La gestion de crise cyber et classique, entre similitudes et divergences

Raphael de Vittoris

La gestion de crise cyber et classique, entre similitudes et divergences

Note : afin de ne pas alourdir la lecture, l'auteur a préféré faire figurer les références bibliographiques justifiant ses analyses en fin de chapitre plutôt au fil des paragraphes. En outre un glossaire est fourni en fin d'article, les mots qui y sont détaillés sont indiqués par un astérisque.

Introduction

La crise fait malheureusement désormais partie de notre quotidien. Les attentats terroristes succèdent aux crises économiques, ils laissent la place aux pandémies qui génèrent quant à elles des crises sociales et politiques. La crise semble désormais plus présente et plus destructrice. Notre époque semble ainsi devenue plus incertaine et plus ambiguë. C'est d'ailleurs fort de ce constat que l'acronyme VUCA*[1] fut élaboré.

Dans ce foisonnement de crises, désormais regroupées en familles[2], une typologie de crise inquiète davantage des décideurs des organisations aussi bien publiques que privées : il s'agit de la cyberattaque. Cette crise est en effet la plus crainte par les comités exécutifs des entreprises et les directeurs d'organisations publiques du fait de certains caractères particuliers qui s'ajoutent aux dimensions déjà ambiguës, anxiogènes et incertaines des autres types de crise.

La cyberattaque est donc l'évènement qui empêche de dormir les décideurs. Mais pourquoi ? Avant de traiter de la nature toute singulière de cette typologie de crise nous pouvons nous interroger sur le déclic de cette peur qui étreint les grands responsables. Quel évènement cyber a-t-il pu effrayer à ce point les organisations ? Selon nous, deux évènements qui ont secoué l'année 2017 (les cyberattaques mondiales Wannacry* et NotPetya*) sont à l'origine de cette prise de conscience de la faiblesse généralisée des systèmes d'informations et de communications de la plupart (toutes ?) les institutions. Le monde a vu des multinationales entières, des secteurs d'activités complets voire des ministères de pays développés s'effondrer ou menacer de s'effondrer lors de ces deux attaques. Les grands décideurs ont alors pu s'interroger quant à leur propre structure et constater, pour ceux qui n'avaient pas été impactés, qu'ils avaient été chanceux de n'avoir pas compté parmi les malheureux frappés par cette foudre numérique. Ils ont pu appréhender la pleine réalité de cette course effrénée (et perdue d'avance) qui oppose les organisations aux cyber-assaillants. Ils ont constaté que l'objet même qu'ils se réjouissaient d'implanter au sein de la totalité de leurs processus, à savoir les systèmes informatiques[3], est devenu la cible d'attaquants dont ils ne connaissent ou comprennent ni le profil, ni les motivations et encore moins les modes opératoires.

[1] Terme apparu en 1987 et publié en 1991 dans un document de recherche réalisé par Herbert F. Barber et intitulé "*Developing Strategic Leadership: The US Army War College Experience, Strategic Leadership Primer*" et publié sous la coordination du Dr Rod Mage

[2] Crises économiques, environnementales, sociales, industrielles, technologiques, financières, sécuritaires, etc.

[3] Et dont ils ne maîtrisent aucunement les arcanes

Penser la cyberattaque en gestion de crise, c'est se pencher sur la crise-mère dont les conséquences peuvent toucher les points les plus éloignés de l'organisation. C'est se confronter véritablement à la théorie des systèmes complexes* et admettre… qu'on ne comprend pas ses propres systèmes.

Dans ce chapitre nous détaillerons les principes clefs du phénomène de crise et les spécificités de la crise cyber ; les biais cognitifs et heuristiques* qui s'expriment dans les cellules de crises ; et les notions de fragilité, de résilience et d'antifragilité pouvant offrir une réflexion nouvelle quant à l'anticipation de ces crises particulières. Nous conclurons sur un questionnement fondamental sur ce que constitue réellement la cybercrise ainsi que l'origine numérique de la volatilité ambiante.

La crise

Nombre de définitions existent en ce qui concerne le phénomène de crise. Si ces dernières peuvent varier sensiblement et ainsi en offrir des conceptions très différentes, certaines caractéristiques clefs semblent composer le phénomène crisogène[4] pour les chercheurs et les praticiens, à savoir : 1) une rupture fondamentale de la continuité des activités usuelles, 2) une contrainte temporelle sensible de gestion, 3) l'omniprésence (au moins en début de crise) de l'ambiguïté et 4) l'incertitude quant à la dynamique et la gravité de la situation.

L'analyse des recherches en sciences de gestion et des travaux des praticiens a amené les chercheurs à distinguer trois approches différentes du concept de crise :

L'approche par l'impact

Cette approche repose essentiellement sur la prise en compte des conséquences de la crise. Elle considère ainsi la crise d'abord comme : 1) une source d'impacts négatifs (parfois positifs) et 2) sur des plans variés (humains, économiques, financiers, politiques, géopolitiques, juridiques, etc.). À ces deux notions essentielles, cette approche y associe parfois les notions de 3) probabilité et/ou d'occurrence. Certains auteurs ont, dans cette optique, définit la crise comme étant « *a low-probability, high-impact situation that is perceived by critical stakeholders to threaten the viability of the organization and that is subjectively experienced by these individuals as personally and socially threatening*[5] ».

Par son analyse de l'évènement depuis ses manifestations extérieures, elle offre une approche totalement opérationnelle. L'approche par l'impact ne considérant les crises qu'après leur déclenchement, cette vision amène les praticiens et les chercheurs à un comportement et une vision essentiellement réactifs.

L'approche sectorielle

[4] Vous noterez que l'auteur se donne le droit d'inventer des mots 😊
[5] Pearson & Clair (1998)

Cette seconde approche, (aussi qualifiée de processuelle), se fonde essentiellement sur les causes et la dynamique de la crise. Ici la crise est perçue comme le résultat de dysfonctionnements cumulés et potentiellement repérables. Plusieurs crises industrielles et technologiques ont fait l'objet de cette approche lors de leur analyse[6].

La notion de causalité y est prépondérante. On se repose sur une analyse *a posteriori* des évènements détectés et formalisés, ceci amenant naturellement à considérer la crise comme une situation prévisible et même logique dans la cascade des causes successives ayant permis l'évènement[7]. Cette approche conduit donc à considérer que les crises « *may not reflect accident or random misfortune so much as they express "the outcome of normal functioning of a dysfunctional system*[8]."»

Cette approche a ouvert la voie à des systèmes d'analyses d'accident (exemple le « Swiss Cheese Model »[9]) basés sur la superposition des erreurs et la focalisation sur les barrières d'évitement des conséquences. En d'autres termes une considération que la crise est rendue possible par la superposition des failles des barrières en place, et que tout l'art de son évitement est dans la mise en place de barrières diverses comblant mutuellement leurs failles respectives. De telles méthodologies conduisent à considérer évidentes et peu contestables des chaînes causales[10] sans pour autant ouvrir vers une réelle élimination des causes de la crise.

L'approche complexe

Ici la crise n'est plus une source de conséquences néfastes (approche « par l'impact ») ou encore d'une causalité mécanique fruit d'une analyse narrative de l'évènement (approche « sectorielle »), mais tout simplement un évènement « *unexpected, undesirable, unpredictable and unthinkable which most of the time produce uncertainty and disbelief*[11] ». C'est tout simplement l'expression même de l'incertitude la plus complète quant aux comportements d'un système d'une complexité qui nous échappe[12].

Cette considération a été largement alimentée par l'apport de Charles Perrow qui a influencé de manière irréversible l'approche analytique des accidents, des désastres et des crises. Son travail, originellement focalisé sur les systèmes industriels à haut risque, fait appel à deux concepts clefs qui expliquent, via la notion complexité, l'inéluctabilité des crises.

- D'une part le degré de complexité des systèmes est en constante augmentation : en effet les systèmes modernes voient le nombre de leurs processus (et donc sous-processus) et

[6] Par exemple l'approche de la Commission Rogers pour l'analyse de l'accident de la navette spatiale Challenger
[7] Les méthodologies les plus connues pour ces analyses sont pour le plus simples les célèbres « arbres des causes », et pour les plus élaborées les analyses de criticité telles que l'Analyse des Modes de Défaillances et de leur Criticité (AMDEC) ou l'Hazard and Operability study (HAZOP)
[8] Kersten & Sidky, 2005
[9] Reason 1995
[10] Bien que construites de toute pièces par le fruit 1) d'une narration a posteriori et 2) un phénomène inductif influençant la vision des analystes
[11] Milasinovic & al. (2010) ; Heath & al. (2009) ; Quarantelli (1996, 2001)
[12] Toute personne ayant surveillé une classe de maternelle comprend exactement le sens profond (et l'impuissance résolue) de cette phrase

activités (et donc sous-activités) augmenter de manière constante. Cette croissance génère une augmentation statistique naturelle des défaillances et erreurs possibles.

- D'autre part le degré de couplage (voire d'interdépendance) des activités du système : les activités (intra et inter) organisationnelles augmentent de manière naturelle leur état d'interdépendance. Les systèmes sont de plus en plus liés et interconnectés donc de plus interdépendants, ce qui peut alimente un effet « boule de neige » en cas de défaillance ou d'erreur.

La coexistence de la complexité inhérente aux systèmes industriels modernes et de la forte probabilité d'interactions de plusieurs dysfonctionnements locaux s'incarne comme une voie royale pour la survenue de catastrophes. Nous faisons ainsi le cruel constat que les systèmes modernes vont inéluctablement générer des crises, et ceci quelles que soient les mesures mises en place. En d'autres termes, aucune préparation n'évitera la survenue de la crise : le degré de complexité croissant des systèmes offrira le terreau nécessaire à une crise dès qu'une instabilité amorcera une dynamique non-linéaire[13] par cet effet « boule-de-neige ». Cette inéluctabilité assumée des crise, propre à une approche complexe, conduit à ne plus dédier les mesures en « temps de paix » à l'évitement de la crise, mais bien à la mise en place des éléments mobilisables et nécessaires pour affronter la survenue de l'évènement (vision résiliente) ou mieux à l'élaboration d'options qui permettront au contraire de tirer parti de la volatilité…voire même de l'espérer (vision antifragile)[14].

L'approche proposée

Les approches classiques (approche par l'impact ou approche sectorielle) montrent selon nous de réelles limites. L'approche « par l'impact » voit sa portée réduite par sa focalisation des seules manifestations extérieures de l'évènement (victimes, dégâts, coûts, attaques médiatiques, etc.). En outre, lorsqu'elle revêt un aspect probabiliste[15], elle quantifie l'occurrence non pas par observation scientifique mais par phénomène inductif[16].

L'approche « sectorielle », via sa conception causale et narrative[17] de la crise, amène à l'expression débridée d'un biais de narration comme base d'analyse objective (*sic*). De plus selon cette vision causale voire prévisible des crises, qui deviennent donc potentiellement repérables *avant* leur survenue (*re-sic*), la crise n'est donc plus fondamentalement un phénomène imprévisible, inexplicable et potentiellement incompréhensible. Ce postulat, lorsqu'il devient certitude, sera générateur d'une séquence de comportements connus des

[13] Ou non-proportionnelle. Cette non-linéarité est due à la présence d' « effets seuils » où tout dépassement d'un certain niveau critique entraîne un comportement disproportionné au regard de ce qui était préalablement observé

[14] Les principes de ces deux visions seront évoqués plus loin dans le document

[15] En attribuant des probabilités statistiques de survenue aux risques, qui seront mis au regard de (comprenez « multipliés à ») leurs conséquences pour permettre de hiérarchiser les risques alors évalués

[16] Phénomène consistant à estimer les probabilités des évènements futurs au regards des évènements déjà survenus. Cette pratique courante a notamment permis les surprises collectives de la crise des sub-primes, les attentats du 11 septembre, le mouvement des gilets-jaunes, l'élection de D. Trump et la victoire de Mohamed Ali sur Georges Foreman à Kinshasa en 1974

[17] Puisque l'évènement est analysé *a posteriori* en « se racontant » l'enchaînement des évènements en vue d'en tirer un scénario plausible et intelligible qui servira de base à un plan d'actions correctives

organisations peu préparées à la gestion de crise : la procrastination[18], la sidération et enfin la panique, lorsque le « ciel tombera sur la tête » des organisations ayant opté pour cette approche.

Notre proposition pour les organisations (qui sont des systèmes complexes), est d'opter pour une approche « complexe » des crises et de leur gestion. Une crise est un phénomène à « effet seuil* », c'est donc une dynamique qui n'est pas proportionnelle. Elle est au contraire à tendance exponentielle. C'est fort de ce constat que la définissons ainsi : « ***la crise est le produit une dynamique non-linéaire impactant un système complexe (une organisation) ou multi-complexe (un écosystème d'organisations*)** ». Par cette approche, nous assumons donc par principe que l'organisation affronte une situation totalement inattendue, imprévisible, dans une incertitude omniprésente où il devient fondamental de s'adapter avec les moyens disponibles, voire d'improviser, afin de limiter au mieux les conséquences voire de prospérer de (et au sein de) cette instabilité.

Les caractéristiques des crises… et des crises cyber

Une fois éclaircies les approches par lesquelles nous pouvons aborder le phénomène crisogène, nous pouvons dresser une liste de ses caractéristiques fondamentales :

- *La Fortune* : Si certaines crises sont parfois le fruit d'un manque de chance (tsunami 2004, éruption du volcan Eyjafjallajökull 2010, etc.), il en va autrement des crises cyber. En effet, la malveillance est à l'origine de l'ultra-majorité des situations dans le cas de ces crises : phishing*, ransomware*, wiper*, déni de service*, defacement*, watering hole*, spearphishing*, sabotage, etc.
- *Le timing* : comme vous pouvez vous en douter, une crise ne survient jamais au bon moment. Les catastrophes semblent ne jamais survenir aux heures ouvrables mais bien en pleine nuit, durant le weekend, en plein milieu des congés ou au soir de Noël. Dans le cas des crises cyber, basées comme nous venons de le voir sur une malveillance, ce timing malheureux est systématiquement délibérément calculé par l'assaillant.

  Le cas Saudi Aramco (2012) *: le groupe de hackers « Cutting Sword of Justice » organisa une attaque au ransomware auprès du géant saoudien, leader mondial de la production de pétrole (10,5 millions de barils/jour) en plein mois de ramadan. Toutes les activités furent stoppées hormis les activités industrielles, ainsi aucune vente n'était plus possible.*

- *La panique* : dans le contexte d'incertitude et d'ambiguïté caractéristique de la crise, la panique devient une composante naturelle de l'évènement. L'incompréhension et l'impossibilité d'interprétation de la situation présente et à venir causent directement des tensions mentales fortes et influent sur les processus cognitifs des acteurs.
- *La continuité d'activité* : dans de très nombreux cas de crise, la turbulence majeure générée remet en question la continuité des processus et des activités. Si cette

[18] En tant que tendance à repousser l'activation de la cellule de crise et la prise de décisions

conséquence n'est pas absolument systématique, le seul questionnement du risque de discontinuité est, quant à lui, inévitable.

- *La communication* : L'absence de communication de l'entreprise attaquée auprès des parties prenantes ou du grand public est devenue presque impossible. Les média-sociaux et les revendications des assaillants dans le web ou le dark-web* amènent les organisations à préférer révéler (tout ou partie de) la situation afin de maîtriser la communication.

Une fois ce grossier portrait-robot de la crise élaboré, nous listons les caractéristiques propres aux crises cyber :

- *La gouvernance* : il est fondamental de déterminer qui détient l'autorité pour les décisions les plus fondamentale (déconnexion de parties de l'organisation, paiement des cyber-assaillants, etc.). Or, la problématique cyber est plus transverse que la plupart des autres. En effet les TIC* sont tellement omniprésents dans chaque processus de l'organisation que tout évènement les concernant nécessite une gouvernance au bon niveau
- *L'option de paiement*[19] : il est essentiel de déterminer à l'avance les dimensions auxquelles l'organisation de réfèrera pour les décisions de paiement éventuels. Cette décision sera-t-elle basée sur des notions, d'éthique ? de cohérence avec la raison d'être de l'organisation ? d'efficacité ? de rentabilité ?
- *Les signaux avant-coureurs* : si de nombreux signaux permettent d'identifier des probables attaques (activités anormales des serveurs, flux inhabituels des données, etc.), il est fondamental de prendre pour acquis que la veille de ces signaux n'est aucunement une garantie. En effet, la crise est par essence affaire de changement et de nouveauté. Rien de certifie que les signaux avant-coureurs des crises d'aujourd'hui seront ceux de demain (notamment dans le monde digital où l'évolution est extrêmement rapide).
- *L'aide extérieure* : si l'aide extérieure est tout aussi importante dans la crise cyber que dans les autres typologies de crise, les acteurs essentiels en sont toutefois bien différents. Les deux acteurs extérieurs fondamentaux qui pourront aider l'organisation seront l'assureur de l'organisation (sous réserve que les clauses du contrat et que son expertise couvre le domaine cyber) et les organes privés ou nationaux[20] de protection cyber. Tous les autres alliés extérieurs, même s'ils peuvent être précieux, demeurent moins essentiels que ces deux auprès de qui il convient de nouer des liens étroits en temps de paix.
- *La croyance d'impact uniquement processuel et non pas humain* : une des croyances les plus répandue parmi les décideurs est que la cyberattaque cible des logiciels et des données et donc n'impacte que les processus et, *in fine*, uniquement le produit financier. Or ce préjugé doit être combattu. En effet, du fait de l'omniprésence des TIC dans absolument toutes les activités des organisations, une cyberattaque peut tout à fait mettre en péril la vie des individus.

[19] En cas de ransomware

[20] L'ANSSI dans le cas de la France, le BSI pour l'Allemagne, l'ANSSI.lu pour le Luxembourg, l'OCSI pour l'Italie, etc.

Mercks (2017) *: Le wiper NotPetya, ayant bloqué des activités critiques pour l'entreprise durant plusieurs semaines, des patients furent de facto en danger car dépendant des médicaments vitaux produit par l'entreprise. Mercks se focalisa donc sur la restauration des fonctions de base afin de garantir une production critique sa production.*

Colonial Pipeline (2021) ***:*** *l'attaque par un Raas (Ransomware as a service) via le compte VPN et le mot de passe d'un employé glanés sur le darkweb* contraignit Colonial Pipeline à fermer le système industriel afin d'éviter une catastrophe industrielle. La panique des acheteurs généra une pénurie d'essence à grande échelle malgré paiement de la rançon en bitcoins.*

- *L'embarras des décideurs* : une des particularités rarement exposée de la crise cyber est l'embarras profond qu'elle suscite chez les décideurs dussent-ils être rompus à l'exercice de la gestion d'autres typologies de crise :
  - D'une part les top-managers ont du mal à saisir la nature et la portée des problèmes du fait de la dimension ultra-technique de la crise cyber[21]. Cette prévalence technique effraie souvent les décideurs qui ne peuvent conceptualiser l'ensemble de la problématique et les mets en position de faiblesse face aux techniciens.
  - Le monde cyber offre des états de vulnérabilité permanents par des attaquants invisibles et dont on ne comprend ni la motivation ni la méthodologie. Cette ouverture digitale expose à un inconnu malveillant sortant totalement du cadre de l'univers maîtrisé par le top-management (concurrents, marchés, ressources, etc.).
  - L'organisation se trouve parfois face à des attaquant étatiques, infiniment plus puissants et sophistiqués avec qui il est impossible de rivaliser technologiquement. Cette situation peut même renvoyer au simple état de dommage collatéral dans une guerre cyber internationale dont les organisations sont réduites à l'état de spectateurs/victimes inéluctablement mal armés.
  - La police ne fait et ne peut (presque) rien[22] et il revient d'abord à l'organisation de se protéger elle-même. Ceci alors même que l'entreprise assimile avec un temps de retard les évolutions cyber et qu'elle dispose de moins de ressources que les cyberattaquants.
- *Temporalité et espace* : un des propriétés trop rarement évoquées de la crise cyber est qu'elle contredit la vision répandue d'une cinétique de crise suivant un schéma directeur de type : signe avant-coureur, accélération des évènements, perte de repères, prise de décisions et corrections, pic de la crise, retour progressif à la stabilité, rebond éventuel, fin de crise. La crise cyber peut balayer ce schéma temporel et être immédiate. Tout

[21] Au contraire des crises sociales ou encore des catastrophes naturelles dont la nature et la portée sont compréhensibles pour le profane.

[22] Dans le sens où nous l'entendons pour d'autres formes de délits où son intervention peut être plus ou moins immédiate et concrète une fois l'alerte donnée.

stoppe, tout s'éteint et plus rien de fonctionne dans l'intégralité du réseau, donc dans l'intégralité du process. En outre, elle a la capacité de pouvoir être holistique dans le sens où, les TIC touchant toutes les activités actuelles des organisations, la crise cyber peut potentiellement impacter l'intégralité des processus de l'entreprise. Cette double capacité de pouvoir être à la fois immédiate et holistique rend la crise cyber toute singulière dans le bestiaire des crises possibles.

C'est fort de ces points que nous suggérons le conseil suivant : conservez votre bon sens. Ne vous laissez pas impressionner par une surabondance technique et technologique vous ensevelissant sous des acronymes, des concepts et des éléments auxquels vous n'y comprendrez rien dont vous ne parviendrez jamais à disposer d'une vision globale et cohérente. Un système TIC est un organisme complexe dont personne dans l'organisation (lorsqu'elle dépasse une taille critique) n'a de compréhension totale absolue.

Votre seul recours consiste à conserver votre cohérence et l'objectivité de votre jugement pour contribuer à l'expression de l'intelligence collective et à une prise de décision judicieuse. Or la conservation de ce bon sens et de cette objectivité en situation de crise cyber est un défi en soi…devinez quoi, c'est justement l'objet de notre prochaine section…

L'heuristique et les biais cognitifs

La création de sens et la prise de décision

L'étude des fonctionnements cognitifs et d'élaboration de sens est devenue fondamentale en gestion de crise. L'omniprésence de l'ambigüité et de l'incertitude influence nécessairement les réflexions et les schémas mentaux des acteurs des cellules de crise. Le concept de la construction de sens (ou « sensemaking[23] »), est intimement liée aux notions de surprise, d'inattendu ou d'interruption d'un flot d'événements. Cette approche repose sur l'interprétation des acteurs des cellules de crise, segmente le phénomène crisogène en étapes successives :

1) *L'ambiguïté* : où les acteurs font face à une situation totalement incompréhensible, inattendue et imprévisible,
2) *L'interaction* : où les acteurs se forgent ensemble une représentation de la situation via la déconstruction collective de leur vision du monde « d'avant-crise » et la reconstruction d'une nouvelle réalité,
3) *La réification*[24] : où les bribes de schémas et dynamiques comprises collectivement sont assemblées en une interprétation globale cohérente,
4) *La communication* : garantissant l'adoption commune des actions à entreprises et postures à adopter,

[23] En tant qu'interprétation cohérente collective de la cellule de crise dans son ensemble
[24] En tant que transposition d'une abstraction en un objet concret

5) *La plausibilité* : où le la représentation du réel élaborée collectivement est toutefois simplifiée afin d'éviter des incohérences ou paradoxes et de garantir une cohérence,
6) *Le bricolage* : où l'équipe peut utiliser les éléments mobilisés de manière inédites pour répondre à l'évènement.

Il apparaît ainsi que ce processus repose sur une narration, par nature rétrospective, des évènements afin d'expliquer les surprises, en ce sens il est par essence vecteur d'un biais de narration. Cette construction mentale rétrospective, rendue possible grâce à l'agencement de présupposés individuels et collectifs, permet d'assigner un sens aux discontinuités et aux décalages avec les attentes.

Selon cette approche, l'action précède la réflexion et permet ainsi, par le constat de ses conséquences : 1) la base analytique pour échafauder une réponse articulée permettant l'absorption du choc, 2) la proposition de solutions inédites et 3) la capitalisation une fois la crise terminée. Selon les partisans de la théorie de la création de sens, c'est la pleine expression de ce dernier qui confère un niveau de résilience à l'organisation. Ainsi, la résilience devient la finalité-même du sensemaking.

Parmi les nombreux phénomènes cognitifs qui perturbent le raisonnement en situations de crise, deux d'entre eux nous paraissent essentiels à identifier :

- *La régression :* où l'individu, en situation stressante ou anxiogène, a tendance à s'appuyer sur ce qu'il connaît le mieux (donc les schémas mentaux les plus anciens et les plus simples), au détriment des raisonnements complexes et des apprentissages récents qui sont tout simplement « oubliés ».
- *La polarisation des comportements par pression du temps* : où l'individu se montre plus conservateur et moins enclin au risque quand le risque diminue alors qu'au contraire il se montre plus cavalier et plus enclin au risque quand celui-ci augmente[25]. La pression temporelle nous rend plus « joueur » alors même que la situation est plus instable et ambiguë.

Biais cognitifs régulièrement observés en situation de crise

Du fait de ses caractères anxiogènes et d'ambiguïté, la situation de crise est propice au bouleversement de la rationalité et de l'objectivité que les groupes considèrent développer en situation stable. Par conséquent, toute cellule de crise en action sera soumise à l'expression de

[25] En d'autres termes, lorsque le temps presse et qu'il nous stresse, nous pourrions davantage tenter notre chance dans une sortie téméraire entre deux tranchées en situation de guerre que de mise 10% de notre revenu au blackjack dans le casino du coin.

divers biais et heuristiques tant au niveau individuels (chacun des membres de la cellule) que collectif (la cellule de crise elle-même).

En outre, un lien étroit unit la prise de décision en situation de crise à la cognition*. Ce lien a été démontré par diverses études scientifiques. Ainsi, décider en situation de crise met en œuvre de manière particulièrement imbriquée à la fois des processus perceptifs (sensations), de la reconnaissance mémorielle (mémoire) et de la catégorisation (différentiation).

L'expression de ces biais ne doit pas être comprise comme un problème éthique. En effet, ces biais ne sont pas conscients. En outre, le recours à des protections technologiques (logiciels, algorithmes, etc.) ne constitue pas une délivrance des préjugés car ces dernières ont été pensées, construites et programmées par des humains…exprimant leurs biais individuels.

Afin d'étayer notre propos sur la notion parfois floue de ce que peuvent être concrètement les bais cognitifs, nous proposons ici de partager certains d'entre eux régulièrement observés en situation de crise :

- *Biais de narration* : Juger les éléments *a posteriori* pour les articuler en un développement qui nous semble cohérent. Ceci nous permet de (nous) raconter la succession des étapes et évènement et d'ainsi pouvoir attribuer un sens causal.
- *Biais de représentation* : Les crises que nous avons personnellement expérimentées marquent notre mémoire. Ainsi, lorsqu'une nouvelle crise survient, nous faisons naturellement face au risque de considérer cette nouvelle crise sous l'unique perspective des crises que nous connaissons personnellement.
- *Biais du survivant* : Toute expérience d'autres crises amène au risque de généralisation de situations de crises précédentes considérées « satisfaisantes » voire « réussies ». Or les situations étant toutes différentes cela peut amener à répéter aveuglement des principes et routines potentiellement inadaptées voire contre-productives.
- *Biais de présomption* : Ne pas présumer que l'on comprend une problématique du seul fait que l'on dispose d'une routine pour la gérer : il convient d'éviter un excès de confiance dans le protocole et de conserver une marge de manœuvre et d'adaptabilité.
- *Biais du champion* : Il convient d'éviter l'excès de confiance dans les positions des « experts » de l'évènement affronté qui, s'il dispose d'une connaissance spécifique évidente, est enclin à des biais cognitifs réduisant l'anticipation et l'imagination.
- *Biais d'attribution* : attribuer sa réussite à ses qualités personnelles et ses échecs au hasard
- *Biais d'ancrage* : instaurer les termes du débat et influencer la réponse de l'interlocuteur
- *Biais de confirmation:* "*the human mind, when it has once adopted an opinion draws all things else to support and agree with it*[26]"

Après de nombreuses observations de l'expression de ces biais en cellule de crise et d'interrogations quant à leur origine, nous sommes parvenus à la conclusion que trois facteurs contribuaient significativement à leur expression :

[26] Sir Francis Bacon - 1620

1) *L'expérience* : où les schémas mentaux tirés d'expériences personnelles deviennent prépondérants et imposent un schéma directeur (potentiellement inapproprié) pour des situations parfois totalement différentes,
2) *Le grade* : où la légitimité de statut (en temps de paix) au sein de la hiérarchie est considéré implicitement comme une légitimité de cognition tant par les subalternes que par les supérieurs et peuvent conduire à une confiance inappropriée du leader,
3) *La planification* : où les schémas préétablis par l'organisation imposent explicitement une carte mentale occultant implicitement toute réflexion profonde hors des schémas proposés.

La particularité de la cyberattaque

Une fois partagés ces éléments cognitifs inhérents à a gestion de crise, voici ci-dessous les points particuliers qui s'expriment dans les cas spécifiques des cyberattaques :

- *Délégation spontanée par peur de l'incompréhension* : dans de nombreux cas, les décideurs, effrayés par la complexité technique des TIC, préfèrent se reposer totalement sur l'expertise technique dont ils disposent. Cela reviendrait à laisser un conseil scientifique décider des mesures économiques, sociales, politiques et sécuritaires d'un pays en cas de pandémie. La crise cyber pouvant avoir des implications au niveau de l'entièreté des processus de l'organisation (voire même au-delà de l'organisation) il est fondamental que le top-management conserve son caractère décisionnel final. Il est le garant de la politique global car il intègre (ou est supposé intégrer) toutes les dimensions (financières, sociales, techniques, technologiques, commerciales, juridiques, etc.) afin de proposer la direction la plus pertinente. Déléguer les décisions fondamentales via le bouclier de l'expertise revient tout simplement à confier un raisonnement multifactoriel à l'expert d'une seule dimension.
- *Paradoxe d'une vision simplifiée du système* : Si nombre de top-managers se figurent un système trop compliqué pour leur compréhension, certains décideurs développent toutefois une vision mentale simplifiée à outrance (donc tronquée) des systèmes d'information et de communication. Cette sur-simplification amène naturellement à des prises de décisions inadaptées.
- *La difficulté du sensemaking* : Nos l'avons évoqué plus tôt, la construction de sens permet d'élaborer une interprétation de causalité (même erronée) permettant de baser la réflexion et les premières actions. Dans le cas des attaques cyber, la complexité des systèmes d'information et de communication et le couplage intime de la plupart des activités conduit à une incapacité d'anticipation des conséquences. Une des caractéristiques des systèmes complexes et de ne pas pouvoir prédire les conséquences fines des évolutions du système. Ainsi, l'activité anticipatrice, précieuse et fondamentale en gestion de crise, est rendue plus difficile (voire presque impossible dans certains cas) du fait de l'impossibilité cognitive de concevoir les éléments à prévoir en raison de l'explosion combinatoire des conséquences possibles.

Les biais cognitifs font partie intégrante de notre fonctionnement. C'est par ces heuristiques que le genre humain a en partie pu se développer depuis l'aube des temps. Il est illusoire d'imaginer s'affranchir d'un facteur de succès devenu instinct du fait qu'il soit source d'inconvénient dans une quête de rationalité managériale toute récente.

L'anxiété, la pression temporelle, le stress conduisent à une expression plus vive encore des biais cognitifs, et donc renvoie la crise à la situation royale par excellence. La crise cyber en incarne dès lors la plus iconique expression via l'incompréhension et la crainte majeures qu'elle suscite auprès des décideurs.

Notions de fragilité, de résilience et d'antifragilité

Il nous apparait impossible de traiter des cybercrises sans aborder les notions essentielles décrivant la nature des systèmes. Ces concepts, souvent nommés dans les organisations, font toutefois souvent l'objet de compréhension différentes.

La fragilité

La fragilité, telle qu'abordée dans le *Incerto* de Nassim Taleb, se réfère au rapport d'une organisation ou d'un objet (qu'il soit physique ou conceptuel) à la volatilité. Est fragile ce qui supporte mal les turbulences et réagit de manière à la volatilité par effet seuil. Le changement est alors perçu comme une agression qui n'est pas ressentie de manière proportionnelle. Au contraire, le système réagit de manière non-linéaire, c'est-à-dire qu'arrivé à un certain seuil, la volatilité endommage de manière irréversible (et parfois détruit) le système.

Le temps, à une échelle assez grande, pouvant être assimilé à la volatilité, est donc considéré fragile tout ce qui ne résiste pas à l'épreuve du temps[27].

La fragilité amène cependant à de nombreux avantages. En effet, du fait de sa dépendance à la stabilité, elle est synonyme d'optimisation et permet donc une rentabilité augmentée via la sous-traitance et les externalisations. Elle est aussi en lien avec la simplification et l'unification des outils et méthodes (ERP* unique à l'entreprise, etc.). Cette option de fragilité, attirante pour l'expert-comptable comme pour l'industriel, revêt d'une analyse tactique du monde où la stabilité de l'environnement permet un ajustement perpétuel orienté vers la simplification et donc sur l'optimisation continue. Cette tactique offre des perspectives d'économie et de rentabilité significative.

Toutefois, en cas de d'instabilité, toute turbulence (même mineure) au sein ou à l'extérieur du système peut alors revêtir des dimensions cataclysmiques tant l'organisation est articulée en flux tendus et interdit tout ajustement.

[27] Comme les espèces trop spécialisées, les tamagochis, le dernier smartphone, les tubes de l'été post-lambada, les résultats de sondages politiques et les romans contemporains.

Le cas Altran (2018) *: L'entreprise de de conseil en ingénierie fut attaquée via les faiblesses d'un site internet et vit sont Active Directory* être pris d'assaut. Réalisant que plus de 400 serveurs étaient cryptés, l'entreprise décida d'éteindre son système d'information pour éviter la propagation du ransomware et se déconnecter des clients de l'entreprise. Or l'intégralité de l'activité d'Altran (consulting) reposait sur le système d'information. Il devint quasi impossible de permettre une continuité des activités.*

La résilience

Cette aptitude, mainte fois mentionnée dans les organisations, se définit scientifiquement par l'addition de trois capacités complémentaires :

- *Une capacité d'absorption* : en tant que capacité à mobiliser des ressources internes et externes.

  

  Le cas Norsk Hydro (2019) : *La cause première de cette cyberattaque, ainsi que la solution permettant de la contrer furent identifiées grâce à l'aide précieuse de Microsoft et d'autres partenaires de sécurité informatique. En outre, grâce à une solide politique de sauvegarde, l'entreprise savait qu'elle pouvait récupérer les données sans payer la rançon.*

  C'est notamment via cette approche que les consultants et les experts proposent la sollicitation de l'ANSSI en cas de cyber attaque par exemple. De telles considérations ne sont malheureusement pertinentes que pour les OIV* et les grandes entreprises. Que faire quand notre organisation n'entre pas dans ces « joyaux » à protéger à tout prix ? Comment passer en priorité lorsque ce sont des secteurs voire des pays entiers qui sont attaqués ?

- *Une capacité de renouvellement* : en tant que capacité à utiliser les ressources mobilisées pour développer des solutions inédites en réponse à la crise.

  

  Le cas Saudi Aramco (2012) : *Suite à une cyberattaque par phishing un wiper détruisit plus de 35000 postes ce qui contraint l'entreprise à déconnecter manuellement les câbles. Un retour aux procédures manuelles fut ainsi requis le temps de rétablir les capacités numériques. C'est ainsi que plus de 50 000 disques durs furent achetés auprès des fournisseurs du monde entier, afin de de reconstruire le Système d'Information. Cet achat fut possible aux énormes atouts financiers de Saudi Aramco.*

- *Une capacité d'appropriation* : en tant que capitalisation des bonnes et mauvaises pratiques identifiées en vue de rendre l'organisation mieux préparer à la survenue d'une situation similaire.

La résilience, en tant que cumulation des trois capacités évoquées ci-dessus, touche à la stratégie « surfacique ». Elle permet une réflexion et une organisation permettant à une structure

appréciant les systèmes stables (permettant l'optimisation, la rentabilité, l'externalisation, etc.[28]) à résister à la turbulence jusqu'à un retour à un niveau de stabilité acceptable.

Malgré ces nombreux avantages, la problématique intrinsèque que nous identifions à la résilience est sa position vis-à-vis du changement. En effet, la résilience : favorise-elle ou empêche-t-elle l'évolution ? Le refus de s'intégrer à l'essor de la photo numérique (turbulence) de Kodak et de perdurer sur la pellicule (système jusqu'alors stable) est-il le fruit d'une erreur stratégique ou plutôt d'un phénomène de cette résilience justement prônée par les stratèges ?

En d'autres termes et pour revenir au problème cyber, et si les organisations qui 1) furent résilientes à la digitalisation et au « tout numérique » de toutes les activités et qui 2) sont parvenues à survivre, se révélaient moins soumises aux agressions cyber ?

L'antifragilité

Cette approche touche à la stratégie profonde. Elle impose par nature une position stratégique fondamentale jurant avec les postures majoritaires actuelles.

Il faut comprendre l'antifragilité comme une position bénéficiaire vis-à-vis de la volatilité. Comme l'intelligence humaine et la culture qui tirent parti des expériences (même difficiles) et des imprévus afin de s'étoffer de manière non-linéaire et complexe. Par cette capacité d'apprécier la volatilité (qui n'est qu'une expression de la notion de temps), est antifragile ce qui résiste à l'épreuve du temps.

Pour cela quelques attributs semblent se distinguer :

- *Cultiver la redondance :* en tant que disposer de différents (indépendants) canaux de communications, outils, méthodologies et principes. Cela s'applique aussi aux notions de compétences à cultiver en parallèle au sein des divers populations de l'entreprise.
- *Réapprendre le low-tech* :* en tant que conservation de la connaissance profonde des rouages, fonctionnement et implications des processus fondamentaux de l'entreprise (qui n'apparaissent aucunement aux utilisateurs des interfaces numériques).
- *Disposer d'écoutilles :* en tant qu'éviter l'installation de connections toujours plus intimes et toujours plus nombreuses (et de moins en moins visualisées par les équipes des systèmes d'information et de communication) avec les partenaires (fournisseurs, clients, sous-traitants, etc.). Ce point est fondamental car, en cas d'attaque, vous pouvez très bien ne pas représenter la cible véritable finale de l'attaque et n'être qu'un dommage collatéral (ou encore une porte d'entrée) d'une cyberattaque destinée à l'un de vos partenaires directs ou indirects.
- *Identifier précisément la nature et les modalités des supports extérieurs :* en tant que définir, en temps de paix et d'un point de vue macroscopique, des acteurs extérieurs (étatiques ou même privés) et les fonctionnements (en tant que leurs modalités de

[28] En somme les courants stratégiques majoritaires actuels (qui correspond étrangement aux leviers principaux des contrôleurs de gestion)

support auprès de votre organisation) à déployer en temps de crise. Ces modalités doivent justement être très précises afin de garantir l'aide de ces acteurs extérieurs dans toutes les situations comme, par exemple, la prise en charge prioritaire de votre organisation en cas de requêtes simultanées de multiples d'organisations à leur encontre en cas d'attaque cyber généralisée.

> ***Le cas Mercks (2017)*** *: lors de l'attaque par le wiper NotPetya, l'entreprise se retourna auprès de ses assureurs, couvrant le risque de cyberattaque à hauteur de 1,75 milliards de dollars, afin de gérer le paiement d'une rançon s'élevant à 1,3 milliards de dollars. Malgré la couverture contractuelle, les compagnies d'assurance refusèrent alors de payer ce montant du fait de la catégorisation de l'attaque en tant qu'"acte de guerre", catégorie ne figurant pas dans la liste des typologies mentionnées dans les clauses du contrat.*

- *Se préparer au pire* : en tant qu'il ne faut pas considérer la cybercrise résolue au motif de la seule acceptation des requêtes des attaquants (comme un paiement lors d'un ransomware par exemple). En effet un paiement dûment effectué n'implique aucunement la restauration du système. Le décryptage des données est une activité longue et nombre de lignes de données ne pourront être décryptées et seront irrémédiablement perdues sans la garantie d'un back-up disponible.

Conclusion

En conclusion de notre production, nous soulignons le caractère tout à fait singulier de la crise cyber. Elle revêt en effet plus d'opacité et d'immédiateté, elle est plus difficile à comprendre et frappe plus violemment et durement encore l'organisation.

Charles Perrow, sans pour autant traiter de cette catégorie de crise précisément, avait dès 1984 dressés les traits qui lui confèrent cette propriété d'illisibilité profonde et de magnitude démesurée. La complexité de nos processus, tous dépendants de structures numériques et digitales et leur couplage intimes, annoncent l'inéluctabilité de crises cyber à venir. Les mêmes grains de sables, issus de bugs aléatoires ou plus probablement d'attaquants malveillants, perturberont plus gravement nos organisations.

Notre ère du « tout numérique et tout digital » renforce plus encore cette certitude. Désormais inéluctablement numérisées et digitalisées, nos structures (hier encore plus physiques et manuelles, et donc moins dépendante les unes les autres), deviennent immanquablement plus susceptibles d'être l'objet direct ou indirect des cyber crises qui nous attendent. C'est ainsi que nous prédisons que les crises seront pires. Les conséquences seront inexorablement plus rudes dans un monde qui ne peut désormais qu'au moyen de supports techniques que les dirigeants et les managers ne comprennent pas.

Notre réflexion nous pousse même à nous demander si la caractéristique VUCA elle-même n'est pas la simple conséquence que la numérisation/digitalisation de l'intégralité de nos

processus désormais tous interdépendants et échappant à la compréhension humaine. Cela ferait de nous les artisans de notre propre perte. Le progrès, notamment numérique, devient dès lors notre plus grande faiblesse.

Notre conseil est donc de cultiver l'optionalité[29]. L'optimisation et la rentabilisation, qui font du contrôleur de gestion un conseiller stratégique majeur en système stable, rendent ce dernier un artisan de notre perte en système turbulent. L'ère est à la volatilité. Les grands gagnants des crises de demain seront ceux qui seront bénéficiaires des changements, donc ceux qui disposeront d'options. Les super-adaptés, les super-optimisés disparaîtront. C'est darwinien. Les super-adaptés dominent en état stable et les « touche à tout » prolifèrent en système très instable[30]. Or tous les stratèges ne s'accordent-ils pas à qualifier l'époque de VUCA ?

Nous terminerons sur cette réflexion, pouvant choquer les partisans de la gestion de crise traditionnelle. Et si cyber n'était pas une typologie de crise ? Et si sa singularité profonde ne résidait pas en cette incompréhensible interconnexion reliant tout à, à peu près, tout le reste ? Et si la crise cyber était en réalité seulement une nouvelle génération de crise de continuité ? Une méta-crise de continuité des activités à la fois holistique et immédiate ?

[29] En tant que la mise en place constante d'options possibles à exploiter en cas de modifications significatives de l'environnement.

[30] Les petits mammifères rongeurs omnivores (non spécialisés) étaient contraints à des niches réduites au Crétacé. Les dinosaures, espèce vertébrée ultra-majoritaire sur terre, étaient super-adaptés à toutes les niches écologiques disponibles. Ils s'éteignirent suite à l'impact d'une météorite dans le golfe du Mexique. Les petits mammifères purent, par leur flexibilité de comportement, de régime alimentaires, d'exploitation des ressources, de système reproductif, survivre à l'extinction de masse et ainsi bénéficier de tous les systèmes écologiques.

Bibliographie

De Vittoris (2021), Survivre aux crises : idées reçues et vraies pistes pour les entreprises. Dunos, Paris

De Vittoris R. (2021), Cognitive biases in crisis situation. Crisis Response Journal. Vol 16. Issue 1. Pp.21

Donnellon, A., Gray B., Bougon, M. (1986). « Communication, Meaning and Organized Action », Administrative Science Quartely, vol 31; p 43-55. Dror et al. (1999)

Dror I., Busemeyer J., Basola B. (1999). Decision making under time pressure: An independent test of sequential sampling models. Memory & Cognition, 27(4), 713-725

Kersten, A., Sidky, M. (2005). Re-aligning rationality: Crisis management and prisoner abuses in Iraq. Public Relations Review, 31(4), 471–78.

Koenig, G. (2003), « L'organisation dans une perspective interactionniste », In Vidaillet, B. (eds), Le sens de l'action, Vuibert, Paris ; p 15-34 Marsch

Link, S. W. (1992). The wave theory of difference similarity. Hillsdale, NJ: Erlbaum.

Milasinovic, S., Kesetovic, Z . and Nadic, D. (2010). The Power and Importance of Crisis Management in Facing Modern Crises. Megatrend Review, 7 (2), 273-290

Nosofsky, R. M., & Palmeri, T. J. (1997). An exemplar based random walk model of speeded classification. Psychological Review, 104, 266-300.

Passè E. (2011). Gestion de crise et improvisation, les leçons de 4 études de cas. Thèse de doctorat, Université de Strasbourg

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. Academy of Management Review, 23(1), 59–76.

Perrow, C. (1984). Normal accidents : Living with High-Risk Technologies. Basic Books, New York. ISBN 978-0465051427

Quarantelli, E.L. (1996), 'The future is not the past repeated: Projecting disasters in the 21st century from current trends', Journal of Contingencies and Crisis Management, Volume 4, Number 4, pp. 228–240.

Quarantelli, E. (2001) 'Another Selective Look at Future Social Crises : Some Aspects of Which We Can Already See in the Present'. Journal of Contingencies and Crisis Management, 9(4), 233-237.

Ratcliff, R. (1978). A theory of memory retrieval. Psychological Review, 85, 59-108.

Reason J. (1995), Understanding adverse events: human factors. Quality in Health Care 1995;4:80-89

Reason J. (2000), Human error: models and management. BMJ VOLUME 320 18 MARCH 2000 www.bmj.com

Taleb NN. (2004). Fooled by randomness: the hidden role of chance in life and in the markets. South Western, Thomson Learning company

Taleb NN. (2010). Le Cygne noir : La puissance de l'imprévisible, Les Belles Lettres, Paris, 2010,

Taleb NN. (2013). Antifragile : Les bienfaits du désordre, Les Belles Lettres, Paris, 2013

Topper B., Lagadec P., (2013), Fractal Crises – A New Path for Crisis Theory and Management. Journal of Contingencies and Crisis Management Volume 21 Number 1 March 2013

Vandangeon-Derumez I. Autissier D. (2006) 'Construire du sens pour réussir les projets de changement. Les Défis du Sensemaking en Entreprise. Economica.

Vraie B (2017). Management sous stress - Prise en compte du facteur « stress aigu » dans la gestion de crise. Thèse de doctorat. Université Paris I Panthéon-Sorbonne.

Weick K.E., (1979), The social Psychology of Organizing, Reading, MA : Random House

Weick, K. E. (1988). 'Enacted sensemaking in crisis situations'. Journal of Management Studies, 25, 305–17.

Weick K., Sutcliffe KM., (2007), Managing the unexpected - Resilient Performance in an Age of Uncertainty. 20172017

Weick, K. E. (1993). 'The collapse of sensemaking in organizations: the Mann Gulch disaster'. Administrative Science Quarterly, 38, 628–52.

Weick, K. E. (1995). Sensemaking in organizations (Foundations for organizational science). Sage Publications, Thousand Oaks, CA. ISBN 978-0803971776, 235 pages.

Weick K.E., Sutcliffe K.M. & Obstfeld D. (1999), Organizing for High Reliability: Processes of Collective Mindfulness. R.S. Sutton and B.M. Staw (eds), Research in Organizational Behavior, Volume 1 (Stanford: Jai Press, 1999), pp. 81–123.

Weick, K. E. (2010). Reflections on enacted sensemaking in the Bhopal disaster. Journal of Management Studies, 47(3) :537–550.

Glossaire

Active Directory : Annuaire (au sens informatique) répertoriant tout ce qui touche au réseau (noms des utilisateurs, des imprimantes, des serveurs, des dossiers partagés, etc.) permettant à l'utilisateur d'accéder aux ressources partagées, et aux administrateurs de contrôler leurs utilisations.

Cognition : Processus par lequel un organisme acquiert la conscience des évènements et objets de son environnement.

Darkweb : Partie du web regroupant ce qui n'est pas accessible via des navigateurs standard (Google Chrome ou Firefox). C'est la difficulté d'accès des informations qui leur confèrent un statut de « dark ».

Defacement : Résultat d'une activité malveillante qui a modifié l'apparence ou le contenu d'un serveur internet, et a donc violé l'intégrité des pages en les altérant.

Déni de service : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. Il est parfois seulement le fruit d'un dimensionnement inadapté du service (et non pas d'une attaque malveillante), incapable de fournir la réponse à une forte demande.

Effet de seuil : Un système peut se caractériser par un état stable (où les relations entre les éléments ne sont pas altérées et où les perturbations ont un effet prévisible et temporaire), jusqu'à un seuil d'instabilité au-delà duquel une perturbation minime peut provoquer une évolution catastrophique (développement non-linéaire). Dans ce dernier cas, l'évolution des paramètres observés connaît alors une discontinuité ou la proportionnalité n'a plus cours.

Enterprise Ressource Planning (ERP) : Groupe de modules relié à une base de données unique qui permet de gérer l'ensemble des processus opérationnels d'une entreprise en intégrant plusieurs fonctions de gestion (gestion des commandes, des stocks, de la paie, de la comptabilité, de commerce BtoB ou BtoC, etc.)

Heuristiques : raccourcis mentaux permettant des réactions spontanées.

Low-Tech : Approche basée sur la mise en œuvre de technologies simples, peu onéreuses, accessibles à tous et facilement réparables, faisant appel à des moyens courants et localement disponibles.

NotPetya : Malware, apparu en Ukraine avant de se propager au monde entier. Il fut improprement considéré comme une nouvelle souche de la famille des ransomware Petya, et fut justement baptisé "NotPetya" après rectification. Ce malware se caractérise par un caractère destructeur davantage que par une volonté de collecter des rançons.

Opérateur d'Importance Vitale (OIV) : Organisation publique ou privée qui est identifiée par l'État comme ayant des activités indispensables pour le pays (dans des secteurs d'activité

tels que la santé, l'eau, l'électricité et le gaz, l'alimentation, les hydrocarbures, les transports, l'audiovisuel et les télécommunications, l'industrie, la finance, le nucléaire, l'armement ou l'espace.

Phishing : Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge. Dans ce cas un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Ransomware : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système qui lui empêche l'accès à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon.

Spearfishing : Attaque reposant sur une usurpation de l'identité de l'expéditeur dans le but de duper le destinataire alors invité à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois la première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation constituant la véritable cible.

Théorie des systèmes complexes : Un système complexe est irréductible à un modèle fini quelle que soit sa taille, le nombre de ses composants, l'intensité de leur interaction. Pour un observateur, il est complexe parce qu'il tient pour certain l'imprévisibilité potentielle des comportements.

TIC : Technologies de l'information et de la communication

VUCA : Volatility Uncertainty Complexity Ambiguity

Wannacry : Ransomware capable de se propager d'un ordinateur et d'un réseau à un autre automatiquement, sans nécessiter d'interaction humaine, WannaCry s'est appuyé sur un exploit Windows qui a rendu des millions d'appareils vulnérables. Ses méfaits ont provoqué des dégâts à hauteur de centaines de millions (peut-être même de milliards) de dollars.

Watering hole : Attaque est destiné à infecter les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée. La technique consiste à piéger un site Internet légitime afin d'infecter les machines des visiteurs du domaine d'intérêt pour l'attaquant.

Wiper : Attaque reposant sur l'effacement de toutes les données des ordinateurs des victimes. Certains d'entre eux lancent une attaque ponctuelle à une date spécifique et effacent les disques durs, tandis que d'autres corrompent graduellement les disques pendant une longue période.