dernier.

### ◊ Ratio préjudices/rançons

Dans les entreprises < 50 personnes, ces dégâts chez l'ensemble des victimes sont apparus être 35 fois le multiple du montant estimé des rançons versées au profit de pirates (Nb, ce ratio 1/35 ne signifie pas qu'une entreprise ayant versé une rançon a auparavant subi un préjudice 35 fois supérieur, puisque l'estimation du préjudice total proche d'un milliard d'euros par an englobe aussi les entreprises ayant refusé de céder. Mais ce ratio a son utilité pour le monde des assureurs, afin de rendre palpable la différence de surface de ces deux marchés que sont ceux des cyber-préjudices et des cyber-rançons. Ces dernières se réduisent à ce jour à une niche de petit format).

> *(Rien ne permet de conclure à une proportion stable, selon la taille des entreprises, entre préjudice et rançon. Le chaînage « valeur ajoutée-préjudice moyen-montant de rançon », pertinent dans l'esprit, subit trop de pondérations et d'influences externes, pour s'imposer comme la référence définitive. Ainsi, le paiement de rançon a été signalé comme davantage à relier à la trésorerie des entreprises –voir l'aparté précédent sur les caisses noires- : les petites payent lorsque leur trésorerie fond et laisse présager à terme un dépôt de bilan ; il n'est pas exclu au contraire que les grandes payent lorsque leur trésorerie est abondante au point de ne pas faire regretter une petite ponction financière moins gênante qu'un blocage informatique durable ; une hypothèse initiale serait donc celle d'une courbe en U, où les deux extrêmes –trésorerie basse ou abondante- inciteraient davantage à payer rançon.)*

Au sein de la sous-population des victimes consentant à payer, le ratio entre rançon et dégâts se révèle assez hétérogène. Une sensation est que ce qui les motive ne soit pas ce ratio entre rançon et dégâts subis donc déjà passés, mais entre rançon et dégâts à venir. En effet, de manière individualisée, on observe que souvent lorsqu'une petite entreprise paye,

- c'est qu'elle a épuisé une partie importante de sa trésorerie,

qu'elle parvient en limite de fragilisation

ce n'est donc pas le montant dans l'absolu des dégâts subis, mais celui-ci rapporté à la capacité de résistance de chaque victime.

- et qu'au-delà, les dégâts à venir suivraient une courbe exponentielle mortelle ce sont les futurs dégâts rapportés à cette même capacité de résistance.

En cela, la décision de payer est avant tout proportionnée aux faiblesses et faiblesses d'une entreprise, dont les niveaux variés de l'une à l'autre expliqueraient l'hétérogénéité de leurs attitudes.

## B- FAUX BESOINS ET VRAIS CHANTIERS

Notre étude fait ressortir :

**• à propos des paiements de rançons, un antagonisme et deux carences –celle d'un mécanisme compensateur et celle d'un mécanisme récupérateur-.**

### Un taux de récupération de l'argent versé infime

L'essentiel des flux qui parviennent à cette criminalité -envisagés voisins d'une centaine de millions d'euros au moins- ne donnant pas lieu de sa part à réinvestissement dans des équipements informatiques d'attaque, dont le coût de mise à niveau est négligeable au regard des sommes extorquées, le patrimoine des pirates –y compris leurs protecteurs, parrains, et leurs fournisseurs de moyens d'attaques- présente un caractère accumulatif fort qui le situe à un **volume capitalisé –un trésor de guerre- en centaines de millions d'euros** au moins, concernant la France et depuis l'apparition des cryptovirus ou autres bombes logiques. Cette masse financière laisse d'ailleurs envisager que la détectabilité de ces acteurs soit moins ardue sur le versant financier, lors des phases ultérieures de

blanchiment et de dépense[39], que sur le versant informatique aujourd'hui souvent bredouille dans sa chasse aux pirates ; attaquer le crime organisé au portefeuille avait été la tactique efficace retenue par le Préfet de Palerme Alberto Dalla Chiesa, relayé par la loi Rognoni-La Torre qui stipulait que les biens appartenant aux mafieux ainsi qu'à leurs parents ou partenaires ayant joué un rôle dans le dispositif criminel pouvaient être saisis). Aucune des entreprises rencontrées lors de l'étude n'a mentionné une identification ou une arrestation de l'auteur de leur piratage par cryptovirus ; sur notre échantillon et sur ce type d'agression, le taux d'élucidation est égal à zéro (trois dossiers d'indélicatesses impliquaient d'anciens employés ou stagiaires, mais sans recours au chiffrement de données. D'autres parmi nos dossiers, relatifs à de l'espionnage commercial ou à des attaques par déni de service, conduisaient à des concurrents).

**-> Le mécanisme récupérateur de l'argent reste en chantier.**

Cet état de fait se caractérise par un coût d'investissement faible pour le pirate et un « coût judiciaire » (amendes, condamnations en peine de temps ou d'argent) quasi-nul : r**entabilité brute du pirate ≈ rentabilité nette**. Peu de coûts, peu de risques. Le seul limitateur à l'expansion du « marché de l'extorsion » devient, outre bien sûr le nombre d'attaques réussies donc de victimes, leur propension à payer. Situation incongrue puisque la lutte contre l'essor de la criminalité y repose pour l'essentiel sur les épaules des seules victimes. Ces dernières sont le facteur premier qui influe sur l'évènement venant les frapper. Responsabilité en partie imméritée car ce poids qui pèse sur la victime résulte aussi de l'absentéisme ou de l'inefficacité relative des autres composantes de l'habituelle panoplie préventive ou répressive, tant sur les outils techniques que les outils juridiques[40].

39 Les cryptomonnaies les plus utilisées (BitCoin), malgré leur image d'anonymat des porteurs, sont des outils de traçabilité efficaces des flux. L'anonymat porte sur le détenteur d'un portefeuille, mais ces monnaies ont quant à elles des « identités » qui permettent de repérer leur revente ultérieure.

40 A souligner cependant plusieurs initiatives s'adressant aux victimes, tels que la plateforme Acyma (https://www.cybermalveillance.gouv.fr/) proposant aux entreprises des didacticiels, une aide à l'analyse de problème, etc. Le site nomoreransom.org fondé par Europol et la police des Pays-Bas met à disposition des outils téléchargeables de désinfection ou encore de déchiffrement (appuyés sur « un référentiel des clés et des applications qui permettent de déchiffrer les fichiers bloqués par différents types de rançongiciels »)

**Investir plus et investir mieux dans la sécurité publique**

Il est indubitable que la présence et la circulation dans l'économie de l'argent extorqué par les pirates internationaux, auraient apporté au Trésor public des recettes supérieures aux moyens judiciaires alloués parallèlement pour combattre et réduire cette criminalité (la seule TVA occasionnée par la rotation de cette monnaie dans les rouages économiques paraît d'emblée très au-dessus des allocations budgétaires aux acteurs judiciaires concernés –y compris police et gendarmerie-). La question s'affine par une approche marginale, sur les moyens allouables : octroyer un euro supplémentaire à l'action judiciaire contre les cryptovirus drainera-t-il au moins un euro supplémentaire au Trésor, dans une logique autofinancée ? Il est vraisemblable que la France soit sur ce point en sous-investissement non seulement au regard des besoins et de sa mission régalienne, mais également au regard de la rentabilité latente de tels investissements sécuritaires qui rapporteraient comptablement davantage à la Direction des impôts qu'ils ne coûteraient. Leur Valeur Actuelle Nette serait à calculer plus en détail, sur l'hypothèse crédible que leur Taux de rentabilité interne soit supérieur à bien des projets actuellement financés par le denier public.

Un bémol d'ordre technologique perdure cependant, qui demandera si en l'état de porosité et de vulnérabilité des systèmes d'information et de communication aujourd'hui déployés dans le public, un surcroît de moyens d'investigation apporterait ou non une quelconque amélioration au faible niveau d'affaires judiciaires résolues (Pour en sourire, doubler des moyens qui n'obtiennent guère de résultats ne se traduira-t-il pas par 2 x 0 ?).

Le type d'adaptation requis demandera un saut qualitatif (organisationnel …) et non pas seulement quantitatif, afin de faire évoluer favorablement le rapport de force engagé avec les milieux criminels.

## Ce que coûtent et économisent les rançons

Les observations faites auprès de petites entreprises victimes montrent que, par principe ou par crainte, elles sont réticentes à acquitter une rançon, même inférieure à l'économie de préjudice qu'elles en attendent, tant que cette économie n'équivaut pas à un

multiple de la rançon. En cela, ces petites entreprises peuvent être qualifiées d'acteurs globalement vertueux, qui pour la plupart ne consentent à payer que sous contrainte forte. Malgré l'imprécision de ce repère qu'est le multiple économie générée/rançon versée, il éclaire le fait que la richesse « sauvée » par les victimes lorsqu'elles versent des volumes présentement en dizaines de millions d'euros annuelles, se situe vraisemblablement en centaines de millions d'euros.

Comparés aux préjudices advenus –non pas ceux évités- mesurés par notre étude à un plancher d'un milliard d'euros par an pour les entreprises < 50 employés, et au moins le double pour l'ensemble des impacts en entreprises, « l'économie » obtenue par les versements de rançons apparaît conséquente, tout au moins de prime abord : s'il est incertain que, sans rançon, le total des préjudices doublerait, tout au moins se révèle-t-il équivaloir une hausse de plusieurs dizaines de pourcents, soit pour les entreprises < 50 employés, plusieurs centaines d'euros « économisés » annuellement ; bien au-dessus de ce que captent les rançons. L'imprécision de tels chiffrages, notamment sur les grandes entreprises où les ratios sont probablement différents, fournit toutefois des ordres de grandeur qui aident à situer l'enjeu. Le débat n'est pas uniquement moral mais pécuniaire, puisqu'il met en balance la rentabilité comparée des deux options de payer la rançon ou pas.

Il sera analysé (**3ème partie**) si cette précédente « richesse sauvée » l'est vraiment ou si cette captation se voit simplement repoussée à dates ultérieures ; ce, de par un conflit d'intérêt à propos des rançons, entre leur rentabilité individuelle à court terme –en faveur de la victime qui s'exonère ainsi d'un lourd préjudice informatique personnel-, mais une déperdition économique collective à plus long terme. De fait, l'attaquant recommencera en étant plus riche et peu à peu dominateur dans son rapport de force, mieux instrumenté, plus aguerri dans ses chantages (il aura appris les points faibles de ses précédentes cibles) et plus nombreux puisque ses succès suscitent des émules. Il sera davantage préjudiciable à davantage de victimes.

Raisonner en faveur du court terme s'appliquerait à un sacrifice aux dieux venant stopper miraculeusement sur l'instant un orage ou une inondation, mais il perd de sa substance dès lors que le paiement renforce la soif des dieux et la probabilité de réédition de l'évènement. Car il aggrave pour demain un problème, en le résolvant pour aujourd'hui. Le plaidoyer apparaît par conséquent vrai à court terme

mais faux à long terme, ou, pour le formuler dans sa gradualité, il sera de moins en moins vrai avec le temps ; seul le premier paiement est pleinement rentable, mais chacun d'eux rognera la rentabilité du suivant … Formulé autrement, chaque paiement consenti par vous bénéficie d'un crédit que paiera votre successeur, à l'image des dettes qu'une génération laisse à ses enfants.

> La victime qui paye une rançon a une responsabilité –une dette qui n'est pas que morale- envers la collectivité, laquelle en supportera des conséquences ultérieures. Payer s'apparente à « refiler la patate chaude » à autrui, pour le prix au rabais d'une rançon. Quiconque paye bénéficie d'une remise immédiate sur son malheur personnel, d'une ristourne accordée par le pirate ; mais à l'échelle cette fois de la communauté ne s'agit-il que d'escompte obtenu, puisqu'elle finira par devoir payer au terme de ce compte à rebours.
>
> La collectivité a inversement une dette envers toute victime qui ne paye pas la rançon malgré un préjudice à venir supérieur (si elle avait payé, elle aurait subi un préjudice total x. Si elle ne la paye pas malgré qu'elle subisse au total un préjudice supérieur X, son refus lui coûte X – x, abnégation dont profitera la collectivité à long terme). Un malentendu mérite d'être levé : une assurance cyber, bien qu'elle rembourse effectivement une partie dudit préjudice –plafonné et assorti d'une franchise-, n'est pas véritablement ce mécanisme compensateur par lequel la collectivité assumerait tout ou partie du surcoût X – x, car ce que versera l'assureur est un dû à la victime du fait qu'indépendamment elle a par avance cotisé au pot commun, elle a acquitté sa prime d'assurance[41] avec de l'argent sorti de sa poche ; la collectivité ne consent pour l'occasion aucun effort additionnel de remerciement et de compensation. Il en ressort qu'une passerelle manque, entre la collectivité et la victime, et surtout entre le long terme et le court terme (en fait le très court terme, puisqu'une rançon propose une « solution » à l'horizon de quelques heures ou quelques jours, délai précieux par sa brièveté, elle-même ardue à compenser avec un remboursement qui vous sera versé

41 L'arbitrage voulant que chaque rançon payée économise sur l'instant à la victime des préjudices supplémentaires, est applicable à l'assureur si une assurance contre les attaques informatique a été souscrite : ne sera-t-il pas enclin à favoriser son intérêt à court terme, en voyant qu'il aura moins de dégâts à prendre en charge si son client verse la rançon ? Inversement, à l'échelle de la collectivité des assureurs et sur le long terme, l'intérêt de ne pas payer redevient prédominant.

au mieux dans plusieurs mois. Paraphrasant mais inversant Benjamin Franklin, le temps n'est pas de l'argent : le temps présent n'équivaut pas sa valeur en argent futur si vous êtes mort dans l'intervalle). Une rançon propose d'économiser du temps + de l'argent. Sur le court terme si précieux, « la proposition de valeur » formulée par le pirate ne trouve pas encore de contrepoids curateur efficace, dès que les préjudices s'annoncent très élevés et irréparables.

**-> Le mécanisme compensateur reste en chantier.**

**• A propos des assurances sur le paiement de rançon (qui remboursent la rançon versée), leur relative inutilité économique et une dangerosité :**

L'existence d'une assurance contre le rançonnage après une attaque par cryptovirus, ne répond pas à une demande manifeste, tout au moins des petites entreprises rencontrées lors de l'étude, pour deux raisons principales :

- La majorité des rançons contre les petites entreprises sont d'un montant objectivement modeste, qui peinerait à les motiver d'être assurées.

- Contrairement à un évènement tel que climatique, frappant aveuglément et sans dosage de son amplitude, l'adaptativité qui guide un actuel pirate le fait se calquer généralement sur les capacités financières supposées de la victime (nous n'avons pas connaissance de rançon en France contre des petites entreprises, qui ne serait pas au final d'un montant acquittable par la victime. Sans généraliser à l'ensemble des faits puisque des cas d'enchères montantes existent çà et là, plusieurs interviewés ont rapporté des négociations pirate-victime ayant abouti au bout de plusieurs jours ou semaines à des baisses d'exigence, s'agissant de petites entreprises aux ressources effectivement limitées). Hors exceptions rares à ce jour, il n'y a pas de menace létale par rançon ruineuse. Ce sont les cyber-préjudices directs subis par les TPE et PME qui présentent parfois une capacité à les tuer, non pas le montant des rançons demandées.

La formulation paradoxale qui en résulte pour toute proposition d'assurance-rançon équivaudra à demander si vous souhaitez vous assurer contre un aléa ; mais aléa que vous êtes par

avance certain de pouvoir assumer financièrement seul.

- En prolongement, un danger existe, que l'arrivée d'un filet de sécurité assurantiel soit haussière sur les tarifs de rançon exigés, en poussant ces demandes à se conformer au maximum obtenable de la victime et désormais de son assureur.

- Un deuxième danger serait une élévation de la propension à payer, chez les victimes désormais assurées et plus indifférentes à ce débours (ou à sa variante que serait en amont une moindre propension à sécuriser son informatique, de la part de celui qui accepte par avance l'échappatoire du paiement de rançon).

- Une menace plus globale résidera dans l'habituation à l'acte de payer (diminution de le regarder comme une transgression sociale). Et parallèlement pour le pirate dans la banalisation de se voir payé, avec ses effets incitateurs d'accroissement des montants exigés et de la fréquence des rançonnages. Habituation accrue à payer les rançons déjà palpable à ce jour, d'après ce qui ressort de nos interviews menées au fil des années, où la barrière psychologique initiale s'atténue peu à peu, laissant place à un sentiment d'amoralité –non pas immoralité- de l'acte de payer.

  Si la *réticence à payer* diminue, la r*éticence à payer toujours un peu plus* diminuera probablement ensuite (les bons camelots utilisent l'expression « briser la glace » lorsqu'ils commencent par vous vendre un premier bibelot à prix bradé, pour vous mettre en confiance, avant de vous entraîner ensuite vers d'autres achats plus onéreux. Les montants imposés par les pirates depuis plusieurs années sont assimilables à des posologies d'accoutumance, avant de profiter peut-être des nouveaux réflexes acquis par les victimes pour augmenter les tarifs).

- Enfin, vue en **première partie**, une présomption plus difficile à mesurer s'inquiétera d'un aiguillon, où l'existence en soi d'une assurance incite à la frauder, avec de fausses-vraies attaques et rançons alléchées par la perspective d'être remboursé : le profil particulier d'une garantie qui consiste à rembourser non pas le coût d'un dégât (usine incendiée ou inondée) mais l'achat d'un non-dégât (à savoir le montant de la rançon pour garder l'usine en fonctionnement) ne s'en remet qu'à la fin vérifiable d'un évènement (cessation du chiffrement de données) dont lorigine

restera invérifiable (impossibilité de sonder la réalité ou non d'un pirate anonyme) ; en guise de synthèse s'agit-il d'acheter un non-dégât sans vérifiabilité autre que l'effectivité du non-dégât. Faute d'audit possible sur le maillon originel de la chaîne d'évènements –maillon clé-, la confiance aveugle risque d'être l'alpha et l'oméga d'un tel marché assurantiel.

# PREMIERE PARTIE

# Faut-il autoriser les assurances sur les paiements de rançons et les prêts bancaires aux rançonnés ?

## A – FAUT-IL LAISSER ASSURER LE PAIEMENT DES RANCONS ? Du « Connaissez votre victime » au « Connaissez son assureur »

« Je n'insisterai jamais assez pour dire à quel point [la cyber-assurance] a sauvé notre collectivité. »

Le chef de la police municipale de la ville de Valdez, Alaska, frappée en 2018 par un virus et ayant en accord avec son assureur versé une rançon de 4 bitcoins soit 26 624 dollars-[42]

Un constat préalable est la nette différence contre les grandes entreprises, notamment :

- Deux formes différentes de rançon. Les montants des rançons contre les TPE PME sont formatés de manière assez standardisée, et se terminent souvent à quelques milliers d'euros (dans nos contacts, les cas dépassant la dizaine de milliers d'euros sont minoritaires, quoiqu'en croissance). A contrario les grandes entreprises risquent de recevoir des montants plus individualisés, et alignés sur leur capacité haute à payer. Pour recourir à une image simplificatrice, se trouve d'un côté un marché des entreprises « pauvres » ou « modestes » subissant des attaques souvent automatisées (du prêt-à-porter) avec de petites rançons (unitaires et par leur total), et de l'autre *un marché des entreprises riches ou tout au moins grandes*, avec des attaques davan-

42 Bart Hinkle. D'après Edge Editors : « *15% of Ransomware Victims Paid Ransom in 2019, Quadrupling 2018* »), qui ajoute « Une note plus gaie est que davantage d'entreprises paieront des rançons car elles ont des assureurs pour les aider à supporter le coût de tels paiements. »

tage sur-mesure y compris sur le montant de la rançon.

Le « marché » visé par les pirates est segmenté en deux créneaux.

Le prêt à porter se structure autour de prix assez standardisés, éventuellement pondérés par ce que le pirate pressent être la taille et la fortune de la victime, par exemple si celui-ci lui paraît être une SSII plutôt qu'un cordonnier de quartier –« à la tête du client », ou selon ce que laisse interpréter sa marque, son nom de domaine, le pays ou la zone où il est situé, son statut de SA ou Sarl, etc.-. Le standard a longtemps oscillé autour de 2 à 3 000 dollars ou euros, payables en cryptomonnaie.

Rappelons le grand ressort des dispositifs d'assurance : j'ai une probabilité sur x de tomber de cette échelle cette année ou de subir un incendie, et je désire que ce coût jusqu'à lors individuel devienne davantage prévisible en se rapprochant du coût moyen pour tous, c'est-à-dire en le mêlant aux coûts du plus grand nombre, de la collectivité. Or ici coexistent deux types de coûts « moyens » puisque les rançongiciels se divisent sur deux types de tarification :

un prix moyen destiné au grand public indifférencié, pour lequel l'écart-type est faible. Cette moyenne devient en soi une information utile car la connaître aide un entrepreneur à anticiper ce qu'il paierait probablement ;

un prix personnalisé dès lors que vous êtes identifiable et riche. La moyenne de ces prix est une information de faible intérêt, du fait de la forte dispersion des données autour de cette moyenne (écart-type important).

Les pirates informatiques renversent à leur avantage l'actuelle propension des assureurs qui proposent à leur clientèle d'individualiser ses tarifs en la connaissant toujours mieux, le fameux KYC, ou ici le KYV : *know your victim*, connaissez votre victime pour lui proposer une rançon proportionnée à sa capacité de payer, à la valeur de ses biens, au montant du préjudice que vous pouvez lui causer, etc.

- Deux seuils déclencheurs de paiement différents. Des situations très disparates prévalent quant au seuil à partir duquel les victimes se décident au paiement de rançon. Dans la majorité des petites entreprises rencontrées, le choix de payer survient non seulement quand le coût à venir devient un multiple du

montant exigé, mais surtout quand ce futur coût met en péril l'entreprise, la faisant entrer dans une *zone mortelle*. Tandis que dans les grandes entreprises, quoique les témoignages directs aient été plus rares, les échos recueillis placent l'acceptation plutôt dans ce qui est nommable *zone d'inconfort*, lorsque la nuisance comptable ou à l'image de marque -la notoriété- est jugée suffisamment gênante au regard des objectifs de l'entreprise . Non plus donc lorsque l'impact risque de bientôt dépasser la capacité financière de la victime (sa capacité à encaisser un coup) comme chez les TPE, mais lorsque simplement il obère la rentabilité attendue de l'entreprise. Certains sondages aux Etats-Unis ont dès les premières années de la vague des rançongiciels fait ressortir que les deux tiers des responsables d'entreprises interrogés seraient ouverts à verser la rançon ; pourcentage qui se confirmait chez ceux ayant été déjà victime. Dans un idéal-type de très grande entreprise, à moduler au cas par cas, payer relève davantage d'un arbitrage froid avantage/désavantage, où a contrario une partie des réticences à payer tient compte aussi du risque d'écorner l'image de l'entreprise si l'information de ce tribut versé devenait publique : l'arbitrage se fait entre deux sources de nuisance à l'image (effet contreproductif d'être piraté de manière publique versus effet contreproductif d'accepter publiquement de payer un racketteur).

- <u>Une inégalité devant la mort.</u> Une dissymétrie existe, quant à leur exposition respective à un dépôt de bilan : l'argent en trésorerie pour affronter un coup dur sur quelques semaines ou quelques mois diffère, d'autant qu'une grande entreprise trouvera un appui bancaire ou via les marchés financiers[43]. De même dispose-t-elle souvent d'une puissance de négociation pour des facilités accordées par ses créanciers ou fournisseurs. Quoique des échéances de remboursement de gros emprunts ponctuent la vie des grandes entreprises, elles se sont beaucoup préoccupées d'augmenter leur solidité comptable après la crise de 2008 à la suite de laquelle elles ont privilégié la reconstitution d'un

43 Une autre discrimination risque de naître cette fois entre entreprises bien notées, mal notées ou pas notées par les agences de notation, quant à la prise en compte du risque cyber dans leur stratégie et leur réputation : « les entreprises seront de plus en plus challengées sur les impacts des risques (envers …) leur capacité de crédit ». Or « Le risque cyber est difficile à prendre en compte par les agences de notation. Il présente un risque de cumul certain qui est difficile à appréhender ». In Philippe Cotelle, Philippe Wolf, Bénédicte Suzan : « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance ». IRT SystemX. 2017.

matelas financier, aujourd'hui bienvenu face aux aléas informatiques. Au contraire, une TPE doit d'abord compter sur ses réserves propres, souvent modestes et équivalentes à quelques semaines de dépenses au rythme normal (dont une part importante n'est pas aisément reportable : factures d'électricité, impôts, charges sociales, etc.).

- Une inégalité devant la solitude. L'isolement des grandes entreprises est moins opprimant que pour leurs petites consœurs, que l'étude a constaté être sans relais souvent auprès des autorités publiques locales –préfet, procureur, enquêteurs de police …- ou privées. Certains cas ont révélé l'ampleur parfois caricaturale d'un tel décalage, où, sur une même affaire, la petite entreprise victime directe d'une attaque s'est trouvée nettement moins informée de la progression de l'enquête judiciaire, que ne l'a été simultanément une grande entreprise seulement victime collatérale de la même attaque.

Grandes et petites entreprises s'avèrent être deux profils distincts face aux cryptovirus, qui méritent une analyse et un mode de soutien différenciés.

## 1 - Le cas des petites entreprises attaquées

Les estimations issues de notre étude sont, pour les petites entreprises de moins de 50 personnes, d'une probabilité d'être affectées par un cryptovirus de l'ordre de 4 à 5 % par an[44], c'est-à-dire environ une « chance » sur vingt. Une minorité parmi ces victimes -qui d'après nos observations néanmoins fragmentaires et sur un échantillon limité, approchait grossièrement le dixième sur la période 2017-2018- accepte de verser une rançon. D'autre part les niveaux de rançons demandées, s'ils oscillent entre 600 et 20 000 dollars ou euros au sein de notre échantillon, se concentrent pour beaucoup d'entre eux typiquement dans une tranche entre 2 et 3 000 dollars ou euros (pour la période 2017-2018).

Il en ressortait un total de rançons versées par ces petites entreprises de l'ordre d'une vingtaine de millions d'euros par an, toujours sur la période 2017-2018, avec plus probablement pour 2020 un plancher

44 Notre précédent livret « Les cyberattaques et leurs préjudices dans les entreprises » (p. 47 et suivantes) délimitait une fourchette de probabilités pouvant montant jusqu'à 4,5 %, avec une moyenne autour de 3 %. Depuis lors, les contacts avec des victimes ont renforcé la crédibilité de l'estimation haute aux alentours de 4 à 5 %, ici retenue.

de 40 millions. Sachant que ces petites structures représentent 3,7 millions d'entités en France (exploitations agricoles non comprises), ces montants équivalent à une moyenne arrondie de 10 euros par an et par entreprise. Soit presque un euro par mois et par entreprise française.

Ayons ainsi à l'esprit cinq grandeurs arrondies :

- Une rançon type (dans sa version standard à bas prix) : 3 000 euros

- Un volume total de ces rançons standard à bas prix pour la France : 40 millions d'euros (2020)

- Le nombre de petites entreprises < 50 personnes en France : près de 4 millions

- Le nombre estimé d'entreprises < 50 personnes frappées par des cryptovirus : 180 000

- Le nombre approximatif d'entreprises < 50 personnes versant une rançon : ≥ 20 000 par an

Le montant standard de la rançon, assez bas, est peu à même de motiver les victimes à se couvrir par une assurance sur le paiement de rançon. L'assureur à son tour, connaissant la probabilité de survenance d'un tel cryptovirus, de l'ordre d'une entreprise sur vingt annuellement, pondérée par le fait qu'une minorité des victimes – plus de 10 % désormais- accepte de verser une rançon, aboutirait à une prime d'assurance – hors marge de l'assureur et frais, etc.- d'une quinzaine d'euros par an (2018). Chiffre atténué par l'existence de franchise (tout n'étant pas pris en charge), et par le fait qu'un nombre étonnamment élevé de petits patrons ne remplissent pas leur dossier en cas de tel petit sinistre, par aversion pour ces travaux administratifs supplémentaires mais aussi car ils ne sont pas certains qu'un éventuel audit de leur système de sécurité par l'assureur ne soulignerait pas des points de faiblesse les rendant fautifs (Beaucoup de petits patrons hésiteront à s'engager dans cette voie assurantielle, d'autant que la présence de la franchise ne leur permettrait pas d'espérer tout récupérer).

*Une interrogation initiale -hors aspect de légalité et d'acceptabilité morale- se trouve introduite à propos des assurances proposant d'indemniser le paiement de rançons : peut-il y avoir autonomie commerciale d'une assurance lorsqu'elle brasse -hors frais- environ un*

*euro par client par mois (et ce mini-marché sera-t-il le champ d'une réelle compétition ?), ou n'est-elle pas vouée en l'état à constituer la sous-partie accessoire d'une offre plus large ?*

## Un dilemme débouchant sur un pari

Une « proposition de valeur » à un petit patron s'exprimerait de la sorte : sachant que vous avez une probabilité sur 200 (de manière décomposée et arrondie, 1/20 de subir une attaque réussie x 1/10 de verser alors une rançon) de payer une rançon cette année, et sachant que cette rançon sera de 3 000 euros, accepteriez-vous la certitude de payer une prime de 15 euros (+ frais de l'assureur) afin d'avoir 1/200 probabilité d'être remboursé de 3 000 euros (- franchise, etc.) ?

> … Où il s'avère par ailleurs, et comme pour la plupart des petits rackets et autres *pizzos*, que la quasi-certitude en cas de cryptovirus de se voir demander une rançon d'un montant assez standardisé octroie à cette dernière les vertus d'une assurance *a posteriori* (d'un tarif forfaitaire de 3 000 euros), qui ravale celle de l'assureur officiel au rang de solution acceptée *ex ante* à l'attaque virale, et destinée à rembourser la solution acceptée *ex post* (celle du rançonneur). De la sorte serions-nous en présence d'une assurance légale sur l'assurance illégale.

Il est assez vraisemblable que ce petit patron, qui en cas de rançon aurait toute latitude de débourser cette somme de 3 000 euros sur ses fonds personnels, préférera parier sur l'espoir au demeurant élevé car de 99,5 %, d'économiser 15 euros (+ frais). S'il perd *son pari*, un tel versement de rançon libérateur sera, dans l'esprit de la victime, simplement passé par pertes et profits, comptablement et intellectuellement, lui permettant d'éviter beaucoup de paperasse. Elle ne se départira pas du quotidien d'un entrepreneur exposé aux aléas de taille gérable.

Le dilemme n'est pas d'essence comptable puisque l'équation respecte un équilibre neutre où

*coût de l' assurance rançon=(coût de la rançon)/(fréquence de la rançon)*

mais elle renvoie à la perception psychologique qu'en aura le décideur, à ses aversions (son aversion au risque, mais aussi aversion

aux pressions émanant d'un racketteur, ou parfois aversion aux insistances commerciales émanant d'un vendeur de sécurité, aversion à remplir des formulaires pour s'assurer ou pour porter plainte, etc.).

Deux critères semblent prépondérants dans la réaction de nombreuses victimes : le **niveau d'incertitude** auquel elles font face, et le **niveau de risque** qu'elles courent (risque d'attaque et de préjudice, mais par-dessus tout leur traduction par exemple en dépôt de bilan : le niveau de risque n'est pas le niveau du choc dans l'absolu mais le niveau de ses conséquences pour moi, il est relatif. Ce qui compte pour l'entrepreneur n'est pas la grandeur globale de l'attaque –de type Echelle de Richter-, mais la grandeur de son impact individualisé).

## La pluralité des formes de certitudes

> « En réduisant l'incertitude entre le coût psychologique et le coût mathématique, l'assurance r**emplace l'incertitude** que constitue ce risque psychologique p**ar une perte certaine limitée** à la probabilité mathématique du sinistre. » [45]

L'aversion au risque de cet entrepreneur s'exprime tout d'abord différemment selon le **type et le niveau d'incertitude**, à chaque fois spécifique à une menace :

- Incertitude élevée : son aversion opèrerait pleinement face à la menace potentiellement mortelle d'une absence de demande de rançons, suite à un chiffrement effectué sur ses données (il ignore si un pirate viendra lui proposer une solution salvatrice. Ses données risquant sinon de rester définitivement chiffrées, avec un coût maximal) ;

- Incertitude moyenne : elle opérerait dans une moindre mesure si des doutes subsistaient sur le montant d'une future demande de rançon quant à elle sûre (la victime anticipe qu'un pirate viendra à coup sûr lui proposer une solution salvatrice, mais d'un prix encore inconnu. L'incertitude est réduite) ;

- Incertitude basse ou nulle : enfin elle opèrera peu s'il y a certitude quant à la réception d'une demande de rançon elle-même de montant déjà répertorié et su aisément mobilisable

45 Irving Fisher, *Nature of capital and income*, 1906.

par la victime.

Un calcul de l'utilité espérée perd de sa substance, lorsque ne subsiste qu'une petite incertitude, en l'occurrence ici votre probabilité personnelle d'être touché par un cryptovirus (probabilité toutefois assez bien circonscrite dès lors qu'on parvient à la situer en moyenne entre 4 et 5 % par an) : en conséquence, le système actuel des rançons envers les petites entreprises se caractérise par une incertitude faible : probabilité d'occurrence assez bien cernée, quasi-certitude d'une demande de rançon à suivre, visibilité « honorable » sur le futur montant type de la rançon.

Beaucoup de petits patrons hésiteront donc à s'engager dans la voie assurantielle, qui ne peut se poser en alternative à une incertitude globale elle-même faible, et qui apporte simplement la certitude d'être remboursé sur une sous-partie du préjudice. Ils seront d'autant plus hésitants que la présence d'une franchise ne leur laisserait pas espérer tout récupérer (la certitude est aussi celle de n'être pas complétement remboursé) ; à laquelle ajouter un possible audit après-coup du niveau de sécurité effectif de son système d'information, susceptible de conclure à sa faute (… la certitude d'être remboursé s'estompe).

## Entre fiabilité de l'information et rétention d'information

> « La certitude d'être remboursé du dommage est de la sécurité. Fabriquer de la sécurité, c'est donner aux intéressés la certitude d'être intégralement indemnisés de leurs dommages. » [46]

Néanmoins deux cas de figure notables inciteraient un patron à déroger à ce probable réflexe de ne pas souscrire une police d'assurance :

- Que sa sécurité informatique soit faible au point que sa probabilité personnelle d'être rançonné en devienne supérieure à 1/20 (ou que sa propension personnelle à payer soit forte). Auquel cas l'assureur glanera d'abord une clientèle de mauvaise qualité pour lui.

Autant un niveau qualitatif de sécurité informatique est auditable, autant une propension personnelle intime à payer une rançon l'est difficilement. Une asymétrie d'information survient en ce que l'as-

46 Gabriel Cheneaux de Leyritz : « Les cours du droit » (Assurances), 1957.

suré se connaît un caractère à payer, tempérament indétectable par l'assureur. De telles personnes auront davantage intérêt à s'assurer ; elles se savent enclines à cette dépense. (Problème « d'anti-sélection », tel que formalisé par G. Akerlof, qui incitera qui-sait l'assureur à, par prudence, traiter tout prochain client comme ayant cette tendance forte à payer, donc lui fera une offre tarifaire intégrant ce coût, laquelle en retour découragera un client de s'assurer lorsqu'il a une propension faible à payer).

D'autre part, une possible conséquence d'une assurance serait une propension extensible à payer la rançon –solution de facilité pour la victime- même si les préjudices du chiffrement de données sont faibles mais désagréables à gérer pour lui : je préfère payer une rançon de 1 000 qui me sera remboursée puisque l'assureur en aura été témoin, pour éviter un préjudice interne de 900 que mon assureur me demanderait de justifier (le fait que ces deux dépenses subissent une franchise ne modifie pas le fond du raisonnement).

- Que le montant de la rançon soit plus erratique et en devienne imprévisible, auquel cas le but du petit patron sera de se couvrir contre d'éventuelles rançons moins proches de leur moyenne ou de leur médiane (l'écart type augmentant alors). Rappelons en effet l'un des motifs du réflexe de s'assurer : bien sûr se garantir contre la survenue d'un évènement, mais plus encore palier à l'incertitude sur son montant (lorsque l'écart-type est grand à l'extrême) ; incertitude préoccupante et qui s'apparente à une épée de Damoclès pour chaque victime potentielle. Or si comme aujourd'hui le montant de la rançon est standardisé, connaissable par avance, et d'un montant accessible pour l'épargne ou l'encaisse habituelles d'un entrepreneur, le motif de se prémunir contre cette pseudo incertitude s'atténue.

Les entretiens menés avec les victimes soulignent que leur besoin de lever des incertitudes se préoccupe de deux priorités : la crainte en cas de paiement que le pirate ne livre pas la clé de déchiffrement promise, et accessoirement la probabilité que la clé reçue ne fonctionne pas comme attendu (Les victimes rencontrées n'envisagent pas spontanément que le montant exigé des rançons soit au-dessus de leurs capacités). Deux aspects où d'ailleurs l'intérêt d'un pirate est d'apporter des apaisements à sa chalandise, pour conforter l'acceptation de payer. Son fonds de commerce consiste à fournir des certitudes, alors qu'un assureur classique propose ici de palier aux incertitudes

; ils sont à ce stade sur un mode non-coopératif, mais dans un séquencement où le pirate aura de manière avantagée le droit de jouer d'abord (tout comme aux échecs les blancs jouent le premier coup de la partie).

## Jeux coopératifs et non-coopératifs

Un paradoxe réside dans ce constat, d'une rançon type d'un montant trop sage pour motiver sa couverture assurantielle. Il est vraisemblable qu'il n'y ait aujourd'hui guère de marché de l'assurance (s'agissant des petites et moyennes entreprises), pour un préjudice qui présente ce profil statistique, avec un débours normalisé, relativement faible et prévisible.

En d'autres termes, le décollage d'un marché de l'assurance sur les rançons irait de pair avec

- Soit l'accentuation de la virulence de ces dernières, en fréquence ou en montant demandé.

- Soit l'accentuation de leur imprévisibilité (de la fréquence ou du montant).

Or proposer de couvrir de tels risques accentués n'est rien moins qu'une incitation à leur survenance : si le pirate apprend que sa victime sera soutenue à acquitter des montants plus élevés ou plus erratiques, car remboursés, l'adaptation de ses exigences à la hausse sera une conséquence plausible.

Paradoxalement, les pirates ne demandent pas assez d'argent pour motiver l'émergence d'une demande de couverture assurantielle de la rançon. Le point de rencontre entre ces divers acteurs se placerait au-dessus des petites rançons actuelles.

Là se situe un danger de convergence tacite entre deux acteurs, le premier étant l'assureur de rançons, qui trouverait des clients grâce à une accentuation de l'agressivité des rançonnages, à leur enchérissement reportable tarifairement sur ce même client de plus en plus inquiet de sa sécurité ; le deuxième étant le pirate, qui trouverait double profit à exiger d'avantage tout en maintenant voire augmentant la propension de sa victime à payer (Situation ubuesque, qui déroge au schéma d'un Adam Smith, d'une offre et d'une demande en confrontation opposée puis trouvant leur équilibre ; car ici au contraire deux protagonistes partagent un commun intérêt à

une inflation sur la mise d'un jeu -au sens où il relève davantage de la théorie des jeux que du schéma des Classiques. La présente situation relève en partie d'un *jeu coopératif*-).

Peut-être d'ailleurs le tiers acteur qu'est la victime croirait-il également trouver son compte dans ce jeu, par un montant plus élevé mais davantage remboursé ; bénéfice en trompe l'œil puisque le remboursement, dans son principe même de mutualiser le coût du risque, ne fait que recycler au profit de l'un –une victime-, les primes versées par tous –les assurés en général-. Auquel cas la convergence d'intérêt réunit trois acteurs au détriment de la collectivité.

Préférence pour la sécurité ou pour l'insécurité, en situation de quasi-certitude

Que la plupart des petits entrepreneurs ne soient pas en demande d'une assurance-rançon s'interprétera comme un processus intellectuel structuré autour de deux choix successifs :

1er choix pour décider de s'assurer ou non contre le versement de rançon[47] (« 1ère partie du jeu » où une entreprise « joue » à l'informatique avec ses risques ; si elle n'est pas assurée, elle gagne lorsqu'elle n'est pas amenée à verser de rançon, elle perd si elle la paie[48]), avec chez les chefs d'entreprises une fréquente préférence pour l'insécurité au voisinage de la certitude, tout au moins tant que cette insécurité ne sera pas coûteuse si elle se concrétise (ici, typiquement 3 000 euros) : les petites entreprises choisissent souvent l'insécurité toute relative de ne pas s'assurer. De fait, la probabilité de devoir payer une rançon –puis d'en demander le remboursement par l'assurance- est faible, égale à 1/200 environ par an ; il y a quasi-certitude (199/200) de ne pas avoir à payer de rançon au vu de l'actuel décompte des attaques par cryptovirus.

47 Si elle est assurée, le jeu revient à miser une prime annuelle supérieure à une quinzaine d'euros, pour avoir une chance sur 200 de toucher le remboursement de 3 000 euros (moins la franchise, et avec pour phénomène perturbateur que votre propension à payer la rançon augmentera probablement si vous êtes assuré contre cet aléas).

48 Soit qu'elle ne subisse aucun cryptovirus avec demande, soit qu'elle en subisse un mais ne verse pas de rançon.

2ème choix (« Partie du jeu » où une entreprise « joue » à payer la rançon = sa mise au jeu ; elle gagne si elle reçoit ensuite la clé de déchiffrement ; elle perd dans le cas inverse[49]) pour décider de verser ou non la rançon. Les témoignages recueillis durant notre étude ont confirmé que lorsque la victime paye la rançon, la probabilité de ne pas obtenir de clé de déchiffrement est tout à fait faible : il y a quasi-certitude de « gain » à ce « jeu », néanmoins les dialogues noués lors de l'étude avec des victimes confrontées à un choix de payer ou pas, montrent que leur question centrale tourne autour de l'inquiétude persistante de ne pas obtenir la clé après paiement (objectivement, il y a quasi-certitude de recevoir la clé, mais psychologiquement la peur demeure tant que la clé n'a pas été reçue et testée). Le fait qu'il y ait seulement quasi-certitude mais non pas certitude, laissant un doute résiduel, soucie considérablement ceux placés en situation de choisir ; souci qui souligne leur préférence inassouvie pour la sécurité sur ce point où le coût de l'échec au « jeu » serait élevé pour eux. Pareil cas de figure rejoint le Paradoxe d'Allais avec une préférence pour la sécurité au voisinage de la certitude : Maurice Allais conçoit un joueur devant miser avec une quasi-certitude de gain, mais où le doute résiduel de perdre s'avère psychologiquement mal supporté pour ce décideur. Si lors d'une loterie j'ai 99 % de probabilités de gain, donc une seule chance sur cent de perdre le million du gros lot, souvent ma préférence ira pour me contenter par exemple de 970 000 mais enfin assortie d'une probabilité de gagner de 100 %. L'élimination du 1 % de doute me coûte 3 % du gros lot, mais j'y gagne une sécurité psychologique désirable au moment du choix.

49 Une question reste en suspens : l'incitation qu'a un pirate à livrer la clé achetée – qualité de service et respect de sa promesse qui constituent son fonds de commerce réputationnel- serait-elle modifiée s'il sait que la victime est assurée ? L'intérêt du pirate est d'être un bon livreur connu et reconnu, à l'instar d'un bon débiteur (je vous dois une clé puisque vous venez de me la payer) bénéficiant d'un avis positif d'un assureur-rançon faisant office d'agence de notation (scénario de notation qui constituerait un pas supplémentaire dans la légitimation du racket). Inversement, une victime assurée et sachant que sa rançon sera remboursée sera plus ouverte à prendre le risque –quasi gratuit pour elle- de payer même un pirate mal noté ou inconnu.

Ces deux types successifs de préférence que sont a) et b) ont en commun d'être confrontés à une probabilité d'occurrence de l'échec faible ou très faible, mais avec des coûts de l'échec quant à eux diamétralement différents, explicatifs semble-t-il des choix également différents du « joueur ». Rappel du niveau de perte si l'échec au « jeu » advient :

le 1er choix lui coûterait 3 000 euros en cas d'échec (vous tombez sur le 1/200), somme relativement modeste puisqu'elle ne ferait qu'écorner son patrimoine.

Le 2ème choix lui coûterait cher en cas d'échec, jusqu'à peut-être une faillite. La clé de déchiffrement n'est pas livrée ou ne fonctionne pas, avec des conséquences lourdes qui rejoignent le schéma développé par Allais, où sa perte en cas d'échec lors du tirage lui apparaît difficilement supportable.

Ce dilemme rappelle que la théorie de l'utilité espérée -votre mise et votre gain- ne prend de sens que rapportée d'une part à la taille de votre patrimoine et d'autre part à sa proportion engagée dans le pari. Elle est « l'espérance morale » définie par Daniel Bernoulli (« La valeur relative d'une somme (..) est égale à sa valeur absolue divisée par le bien total de la personne intéressée »[50]), où 3 000 euros représentent une fraction modeste du patrimoine d'un entrepreneur moyen. Il ne se tracasse guère de savoir s'il en sera remboursé par un assureur ; son inquiétude se cristallise davantage sur l'incomplétude de la garantie de sauver son entreprise avec cette mise de 3 000 euros, c'est-à-dire sauver tout ou grande partie de son patrimoine : mise faible (faible pourcentage de son patrimoine), avec une espérance de gain « infinie » au sens où elle peut sauver 100 % de ce qui le fait vivre.

L'état d'esprit du « joueur » à la fois rationnel et subjectif qu'est la victime, confronte un infini et un infime :

50 G. Crave, L. Delcroix, E. Hallouard, G. Kuwata et B. Tigroussine, Les probabilités selon le texte de Laplace. Principes généraux du Calcul des Probabilités, I.R.E.M. Caen Basse-Normandie, 2011.

3 000 euros est comparé à l'espérance de gain « infini » (sauver mon patrimoine), qui justifie de jouer à payer la rançon ;

3 000 euros est comparé à la taille de mon patrimoine (une fraction « infime »), qui justifie qu'on ne se tracasse pas d'en être remboursé, donc cet entrepreneur ne s'assurera probablement pas.

-> Au regard de la théorie de la décision, la victime placée lors du 2ème choix (b) devant une décision à prendre est en désir de certitude du gain (gain infini) -ici certitude de livraison de la clé- et non pas en désir de certitude de remboursement de la rançon (mise infime).

-> Lorsque la mise est infime et le gain infini, la certitude de gain est un genre d'assurance ardemment désiré, or pareille promesse ne saurait être inscrite par un assureur à son catalogue, puisqu'elle relève ici du bon vouloir du pirate.

-> Lorsqu'à un jeu, la mise est infime et le gain infini, ce n'est pas le remboursement de la mise par l'assureur qui intéresse la victime mais le remboursement du gain espéré puis échappé.

De manière plus littéraire, un apologue décrirait la psychologie du décideur de manière suivante : si vous êtes dans un ballon gonflable qui perd de l'altitude irrémédiablement au milieu de l'océan, et que peut-être pourriez-vous être sauvé en jetant pour ultime lest votre porte-monnaie, l'interrogation qui vous importe en cet instant est de savoir si ce geste sera efficace, pas si votre assureur vous remboursera votre monnaie. Cet arbitrage intellectuel est déjà présent chez l'entrepreneur lorsqu'on vient lui proposer de contracter une assurance rançon, quoiqu'il ait à cet instant en doute ce que serait le montant d'une future rançon ; à nouveau la visibilité par avance sur le respect des montants types est un autre facteur clé de sa décision de souscrire ou non.

Si les petites entreprises décrites ci-avant s'en remettent pour la plu-

part au choix du patron lors de pareils évènements, la décision dans les grandes entreprises ci-après a semblée plus diluée, ou au moins orientée par des subordonnés avant soumission à un décideur final au sommet d'une hiérarchie. La notion de mise (un petit patron mise parfois la vie de son entreprise, constitutive peut-être de tout son patrimoine) s'applique dans une moindre mesure à propos d'un cadre salarié, qui ne sera pas le payeur de sa poche. Toutefois sa décision est susceptible d'impacter sa carrière, par l'inflexion de trajectoire qu'elle est susceptible de lui imprimer ; laquelle carrière construit son futur patrimoine personnel. Il serait intéressant de mieux discerner si son choix de payer ou non est inspiré par l'intérêt de l'entreprise ou par son intérêt de carrière personnel.

Ce cas de figure évoque l'ancien adage connu des directeurs informatiques, au temps où la marque IBM régnait sur l'informatique : si vous avez choisi un ordinateur non IBM et qu'il tombe en panne, c'est de la faute de votre directeur de l'informatique qui accorde avec trop de légèreté sa confiance à des petits fabricants ; si vous avez choisi un ordinateur IBM et qu'il tombe en panne, c'est la faute de la technologie qui connaît des limites. Aujourd'hui, il est plausible qu'un motif de paiement de rançons par les grosses structures rejoint cette configuration, où un cadre supérieur qui ne paye pas la rançon se place en situation professionnelle plus exposée aux récriminations venant de ses collègues obligés de reconstituer des données, de perdre des clients, etc., que s'il la verse et obtient la cessation de l'attaque. Le microcosme social que constitue une grande entreprise est facteur de pressions internes exerçables sur « un/le responsable » (à l'image d'un bouc émissaire) auquel certains pardonneront parfois plus aisément le prix de la solution trouvée que le coût collectif du problème sans solution[51].

D'autant, aspect essentiel, que le prix de la solution trouvée ne sortira pas non plus de la poche de ces collègues ; la différence est ici nette avec des TPE où souvent la rançon sera acquittée par le petit patron

51 Les petites entreprises rencontrées ont souvent témoigné de tensions intra-familiales ou au contraire d'union sacrée familiale, autour des choix de payer ou non. Elles n'ont jusqu'à récemment pas présenté de cas marquant de pression émanant des employés sur leur patron, pour qu'il accepte de payer. Quelques signes d'évolution actuels sont néanmoins peut-être annonciateurs de nouvelles attentes, où le personnel escompte de ses chefs une « solution de facilité » pour leur éviter du chômage. Cette mutation serait alors parallèle à la propension grandissante des dirigeants à payer.

sur ses deniers personnels (il lui est délicat de justifier ce débours à l'expert-comptable de l'entreprise).

## 2 - Le cas des grandes entreprises victimes de demande de rançons

### Une transparence variable quant aux attaques subies

Contrairement aux petites entreprises où la transparence résulte pour beaucoup du choix de leur patron, les grandes structures offrent un paysage contrasté, entre d'une part une communication des multinationales qui devient un exercice encadré, parfois aseptisé et minimal (les pays anglo-saxons se montrent sur cet aspects plus ouverts à informer, que ne le sont bien des grands groupes français), d'autre part, comme à l'autre extrême d'un spectre, des hôpitaux piratés dont la liste des déclarants s'actualise jour par jour, et effectivement au grand jour.

Mondialement, les hôpitaux sont ciblés de par leur sécurité informatique parfois lacunaire -budgets en berne, politique de sécurité élaborée empiriquement, priorité accordée à l'usage des données plutôt qu'à leur protection …- , de par la valeur marchande ou intime des données médicales stockées, de par la nuisance que leur indisponibilité engendre au sein des unités de soin intensif dont la dépendance aux impératifs de fonctionnement en continu est potentiellement mortelle au sens le plus littéral. Une spécificité est leur difficulté à cacher une attaque réussie à leurs employés et patients, qui se comptent par milliers ; la presse recevra l'écho de ce qui frappe de telles institutions en prise avec la vie d'une cité.

La comparaison des recensements de rançons sur les deux extrêmes que sont les grands hôpitaux et les grandes entreprises révèle un écart qui fait s'interroger sur ses causes, afin de déterminer s'il résulte uniquement de ce que les grandes entreprises sont effectivement en meilleure capacité de se protéger, ou si elles ont parallèlement une meilleure capacité de préservation du secret, tant que la faible visibilité d'un accident n'oblige pas à l'avouer publiquement (Il est incertain que les récentes obligations de communiquer tout piratage aux autorités et aux partenaires commerciaux soient complè-

tement entrées dans les mœurs). Auquel cas le « cyber-baromètre » que sont les hôpitaux transcrirait les moyennes d'impacts de manière amplifiée, là où certaines grandes entreprises sont soupçonnables de le faire de manière assourdie. Le premier étant en partie révélateur de non-dits des secondes.

## Une attractivité élevée

Ces grandes entreprises ont cependant plusieurs désavantages, par comparaison avec des TPE-PME :

- Leur exposition vis-à-vis de leurs propres actionnaires. S'il est vrai qu'un directeur financier d'une grosse structure a plus aisément l'oreille de son banquier qu'un petit commerçant, pour lui faire part d'un coup du sort et obtenir des facilités de caisse, une telle proximité avec la sphère financière n'est pas moins une faiblesse qu'une force. Car la simple médiatisation d'une attaque aura un possible effet sur sa valeur boursière ; à moins que par une sorte de prophétie auto-réalisée, la peur d'un tel effet –avéré ou fantasmé- par la grande entreprise, ses actionnaires et les spéculateurs provoque ledit effet (une entreprise déclare par communiqué être attaquée : dans les minutes qui suivent les intervenants qui anticipent une éventuelle baisse du cours -une hausse serait tellement improbable qu'il n'y aura guère de perte à vendre mais beaucoup à gagner- provoquent ou amplifient ce qu'ils redoutent). Raisonné ou irraisonné, cet état d'esprit se concrétise en France par une volonté de discrétion palpable chez de nombreuses grandes entreprises. Goût du secret qui se trouve moins dans les très petites entreprises, où parfois le patron est demandeur d'interlocuteurs à qui parler de l'évènement, puis ouvert à faire part de son vécu à ses pairs.

- Leur exposition vis-à-vis des agresseurs. Leur extrême visibilité sur la place publique procure au pirate davantage d'informations pour ajuster sa demande à la capacité connue de l'entreprise à payer. L'asymétrie d'information est forte, le pirate ayant facilité de connaître l'entreprise, sans réciprocité. Tandis que pour les petites entreprises, la méconnaissance de l'un par l'autre est plus proche.

## L'économie de la rançon, entre logique d'assurance ou logique de marché

« Certains se demanderont si (la garantie cyber-extorsion) relève encore de l'assurance. D'autres considéreront que l'assureur remplit pleinement son rôle et va au-delà du simple remboursement.[52] »

Pour repère, les assurances enlèvement traditionnelles

Les offres d'assistance proposées par certains assureurs et experts en sécurité ou en intelligence économique à propos des risques d'enlèvements d'employés d'entreprises se composent notamment de trois volets : abaissement préventif de l'exposition à un enlèvement, réactivité et prise en charge de la négociation avec les kidnappeurs en cas d'enlèvement réussi, et enfin prise en charge aussi de tout ou partie de la rançon. Le premier volet s'attache en particulier à diminuer la détectabilité et l'identification des employés expatriés des entreprises riches[53] ; conseil sans effet s'agissant d'entreprises ou encore d'hôpitaux dont la politique de communication usuelle est au contraire une quête de notoriété et de visibilité, en particulier pour les entreprises cotées en bourse. Or annoncer à ses actionnaires des profits et une solide assise financière devient contre-productif sécuritairement. Au point que cette exposition et cette cotation soient de vraisemblables facteurs de déclenchement d'attaque ; vis-à-vis de menaces de rançons, l'adage « pour vivre heureux vivons caché » présente une pertinence, sauf cas rare où cette discrétion mène à faire surestimer votre fortune.

-> Un travail culturel en profondeur est à suggérer, incitant les entreprises à intégrer dans leur politique d'affichage des critères essentiels de sécurisation de son patrimoine. Un volet de *sécurité par la discrétion* pour l'entreprise (sur sa communication et sa visibilité) serait une utile déclinaison de l'habituelle *sécurité par l'obscurité* (sur son système informatique).

52 Jean-Laurent Santoni (Clever Courtage) : « Cybercriminalité. Le ransomware est-il assurable ? ». Expertises, juin 2016.

53 L'actuelle accessibilité planétaire aux multiples points d'entrée dans les dizaines de milliers d'ordinateurs des systèmes d'information d'une multinationale équivaudrait en matière de degré de sécurisation à devoir protéger les dizaines de milliers d'employés qu'elle a sur la planète, et non pas seulement les quelques personnes envoyées par elle, qui en Colombie, qui au Nigéria.

## Un fait révélateur : le besoin de discrétion en matière d'assurance sur la rançon

Le danger de personnalisation de la demande de rançon aux encaisses que toute entreprise cotée en bourse publie trimestriellement, se verra accru si le pirate apprend que sa proie a souscrit une assurance contre les rançons, a fortiori s'il peut en deviner le plafond de remboursement convenu. Le jeu se déplace, qui ne consiste plus d'abord à cacher l'entreprise ou sa cagnotte mais à cacher qu'elle est assurée sur le paiement de rançons ; ou tout au moins à cacher le montant de cette assurance (Une fuite d'information ayant touché il y a une dizaine d'années une multinationale pétrolière britannique –le PDG avait transmis son ordinateur personnel à une relation sentimentale en y laissant des dossiers sensibles, contenus plus tard revendus-, a révélé le prix maximal qu'elle accorderait à la vie de ses salariés. Renseignement crucial au regard de négociations lors d'un éventuel enlèvement, et auparavant pour trier les proies les plus juteuses. Tout à l'opposé, un pays asiatique s'est acquis sciemment la réputation, sur les contrats de génie civil étrangers où il envoie des ingénieurs, de répondre à une demande de rançon lorsqu'un d'eux s'est vu enlevé, par l'envoi d'un autre ingénieur en remplacement).

Cette discrétion est traditionnellement la règle des assureurs enlèvement, qui l'imposent à leur clientèle ; cette dernière s'engageant à mobiliser les moyens humains ou techniques de cette confidentialité. Or que devient la solidité de ce rempart lorsque :

- Elle prétend s'appliquer à une entreprise victime d'un cryptovirus, donc subissant une présence étrangère nuisible dans son système d'information. A l'heure où le chiffrement de données par les pirates se double de plus en plus souvent de leur volonté préalable d'explorer le système d'information victime avant de se déclencher, et d'exfiltrer des données, une contradiction se manifeste entre exiger le secret d'un contrat mis au coffre informatique -sur ordinateur- de la part de celui dont ce coffre-fort est violable. D'autant qu'un banal accès à une messagerie d'entreprise suffit à glaner les courriels échangés avec l'assureur (Le recours à une protection par chiffrement de données -cette fois non pas par le pirate mais par les entreprises pour leurs télécommunications-, perd de son rôle dissimulateur lorsque, à réception, le juriste d'entreprise déchiffre le contrat reçu pour

y travailler ; sur son ordinateur se trouvera la version en clair. Les entreprises ont peu recours aux méthodes lourdes des ambassades, qui isolent sur trois machines distinctes la réception d'un message codé, puis son décodage puis l'usage du message décodé par son réceptionnaire).

- La valeur de ces secrets transforme également les assureurs sur les cyber-rançons en cibles idéales, que le talent des pirates voudra forcer en préalable pour identifier leurs clients avec leurs clauses contractuelles (Pareillement, une autre profession de confiance réputée pour être ciblée est celle des avocats, de par l'importance du contenu des dossiers traités, ou par le prestige de ce métier qui incite aux usurpations d'identité par des tiers). La discrétion revendiquée est mise en défaut quand certains assureurs affichent leurs prestations d'assurance-rançon sur leur site internet, et invitent les prospects à télécharger des formulaires ou à les contacter en ligne. Des dérapages ont été enregistrés aux États-Unis, où l'affichage intempestif des marques de leurs clients par certains cabinets d'assurance-rançon a retenu l'attention de cyber-criminels.

Par allusion au KYC –connaissez votre client- qui inspire la pratique suivie par les pirates pour calibrer les montants des rançons personnalisées envers les grandes entreprises -connaissez votre victime-, l'évolution s'orienterait vers un « connaissez son assureur » (plus exactement s'agit-il d'un couple, puisque l'assureur offre des niveaux de couverture proportionnés au montant de la prime choisie par son client).

## Une assurance-rançon modificatrice des comportements

En cas d'assurance souscrite sur les rançons, se met en place une triple incitation, source de possible entraînement entre les trois acteurs impliqués -pirate, piraté, assureur- :

- Pour la victime, à payer la rançon avec meilleure grâce (voire aussi à moins renforcer sa protection informatique, hormis obligation édictée par l'assureur comme préalable à la contractualisation. La présence du parapluie assurantiel pouvant sinon pousser à abaisser la vigilance par parapluie technique).

- Pour l'assureur, à proportionner de manière moins libérale le remboursement, puisqu'il anticipe la propension accrue de la victime à payer (parfois aussi à essayer de contourner les obli-

gations de sécurisation informatique prescrites) … ainsi que la tendance du pirate à essayer d'obtenir davantage via l'assuré. A l'extrême, la propension à payer une rançon chez l'assuré tendra vers 100 %, ce qui ne laissera pour diviseur du prix que la probabilité d'être virussé ; or cette probabilité grimpera chez l'entreprise qui se distingue aux yeux des pirates en souscrivant une assurance-rançon, et ne sera plus égale à la moyenne de toutes les entreprises. Dans un cercle vicieux, il en ressort des primes aux montants élevés, qui inciteront d'autant plus le souscripteur à activer sa garantie en cas d'attaque, comportement qui attirera derechef les pirates, etc.

- Pour le pirate, à positionner son tarif en fonction des montants maximum de remboursement connus ou devinables. Non pas nécessairement pour s'y aligner mais pour l'adopter comme son minimum ; rien n'empêche lorsqu'une entreprise est assurée pour être remboursée de dix millions, de lui en demander onze si elle a un million en trésorerie : elle acquittera ce supplément de sa poche. En quelque sorte, un danger est que l'assurance-rançon vienne s'additionner … à ce qu'aurait payé l'entreprise sans assurance-rançon. La « bourse ou la vie » devient la bourse + l'assurance, ou la vie. Accessoirement, quel sort serait réservé aux entreprises dont le pirate croit à tort qu'elles ont souscrit une telle assurance-rançon, et qui se retrouveront en incapacité de lui prouver le contraire ? La discrétion organisée autour de ces contrats se retourne contre les non-contractants, sauf à rêver avec un peu d'humour qu'on leur délivre des attestations de non-assurance.

Une permutation de référent s'opérerait : si aujourd'hui la plupart des demandes de rançons de montant personnalisé –les quelques-unes ayant trouvé un écho médiatique- se situent à des niveaux finaux d'un coût élevé mais payable par l'entreprise sur sa trésorerie, il est concevable qu'elles passeraient à des niveaux et des fréquences payables par l'assureur et derrière lui par la collectivité des assurés. Si l'effet inflationniste sur les prix des rançons demeurera objet de débat, il est prévisible par contre que la fréquence de l'assentiment de paiement par la victime s'en trouvera accrue.

## La fourniture d'aide à la négociation des rançons

« Nous aidons les sociétés à acquérir des cryptomonnaies et à nouer le dialogue avec les acteurs de la menace pour définir des tactiques appropriées. »

Site d'une société de sécurité américaine

Une prestation relai d'assureurs spécialisés sur les demandes de rançon est la fourniture d'aide à la négociation, déléguée à des experts (De la sorte, pour les assurances enlèvement de personne, ces officines puisent, entre autre par débauchage au sein des unités de police telles que le FBI ou le RAID, dans le vivier des spécialistes en négociation lors de prises d'otages ; un commun dénominateur avec la « prise d'otage de données » est la haute valeur de chaque heure ou journée perdue. Le volet psychologique pour entretenir les pourparlers avec les kidnappeurs est renforcé par un volet renseignement, afin de recueillir toute information susceptible d'aider à les authentifier –des escrocs opportunistes cherchent fréquemment à s'immiscer dans la chaîne de contacts, prétendant être ou connaître ces ravisseurs- puis à comprendre leurs objectifs véritables, leur degré de jusqu'auboutisme, etc. Volet renseignement qui s'appuie sur des réseaux d'informateurs locaux –par ailleurs policiers en exercice, juges, journalistes, autorités religieuses, « anciens » criminels jouant les indicateurs …- souvent tissés par avance par les officines de négociation dans les pays sensibles tels que la Colombie).

Une différence motive à ne pas trop assimiler la négociation de cyber-rançon et celle sur les enlèvements de personnes, et à ne pas croire à la parfaite transposabilité de ces deux types de négociation : le temps d'attente est quasi-gratuit pour le cyber-pirate, temps que lui octroie les décennies nécessaires pour casser son code par force brute. Inversement le temps reste onéreux pour le kidnappeur d'une personne coûteuse en gardiennage et alimentation. De même, et faisant complément à l'aspect temporel, la dimension spatiale et géographique perd la contrainte de se cacher dans une jungle ou une grotte, quand les clés et les authentifiants d'un pirate situé en un quelconque point de la planète logent dans une clé usb. Le cyber-agresseur n'est quasiment soumis ni au temps ni à l'espace.

Par contre, de même que parfois certaines personnes enlevées parviennent à s'évader y compris avec leur gardien qu'elles ont soudoyé, une évasion numérique reste espérable lorsque chiffre-

ment du pirate comporte des défauts, à l'instar de WannaCry dont la propagation a pu être retardée.

Le fait que la personne kidnappée puisse mourir trouve quant à lui un parallèle dans celui que l'entreprise aux données chiffrées peut faire faillite bientôt, auxquels cas le criminel perdrait sa proie et se trouve par avance enclin à conclure plus rapidement.

On peut craindre que la transposition des précédentes méthodes puissantes mais onéreuses au créneau des cyber-rançons pour petites entreprises soit aussi inadaptée que sur le racket d'un cordonnier local sommé par la mafia d'acquitter un *pizzo* de quelques centaines d'euros.

- Les sommes modestes concernées par les crypto-rançons pour PME et TPE ne justifieraient pas l'intervention d'experts précités. Les coûts partiellement fixes d'une telle mission négociatrice videraient et au-delà le gain escompté.

- Les procédures de négociation des pirates sortent du cadre d'un vrai dialogue entre individus, malgré leurs apparences. Les échanges de courriers recueillis lors de notre étude confirment leur caractère standardisé, parsemé de phrases types débitées au fil de l'avancement programmé dudit dialogue. Une ressemblance se fait avec les petites mains utilisées sur des fraudes aux sentiments, où de faux profils de célibataires concoctés par des « brouteurs » -selon l'expression ivoirienne- et mis en ligne sur les réseaux sociaux, sont animés sur les réseaux par de jeunes personnes, parfois des adolescent(e)s chichement rémunérés à la tâche et au résultat, pour donner la réplique aux internautes naïfs. Chapeautés par leurs commanditaires, réunis parfois en atelier de travail, ces jeunes manipulateurs sont interchangeables tant leurs mode opératoire de manipulation est mimétique (« Mon/ma chéri »), calqué sur un savoir-faire mis en commun (« La solitude me pèse »). De fait, il ne serait pas rentable non plus pour les brouteurs de mobiliser des seniors, tant que les enjeux sont faibles.

Au demeurant, plusieurs victimes rencontrées ont obtenu par elles-mêmes ces remises tout en étant novices en négociation ; il n'est pas assuré qu'un négociateur plus chevronné et rompu à ces techniques obtienne davantage de baisse, si tenté au contraire que son absence

d'amateurisme ne vienne cataloguer la victime comme disposant des subsides pour s'adjoindre de tels professionnels, donc soit fortunée.

Quant aux grandes entreprises victimes de criminels organisés, ceux-ci se décomposent en deux grandes catégories, à savoir les gangs réputés ne pas baisser leurs prétentions, et ceux qui les abaissent mais souvent après avoir majoré d'autant leur demande initiale ; l'utilité du négociateur professionnel sera de discerner duquel de ces deux profils relève tel cas de piratage –ou d'envisager un troisième profil, plus amateur par exemple- afin d'éviter des gaspillages de temps ; mais il s'agit jusqu'à ce stade d'aide au diagnostic et à la lisibilité des évènements, qui restent dans le domaine de la gestion de crise.

Qu'il s'agisse d'enlèvements de personnes en série ou de données bloquées là aussi en série, la négociation abandonne une part de sa composante psychologique, davantage utile avec les prises d'otage par un forcené -quoique certains pirates aient des psychologies de joueurs- pour se recentrer sur la valeur marchandable des biens ou personnes. La dite négociation revient à tenter de rapprocher les exigences des pirates des référents du marché (Pour information, dans les régions frappées par l'industrie des enlèvements, telle que le nord de la Cordillère des Andes, existent des « argus » de la valeur des personnes selon leur employeur, leur lieu de résidence familial –beaux quartiers …-, leurs diplômes, etc., aidant à sélectionner les quidams en fonction de leur rentabilité calculable d'après un vulgaire tableur d'ordinateur personnel). En cela, le négociateur est un abaisseur de prix mais par le fait qu'il l'aligne sur une cotation, via des méthodes de valorisation faisant consensus. Avec pour résultat paradoxal qu'il concoure certes à abaisser certains prix, mais également à valider au final un prix conclu, donc à bâtir le consensus. Une seconde incongruité est qu'il accroît ce faisant le nombre d'accords conclus donc de rançons versées.

Le négociateur professionnel participe donc à la formation de ces prix du marché, jugeant que tel rabais obtenu convient ou pas, mais ce faisant il consacre ce prix post-rabais comme référent pour une rançon ultérieure. Certains cabinets de négociation ont leur propre « argus », une grille d'acceptabilité ou non des sommes exigées. L'assuré lui-même participe à cette convergence des vues, en ce qu'il se disqualifierait d'emblée s'il prétendait souscrire pour une couverture trop basse, en quelque sorte inacceptable par le rançonneur, le négociateur et l'assureur. La prestation de négociation et l'assurance-rançon contribuent à l'apparition d'un marché de la rançon assorti de

systèmes de cotation, et au mieux à sa régulation, dans ce que l'ANSSI désigne comme le développement d'une économie autour du paiement des rançons.

Il ressort de ceci un paysage clarifié, qui départage mieux trois fonctions :

- L'aide à la gestion de crise en cas d'attaque, sur un mode urgentiste et en temps réel, est pleinement normale pour les assureurs, et très demandée par les petites victimes sur les aspects informatiques, relationnels avec l'écosystème (banque, commissariat …), prise de décision (bénéficier d'un transfert d'expérience depuis de précédentes gestions d'affaires), soutien moral pour rompre l'isolement intellectuel, etc.

  Cette prestation constitue, sur l'éventail des services possibles autour des cyberattaques, un point d'équilibre neutre qui ne penche ni vers le paiement ni vers le refus de paiement. Il laisse son libre arbitre à la victime aidée.

Le besoin d'assistance aux entreprises touchées par des attaques informatiques a motivé la CCI Pau Béarn à mettre sur pied une cellule de soutien et d'intelligence économique, activable par chacune des 16 000 entreprises du territoire.

Avant attaque. Actions de sensibilisation, de formation et lancement d'alertes en cas d'évènements en cours (tentatives de faux ordres de virement …), etc…

Pendant l'attaque. Les missions sont l'appui à la gestion de crise – aider la victime à maintenir une relation fonctionnelle avec son écosystème que sont les banques ou assureurs, la gendarmerie, les clients ou fournisseurs … - , l'écoute et le transfert de vécu depuis de précédents cas d'attaques pour l'analyse de situation, aider un chef d'entreprise à faire un point lucide et mener ses arbitrages dans les moments de trouble. Il ne s'agit donc pas de se substituer à lui ou d'orienter ses choix, mais de le mettre en capacité de prendre ses propres décisions, après l'avoir placé en situation de meilleure information et de moindre tension psychologique (prise en compte prépondérante du facteur humain).

Après l'attaque. Chacun des évènements fait l'objet d'un retour d'expérience, qui aide à capitaliser un savoir opérationnel sur les

bonnes pratiques, les comportements et réflexes à adopter, à disposition des pairs chefs d'entreprises.

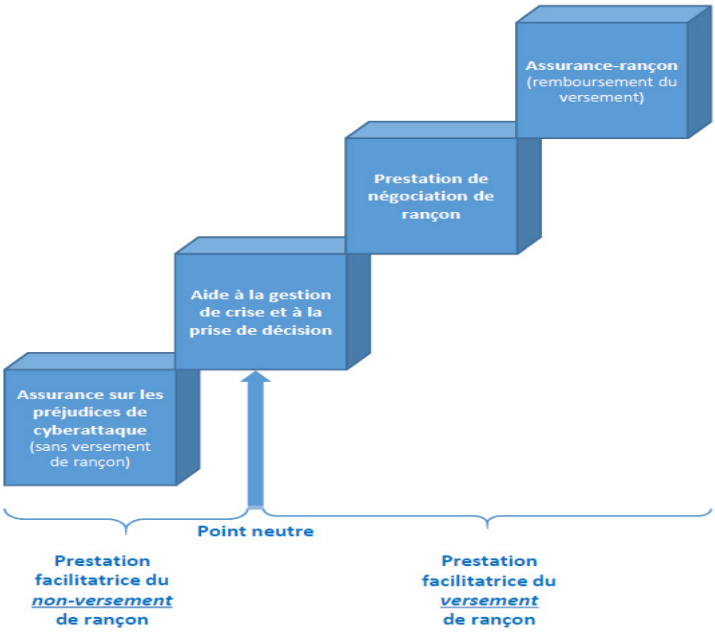
Soutien, présence et éclairages maintiennent la CCI dans un rôle neutre. Elle accompagne au long des jours ou semaines de la crise, mais par exemple si le choix de l'entreprise est de payer, elle n'est prestataire ni d'un service de négociation avec le pirate, ni d'achat ou d'envoi de bitcoins.

- L'aide à la négociation de rançon, même sans assurer celle-ci, est un pas vers la perte de neutralité, puisqu'elle penche en faveur de la réalisation du paiement. Le but basique d'un négociateur d'enlèvement est le bon achèvement de la « libération des données » (telle société de sécurité américaine revendique un taux de réussite de 98 % sur ses dossiers, par tous moyens confondus depuis les précautions informatiques, les sauvetages techniques ou la négociation de clé de déchiffrement), à l'instar de celle des kidnappés, ce qui revient à se faire auxiliaire du principe de rançon, à apporter de l'huile à son mécanisme jusqu'à sa conclusion. A la décharge de ces acteurs, le vide actuel qui prévaut en matière d'assistance apportée par la collectivité est un espace vacant laissé à l'éclosion de demandes et d'offres de négociation.

- Coupler la négociation à une prestation de prise en charge financière de la rançon, qui accolerait les fonctions d'intelligence économique et d'assureur-rançon, constitue un pas supplémentaire vers le délaissement d'une stricte identité d'assureur : vous devenez l'approvisionneur de l'argent d'une rançon -par remboursement à la victime- lors d'une tractation que vous vous évertuez en tant que négociateur à faire aboutir ; vous mutualisez des coûts de rançon mais dont vous contribuez somme toute à la survenance une fois l'attaque perpétrée. Une confusion des objectifs s'accentue autour d'un tel forfait global[54], qui pourrait

54 Pour ne pas endosser un rôle d'acteur qui les exposerait juridiquement, beaucoup de ces assureurs laissent à la victime le choix du négociateur et la réalisation physique du paiement de rançon (ils en acceptent expressément et préalablement le montant fixé, puis le rembourseront). La disjonction des tâches reste limitée et formelle, car l'assureur-rançon aurait sinon également délégué la tâche de négociation à une des mêmes officines enrôlables (celle retenue par la victime aura du recevoir l'aval de l'assureur).

aussi bien émaner d'un « réparateur » rémunéré selon un forfait prédéfini d'après la probabilité d'être activé. La mutualisation est moins flagrante, moins centrale.




Un distinguo prend forme, qui confirme l'impression d'une différence constitutive entre l'assureur de cyber-préjudices et l'assureur de cyber-rançon :

- Le premier n'a pas prise directe sur le coût du sinistre. Bien sûr essaiera-t-il de l'atténuer par des prescriptions préventives (porte pare-feu contre l'incendie, pare-feu informatique …) et des dispositifs de soutien (cellule d'aide à la gestion de crise, plan de reprise d'activité …), qui font le pendant des mêmes précautions chez l'assureur-rançon (éviter aux expatriés d'arborer le logo de leur entreprise …).

- Le second au contraire est co-bâtisseur du prix final de la rançon ; dont le versement change le périmètre du coût global des préjudices parallèlement subis. Les composantes négociantes et négociatrices empiètent, au risque même de prédominer,

sur la fonction d'assureur avec sa philosophie de mutualisation des seuls aléas.

Reste, en préalable à quelques autres ambiguïtés ci-après, une qui survient subtilement si à main gauche l'assureur s'engage à couvrir un sinistre d'attaque informatique, tandis qu'à main droite il facilite une négociation destinée à parvenir à une rançon qui limitera le précédent sinistre. Son intérêt pécuniaire penche vers la main droite, vers un métier de négociateur davantage que d'assureur.

Le club des Juristes, par sa commission Cyber Risk à laquelle participe la Fédération Française de l'Assurance, a publié parmi diverses préconisations à l'attention des instances européennes, celle « d'établir les conditions d'une concurrence équitable entre les assureurs cyber. Inviter les autorités réglementaires de l'Union européenne à adopter un cadre juridique permettant un traitement harmonisé de la question de l'assurabilité des rançons au sein du marché européen.[55]» En Europe, le Royaume-Uni, les Pays-Bas et la Suisse, dans le sillage des Etats-Unis, ont adopté des lignes libérales qui tolèrent cette assurabilité, d'où s'ensuit un risque de concurrence déséquilibrée.

Pour la France, la référence récente reste un communiqué du ministère des Finances favorable à « l'insertion de clauses dans les contrats d'assurance "kidnapping et rançon" excluant le remboursement ou le paiement d'une rançon » lorsqu'elle bénéficierait à Daech et plus généralement à une entité terroriste (l'anonymat des pirates ne permet pas d'affirmer leur appartenance aux mouvances terroristes, ni d'affirmer leur inappartenance). Une étrangeté législative perdure dans le fait de ne pas interdire à une organisation criminelle ce qui l'est pour une organisation terroriste, surtout lorsque des passerelles sont soupçonnées entre ces deux sphères.

## Des ambiguïtés à lever

« Notre compagnie d'assurance a pris la décision pour nous. (..) Le coût de résolution du problème en interne a été comparé à celui de la

55 Rapport « Assurer le risque Cyber », janvier 2018.

rançon » [56]

Le porte-parole de la ville de Lake City, Floride

L'aide à la négociation de rançon, peu pertinente pour des petites structures ou des petites sommes, relève, quand elle vient à être mise en œuvre pour de grandes entreprises, des métiers de l'intelligence économique et de l'ingénierie sociale qui en sont déjà prestataires anciennement. Ces métiers apparaissent complémentaires mais distincts de celui d'assureur, sans validité naturelle à être associés en une seule entité, par risque de conjonction d'intérêts différents.

Par-delà le fait que le négociateur soit au service de l'assureur de rançon, plusieurs observateurs ont estimé qu'une autre frontière s'estompe, qui permettait d'être certain que cette intermédiation est bien au service du client victime, et non pas de fait aussi au service du rançonneur. Faute de quoi l'intermédiaire prendra les traits d'un entremetteur. L'ANSSI a qualifié de phénomène inquiétant l'émergence de cette nébuleuse où « certaines sociétés (négociatrices) camouflent le fait qu'elles payent la rançon en prestations de déchiffrement des fichiers à l'aide d'expertise technique interne. Pire, certaines ont développé des liens parfois étroits avec des groupes cybercriminels afin d'accéder à des réductions des rançons[57]» (Réductions qui évoqueraient un architecte maître d'œuvre dans le BTP, rémunéré sur honoraires pour mener une mission à bonne fin, et grâce auquel son client bénéficie de remises professionnelles de la part des vendeurs de matériaux de construction).

Le débat a été ouvert aux États-Unis également, où assurance-rançon et prestations de négociation sont monnaie plus courante, et de ce fait offrent davantage de recul. Le nombre croissant des municipalités ciblées incite à douter de l'innocuité des lignes de conduite pratiquant le paiement, depuis plusieurs années, à l'encontre desquelles les critiques désormais formulées par des élus ne sont pas seulement d'ordre éthique mais économique de long terme.

## 3 – LA PROBABILITE D'UNE FRAUDE A L'ASSURANCE QUI VIENNE OBERER LES TARIFS DE L'ASSURANCE-RANCON

56 Renee Dudley : « *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks* ». Propublica, août 2019.

57 « Etat de la menace rançongiciel, à l'encontre des entreprises et des institutions ». Anssi, février 2020.

Autant des faux enlèvements et rançonnages de personnes de complaisance appelleraient des complicités et des mises en scène, autant le simple chiffrement de données ultérieurement remises en leur état d'origine constitue un geste moins impliquant physiquement comme psychologiquement, moins lourd à organiser, moins traçable et plus ludique même. Semblable mascarade est menable de bout en bout par un individu seul, surtout s'il dispose d'accès internes au système d'information de l'entreprise. Peu médiatisée à ce jour, l'hypothèse de fraude au cryptovirus reporterait son poids sur des payeurs externes via une mutualisation supportée par les autres assurés, ou sur l'assureur[58]. En cela se poserait la question d'une assurance rançon littéralement criminogène. De plus, l'extrême rareté des arrestations de pirates informatiques, particulièrement lorsqu'ils se contentent de perpétrer un unique coup gagnant, ne suscite pas une peur du gendarme irrépressible.

L'interrogation revient à demander s'il y a assurabilité d'un aléa lorsqu'il réunit plusieurs caractéristiques pénalisantes :

o Pour le faux-vrai pirate : barrière psychologique modérée à la commission de l'acte, coût quasi nul de la réalisation, risque judiciaire négligeable.

o Pour l'assureur : invérifiabilité de la réalité d'un pirate.

Le fait que les assureurs soient vigilants sur la discrétion qui doit entourer de tels contrats de remboursements de rançon, dévoile combien une telle information recèle une capacité déclencheuse de passage à l'acte par un pirate. Or cette discrétion ne s'applique pas aux responsables internes de l'entreprise assurée, qui ont naturellement connaissance de telles clauses dont ils sont signataires.

Selon les divers scénarios envisageables, le faux-vrai pirate pourra être tantôt un dirigeant qui encaissera la rançon avant que son entreprise reçoive remboursement, tantôt un cadre agissant en solitaire et qui encaissera la rançon de manière déculpabilisée puisque son employeur sera remboursé, tantôt encore un entrepreneur démarché par un criminel en col blanc venu lui proposer une telle escroquerie

58 L'Agence pour la Lutte contre la Fraude à l'Assurance recensait sur l'année 2015, 46 255 fraudes frappant l'ensemble des secteurs. Postuler que l'assurance sur les rançons ne serait pas affectée serait déraisonnable.

en duo[59], etc.

Notre étude a mis en relief deux particularités aggravatrices de soupçon :

- La progression du coût total d'un chiffrement de données n'est pas linéaire au fil des jours, mais procède souvent par des bonds et de brusques envolées exponentielles. Tout versement de rançon qui interviendrait fort rationnellement avant ces sauts laisserait l'entreprise avec des dégâts minimaux, qui n'obéreraient pas ses comptes lourdement, tout en alimentant le faux-vrai pirate en argent sonnant et trébuchant.

- Une part notable des PME qui versent une rançon se trouvent parmi celles déjà antérieurement fragiles comptablement, et qui anticipent qu'elles ne résisteraient guère à un blocage long par cryptovirus. Ce contexte ne peut écarter une interférence entre un entrepreneur cherchant un second souffle financier et la remboursabilité d'une rançon, capable de susciter des vocations opportunistes.

Finalement, le meilleur garant contre les tentations de fraude aux assurances est l'actuelle modération fréquente des montants des rançons à l'encontre des TPE-PME, qui paradoxalement décrédibiliseraient des exigences trop élevées. Par une harmonie imprévue, une même cause –ces petits montants- parvient à réconcilier deux abstentions, celle de ne pas désirer s'assurer sur les rançons, et celle de ne pas désirer frauder une telle assurance.

***

59 En matière de scénario à étage qui illustre à l'extrême le champ des possibles, l'affaire John DeLorean fut le cas d'un industriel exsangue financièrement et acculé à une faillite prochaine, qui s'était vu proposer une opération illégale mais rentable par des intermédiaires crapuleux ayant détecté ce besoin urgent d'argent chez lui. Lesquels intermédiaires se sont ultérieurement avérés être des provocateurs au service de la police fédérale américaine, désireux de monter de toute pièce une opération permettant une arrestation spectaculaire et médiatisée.

En synthèse, aussi longtemps que ces incertitudes sur le montant des rançons et la probabilité de livraison de clé après versement resteront limitées, la collectivité ne paraît pas devoir trouver d'efficacité économique dans une offre d'assurance rançon, qui actuellement se définit comme étant à utilité faible voire négative, et à dangerosité de long terme élevée.

Un distinguo est à rappeler entre utilité, rentabilité et marché : certains marchés se maintiennent même sans rentabilité parce que l'offreur y trouve un intérêt indirect (la gratuité des moteurs de recherche en est un exemple), tout comme une rentabilité commerciale circonscrite à ce marché peut se dégager mais avec un produit plus globalement néfaste pour la collectivité alentours (c'est la notion d'externalités négatives).

Concernant un éventuel marché, se constate une absence de débouché patent pour l'assurance-rançon dédiée aux petites entreprises, en l'état des actuelles formes d'attaque. L'interrogation est davantage brouillée pour les grandes entreprises, démarchées par une offre internationale où certains acteurs étrangers de l'assurance pourraient utiliser ce segment comme produit d'appel pour ensuite vendre des cyber-assurances plus globales … que l'on reste en droit de regarder elles-mêmes çà et là comme des produits d'appel pour vendre ensuite des assurances tous domaines, tant certains tarifs cyber bâtis sans recul ont semblé viser d'abord le gain de parts de marché plutôt qu'une saine capacité d'autofinancement du segment faisant appel.

| | Existence d'un marché ? | Rentabilité de ce marché ? | Utilité globale de cette offre ? |
|---|---|---|---|
| TPE et PME | Plutôt non en l'état | Très incertaine | Non pour la collectivité |
| Grandes entreprises | ? | ? | Non pour la collectivité |

## B – FAUT-IL LAISSER SE DEVELOPPER DES PRÊTS AUX RANÇONNÉS ?

Parallèlement au questionnement jusqu'à lors restreint à l'assurabilité des rançons, son vis-à-vis concerne l'autorisation ou non de prêter en urgence de l'argent à une victime qui subit un chantage de montant supérieur à sa capacité de paiement immédiate, concernant cette fois la profession bancaire ou tout autre prêteur –par escompte, découverts, délais de paiement …- y compris une personne privée ou un assureur . Le statut d'un tel créancier doit-il être assimilé à un soutien bienvenu à la victime, ou à un acteur qui accentue la tentation du pirate à exiger davantage que ce que le patrimoine disponible de sa proie peut payer sur le champ, dès lors qu'elle recoure à l'endettement ? Ce créancier peut-il prétendre épauler initialement la victime sans appuyer finalement son agresseur ?

A travers sa finalité, la légitimité du prêt interpelle également, en ce qu'il est sensé répondre à un besoin pressant et souvent vital tout en étant un besoin artificiel et stérile, puisqu'il s'agit d'un racket improductif.

Le contexte du prêt enfin fait réfléchir à la notion de consentement libre ou non, de quiconque est soumis à un tel besoin vital : temps court et enjeu élevé amputent-ils chez le demandeur une partie de sa liberté de choisir, de sa lucidité parfois même, en ne répondant plus à la définition qui fonde le contrat en économie classique ?

### 1 - Un prêt à caractère inflationniste

A ce jour, l'attitude des pirates consiste à demander une somme que leur victime est apte à rassembler pour envoi dans les heures ou jours qui suivent. Il y a là une limite financière dictée par une limite temporelle. Or, dès lors que s'institueraient des facilités de prêt à cette même victime, l'assiette retenue par les pirates est susceptible de ne plus se contenter de la trésorerie interne de l'entreprise (laquelle en matière de liquidité de l'actif correspond grandement en langage monétaire à M1 et M2, à savoir l'argent en caisse ou qui n'est pas bloqué sur des comptes à terme) mais de s'élargir à un patrimoine plus large, certes non mobilisable sur l'instant mais apportable en caution et garantie à un prêteur. L'assiette de l'impôt illégal qu'est une rançon quitterait l'encaisse immédiate –le bas de bilan- et passerait à l'actif

global –le bilan dans son ensemble-.

L'habituel débat sur les causes et la licéité d'un contrat, telles que définies par les articles 1131 et 1133 du Code Civil (« l'obligation sans cause, ou sur une fausse cause, ou sur une cause illicite, ne peut avoir aucun effet ». « La cause est illicite, quand elle est prohibée par la loi, quand elle est contraire aux bonnes mœurs ou à l'ordre public ») se sophistique par la présence d'un engrenage où la mise à disposition d'une autorisation d'emprunt, puisqu'elle risque d'augmenter la somme demandée par le pirate, amènerait la victime à devoir emprunter en proportion de cette augmentation, etc. Toute boucle auto-entretenue (non pas à l'échelle d'une seule attaque mais dans une spirale montant successivement cas après cas) où un prêt se proportionnerait à une rançon qui se proportionnerait en retour à la capacité de prêt, risque de dériver vers une variante de soutien abusif où la capacité de remboursement de la victime cesse d'être la référence obligée et un butoir contre une hausse forcée dans l'urgence.

La relativité de la notion de soutien abusif

La capacité de remboursement étant fonction du temps accordé pour purger sa dette, il suffit d'allonger la durée du prêt pour vider d'une part de sa substance la notion d'abus (comme celle de taux usuraire, quand un taux un peu moindre mais sur un temps nettement plus long revient à des résultats en partie similaires) et étendre la période pendant laquelle le débiteur est redevable à son créancier, dans une relation teintée d'éventuelle soumission.

A l'image des prêts immobiliers standards passés de 20 à 30 voire 50 ans, la capacité d'endettement renvoie à l'espérance de vie de l'emprunteur, ou à son espérance de legs de sa dette à ses successeurs. Cas de figure qui ne peut être écarté dans le monde de l'entreprise où la transmission s'accompagne parfois de reprise de la dette[60].

Hors cas de rançon, une concrétisation d'une relation teintée de soumission a donné lieu à un récent signalement à la justice d'un cas de prêt estimé illégal, en France, depuis une société d'investissement vers une entreprise en situation financière difficile, où

60 Dans les faits, le payeur réel d'une rançon pour cryptovirus est souvent le propriétaire ou patron de l'entreprise, sur ses deniers personnels, pour acheter de la cryptomonnaie.

la première semble avoir profité de son ascendant et des fragilités de la seconde pour négocier parallèlement à son avantage le rachat de son patrimoine immobilier en zone urbaine attractive.

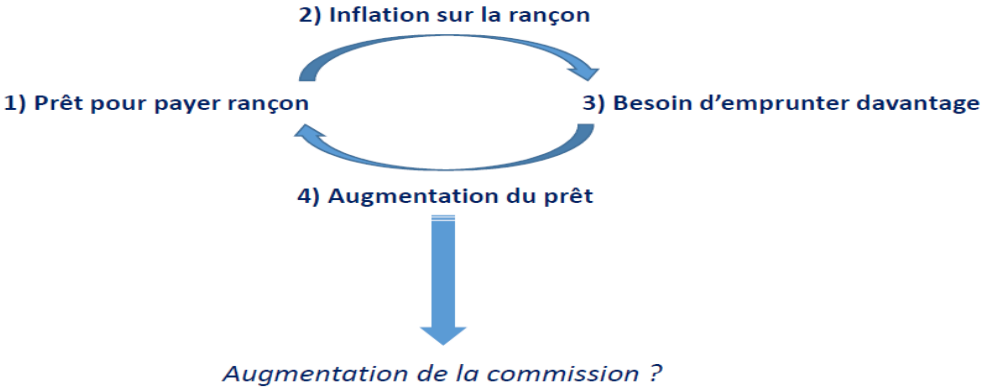
La critique ne se centre par conséquent pas sur le soutien et son motif invoqué d'assistance, mais :

- Sur le fait qu'il nourrit indirectement la criminalité et contribue à la commission d'une action illégale, sans lui irréalisée. Il contribue indirectement aussi, par cet abondement d'argent jusqu'au pirate, à la logistique préparatoire aux actions illégales ultérieures.

- Sur le fait qu'il provoque un effet inflationniste potentiel, également nourrisseur de la criminalité, et où la victime se retrouve de surcroît victime de cette inflation : mon sauveur aggrave ma peine. Je perds en liberté financière ce que je gagne en durée de vie.

Nota : la question se pose un peu à propos d'un don à la victime, par un proche ; ce soutien a aussi un caractère inflationniste, mais moins opportuniste.

Ces interrogations sont amplifiées s'agissant de prêts à intérêt, où le créancier dégagerait un revenu du malheur d'autrui –en sus du « prix du temps » et de la rémunération du risque du prêteur-, après avoir eu de surcroît un effet inflationniste sur le montant de la rançon donc du malheur. Répercussion d'autant plus malvenue que cette augmentation du montant de la rançon incitera à augmenter le montant de l'emprunt destiné à la payer, qui à son tour augmentera le montant de la commission prélevée par le prêteur.



Même à taux identique, tel que 4 %, si le fait de prêter nourrira une hausse des rançons puis des prêts de 10 %, le taux même inchangé de 4 % rapportera 10 % supplémentaires pour le prêteur.

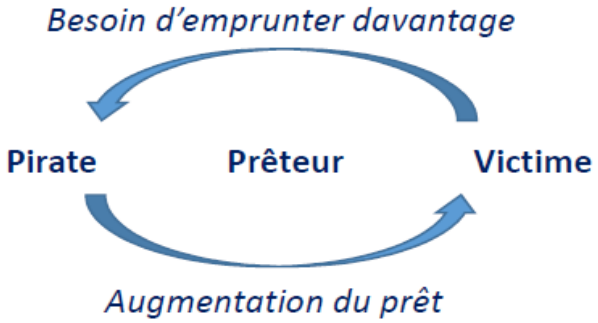
Cette situation est atypique, où l'assouvissement d'un besoin amplifiera le besoin, à l'égal des cas d'école où un verre de vin donne envie d'en boire un autre ; par opposition avec la plupart des besoins humains où l'analyse marginaliste prévoit une décroissance du désir à mesure qu'on boit par exemple des verres d'eau.

Le prêteur agit et interagit :

Le prêteur n'est pas passif, il est agissant sur la demande de monnaie dont il est par ailleurs offreur ;

Le prêteur n'est pas neutre, il modifie son environnement, et à son avantage futur.

On peut douter de la représentation d'un dispositif à trois acteurs au sein duquel le prêteur n'interagirait qu'avec l'emprunteur, puisqu'il influe également sur le racketteur en facilitant ses exigences. En cela sa position tient-elle davantage d'un rôle central, non pas au sens d'intermédiaire mais de diffuseur d'une même tendance à tous.




## 2 - Un prêt pour tenter sa chance

L'essence de ce type de dette amène à l'envisager également comme un prêt à un joueur, puisque la victime d'un cryptovirus n'est jamais certaine d'obtenir une clé de déchiffrement en payant. Elle « joue à la rançon » avec une probabilité de gagner certes élevée mais jamais absolue (au sein de notre échantillon d'entreprises rencontrées, une

des clés effectivement livrées s'est révélée inopérante pour déchiffrer les données, malgré le bon versement préalable de la rançon). L'article 1965 du Code Civil donne une orientation à la réflexion, en ce que « La loi n'accorde aucune action pour une dette du jeu ou pour le paiement d'un pari », susceptible de concerner un contrat de prêt à autrui afin de tenter sa chance à un jeu non pas de hasard mais dont le dénouement dépend du bon vouloir d'un acteur illégal.

Enfin et de manière terre-à-terre, dans un univers numérique où le pirate conserve son anonymat, nul n'est certain que celui-ci et le prêteur constituent deux entités distinctes et sans lien collusif. Il est opportun de rappeler que le crime organisé finance certains piratages mais également fait fonction de banquier dans de nombreux pays, à des taux usuraires ou avec des conditions léonines, pour toute personne ayant des dus à régler sur le champ (« Lors du choc de 2009, certains mafieux italiens prêtaient à un taux annuel de 120 % ; des niveaux à 600 % au Texas ou 3 000 % à New-York ont été relevés, et 10 000 % au Japon de la part de Yakusa »[61]). L'osmose pirate-prêteur ne peut être écartée des hypothèses.

61 Philippe Laurier, *La monnaie dans tous ses états !,* Maxima, 2018.

# DEUXIEME PARTIE

## Le jeu psychologique entre le pirate et le piraté

« Fournir une description exacte des initiatives prises par un individu en vue d'obtenir une utilité maximale, ou un profit maximal s'il s'agit d'un entrepreneur » écrivent Von Neumann et Morgenstern dans leur fameux ouvrage Théorie des jeux et du comportement économique.

« Les utilisateurs de rançongiciels cherchent à maximiser leur retour sur investissement, à gagner des parts de marché. » [62]

Nous verrons que les pirates dérogent à ce schéma d'une priorité absolue accordée au profit, tout au moins à court terme, et que leur posture apparaît être celle d'évangélisateurs, qui instillent progressivement des comportements et des dépendances chez les consommateurs forcés que sont leurs victimes. Quant à l'élargissement progressif de leur clientèle, quoique constatable, il semble modulé par une souplesse qui les recentre de marché en marché au gré des rentabilités sectorielles ; ceci évoque la description faite de la mafia par le juge Giovanni Falcone, non pas d'une pieuvre désireuse d'agrandir sans cesse son territoire d'influence, mais d'un félin qui bondit sur des nouvelles proies plus juteuses lorsqu'elles parviennent à leur portée, quitte à délaisser un temps son ancien gibier.

Une incongruité vient de ce que si le pirate respectait cette prescription de recherche d'un profit maximal, on se serait attendu à ce qu'il réclame une grosse rançon, la plus grosse que la victime soit en mesure de verser. En premier repli s'attendrait-on à ce qu'il exige la plus grosse somme que la victime accepte intellectuellement de verser -le racketteur se ferait homme de marketing-, cas de figure assez en usage à l'encontre de grandes entreprises. Or, pour les petites entreprises, le cas le plus recensé opère un deuxième repli, vers des

62 Patrick Vibert (Control Risks) : « T*he Rapid Evolution of the Ransomware industry ». 2017*

demandes en-deçà de ce qu'aurait pu payer la proie, mais où, à moindre effort, la probabilité d'obtenir d'elle un paiement devient suffisamment élevée : le pirate opère un « mix » entre gain unitaire maximal (espérable) et nombre maximal de gains (espérable) ; mélange qui n'écarte pas l'analyse marketing, mais au contraire la sophistique puisqu'il implique de savoir anticiper les refus d'un client mal connu (Quoique la pratique soit probablement née empiriquement chez les pirates, ce concept est enseigné en école de commerce sous le nom de prix psychologique ou zone d'acceptabilité par le plus grand nombre de prospects). La notion de moindre effort englobe aussi le travail de négocier avec le piraté, puis de blanchir l'argent reçu. On peut supposer que le mix précédent ne procure pas le profit maximal, mais réponde au meilleur ratio profit maximal/effort minimal. Tout ceci s'organisant dans un univers numérique où le coût marginal d'une attaque automatisée supplémentaire contre une petite entreprise est quasi nul, tandis que le temps disponible pour négocier avec les victimes est quant à lui limité par les ressources humaines mobilisables du côté agresseur.

Une autre dérogation au tableau initialement dressé, où les pirates se concurrenceraient pour des parts de marché, transparaît dans leur attitude davantage ressemblante à celle des colons de l'Ouest américain au XIXème siècle, mus par les prochaines vastes terres accessibles, vers une frontière en constant recul. Les pirates ne paraissent pas d'abord en lutte à couteaux tirés les uns contre les autres, mais tous lancés dans une même course, avec ses ruées vers l'or collectives dès qu'un filon se révèle profitable. Ce comportement de dépeceurs rameutés par le même sang évoquerait les conquistadors de José Maria de Heredia : « Comme un vol de gerfauts hors du charnier natal (..) Ils allais conquérir le fabuleux métal ». Chaque révélation d'une vulnérabilité, d'un « Jour zéro », déclenche un land rush, similaire à celui organisé le 22 avril 1889 pour l'Oklahoma, « zero day » durant lequel 50 000 prétendants se lancèrent à midi sonnante sur 8 000 km2 à conquérir en y plantant leurs fanions ; où aujourd'hui des desperados opportunistes se lancent à l'assaut d'entreprises pour y planter leur virus. Ce marché ne se raisonne pas encore comme un gâteau à partager et des parts inextensibles à s'arracher entre brigands, car ce gâteau croît et ouvre de nouveaux territoires de chasse aux pionniers. Leur comportement est à la fois de concurrence mais aussi de coopération –de coopétition-, ou de défis à qui sera le meilleur prédateur, enrichi et craint. Peut-être l'avenir leur réserve-t-il l'équivalent de la fin de la frontière, vécue par les Etats-Unis vers 1890, lorsque ne resteront plus de cibles encore préservées, ou que la saturation d'attaques aura modifié les attitudes envers le numérique.

Concernant la victime, l'*utilité maximale* poursuivie par elle est sa survie. Un cryptovirus, lorsqu'il est susceptible de provoquer la faillite d'une entreprise, met en lumière que son bien le plus important, son actif patrimonial numéro un, est précisément cette vie, le fait d'exister aujourd'hui et encore demain ; en d'autres mots, ce n'est pas telle ligne de l'actif du bilan -actifs matériels tels

qu'une machine ou immatériels tels qu'une marque- mais le simple fait qu'il y ait toujours demain un bilan et un compte d'exploitation.

Etrangement, il sera vu que le premier joueur qu'est le pirate a dans la plupart des cas lui aussi pour objectif tacite la survie de sa victime. On ne tue pas la poule aux œufs d'or, sauf par intervalle pour faire un exemple et imposer la peur aux autres (l'interrogation se portant sur le taux de survie que s'autorise l'attaquant, par catégorie de victimes). Rançonneur et rançonné, leur jeu est à la fois antagoniste puisqu'ils se battent pour une même somme, mais il est codifié en ce que tous deux se rejoignent dans le fait que l'entreprise rackettée les fait vivre, et qu'à ce titre il est désirable qu'elle perdure pour continuer cette tâche.

## A - LA SOURIS QUI VEUT VIVRE ET LE CHAT QUI N'A PAS INTERET A LA TUER

### 1 - Le profil des petites entreprises acceptant de payer une rançon est éclairant quant à leur motivation première : survivre

Certains chiffres interpellent, à l'image de ce rapport estimant que la moitié des victimes de rançongiciels acquittent une rançon[63], niveau en décalage avec notre échantillon, qui l'estimait à un dixième environ (en 2018, pourcentage en hausse depuis). Toutefois, tandis que la première estimation se construit à dires d'expert, à partir d'un panier de 1200 spécialistes de la sécurité informatique, notre recensement se focalise sur des petites entreprises dont beaucoup n'ont pas les finances pour s'adjoindre de tels professionnels de l'informatique. Une hypothèse plausible sera que ces deux ratios s'appliquent à des populations d'entreprises en partie différentes, l'une avec des capacités financières importantes -grandes entreprises ou ETI- où la propension à payer une rançon serait avec toutes réserves de 50 % environ, l'autre où ces capacités sont modestes -TPE et petites entreprises- où la propension baisse jusqu'à 10 à 20 % environ. Compte doit être tenu également qu'une entreprise voyant tout son patrimoine vital chiffré sera à la fois tentée, quelle que soit sa taille, à la fois d'appeler des experts en sécurité à leur secours, et de payer in fine. En cela, outre la taille de l'entreprise, la *taille relative de son préjudice* joue égale-

63 *Cyberthreat Defense Report 2019*, publié par CyberEdge.

ment.

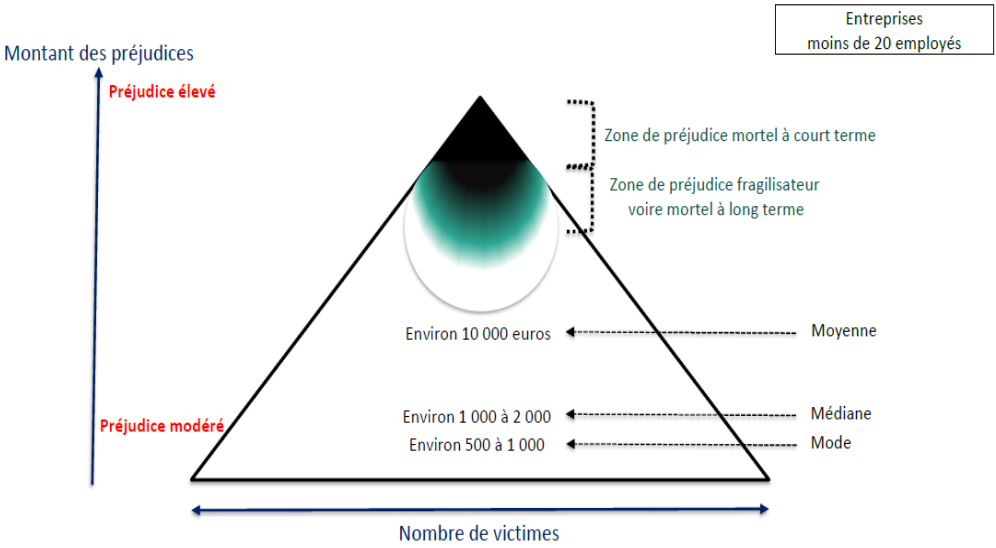
Cette notion de taille relative du préjudice se révèle un facteur essentiel d'explication. Taille qui ne s'exprime pas aux yeux d'un entrepreneur par un pourcentage abstrait mais par des seuils concrets, à la fois comptables et psychologiques, tels que :

- lorsque l'impact s'alourdit jusqu'à signifier l'abandon par exemple d'un investissement ou d'une embauche.

- lorsqu'il s'alourdit jusqu'à mettre en péril la société.

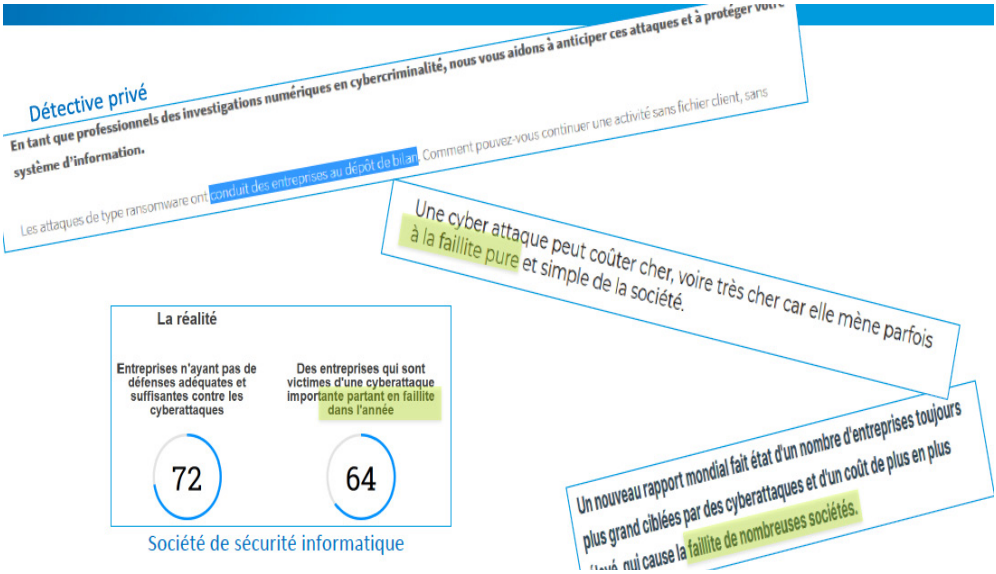
L'inexistence des cas connus où une multinationale se serait trouvée exposée à ce niveau absolu de menace, contraste avec les cas beaucoup moins rares où une petite entreprise y fait face. Pour ces dernières, les observations rapportent une aversion et souvent une répulsion à payer rançon, aussi longtemps que le degré vital de la société n'est pas atteint ; niveau à partir duquel inversement, la propension à payer devient majoritaire dans notre échantillon.

Alors que la moyenne des préjudices pour des entreprises de moins de 20 personnes avoisine 10 000 euros, selon nos estimations-, l'incitation à payer se fait forte lorsque les préjudices deviennent un multiple de cette moyenne, en dizaines de milliers d'euros. Avec pour horizon proche, puisque les coûts sont croissants, la crainte de sommes bientôt plus élevées et au-dessus de la fortune d'une entreprise type de cette taille.



L'invocation morale qui prohibe le paiement de rançon est efficace, aussi longtemps que la destinée de l'entreprise n'en souffre pas ; stade à partir duquel son poids décroît jusqu'à quasiment disparaître à l'entrée dans la zone de préjudice mortel, dans une variante alors de « préférer sa mère à la justice ». Avec, pour précision, deux sous-niveaux dans ce climax, le premier où l'entreprise sera mortellement atteinte mais dépérira lentement de ce choc, le second qui relève d'un scénario de mort subite.

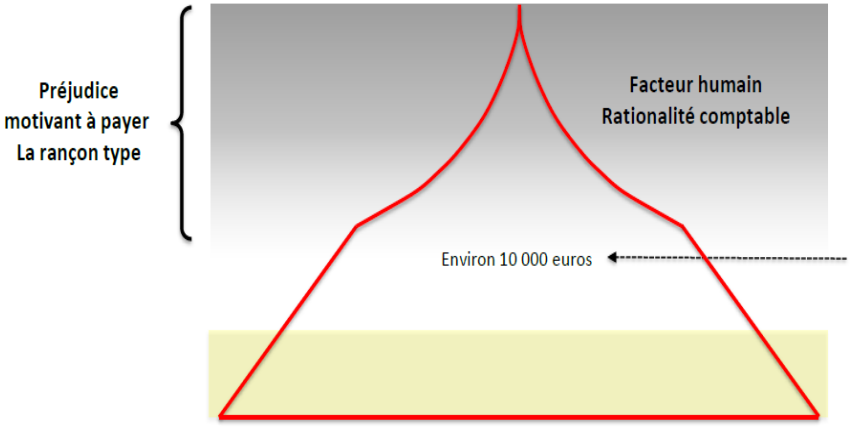
Une confirmation de cette « rationalité de payer » transparaît dans le constat de la rareté des entreprises faisant faillite, suite à un cryptovirus. Rareté qui dément bien des commentaires de presse ou arguments de vente d'outils de sécurité, avec le spectre brandi d'une litanie de faillites supposées déjà advenues.




Au cours de notre étude, un seul et unique cas de faillite par cryptovirus a été enregistré parmi nos interlocuteurs, qui de manière flagrante relie la cause à l'effet ; encore ce cas correspond-il à une mort lente, l'année suivante, et sur une victime déjà fragilisée par la morosité préalable de son activité commerciale (son malheur supplémentaire a été que le cryptovirus s'introduise durant le mois de l'année où son activité saisonnière enregistre les meilleurs chiffres habituellement). En dehors de notre échantillon direct, le peu d'évè-

nements médiatisés, d'ailleurs souvent avec ce profil déjà fragilisé, conforte ce bilan de rareté : le nombre de victimes qui ont *failli* mourir excède largement celui des mourants.

En conséquence, la pyramide des victimes (avec en abscisse horizontale le nombre des victimes, et en ordonnée le préjudice de chacune) ressent ces seuils, avec une atténuation de population dès qu'on approche des niveaux mortels, précisément du fait de l'existence de ce « joker » qui par le paiement de rançon fige les coûts et les empêche de monter encore. De manière simplifiée, ne retenant que des impacts mortels ou non mortels, la pyramide devient rhomboïdale c'est-à-dire à deux plans inclinés au moins. En bas, le nombre des petits dégâts résulte de causes strictement matérielles, qui ne voient pas leur distribution perturbée par des facteurs humains ; en haut au contraire, la capacité d'évitement par l'acceptation de paiement réduit le nombre final des gros impacts (en fait cette pyramide devra-t-elle présenter une probable boursouflure juste au-dessous des seuils à partir desquels les victimes se trouvent -en moyenne- incitées à payer. Bourrelet qui incorpore toutes celles ayant choisi d'abandonner leur bras de fer avec le pirate à ce niveau de dépense).




Le volume d'interviews menées ne permet pas à la présente étude de formaliser en détail la pente de cette pyramide, seuil par seuil, mais elle aide à sérier les niveaux moyens (pour une taille donnée d'entreprises) où la décision humaine interagit avec l'évènement, lorsqu'elle accepte d'emprunter cette échappatoire du paiement qui efflanque alors le haut du triangle. Deux jauges pèsent particulièrement dans la décision, à savoir la trésorerie de ces entreprises -plus globalement

leur fonds de roulement, avec en arrière-plan leurs fonds propres ou leur capacité d'emprunter- ainsi que leur bénéfice.

S'agissant d'une petite PME de quelques dizaines de personnes, un coup dur aussi imprévu qu'une attaque informatique provoquant un trou en centaine(s) de milliers d'euros la fait entrer en zone dangereuse. Par anticipation, la zone de décision entre payer ou non est assez typiquement celle des dizaines de milliers d'euros de préjudice déjà subi.

> La différence d'exposition entre grandes ou petites entreprises se retrouve dans le fait que le fonds de roulement des PME est accaparé déjà par leur Besoin en Fonds de Roulement (« Les PME présentent le BFRE –Besoin en fonds de roulement d'exploitation[64]- le plus élevé, à 32 jours de chiffres d'affaires. (..) Celui des grandes entreprises est nul en 2018 ».) Les PME ont des comptabilités souvent tendues par avance, avec des capacités modérées à sortir sur le champ de leur poche, de leur trésorerie, de quoi acquitter une rançon importante.

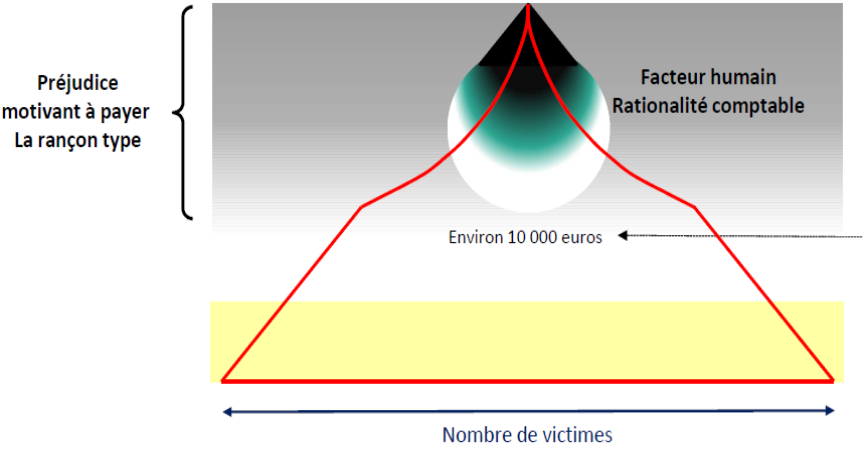
La *zone de décision* est souvent plus basse encore pour celles de moins de dix employés, car « Une TPE sur cinq présente des fonds propres négatifs ou nuls, contre 7 % des PME. »[65]. Le choc que représente un cryptovirus causant plusieurs milliers ou dizaines de milliers d'euros se juge mieux en le comparant à la modestie de leurs profits usuels ; le résultat d'une année de labeur peut être phagocyté en quelques jours : « Le résultat net courant moyen des entreprises de moins de dix salariés s'est élevé, en moyenne, en 2018, à un peu moins de 30 000 euros si on exclut le secteur de la santé (pharmacies …). Un peu plus d'une TPE sur quatre a réalisé un bénéfice net inférieur au Smic annuel net, sachant que pour certaines entreprises individuelles, ce revenu fait vivre l'entrepreneur et son conjoint. »

---

64 Bulletin de la Banque de France, 227/5 - 2020 : « La situation des entreprises en France en 2018 : les PME tirent leur épingle du jeu ».

65 L'analogie entre entreprises déjà fragiles et coup de grâce donné par un cryptovirus serait réductrice ; notre étude a constaté que plusieurs entreprises saines et en croissance rapide s'en trouvaient d'autant plus frappées de plein fouet. Le chiffrement de données brutal casse leur dynamique, remet en cause une relation au client porteuse d'avenir, et vient impacter un fonds de roulement qui était fortement sollicité par le financement de la croissance. Bulletin de la Banque de France, 226/7 - 2019 : « Les PME et TPE en France ».

Les victimes qui payent accentuent la forme trapue de la pyramide, par une pointe étranglée dans sa largeur (pour rappel, le présent profil des pentes illustre la décroissance du nombre de victimes à mesure de l'élévation de leur préjudice total, basé sur notre constat d'un mode et d'une médiane très bas, inférieurs à 2000 euros. Il n'a pas la prétention de restituer l'exacte inclinaison de ces pentes). Sont pyramidion correspond pour une grande part à des entreprises n'ayant pu ou voulu activer le parachute de secours qu'est la rançon ; ou si le parachute ne fonctionne pas.




## 2 - Choisir entre payer ou périr

La précédente référence à l'instinct de survie reformule les craintes types d'un entrepreneur, et introduit deux concepts :

- Avec un glissement depuis le coût moyen jusqu'à l'écart-type ;

- Et un autre glissement depuis la probabilité d'occurrence jusqu'à la récurrence ensuite des futures attaques réussies, où l'intérêt du pirate est que sa victime raisonne à court terme, sans tenir compte de l'accélération de la fréquence des rançons qu'elle favorisera en payant la première dîme.

La relative modestie du montant moyen des préjudices (de l'ordre de 10 000 euros actuellement pour une petite entreprise) n'est pas incitative pour un dirigeant de petite entreprise à investir massivement dans la sécurité technique et dans une protection assurantielle. Les

référents mentaux de ce petit patron lui feront apparenter un tel préjudice aux aléas dont il est coutumier, au même rang que les impayés d'un client.

Son questionnement et son souci premier s'en trouvent déportés : **non plus connaître un coût moyen et une probabilité d'occurrence générale, mais savoir la proportion d'attaques s'écartant de ces moyennes jusqu'à devenir mortelles pour une société comme la sienne :** est-ce une sur dix, une sur cent … ? Quel est mon risque final de faire faillite ? Et dans cette éventualité, combien me coûterait une rançon libératrice ?

La relative modestie de la moyenne des préjudices, agrémentée de cette alternative au trépas qu'est le versement de rançon au cas où le préjudice s'éloigne d'une telle moyenne, accouche d'une « règle du jeu » peu motivante à investir lourdement afin de se protéger informatiquement ; d'autant que le montant type des rançons pour PME –quelques milliers d'euros- s'avère inférieur ou guère supérieur à ce que coûterait le rehaussement de son niveau de sécurité informatique. L'expression « règle du jeu » est ici symptomatique d'un jeu avéré, d'une relation d'attaquant à attaqué où le pirate positionne ses exigences pécuniaires à un niveau intellectuellement acceptable par beaucoup de victimes acculées à choisir entre payer ou périr ; telle est sa « proposition de valeur ». A ce titre, un cryptovirus relève aussi, malgré sa composante informatique, d'une ingénierie sociale mise en œuvre par l'assaillant, faite de négociations avec sa proie, et d'un « positionnement prix » qui le place en position de fréquent vainqueur car il formule « une offre qu'on ne saurait comptablement refuser ». Avec pour rappel que, si la proportion d'entreprises ayant acquitté une rançon est minoritaire au sein des échantillons étudiés, elle devient majoritaire à mesure que la perspective d'un dépôt de bilan se rapproche, jour après jour au fil de l'attaque.

L'argument cynique des pirates est basiquement financier, par la rentabilité objective à acquitter une forme d'impôt arbitraire, à verser tribut au vainqueur, qui laissera la vie sauve au vaincu … jusqu'à la prochaine attaque (déjà programmée parfois, en restant tapi dans le système affecté). Les témoignages soulignent qu'une ancienne victime sera à nouveau ciblée avec persistance, et d'autant plus qu'elle s'est signalée consentante à payer une première fois.

**Le questionnement se voit déporté une seconde fois : non plus mesurer un coût maximal, désormais évitable par paiement de rançon, mais connaître la récurrence de telles extorsions même plafonnées** :

paierai-je en moyenne une fois par décennie, par an, ou par semestre … ?

Le piège tient à la routinisation d'un évènement, jusqu'à un état futur de banalisation aussi du geste d'acquitter la rançon. Les failles de nos systèmes d'information nous confrontent à des acteurs qui exploitent aussi nos failles de raisonnement comptable, par la rentabilité apparente mais de court terme de payer. Les pirates sont tout autant des financiers, qui investissent dans des moyens d'attaque technique puis parachèvent cet arsenal avec une « proposition tarifaire » efficace. Ce sont pour beaucoup des hommes d'affaires qui pratiquent l'art de la guerre, ou plus exactement la poliorcétique : l'art du siège, destiné à reclure sa victime dans une nasse informatique, comptable et psychologique menant à une probable reddition ; vécue comme une délivrance par la victime, à tort car ce sera en réalité un abonnement à un système de prédation, et l'acte d'alimenter régulièrement en argent un agresseur qui assiège pour asservir, pour rendre tributaire, mais non pas tuer sa poule aux œufs d'or.

## B – LE CHAT ET LA SOURIS, LE PIRATE ET SA PROIE

« Considérons un jeu où le gain dépend à la fois du hasard et de l'habileté des joueurs, et bornons-nous au cas de deux joueurs A et B … » [66]

… Considérons un jeu avec trois joueurs A, B et l'assureur C

L'absence quasiment d'arrestation de crypto-pirates n'apparente pas l'état des lieux à un jeu du gendarme et du voleur ; ce dernier, laissé face-à-face avec sa proie, évoque davantage l'autre jeu qu'est le chat et la souris. Leur confrontation tient du huis-clos, d'une pièce en plusieurs actes puisqu'un peu de temps est accordé à la victime pour faire évoluer sa position, réfléchir aux enjeux, pour chercher souvent vainement des solutions dans un effort que le chat sait précisément vain par avance ; ce dernier laisse la souris prendre conscience de son

66 Émile Borel, « La théorie du jeu et les équations intégrales à noyau symétrique », 1921. Oskar Morgenstern et John von Neumann ont appliqué aux comportements économiques des réflexions mûries depuis plusieurs siècles sur les choix des participants à un jeu, les interactions entre ces choix, et la répartition de leurs gains, de Pascal à Ernst Zermelo.

enfermement dans un labyrinthe dont il maîtrise les clés de la seule issue négociable (nous adopterons le cas majoritaire d'un pirate qui dialogue puis tient sa promesse de livraison de clé). Temps également imparti à l'attaquant puisqu'il l'utilise pour jouer avec la psychologie d'un captif qui se débat, en agitant des menaces de hausse de la rançon ou en accordant des baisses faussement généreuses.

Cet attaquant est pour une grande part le maître des horloges, puisqu'il peut cesser le dialogue, instaurer des dates butoir, y mettre fin selon son seul vouloir. L'autre n'a autorité ni pour commencer la partie, ni pour la clore sauf en se soumettant aux desideratas de son rançonneur (ou en assumant les frais, lorsqu'ils restent dans sa capacité financière ; cas heureusement majoritaire). Cette maîtrise du temps applique les modes opératoires des mises sous influence caractéristiques de l'ingéniérie sociale, et empruntent notamment à des précurseurs tels que Kevin Mitnick le déroulement d'un scénario préparé, selon un tempo et dans une atmosphère que l'assaillant parvient à imposer (Mitnick cependant, sorte de hacker ludique, adaptait en permanence ses scénarios à la situation du moment, réactivité dont les actuels rançonneurs contre les petites entreprises ne font pas preuve, avec de leur part un registre de réponses réduit et stéréotypé).

## 1 - Une ingéniérie sociale aussi présente chez l'attaquant que l'ingéniérie informatique

Dans un nombre très élevé de cas, les sommes demandées -avant comme après la baisse- étaient d'un montant pécuniairement accessible à la victime au regard de ses encaisses sur son compte en banque. Son refus initial ne tenait donc pas à une impossibilité matérielle de payer, mais au fait de considérer soit l'acte soit la somme comme inacceptable en soi, dans l'absolu ; que soudain au bout par exemple du dixième jour de blocage des données, le pirate accorde une remise de 50 %, a tendance chez beaucoup de ces victimes à rendre la nouvelle somme acceptable relativement, car elles ont l'impression diffuse d'avoir économisé autant qu'elles vont payer ; on me demandait une somme arbitraire et je m'en sors avec un demi-arbitraire. La bouteille devenue à moitié vide n'est pas loin d'être vue à moitié pleine. Demi-prix leur apparaît plus tolérable, non pas tant du fait du prix mais du fait de la demie. Dans son principe, quel qu'ait été

l'exigence initiale, c'est subjectivement mieux (mieux qu'un quelque chose indifférent. Rares sont les victimes calculant que la demande du pirate correspondait par exemple au centième du patrimoine de leur entreprise, et pesant si ce ratio était « déraisonnable » ou pas, mais le demi-centième leur apparaît plus « raisonnable », puisque le ratio de substitution qui s'impose à leur entendement est un ½ bienvenu). Le payeur ne diffère pas tant d'un touriste qui visite un bazar à l'escale du paquebot, sait que ce dernier repart irrémédiablement dans deux heures et qu'après il sera trop tard, mais que dans l'intervalle il a réussi par son bagout à arracher une baisse au vendeur de faux artisanat du cru … Tout en sachant confusément que la négociation fait partie du jeu local pour chaque fournée de touristes, et qu'elle aboutira à un chiffre terminal qui a toujours été l'objectif réel du vendeur.

La victime ressort de cette guerre d'usure avec l'intime conviction d'avoir lutté (j'ai discuté pied à pied), d'avoir fait jouer sa volonté ou son habilité (j'ai dit NON -non … à cette somme- et le pirate a bien été obligé de revoir ses prétentions ; ou, variante, je l'ai berné en lui faisant croire que je n'avais que 2 000 euros à disposition), d'avoir été vaincu avec les honneurs en ayant sauvé la face. Tope-là à moitié prix.

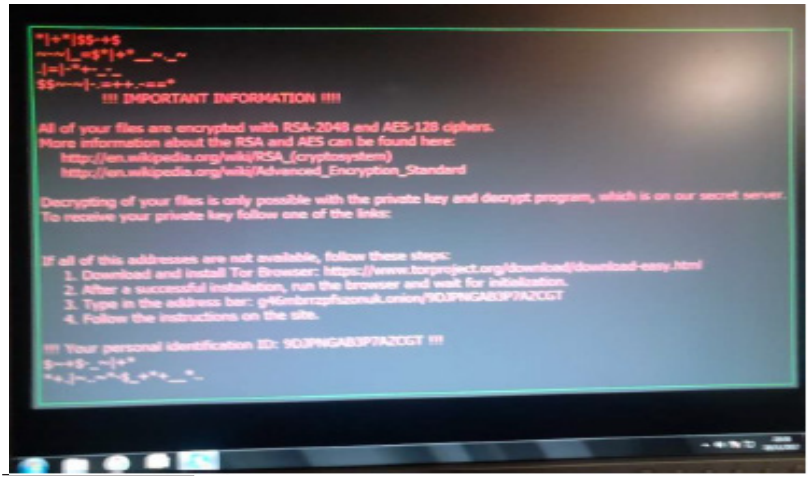
## 2 – Des « liens » psychologiques

Le seul fait de la part de la victime d'entrer en négociation est cpendant une première victoire du pirate, car c'est accepter non pas encore de payer mais d'ores et déjà de tisser un lien au sens de carcan mais également au sens relationnel. Relation dont l'évolution sera aussi balisée qu'un parcours du jeu de l'oie ponctué de puits et de prisons.

Côté assaillant, et loin de l'image de l'informaticien solitaire, la montée en puissance des équipes de crypto-pirates provoque une fréquente division du travail qui permet la spécialisation de la fonction du négociateur, distincte de celle de l'informaticien qui lance les attaques en série, puis du blanchisseur d'argent, et complémentaire à eux. Ce négociateur dispose d'une palette de phrases type pour échanger avec ses victimes, et il déroule des dialogues pré-écrits pour la plupart, mais avec un phasage adaptable à la vitesse de maturation de chacune de ces victimes. Ce qui est formaté y revêt des allures individualisées, ce qui était désincarné par le numérique trouve une humanisation de façade. En référence au jeu du gendarme et

du voleur, la victime, alors fréquemment en situation psychologique de solitude, trouve un interlocuteur, une présence même virtuelle et une écoute même artificielle … non pas chez le gendarme mais chez le voleur. Faire référence au Syndrome de Stockholm et à l'empathie ressentie par des otages envers leur geolier serait néanmoins inadapté[67], bien que plusieurs de ses ingrédients se retrouvent :

> le pirate fait œuvre pédagogique en laissant un message explicatif à l'écran, qui contient quelques rudiments de cryptologie pour aider à comprendre la gravité de la situation -c'est l'agresseur qui enseigne à l'agressé la nature et l'ampleur du coup asséné, comme on l'attendrait d'un diagnostic de médecin après une agression physique-. Lire ce message est un pas franchi vers lui, même minuscule et instinctif : vous acceptez d'obéir à cette proposition de lecture explicative qui vous devient moins insupportable que de rester dans l'ignorance. Vous acceptez de savoir, même quand l'instructeur est votre bourreau.




67 Syndrome décrit par le psychiatre Nils Bejerot à partir de l'étude d'un braquage de banque en 1973 ayant dérivé en prise d'otage sur des employés. Affaire qui néanmoins recouvre pour une part notable un phénomène bien répertorié anciennement d'hybristophilie (attirance addictive envers un criminel de sexe opposé. Voir également le cas Patricia Hearst, enlevée en 1974 et qui adhèrera à la cause de ses ravisseurs, puis qui après son arrestation épousera un ancien policier affecté à sa protection en attente du procès). En effet, ce cas d'école minore ici le fait que 3 des 4 otages étaient des femmes, dont la plus engagée a été au fil des jours très en pointe dans le soutien à son principal ravisseur durant les négociations téléphoniques avec la police qui encerclait la banque. Ce preneur d'otage, incarcéré ensuite, a reçu en prison de nombreuses lettres sentimentales d'inconnues, phénomène observé couramment sur des cas similaires (affaire Alègre en France, etc.)

- Il devient votre guide, vous indique comment se procurer des cryptomonnaies.

- Ce pirate ne montre que ponctuellement une agressivité verbale inutile, à part des épisodes de culpabilisation de la victime -vous avez visité tel site, vous avez été imprudent- ou de provocation à réagir. Il est factuel, ses propos sont relativement neutres. En quelque sorte est-il professionnel, il parle affaires et vous invite à dépassionner l'enjeu pour soupeser la compétitivité de son offre de service.

- Il fait preuve souvent de rationalité, qui sert d'ancrage fiable pour la victime désorientée. Même ses moments d'irrationalité ou de colère trouvent souvent une explication intelligible par la victime, et parfois même explicitée par le pirate : vous m'avez menti en essayant de me faire croire que vous êtes un pauvre particulier alors que vous êtes une entreprise ; ou : je vous avais prévenu d'une date butoir que vous avez laissé passer, etc.

- Celui qui accepte d'être ainsi conduit vers la levée d'écrou et le bout du tunnel s'en remet à ce tiers auquel il accorde un peu de confiance non pas en tant que racketteur mais en tant qu'homme de parole qui transmettra la clé : sans foi mais pas sans sa propre loi.

En comparaison, et face au besoin humain de rompre l'isolement et de trouver conseil, un constat fréquent est la parcimonie des manifestations de présence personnalisée venant des acteurs institutionnels publics ou privés, lors de la crise : pédagogie, écoute, guidage, sont laissés au hasard des circonstances, au gré des acteurs locaux eux-mêmes parfois peu sensibilisés ou formés à ces prises en charge, et en tout cas accaparés par d'autres priorités au quotidien (Aucun signalement d'intervention effectuée par une préfecture n'est ressorti de nos entretiens de terrain. Plusieurs cadres ou entrepreneurs ont rapporté des accueils froids ou des quiproquos ubuesques lorsqu'ils sont allés déposer plainte –des exceptions ont été signalées aussi, mais qui dessinent un tableau d'ensemble national trop variable-. Beaucoup de leurs interlocuteurs n'ont pas été formés pour saisir qu'il ne s'agit pas d'un évènement passé mais souvent toujours en cours, d'une prise en otage de données qui si elles sont stratégiques mérite l'étiquette de PRISE EN OTAGE D'UNE ENTREPRISE). Le « comment payer » s'en trouve mieux servi que le « comment ne pas payer

». La réactivité est du côté du pirate-infirmier, immédiatement disponible pour entamer une discussion dès après le virus installé (Un entrepreneur victime « pris dans des rets, dont ses rugissements ne le purent défaire. Sire pirate accourut, et fit tant … »).

Un travail est à parachever afin de créer un équivalent, dans l'esprit, d'une « police informatique de proximité » (ou d'assurance et d'assistance de proximité …), apte à contrebalancer l'attractivité de la bulle de dialogue donc d'intimité liant le chat et la souris, avec le parcours fléché proposé à cette dernière. Contrepoids qui sache dépasser le traditionnel formulaire de dépôt de plainte dont la dématérialisation en marche s'est étoffée d'une pré-déclaration en ligne peu propice à apporter un soutien affectif (« Les renseignements demandés sont exclusivement destinés au traitement informatisé de la déclaration »). A titre d'illustration du statut encore peu reconnu de victime de cyberattaque, la rubrique en ligne « Préjudice matériel » n'y intègre pas l'intitulé ordinateur ou données numériques dans la liste des objets concernés -sauf une ligne « multimédia » très généraliste-, et se contente en complément d'un « Si l'objet concerné ne figure pas dans la liste déroulante, cochez la case suivante » ouvrant une fenêtre à remplir.

Un simple test comparatif montre que le temps requis pour remplir la pré-plainte puis aller déposer plainte n'est pas inférieur à celui de se procurer des bitcoins puis les envoyer, pour une personne maîtrisant bien le numérique. Il n'est d'ailleurs pas exclu qu'une part des refus de payer la rançon provienne, au-delà des postures morales, d'un manque de familiarité intellectuelle d'une victime avec cet univers des blockchains ; or la frange de population néophyte en informatique et en cryptomonnaies diminue progressivement, ce qui fait entrevoir pour l'avenir un réflexe facilité de payer.

-> La nécessité d'un travail d'homogénéisation par le haut, et d'un recueil d'informations judiciairement exploitables, se verra renforcée à chaque hausse du nombre des attaques.

L'entrelacs des liens entre ces deux protagonistes est densifié par le sentiment d'une présence. Celle-ci se voit confirmée par défaut puisque des témoignages ont souligné à quel point lorsque le pirate,

ludiquement ou pour affermir son emprise, devient soudain silencieux et injoignable durant plusieurs jours, ce cordon coupé est ressenti avec angoisse comme le présage d'un chiffrement définitif des données ; mais ressenti aussi avec culpabilité par la victime qui se reproche d'avoir mal compris une étape des procédures à suivre dans le manuel du parfait rançonné, ou commis une erreur de formulation dans ses doléances (ces reproches sont palpables lorsque plusieurs personnes ont co-agi et ignorent laquelle aurait mal compris ou fait). Elle se sent doublement fautive, d'avoir cliqué à tort sur une pièce jointe, puis d'avoir mal dialogué.

## 3 – Des comportements qui renvoient à la théorie des jeux

Quelques composantes de ce drame sont isolables, qui le rapprochent de la *théorie des jeux* (dont l'expression la plus célèbre est le dilemme du prisonnier, dans une version du jeu qui est à somme non nulle) : agresseur caché A et agressé B négocient une même somme nommée rançon, qui sera au final propriété soit de A soit de B, mais jamais des deux. La symétrie n'est cependant pas atteinte :

- Car seule la souris B fournit l'éventuelle mise qu'est la rançon, et elle seule supporte l'impact de l'attaque. Le chat A n'enregistre aucun débours à ce stade. La rançon est une perte dans l'absolu pour la souris si elle est versée, alors qu'elle n'est qu'une perte de gain pour le chat si elle ne l'est pas. Quoique leur valeur psychologique et même pratique diffère, entre renoncer à un avoir ou à un espoir.

- Car ce qu'aurait à perdre la souris est plus gros que pour le chat (dont la seule vraie perte serait celle de sa liberté en cas d'arrestation par la police, or le risque est actuellement trop faible presque pour entrer dans des statistiques).

Ainsi lorsqu'ils « perdent au jeu », respectivement, le pirate ne perd quasiment rien, tandis que sa victime peut perdre jusqu'à quasiment tout son patrimoine. Première asymétrie.

Pour rapprocher cette situation de la théorie des jeux, une reformulation serait que :

- A et B apportent tous deux une mise : le pirate investit une petite somme dans des outils d'attaque installant des clés de chiffrement, et en attend une retombée positive mais qui sera

nulle en cas d'échec ; le piraté investit ultérieurement une petite somme pour acheter une clé de déchiffrement, et en attend une retombée positive mais qui sera nulle en cas d'échec. Leurs mises sont asynchrones, la fin de l'une est déclencheuse du début de l'autre.

- tous deux se battent pour un espoir : pour le pirate est-ce l'espoir de gagner une somme x nommée rançon, pour l'entreprise est-ce celui de sauver une somme X correspondant au préjudice encore évitable -ce qui est *à perdre* se transforme donc en à sauver au sens presque de « à gagner »-. La question tourne autour de la comparaison entre x et X : lequel est supérieur à l'autre ($x < X$, ou $x > X$, ce dernier cas étant majoritaire dans nos observations puisque la médiane et le mode en matière de préjudices s'avèrent inférieurs à la rançon type de 2 000 à 3 000 euros). Et quelle ampleur de supériorité de X sur x sera-t-elle déclencheuse d'un paiement (nos observations, bien qu'encore imprécises, convergent vers des ratios supérieurs voire très supérieurs au décuple : $X \geq 10\ x$. Un tel ordre de grandeur égal ou supérieur au décuple, s'impose psychologiquement à la victime car il n'est plus écartable dans ses réflexions. La société de cybersécurité Coveware retient des grandeurs similaires, avec pour la seule composante des coûts d'arrêt –incluant les pertes d'opportunités de chiffre d'affaires- un multiple entre 5 et 10) ?

La théorie des jeux est teintée ici de guerre asymétrique : asymétrie quant à la capacité d'initier l'évènement, sur le coût supporté par chacun en cas d'échec (minuscule pour le pirate d'autant que l'investissement informatique n'est pas perdu et pourra resservir ; potentiellement énorme pour le piraté), sur l'ampleur du gain espérable. Asymétrie donc sur qui décide, qui gagne et combien, qui perd et combien.

## 4 - Enoncé de la « règle du jeu »

De manière cocasse, le seul dont la dépense est certaine est le pirate A, car à l'origine il a investi dans un dispositif d'attaque et de propagation du cryptovirus, ainsi que dans un travail préparatoire.

Sachant que la grande majorité des attaques échouent, A ne touche rien mais ne perd que ses menus frais et du temps. La

cible B n'enregistre aucune dépense. Le jeu se résume à A sans B. A est perdant.

Sachant ensuite que dans près de 9/10 attaques réussies contre des petites entreprises, le versement d'une rançon n'a pas lieu, le pirate repart bredouille. A perd à nouveau, peu, tandis que B cette fois devient perdant également, par les préjudices de l'attaque.

Le système de tarification du pirate ne se fonde cependant que modérément sur des coûts de production (coûts informatiques complétés par ce qu'il estime son temps de travail) assortis d'une marge bénéficiaire, selon les préceptes des économistes Classiques -Smith, Ricardo …-, mais davantage sur l'utilité de la clé de déchiffrement promise, selon les préceptes Néoclassiques -Jevons, Walras et avant eux Daniel Bernoulli à partir de son Paradoxe de Saint-Pétersbourg-.

-> Dans une première tentative simpliste de définition, le modèle économique d'un pirate par cryptovirus consisterait à engendrer le maximum de préjudice pour accroître d'autant la valeur de la clé de déchiffrement.

L'approche néoclassique focalisée sur l'utilité marginale se redéfinit ici en « utilité résiduelle » de la clé, au sens de valeur encore sauvable par l'entreprise affectée, jour après jour ; le résidu qui n'a pas encore été détruit fait intervenir le temps futur. Le pirate se trouve en position de force proportionnée à l'utilité résiduelle de ce qu'il détient, utilité est elle-même proportionnée aux dégâts évitables par obtention de la clé de déchiffrement (en quelque sorte, les dégâts déjà actés lui servent à titre d'échantillon, de preuve de savoir-faire, tout comme certains pirates livrent une clé échantillon capable de déchiffrer une petite partie des données corrompues afin de prouver être en mesure de livrer d'autres clés contre d'autres paiements).

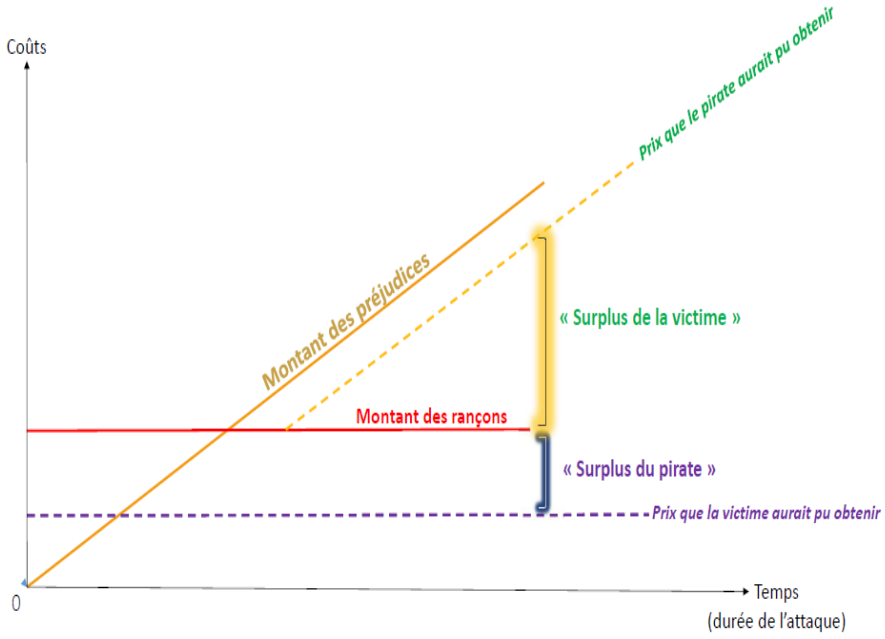
-> Dans une deuxième tentative de définition du modèle économique du pirate, son objectif n'apparaît plus directement d'engendrer le maximum de dégâts initiaux mais potentiels, en attente (préjudice résiduel, donnant la valeur résiduelle de la clé), toujours pour vendre un évitement de coût X, pour un prix x inférieur à X.

Coûts évitables X qui devraient lui servir de référent pour positionner son exigence d'argent ; or ce pirate est dans l'ignorance du montant de X puisque la plupart de ses victimes sont des inconnues pour lui,

tout comme l'est l'ampleur des dégâts effectifs qu'il y a déjà causés.

Le pirate ne cherche par conséquent pas initialement à s'ajuster sur ce coût inconnaissable et, sauf à avoir la chance que d'emblée la victime accepte de payer au vu des premiers dégâts, sa tactique va être au contraire :

a) soit de de laisser ce coût X inconnaissable s'ajuster par rapport à son tarif x, ce qui privilégie des entreprises chez lesquelles le blocage des données engendre des préjudices totaux durablement croissants dans la durée, et qui se signaleront d'elles-mêmes tôt ou tard être disposées à payer. Le pirate se met en mode passif, il attend et maintient un lien de dialogue non pas dans une optique de réelle négociation mais de disponibilité. Il s'exonère ainsi du besoin de deviner quand la victime paiera, puisque c'est elle qui saura le moment où céder sera devenu inéluctable ; ce pirate joue sur le temps, ou plutôt le temps joue pour lui : sa proposition gagne de l'intérêt progressivement, elle prend de la valeur (elle enregistre une plus-value), jusqu'à devenir déclencheuse d'un paiement. Le schéma ci-après retient l'hypothèse d'un montant de rançon fixe, quoiqu'une sorte d'enchère montante serait envisageable tant qu'elle ne dépasse pas le montant prévisible des préjudices.



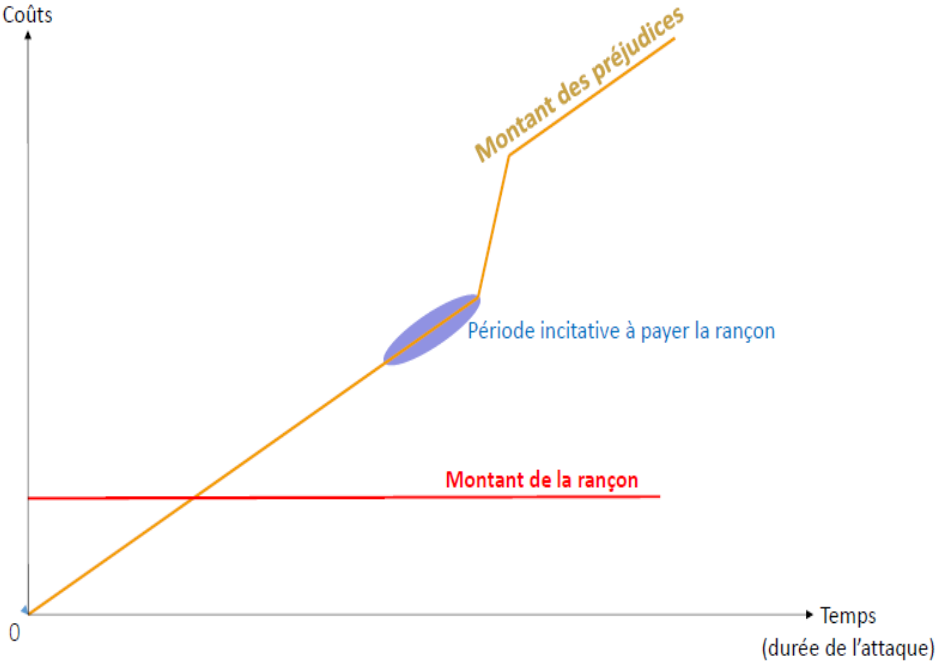
Malgré ses dehors frustres, cette première tactique tarifaire du pirate met en application les principes économiques de Jules Dupuit : de même que le « surplus du consommateur » désigne l'écart entre le prix que paye un client et le prix jusqu'auquel secrètement il aurait consenti à monter (écart qui incite à acheter le bien concerné, puisque le client lui accorde une valeur supérieure à son prix, et y trouve un « bénéfice »), serait à définir un « surplus de la victime » : pour éviter un préjudice de 100 000, il serait rationnel de se tourner vers une solution < 100 000 puisqu'elle dégage une économie. Plus l'économie sera importante, plus la tentation de payer se fera pressante. Cette économie dégagée est le « surplus de la victime », égal ici à X-x (Préjudice moins tarif de la rançon).

> Une troisième tentative de définition du modèle économique du pirate consiste de sa part à proposer une rançon d'un montant qui gonfle suffisamment le « surplus de la victime » pour encourager l'acceptation de paiement (le bénéfice de l'agresseur = X – x – surplus). Il ne prend pas le maximum prenable, mais en laisse une part ; il pratique une répartition du gain potentiel avec sa propre victime, à l'image de ce qui se pratique d'habitude avec un complice).

L'écart entre X et x a besoin d'être significatif, puisque la proposition du pirate n'est pas seulement de « vendre une économie de préjudice » mais aussi d'acheter une conscience -celle du payeur qui se reconnaît vaincu, même honorablement-, laquelle a en quelque sorte un prix.

Quant au pirate, en situation d'ignorance élevée qui fait de lui un rançonneur à l'aveuglette, il ne sait généralement pas si le surplus sera durablement croissant, et si son intérêt est ou non de continuer à attendre ou de hâter le dénouement. Il est parieur sur ce point.

Les entreprises touchées se signaleront avec d'autant plus d'incitation quand le coût total va subir une prochaine accélération à la hausse -coût marginal fortement croissant- aggravatrice de cette situation, et que l'économie générable va grandir d'autant si l'on paye auparavant.




b) soit de laisser son tarif de rançon descendre au fil du temps vers ce coût inconnaissable, ce qui privilégie des entreprises chez lesquelles le blocage des données engendre des préjudices suivant par exemple une courbe en cloche, c'est-à-dire qui s'atténuent à partir d'un moment donné : le coût de reconstitution des données chiffrées de cette société équivaut à 30 000 euros au total, depuis le premier jour, action qui nécessitera 3 semaines de travail à raison de 10 000 euros par semaine. Au bout d'une semaine, le reliquat d'effort à consentir ne vaut plus que 20 000, il est sur une pente décroissante (la dépense totale grandit au fur et à mesure des semaines, mais en courbe asymptote). Le temps ne joue plus éternellement contre la victime. Dans cette configuration, l'intérêt du pirate sera de monnayer à la baisse son tarif de rançon.

Un autre motif incitera le pirate à diminuer ses prétentions, assimilable à la parabole du pont inachevé dont les neuf arches déjà construites couteusement sont inutiles tant que n'est pas achevée la

dixième et dernière arche ; de même, une négociation sur neuf jours mais qui n'aboutit pas a coûté du temps de négociation au pirate, inutilement. Il peut supposer que baisser un peu ses prétentions lui permettrait de ne pas perdre son investissement. Prenant davantage de recul, l'espérance d'un gain même moindre (rançon – remise) sera de sa part mise en balance avec l'effort qui lui serait à consacrer pour se remettre en chasse en partant de zéro, afin de réussir une autre attaque contre une autre victime, synonyme du coût d'acquisition d'un nouveau client.

## 5 – Un jeu où le temps modifie les valeurs et le rapport de force

Ces divers cas soulignent l'importance du facteur temporel. Le pirate pour sa part concentre ses dépenses matérielles au début. Le temps qui suit lui coûte un peu, tandis qu'il peut engendrer chez la victime des coûts tantôt croissants tantôt décroissants, lesquels influent sur la tactique tarifaire adoptable par lui puisque la valeur marchande de sa clé augmente ou diminue.

Le facteur temporel intervient une première fois pour faire varier la valeur de la clé, et parallèlement aussi pour faire varier la capacité financière de la victime à acheter cette clé, lorsque des préjudices totaux croissants l'affaiblissent et réduisent sa capacité à résister, à perdurer, à s'autofinancer sur ses réserves et acheter du temps de survie. Les deux protagonistes s'interrogent sur la question de savoir à qui profite le temps.

Cette interrogation est marquée par une asymétrie d'information renversée, puisque cette fois le condamné en sait davantage que son bourreau sur l'évolution passée et prochaine des coûts. Ce dernier ne conserve de meilleure connaissance que sur le devenir du tarif évolutif de sa rançon.

Confronté à des montants de préjudices qui lui sont inconnaissables, le pirate adopte souvent un processus de tâtonnement walrassien, qui l'assimile à un commissaire-priseur (priseur : littérairement, celui qui définit et propose un prix, accepté ou non par la partie adverse). A partir d'une proposition de prix initial va s'opérer un ajustement éventuel, soit car la valeur du bien proposé –la clé- augmente, soit en baissant la rançon. Tandis que la victime quant à elle cherche à le convaincre que le montant exigé est trop élevé.

On rappellera, même si cette option est inusitée, que le pirate pourrait renoncer à son statut de priseur, et au contraire demander à la victime combien elle donnerait pour obtenir la clé, comme début d'une enchère cette fois montante. Mais même ainsi lorsqu'elle est déléguée à la victime pour que cette dernière dévoile ses positions et accepte le jeu de négociation, la règle du jeu dépend du vouloir de l'attaquant.

Dans l'ensemble, la réflexion de la victime au moment d'une attaque –la durée pouvant être de plusieurs jours ou semaines- s'articule autour de quelques grandeurs, et de la trajectoire qu'elles dessinent ensemble, donc de leur dynamique (à nouveau le facteur temps) :

- le préjudice déjà occasionné et irréversible (essentiellement le passé) ;

- le préjudice ultérieur occasionnable mais évitable, ou celui déjà acté mais réversible (essentiellement le futur) ;

- le montant de la rançon demandée ;

- le patrimoine total de la victime, avant et après préjudices.

- Le patrimoine immédiatement mobilisable par la victime, l'argent qui aidera à se ménager un temps de survie, ou acheter la clé de déchiffrement.

La réflexion du pirate, qui ignore la plupart de ces grandeurs quand elles concernent une petite entreprise, le fait se positionner selon son intuition ou quelques éventuels indices à propos de son gibier, entre deux extrêmes : un risque maximal d'obtenir zéro en demandant une grosse rançon, mais qui lui apporterait sinon une rentabilité élevée par attaque réussie, ou un risque insignifiant de repartir bredouille mais muni d'un magot tout aussi insignifiant. La première option est tentable face à une entreprise que l'on sait très riche ; la deuxième option présente du sens dès lors qu'on sait la multiplier à l'infini presque avec la robotisation des attaques qui autorise leur envoi en rafales à coût marginal tendant vers zéro lui aussi. Option qui nécessite un important vivier de cibles, trouvable surtout chez les TPE et PME.

# TROISIEME PARTIE

# Les préjudices à court et long terme, à l'échelle individuelle et collective : qui paiera véritablement ?

## A – DES BILANS DE RENTABILITÉ DIFFÉRENTS Á COURT OU LONG TERME

### 1 - Du ici et maintenant, au partout et toujours

La convergence entre pirate, piraté et assureur autour d'une banalisation du paiement de rançon –même de coût plus élevé-, revêtirait à première analyse l'apparence d'un intérêt universel bien compris et bien partagé, basé sur le fait qu'une rançon n'est acceptée que si elle est moins onéreuse que le préjudice ainsi évité. L'intérêt universel consisterait donc à avoir économisé un supplément de coût, dans l'absolu. Le contre-sens auquel conduit un tel raisonnement s'illustrera en poussant son biais principal jusqu'à la caricature :

> À chaque fois que je paye une rançon, j'économise un préjudice plus coûteux …
>
> … Donc plus je paierai de rançons, plus j'économiserai de préjudices plus coûteux
>
> … Donc si je paie une infinité de rançons, j'aurai réalisé des économies infinies, gage de prospérité

Un meilleur plaidoyer voudrait retenir que chaque évitement de frais additionnels dégage dès maintenant des économies investissables pour préparer la sécurité de l'avenir. Hélas, ce paiement octroie également à court terme des moyens au pirate, qui l'aident à préparer ses attaques à venir. Nous retrouvons l'interrogation de déterminer à qui profite le temps ; actuellement, et d'après ce que l'on peut anticiper des évolutions technologiques en germe, apparaît-il pencher du côté de l'épée davantage que du bouclier.

Le bénéfice sur papier, qui compare un coût de rançon x à un coût > x évité par la rançon, devient insaisissable si toute chose ne reste pas égale par ailleurs, en particulier l'incitation du pirate –accrue par

la facilité de collecte- et sa capacité financière de nuire –également accrue-. Payer une rançon revient à modifier le futur. En sus de sa capacité d'investissement ou d'activisme ultérieure, l'encouragement modificateur pourrait affecter soit le montant de x soit la fréquence des rançons (nombre de x), deux tendances précisément observables aujourd'hui. Tout ceci renforce à la fois ses moyens d'action offensive et leur future rentabilité, dans un enchaînement néfaste.

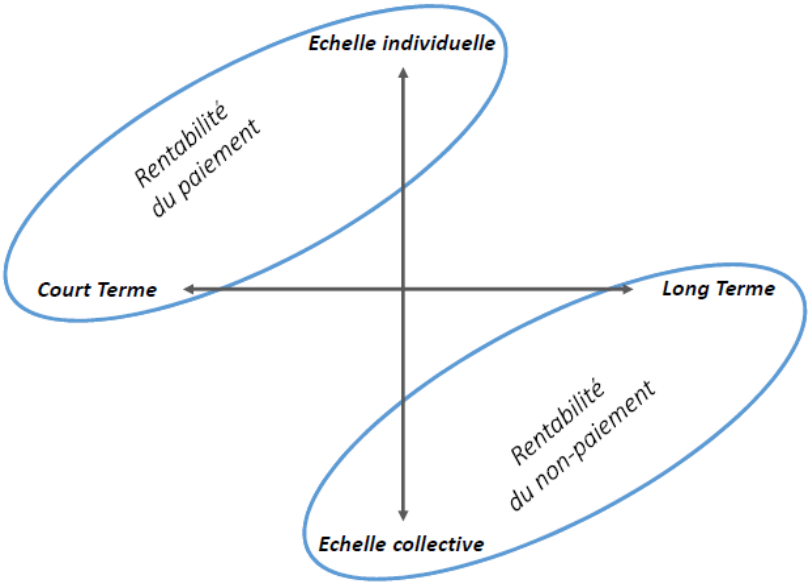
> Le principe de payer maintenant, crédibilise la perspective de futures attaques répétées et plus performantes (l'étude de terrain menée par l'IRT SystemX a mis en lumière une répétition presque mécanique des attaques chez les entreprises ayant déjà été victimes, y compris si elles ont payé une première fois puisqu'elles manifestent leur inclinaison à accepter. Commencer à verser s'apparente à un possible abonnement), donc de nouveaux paiements ultérieurs, avec une fin de partie qu'il convient de définir : la crypto-rançon ne rentre pas ni dans la catégorie des évènements uniques ni dans celle des évènements en nombre infiniment grand -à l'échelle du joueur victime-, mais dans celle des parties rejouables dans des limites quantitatives ; limites d'origine logistique du côté assaillant, avec sa capacité à multiplier puis gérer les offensives, ou buttant par exemple sur la ruine de la victime. Jeu répété, fini à l'échelle individuelle puisque susceptible de s'achever avec l'agonie financière du pion, où l'on vous propose de mourir lentement pour éviter de rapidement mourir –ou d'être blessé-, hormis apparition entretemps d'une solution technique de sécurisation, actuellement introuvable (Le jeu à l'échelle de la collectivité n'a pas de limite temporelle tant que rien ne laisse espérer une solution technique) ? Le maintenant devient jusqu'à la fin de la victime ou de sa capacité de paiement, et toujours pour la collectivité puisque le pirate y trouvera sans cesse de nouvelles proies de substitution.
>
> Le second principe, de payer ici (au niveau de la victime), lorsqu'il est amorti par un mécanisme d'assurance qui le remboursera, reporte sur la collectivité le coût du paiement effectué par une victime isolée. Le gain individuel –le dédommagement- s'obtient par une dépense collective. ? Le ici devient partout et cesse d'apparaître automatiquement rentable à tous.

### 2 - L'infini long terme contre l'infini court terme

S'agissant, à l'échelle de la communauté, d'un « jeu » sans limite de durée, où le nombre de parties est infini, elle n'a aucunement intérêt à se laisser engager dans du paiement de rançon ad vitam dès lors surtout que sa fréquence ou son montant sont sur une tendance durablement croissante.

A l'échelle de la victime, et comme dans tout jeu où la tendance de long terme est perdante, l'entreprise virussée pourrait cependant se considérer gagnante de payer si elle avait la garantie de ne jouer qu'une fois, dans un jeu à partie unique et de parfait court terme.

Une opposition d'intérêts se révèle, où le bénéfice de court terme est contredit par ses conséquences de long terme, où l'intérêt ressenti à l'échelle individuelle est remis en cause à l'échelle collective.




## B – LA DIFFICULTÉ A PASSER DU ICI AU PARTOUT (DU UN AU TOUS) ET DU MAINTENANT A DEMAIN

Acquitter une rançon révèle une « préférence pour le présent », et un parti-pris individualiste. Il est vrai que ce paiement est objectivement rentable ici et maintenant.

### 1 - Le Ici individuel exprime avant tout une solitude

L'isolement physique et moral dont souffrent les victimes est contributeur à leur décision de verser une rançon. La collectivité est en mauvaise position pour lui demander un effort qu'elle-même fournit parcimonieusement, et le ici se verra d'autant plus privilégié par un petit patron qu'il sera laissé seul à son sort. Une traduction aigüe de la mollesse de mobilisation de la communauté se ressent dans les témoignages de solitude des dirigeants d'entreprise lors de l'extrême court terme qu'est une gestion de crise durant une attaque, où les pouvoirs publics autant que l'écosystème de chaque société –banquier, opérateur téléphonique …- sont signalés fréquemment par leur faible écoute ou disponibilité. Non seulement la communauté n'apporte guère un soutien compensateur gratuit à celui qui refuse de payer une rançon, mais même un éventuel soutien prépayé fait parfois défaut : l'impôt (autrement dit le prépaiement, par chacun, des services que lui rendra par la suite la collectivité, au premier rang desquels se trouve la sécurité des biens et des personnes) ou les diverses cotisations et abonnements (l'abonnement téléphonique fournit des communications, mais sans garantie de sécurité des communications ni d'assistance immédiate. Parmi d'autres, le choix du tout IP dans les réseaux contribue à cet état sans garantie de sécurité) que paye chaque contribuable et client ne se matérialisent pas suffisamment à ses yeux lorsqu'il fait face à un besoin crucial d'assistance de la part des secteurs publics ou privés. Bien qu'une cyberattaque soit une agression, avec ses conséquences sur l'emploi, la mobilisation n'est pas à la hauteur de la réaction que recevrait un infarctus, un incendie ou un vol à la tire. Une prise de conscience reste à accomplir pour lui reconnaître un statut.

> Une évolution positive de l'attitude des banques n'appelle pas un assouplissement de leur politique de sécurité et des règles prudentielles en vigueur, et il n'est pas attendu qu'elles ouvrent sur l'heure une ligne de crédit lors d'une attaque informatique d'un client. De même est-il compréhensible qu'un responsable d'agence s'inquiète, lorsqu'une entreprise se trouve bloquée de la sorte avec une perspective de dépôt de bilan, d'être engrainé dans une accusation de soutien abusif en voulant aider cette victime à se relever.

Toutefois serait à conseiller la constitution ou le renforcement d'équipes d'experts internes capables au fil des jours (beaucoup d'attaques voient leur phase névralgique durer une à deux semaines) de jauger si une entreprise attaquée reste viable –notamment quand son problème est de liquidité ponctuelle pour passer le cap mais non pas de solvabilité sur la durée-. Équipe coordonnée avec le responsable d'agence local qui a une connaissance intime du client concerné. Un premier pas pour les banques serait de se mettre en situation de comprendre les évènements pour mesurer rapidement leurs conséquences et le champ des possibles en matière de réaction.

### 2 - Le Maintenant reflète une urgence

Le facteur temps met en relief l'urgence et l'immédiateté du besoin d'aide, dans les heures qui suivent, et durant une période d'intensité du conflit de l'ordre fréquemment de une à deux voire trois semaines.

Le bilan contradictoire selon l'horizon adopté nous plonge dans sa dimension humaine : le décideur entre payer ou non, en l'occurrence un patron d'entreprise, est celui qui trouvera le maximum d'intérêt à payer. Ceci réécrit la phrase de Keynes : « A long terme nous serons tous morts » (si l'on prend ici l'habitude de payer des rançons) … mais à court terme, moi, la victime de l'attaque, je serai le seul mort (si je ne verse pas la rançon). De même pour les employés : perdre leurs emplois se suffit-il d'un dédommagement compensateur ultérieur ?

Par une autre formulation du dilemme, proposer de rembourser une rançon est préjudiciable au long terme ; ne pas payer de rançon est préjudiciable au court terme, or sans court terme point de long terme. L'équilibre entre intérêts de court terme, prioritaire pour le décideur, et de long terme, prioritaire pour les tiers, n'est pas naturellement réalisé. Des mécanismes externes doivent être échafaudés pour leur rééquilibrage.

## C – LA DIFFICULTÉ A PASSER DU PARTOUT AU ICI, ET DU TOUS AU UN

Considérant que la communauté devient victime … de la victime qui paye une rançon, il serait équilibré lorsqu'elle demande au payeur

de rançon de cesser de lui nuire, de lui faire la promesse compensatoire de partager son fardeau des actuels préjudices : si Un pour tous, alors Tous pour un. En partie, un mécanisme de mutualisation des préjudices serait une première incarnation d'un soutien à la victime de la part de la collectivité ; dans la pratique un tel mode de partage, quoique constructif, ne fournit cependant qu'un des éléments nécessaires à une panoplie complète. On ne saurait attendre du principe assuranciel davantage qu'il ne peut fournir, à savoir une forme de dédommagement ou de remboursement par voie mutualisée, donc de soutien a posteriori venant plus tard –et parfois trop tard, si l'entreprise fait faillite dans l'intervalle-. S'ajoute à l'absence d'immédiateté, l'absence de complétude -tout n'est pas remboursé- et de certitude -le remboursement reste soumis à des clauses et audits- … Un pour tous, puis, peut-être et partiellement, Tous pour un.

## 1 - Le mécanisme compensateur ne pourra se suffire du volet assurantiel

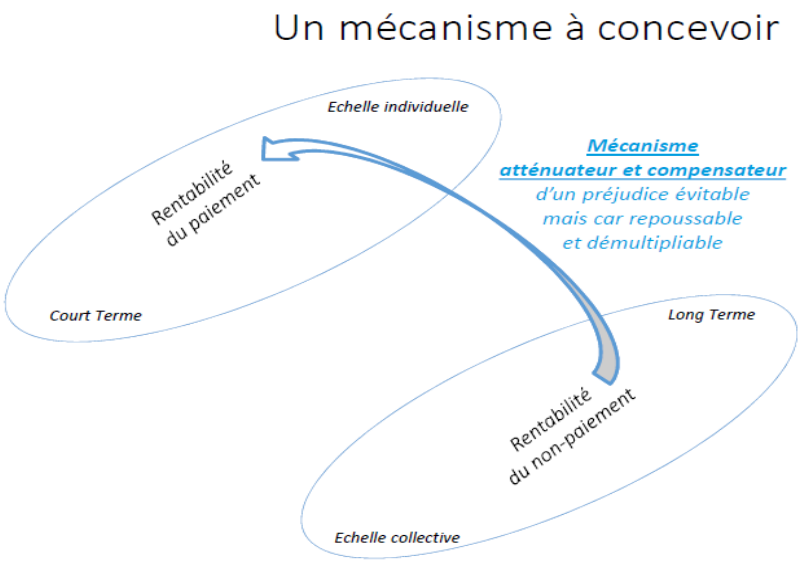
Du fait d'un paiement de rançon, l'*appauvrissement moindre de l'un engendrera un plus grand appauvrissement futur de tous* ; sans que fasse consensus à l'heure actuelle un mécanisme compensateur[68], depuis la collectivité qui se trouve redevable envers chaque victime refusant d'acquitter une rançon au pirate. De manière inversée : *l'appauvrissement moindre de tous provient de l'acceptation d'un plus grand appauvrissement immédiat de l'un*. Or en vue de faire entendre son intérêt, cette collectivité ne parvient pas encore à mobiliser et coordonner trois axes d'amélioration pour donner naissance à un véritable mécanisme compensateur, indispensable à un soutien enfin efficace :

- Protection régalienne : l'impôt acquitté par chaque citoyen et entreprise, qui en théorie obtiendra compensation de cette contribution obligatoire par un apport de sécurité policière, reste sans résultat pleinement satisfaisant à ce jour sur les cryptovirus ;

- Protection technique : les grands systèmes de communication modernes et une part des logiciels en circulation n'ont pas retenu des options techniques raisonnablement sécurisées ;

68 Une minorité des TPE rencontrées avaient contracté une assurance cyber, et plusieurs parmi celles qui en possédaient une n'ont pas rempli un dossier de remboursement post-attaque.

- Protection assurantielle encore en recherche de modèles – pour la prévention, l'appui et le dédommagement- ad hoc économiquement comme socialement.




## 2 - Un mécanisme compensateur pour surmonter l'actuelle répartition injuste et inefficace du préjudice

Les cyber-préjudices en milliards d'euros annuellement ont des payeurs finaux, ainsi recensables :

- Le plus courant à ce jour est que la victime soit son propre assuré, situation traditionnelle à propos de l'Etat, et courante chez les petites entreprises. L'essentiel des milliards d'euros perdus est supporté à leur niveau, bien au-dessus de 90 % du total pour les petites entreprises.

- Ce peut être un preneur de risques, un spéculateur au sens légitime du terme. Un entrepreneur transmet son risque à ce tiers, accompagné d'un peu de son argent, de gré à gré ou via les marchés financiers. Un tel modèle existe en partie sur les cyber-attaques, et le fonctionnement originel des Lloyds s'en ins-

pirait avec des individus –names- regroupés au sein d'équipes –syndicates- qui acceptent conjointement d'endosser un risque identifié.

- Ou un assureur, dans une logique de mutualisation des frais individuels au sein d'une population plus large ; afin d'offrir à chaque assuré la promesse que le coût supporté par lui se rapprochera de la moyenne de tous. Définition essentielle car il a été vu la difficulté de commercialiser ce modèle de protection pour une assurance-rançon lorsque cette rançon a elle-même un coût standardisé autour d'un montant-type (montant par ailleurs « compétitif »).

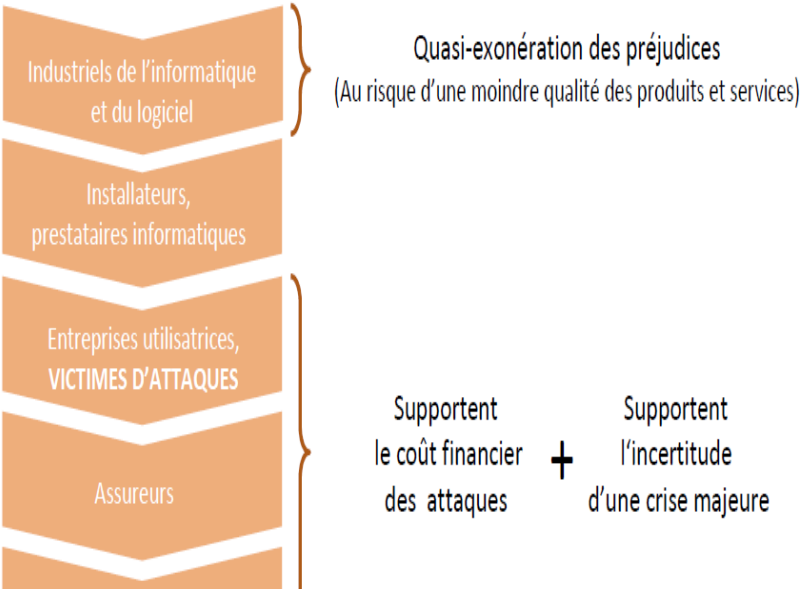
Vous êtes moins enclin à vous assurer contre un sinistre dont vous savez par avance qu'il coûtera par exemple 1 000 euros s'il survient, que si vous ignorez s'il coûtera 100, 1 000 ou un million. Car c'est contre l'épouvantail du million que vous vous assurez prioritairement.

Accessoirement, ce dernier point met l'accent sur le réflexe des systèmes d'assurance de caper les remboursements, c'est-à-dire de leur fixer un plafond au-dessus duquel la victime redevient son propre assureur. Or une assurance reste partiellement démotivante si la victime ignore absolument le montant d'un futur sinistre mais sait qu'il sera potentiellement supérieur à celui du plafond de remboursement ; elle est à ses yeux une assurance partielle.

- Le contribuable, si l'impôt ou une cotisation sert à couvrir de tels coûts, assimilés à des catastrophes irrésistibles et indépendantes de la volonté des parties. Une attaque informatique n'étant toutefois pas indépendante de la volonté du pirate, la situation s'apparente davantage aux dommages de guerre.

- Ces dommages de guerre trouvent parfois payeur chez l'auteur de la guerre, jugé fautif et prié de supporter les torts causés par ses agissements. Démarche ici rationnelle si elle s'appliquait au pirate, mais qui suppose de le voir jugé, évènement rare aujourd'hui. La fausse naïveté qui demande pourquoi est-ce la victime et non le coupable qui paye, devient pédagogique en ce qu'elle tend un miroir qui nous renvoie l'image d'un tissu industriel non protégé, une sorte de « zone de non-droit » numérique à l'égal de certains quartiers dits sensibles.

- Enfin et surtout dans cette recherche de responsabilités, à l'interface entre la victime et le coupable se trouvent des logiciels ou matériels, provenant d'industriels et d'éditeurs de logiciels qui mettent sur le marché des produits fréquemment imparfaits, inachevés et dès lors vecteurs d'attaques. Les attaques « jour zéro » (zero day), qui exploitent la soudaine découverte d'un défaut dans un logiciel installé sur vos ordinateurs, à la suite desquelles on culpabilise la victime de ne pas avoir mis à jour son système d'information, recèlent avant tout une défectuosité trop aisément dédouanée par le droit contemporain ou les flous contractuels. La situation équivaut à ce que serait le secteur aéronautique si les constructeurs d'avions avaient toute latitude de livrer leurs appareils sans garantie et aux seuls risques de l'acheteur, les laissant peser sur les seules épaules des compagnies aériennes clientes. Plus fondamentalement se pose la question de la gratuité réelle de la sécurité d'un produit informatique que l'on a acquis : soit on considère que cette sécurité est déjà incluse dans le prix d'achat mais n'a pas été pas fournie, soit le produit doit avoir l'honnêteté de se reconnaître SGDF, Sans Garantie Du Fournisseur.



Seule la partie aval de la chaîne informatique supporte aujourd'hui le poids des préjudices, d'où s'ensuit un débat tronqué de savoir si les entreprises doivent prendre appui sur les assurances, puis de demander si les assurances doivent être épaulées par la nation (soutien de type catastrophe naturelle ou impôt sécheresse). Ce périmètre trop étriqué, circonscrit à l'autofinancement individuel ou à l'autofinancement collectif –versement d'une prime d'assurance, impôt- fait renvoyer le mistigri de Pierre à son voisin Paul ou réciproquement.

L'exonération de responsabilité dont bénéficie l'amont est immense, puisque sans limite. Dans les scénarios noirs, un chavirage depuis les actuels milliards d'euros par an de préjudices aux entreprises de France jusqu'à par exemple des dizaines de milliards en cas de « rupture de digue » numérique, est susceptible de se traduire par des centaines ou milliers de faillites d'entreprises de toutes tailles, selon la forme de propagation des chocs (les scénarios sont nombreux, tantôt avec effets boule de neige –les destructions gagnant en puissance-, tantôt au contraire avec atténuation progressive des impacts, à l'image de l'expansion des ondes en cercles concentriques sur l'eau –l'énergie destructrice originelle perdant de la force-, etc.). De pareils niveaux brusquement hauts provoqueraient une sape du système assuranciel, et mettraient en péril certains assureurs ou réassureurs.

Que le tissu socio-économique des utilisateurs soit ainsi engagé malgré lui pour des montants inconnaissables à l'avance, fournirait une déclinaison civile du concept régalien de crise informatique majeure, consigné dans la récente publication d'une « Stratégie nationale pour la sécurité informatique ».

Au regard de l'ampleur des incertitudes, une protection raisonnée ne saurait se contenter d'un chaînage qui relie des entreprises jusqu'à une collectivité payeuse symbolisée par les assureurs ou par l'État. **Le système d'assurances, s'il était laissé seul en ligne pour régler le problème économique et social des cyberattaques, aboutirait d'une part à fournir des prestations nécessairement en retrait des immense besoins, d'autre part à se mettre en péril lui-même**. L'assurance peut néanmoins bien sûr être une composante indispensable mais d'un mécanisme plus global.

Prôner un adossement du système assurantiel aux procédures de déclaration de catastrophe naturelle peut se réfléchir comme expédient face à une catastrophe advenue, en tant que remède provisoire, mais ne peut prétendre servir de socle durable au dispositif compensateur ; au risque sinon de devenir un tonneau des Danaïdes dont la

profondeur –puisant chez le contribuable- déresponsabiliserait une grande partie de la chaîne informatique, espérant que le maillon final se muera en payeur en dernier ressort. De surcroît, une déclaration de type catastrophe naturelle ne viendrait pas sauver les entreprises entretemps liquidées.

La pérennité du système compensateur appelle son extension par voie législative non pas tant ou pas uniquement sur la partie aval mais sur la partie amont de la chaîne informatique. L'alternative d'un procès engagé par une entreprise victime contre par exemple l'éditeur de logiciel à l'origine d'une faille est insuffisante, en ce qu'elle suppose que cette entreprise soit toujours vivante –cas de figure précisément incertain- et pourvue des moyens et de la patience pour financer un tel contentieux au long cours.

### 3 – Pour un mécanisme compensateur inspiré du principe pollueur-payeur

« Une mère de famille américaine victime d'un hacker porte plainte contre Microsoft, lui reprochant les failles de sécurité de ses produits. (..) Microsoft prend l'affaire au sérieux, tout en faisant observer que (..) les virus ou toute attaque informatique sont en premier lieu la conséquence d'actes délictueux commis par des personnes physiques malintentionnées. Et que ce sont ces personnes qu'il faut poursuivre et condamner.[69]»

Une hiérarchie rationnelle des payeurs s'étagerait de la sorte :

- N°1 : le pirate, redevable sur son patrimoine et ses revenus, en proportion de l'entièreté des conséquences et non pas par une amende forfaitaire pour outrepassement d'une loi.

- N°2 : l'éditeur ou prestataire informatique, s'il a commis une faute ou un défaut de fabrication –une malfaçon-.

- N°3 : la victime, si elle a commis une faute.

- N°4 : la collectivité –par l'assurance ou l'impôt-, si l'informaticien et la victime n'ont pas commis de faute. Ou une mini-communauté telle que les anciens syndicates des Lloyds.

Actuellement, le payeur prépondérant est le n°3, suivi à distance par le n°4. Les n° 1 et 2, bien que concernés, sont grandement absous de

69 « Quand une mère de famille californienne défie Microsoft ». ITespresso, 8 octobre 2003.

jure ou de facto. Une des clés du problème tient à cette indulgence, qui oblige les n° 3 et 4 à tenter un impossible mode de partage à deux, et non à quatre. La présente règle de partage est structurellement déséquilibrée puisqu'elle consiste chez les deux payeurs à supporter plus que leur part, puis à essayer de se reporter la surcharge au sein de ce couple, l'un sur l'autre, de manière stérile. Dans ce cercle de partage incomplet, l'assureur ne peut entrevoir de bénéfice suffisamment sûr et raisonnable, tandis que l'assuré ne peut en attendre une protection à hauteur de son risque. Le présent statu quo est un pis-aller et une bride économique.

> Une répartition des préjudices d'attaques informatiques véritablement sur les quatre types d'acteurs précités est le préalable à l'essor d'un mécanisme compensatoire et préventif, dont une composante sera un système assurantiel enfin viable et acceptable par les petites et moyennes entreprises : coût mieux réparti, risque mieux réparti aussi, sentiment d'équité chez l'assureur comme l'assuré.

## 4 – Qualité du service, qualité de l'information

Repenser la sécurité le plus en amont possible

> « Petit éditeur de logiciels ou grand fabricant de matériels informatiques, tous les systèmes d'exploitations, logiciels ou hardware, présentent des failles de sécurité »[70]

Renforcer l'implication de l'amont de la chaîne informatique aurait un double effet vertueux : bien sûr améliorer la répartition de la charge, mais aussi et surtout réduire le degré de porosité et d'imperfection toléré dès la conception des systèmes d'information, aujourd'hui dotés d'une qualité de finition insuffisante pour beaucoup d'entre eux. L'exigence de qualité –qualifiable d'obligation de qualité- est trop absente, puisqu'on attend du monde des informaticiens une obligation tout au plus de moyen (la référence parfois faite à l'idée que « le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis du commanditaire »[71], pour louable qu'elle soit, offre un parallèle cocasse avec la même obligation imposée à un fonds d'investissement qui a un devoir de conseil auprès des épargnants, mais atteste d'une

70 Frédéric Raynal : « Écosystème et économie des vulnérabilités », 2019.

71 ANSSI : « Exigences de cybersécurité pour les prestataires d'intégration et de maintenance des systèmes industriels ». Mars 2016.

logique de jeu spéculatif ; ici miser un investissement dans de la sécurité en espérant en retirer un gain, là miser un investissement en bourse en espérant en retirer un gain).

Un tel changement de paradigme impliquerait chez les concepteurs de systèmes et de logiciels l'adoption de méthodes qualifiables de « sécurité par conception » (security by design) ou de « conception orientée sécurité » à l'image de la conception orientée coût.

> **-> L'obligation de qualité du produit ou du service, en termes de sécurité, sera la clé de voûte de tout édifice sécuritaire à l'échelle de la collectivité**. Faute de quoi, le dérapage des préjudices, donc leur insupportabilité, sont inscrits dans le droit fil de ce laxisme.

L'obligation de résultat nous apparaît néanmoins à éviter, qui serait trop contraignante, et injuste également en ce qu'elle frapperait les offreurs les plus innovants. Leur volontarisme se retournerait contre eux.

Cesser d'accepter l'insécurité comme une fatalité sans origines est un exercice de bon sens qui tient de l'investissement ;

> insécurité où les fautifs étaient jusqu'à lors l'ultime intervenant, le client utilisateur ;
>
> insécurité dont le coût était à partager uniquement entre victimes individuelles ou collectives,

La visée est doublement économique, de mieux partager des coûts mais ce faisant de diminuer ces mêmes coûts, car obliger à supprimer les vices cachés plus en amont évitera des frais quant à eux visibles en aval. Les spécialistes en gestion de projets de développement de nouveau produit (nouvel avion, nouvelle voiture…) aiment retenir le principe qu'un défaut corrigé en phase n coûtera par exemple dix fois plus cher que si la correction avait été apportée en phase n-1, et cent fois plus cher qu'en phase n-2, soit une progression exponentielle, ici de facteur dix mais adaptable à chaque contexte.

Par-delà les économies quantifiables apparaît l'amélioration plus intangible de la confiance, puisque chaque réduction des imperfections et vulnérabilités originelles des produits informatiques et logiciels = réduction des risques + réduction de l'incertitude.

Ce chantier avait vu une première pierre posée par le Conseil natio-

nal de la recherche des États-Unis (*National Research Council*), un organisme de réflexion souvent force de proposition. Sa pensée s'est structurée en deux volets, le premier qui constate une absence de régulation socio-économique spontanée autour des enjeux de sécurité :

> « Les consommateurs achètent des caractéristiques utiles et des performances, plutôt que de la sécurité » [72]
>
> « (En matière de sécurité) on ne peut escompter des seules incitations financières ou du marché qu'elles puissent guider les décisions. »

Le second qui propose d'autres voies d'amélioration :

> « Les autorités publiques devraient envisager la loi comme un moyen de palier aux déficiences du marché face aux besoins de sécurité. Parmi les options se trouve une plus forte implication des fournisseurs de systèmes et de logiciels ainsi que des opérateurs de systèmes, sur leur responsabilité dans les brèches de sécurité, et sur leurs obligations de rendre compte des brèches de sécurité capables de mettre en danger les fonctions sociales vitales. »
>
> « Les marchands de systèmes d'information devraient conduire des tests de manière plus rigoureuse à propos de défauts de sécurité, et le faire avant la mise sur le marché plutôt que d'utiliser les consommateurs comme des bêta testeurs. Changer cette manière de penser est une composante essentielle pour parvenir à une situation de cybersécurité améliorée. »
>
> « Afin de répondre aux carences du marché pour répondre au défi de la sécurité, le gouvernement devrait soutenir la recherche sur la sécurité des systèmes d'information. »

Le souci de placer les auteurs de vulnérabilités ou tout au moins de non-qualité face à leurs responsabilités sociales, tranche avec l'habituel discours qui incrimine plus facilement les usagers. La NAS mentionne à ce sujet que « L'erreur humaine n'est souvent pas une explication constructive pour les problèmes de sécurité. Couramment nos pratiques organisationnelles ou techniques se trouvent en faute : ce sont elles qui attendent des gens qu'ils sachent exécuter une multi-

72 Op. Cit. Computer Science and Telecommunications Board de la NAS : « Cybersecurity Today and Tomorrow: Pay Now or Pay Later », 2002, pages 9 à 15.

tude de détails sans jamais se tromper (…) ».

**Repenser la sécurité juste en amont de l'utilisateur (la logistique du « dernier kilomètre »)**

Brièvement évoqué par la NAS, l'autre protagoniste que sont les prestataires de solutions de sécurité complétera la liste des besoins d'excellence et d'efficacité (Loin du « satisfait ou remboursé », le slogan connu « le risque zéro n'existe pas » n'incite pas un petit patron à doubler ses investissements concernés).

Le petit tour de France des prestataires informatiques occasionné par notre étude de terrain a mis en relief un nombre étonnamment élevé de victimes pour lesquelles un talon d'Achille a été un prestataire défaillant : paramétrage inadéquat des systèmes, politique d'accès au réseau qui laisse trop de ports ouverts (parfois volontairement pour faciliter les télédiagnostics ou la télémaintenance), méconnaissance des mécanismes cryptographiques, absence trop fréquente d'un test grandeur réel par exemple des dispositifs de sauvegarde après installation, lenteur du service d'assistance, gestion de crise parfois teintée d'amateurisme, etc. Le paysage français en matière de prestataires informatiques se révèle très disparate et hétérogène, où se côtoient des experts de haut niveau et d'autres plus faibles. Deux excuses sont toutefois avançables, à savoir la grande variété des requêtes émanant de leur clientèle, qui va des progiciels de gestion intégrés à la CAO et fait de ces prestataires des touche-à-tout par obligation ; d'autre part l'impossibilité pour un tel praticien multitâches de rivaliser en compétence avec des pirates dont c'est l'activité principale et qui ont le choix de l'arme, du lieu, du moment. Une injustice veut que l'immense majorité des tentatives d'attaques échouent, mais que les rares succès sonnent comme la défaite des défenseurs.

Devant l'impossibilité d'attendre un niveau sans faille de l'ensemble des prestataires informatiques, dont l'ancrage local et la proximité avec le client restent essentiels pour la plupart des PME-TPE, un travail de mise en visibilité des meilleures compétences en sécurité des systèmes d'information est à soutenir. La plateforme Acyma constitue une première étape, qui permet aux prestataires en sécurité de se référencer[73]. Une étape ultérieure proviendra du bouche-à-oreille

73 Plateforme Cybermalveillance.gouv.fr sur laquelle une société d'informatique peut déposer une candidature pour être référencée dans l'espace prestataire, https://www.cybermalveillance.gouv.fr/prestataire/connectez-vous. Acyma est un dispositif gouvernemental contre la cybermalveillance dont la mission est de prévenir et aider la population en matière de sécurité numérique.

faisant office de notation par les utilisateurs eux-mêmes, à propos de ces déclarations de compétence. Sans exigence de qualité du service –toute non qualité devenant alors une responsabilité de son auteur- la vente de sécurité, lorsqu'elle s'abaisse à déporter son argumentaire et prétendre se vendre pour la valeur du danger brandi, se fait anxiogène pour justifier ses tarifs, mais ne gagne pas longtemps en force de conviction ; à l'habituel dicton qui professe que votre sécurité ne vous paraît cher qu'avant une attaque réussie, vient s'opposer le fait qu'elle vous paraîtra rétrospectivement encore plus chère après une telle attaque réussie.

**Repenser le devoir d'information, actuellement circonscrit à un ersatz quasi-publicitaire**

Pour intéressante que soit l'obligation de conseil d'un fournisseur informatique à son client, une expression plus concrète est celle de bonne et pleine information. De fait, un catalyseur des investissements en sécurité informatique sera la transparence, la gratuité et la fiabilité de l'information sur la qualité de ces produits de sécurité. Une telle absence est nuisible aux entreprises clientes, en ce qu'elle oriente les investissements vers un outillage qui n'est pas nécessairement le meilleur, et en ce qu'elle réfrène les velléités de s'équiper en entretenant le doute sur les performances. Au regard du plancher de deux milliards d'euros de préjudice évalués annuellement à cause de cryptovirus, et dans l'hypothèse basse où le manque de transparence et d'objectivité des informations n'occasionnerait que quelques pourcents de ce montant, le gaspillage se monterait à plusieurs dizaines de millions par an. Probablement la réalité se situe-t-elle au-dessus.

Deux déclencheurs parallèles d'essor d'un marché assaini de la sécurité informatique restent activables : l'un dur, qui rende « obligatoire » un niveau donné de sécurité, au moins contractuellement entre entreprises partenaires au sein d'une chaîne de sous-traitance ou via les assureurs ; ce qui implique de connaître et certifier la qualité des produits et méthodes de sécurité recommandés. L'autre doux, par des mesures de qualité enfin fiables et effectuées par des tiers neutres, à l'instar des procédures d'agrément ou de labellisation de l'ANSSI.

Le trop fréquent renoncement à la mesurabilité de la sécurité du numérique, et à se mettre en capacité de juger son efficacité ou sa rentabilité, est un choix industriel et sociétal coûteux.

# CONCLUSION : QUATRE SCENARIOS + UN

L'éventail possible des évolutions futures de nos actuels équilibres -comme rapport de force et presque au sens d'équilibre de la terreur- est résumable par quelques scénarios en crescendo :

- Celui intitulé Scénario zéro verrait une **nette amélioration** de la sécurité des systèmes d'information et de communication. Une telle sortie de danger s'appuyant sur une évolution –sans besoin de révolution- d'internet et de ses protocoles. Le faible nombre des initiatives en ce sens ne doit pas laisser minorer leur réelle qualité intrinsèque, à l'instar de Rina (*Recursive Inter-Network Architecture*) destinée -parmi quelques autres options innovantes disponibles- à offrir une alternative aux actuels systèmes de communication qualifiés « d'ensemble instable et non prévisible » (Louis Pouzin)[74].

- Le scénario 1 enregistrerait une amélioration modérée et continue du degré d'exposition des entreprises, par une combinaison de petites améliorations techniques et comportementales chez les cibles des pirates. Cependant ces améliorations seront d'une portée faible, qui apparaît d'emblée compensée par la tendance profonde à se numériser et se connecter toujours d'avantage dans les entreprises. D'autre part ce scénario suppose une relative stagnation des méthodes et volumes d'attaques, supposition entachée d'illusions tant que perdurera la rentabilité et l'impunité de la piraterie contemporaine.

- Le scénario 2, variante moins optimiste du précédent, consisterait en une s**tabilité de l'équilibre** entre l'épée et le bouclier. Option qui, puisque les améliorations technologiques escomptées prochainement sur le bouclier n'apportent pas des ruptures sécuritaires radicales, repose à nouveau sur le pari presque contemplatif que les pirates informatiques ne fassent pas progresser leur nuisance ; gageure probablement perdue au vu du professionnalisme accru des attaques, sensible depuis 2019 et

74 https://la-rem.eu/2019/09/rina-un-projet-pour-linternet-de-nouvelle-generation/

qui a amené de nombreux commentateurs à considérer que les pirates utilisent de plus en plus un outillage autrefois apanage des services de renseignement étatiques. Auparavant il est vrai et pendant une pause de quelques années, les grandes entreprises ont pu espérer avoir globalement endigué les attaques par une montée en puissance de leurs protections. 2017 les avait en partie détrompés en franchissant une marche avec les assauts de type WannaCry (Saint-Gobain, tout en officialisant l'impact estimé sur son résultat financier du fait de NotPetya[75], avait rendu public le déploiement en interne d'une solution de détection d'intrusion s'appuyant sur l'intelligence artificielle). Toute projection serait imprudente mais le sentiment présent est celui d'aggravations par intervalles d'environ deux ans –sous réserve de confirmation à l'avenir- ; selon un calendrier marqué dans un premier temps par un envahissement de cryptovirus contre les entreprises vers 2015, puis un saut donc en 2017, et présentement l'ébauche d'un nouveau haussement à partir de 2019.

D'autre part, cette sécurisation des grandes sociétés a dévié une part des agressions vers les petites entreprises ne disposant pas de mêmes moyens à portée de leurs budgets. Les pirates visent les proies les plus exposées, à savoir les TPE et PME, les hôpitaux et les municipalités, voire demain les particuliers ; tout comme un déport des fraudes au président s'est observé au fil des années à l'encontre des PME provinciales, dont les comptables étaient moins sensibilisés face à leur ingénierie sociale. Un tel sous-scénario inquiétant dévoile une autre « fracture numérique » où les gros budgets ont su un temps se protéger mieux, mais où les petits restaient et resteront exposés ; sorte de féodalité moderne, quand le château seigneurial mieux barricadé détourne les attaques vikings sur les abbayes ou les villages environnants, ou lorsque la présence d'une caméra de surveillance dans une rue repoussera les agressions vers une rue adjacente.

- Le scénario 3 d'**aggravation progressive** gagne en potentia-

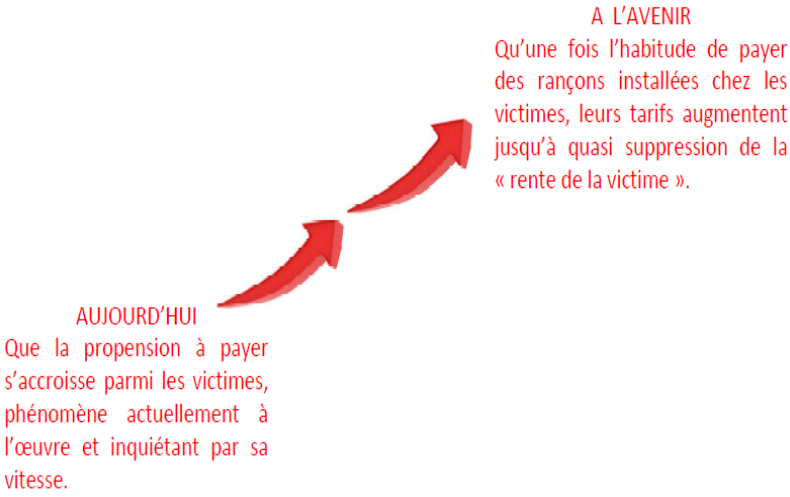
75 « L'impact sur le premier semestre est estimé à 220 millions d'euros sur les ventes et à 65 millions d'euros sur le résultat d'exploitation. Sur l'ensemble de l'année, l'impact est évalué à moins de 250 millions d'euros sur les ventes et 80 millions d'euros sur le résultat d'exploitation. ». Saint Gobain, Rapport semestriel d'Activité. Comptes consolidés au 30 Juin 2017.

lité, jusqu'à devenir l'hypothèse première, très crédible en ce qu'elle se fonde sur trois tendances de fond négatives d'ores et déjà à l'œuvre, et appelées à perdurer :

- une augmentation assez régulière du nombre d'attaques tentées, observée depuis plusieurs années par le dispositif technique de décompte d'attaques automatisées élaboré par l'IRT-SystemX –une pseudo entreprise présente sur les réseaux et servant d'appât pour les pirates-. Kaspersky a signalé le fait que depuis 5 ans environ les attaques ciblées se substituent progressivement aux envois massifs de courriers piégés mais donc standardisés et désormais peu efficaces ; les deux procédés ne s'excluent pas, qui par une meilleure segmentation des cibles autorise une certaine standardisation pour chaque segment et sous-segment mieux délimité. L'intelligence artificielle ne se met pas moins au service des agresseurs que des défenseurs.

- L'accroissement du nombre de points d'accès numériques ouverts par les futures cibles, comme autant d'invites à une attaque, et qui s'inscrit dans la vogue des objets communicants. Ainsi que la valeur croissante du patrimoine numérisé et ipso facto destructible (comptabilité, documentations techniques, systèmes de commande de machines, etc.).

- La hausse aujourd'hui patente de la propension des victimes à payer des rançons, qui laisse présager un enchaînement en deux étapes, actuellement lorsque les victimes s'accoutument peu à peu au principe d'une rançon, comme s'il s'agissait d'un banal impôt sur la malchance. Puis, chaque victime acceptant de payer, révèlera en cela à son attaquant le caractère supportable de ce montant par elle, laissant deviner que son seuil de refus se situe plus haut. Le pirate pourra être tenté de tester ce plafond.




- Le scénario 4 d'**aggravation brusque** s'inquiète d'une amélioration de l'efficacité des cryptovirus (dans leur mode d'attaque et de leurre, dans leur capacité de propagation, dans leur vitesse de chiffrement d'un SI pénétré, dans leur résilience et leur aptitude à rester dormant dans un SI pour infecter y compris les sauvegardes anciennes, etc.). Cette option pouvant revêtir la forme d'un scénario catastrophe qui, en l'état, n'est pas écartable, et fait planer une ombre permanente sur l'éventail des menaces, de soudain pousser le curseur à son extrême.

Le scénario le plus probable aujourd'hui apparaît être le 3, c'est-à-dire d'aggravation progressive soit pour tous, soit pour la majorité que sont les petits acteurs. Considération soumise toutefois à l'hypothèse difficilement mesurable de matérialisation soudaine du 4. Le scénario 0 quant à lui n'est pas assorti d'un pourcentage car il ne dépend sommes toutes que de nous : il n'aura aucune probabilité de réussite si nul ne s'y consacre, mais toute probabilité d'achèvement si une mobilisation se fait. Une morale imprévue s'en dégage, qui nous rend responsable de nos futurs malheurs, morale porteuse de logique puisque les autres scénarios moins optimistes reviennent à laisser l'initiative et l'occupation du terrain aux pirates.