La résilience dans le système d'informations

Daniele Pitrolo

Mémoire
Master MIMO

Université Paris 1
Panthéon - Sorbonne

Contents

Introduction

La résilience pourrait sans doute rentrer dans le compte des concepts que seuls les philologues maîtrisent : avec son étymologie latine et sa présence attestée dans l'horizon culturel des philosophes dès le XVIIe siècle (Bacon [TLFi], Descartes [Cresti, 2014]), le mot « résilience » ne manque d'ailleurs pas de les intéresser.
Au cours des siècles, en effet, son contenu sémantique s'est renouvelé plusieurs fois : si le mot d'origine est la crase latine de « re » et « silire », c'est dans cette acception, de « rebondir », qu'il est introduit dans l'anglais du XVIIe siècle. Perçu comme un anglicisme [TLFi], attesté en effet dans les *Notes* de Thomson [Bucharles, 2008], il est employé en français déjà au début du XXe siècle : nouvelle acception, le terme sert à décrire la force morale de ceux qui accablés par des circonstances opposées, resurgissent. Dans une signification proche, le terme est également choisi par la discipline, bien éloignée, de la physique des matériaux : pour celle-ci résilience est la propriété d'absorber un choc et de savoir ensuite retrouver sa forme précédente [TLFi].

Le vingtième siècle aura sans doute été, pour la société occidentale, celui du choc, du traumatisme : deux guerres mondiales ont marqué sa première moitié et la deuxième a été également conditionnée, en creux, par le déchaînement dés puissances destructrices humaines. Un tel traumatisme était aussi bien présent comme souvenir des survivants, de ce qui s'était passé, que comme menace quotidienne de la guerre froide : danger toujours imminent qui faisait désespérer de la possibilité de rebondir.
Fort de son histoire, « résilience » est un mot qui dispose d'une vaste assise conceptuelle et celle-ci a permis qu'il devienne un réceptacle de ce Zeitgeist inquiet marquant l'époque actuelle et qu'il serve donc de synthèse populaire à l'élitiste aphorisme de Nietzsche sur ce qui détruit et ce qui rend plus fort. Cela participe sans doute à la spectaculaire inflation de l'utilisation du terme et du concept : l'étude de la résilience se décline désormais dans un très grand nombre de disciplines venues s'ajouter aux autres champs évoqués, telle que la psychologie et l'étude du développement infantile, la pathologie médicale [RP] ainsi que la recherche militaire [Comfort, Boin, Demchak, 2010], la sociologie aussi bien que la géographie [Dauphiné, Provitolo, 2007].

Le concept de résilience est donc assez couramment connu et même à la mode. En 2012 des chercheurs relevaient d'ailleurs que le terme était devenu, dans les États Unis, un élément presque incontournable de toute conversation – qu'elle porte sur les qualités nécessaires des écoliers ou bien du président de la république – évoqué aussi bien pour les équipes sportives que pour les infrastructures critiques [Comfort, Boin, Demchak, 2010]. Une telle présence forte dans une région aussi bien définie est d'ailleurs à mettre en lien avec le concept de « disruption », élément de langage de l'industrie de la Silicon Valley, et justement les éditions O'Reilly inauguraient l'année 2016 en listant « 5 ways to be more resilient in 2016 » [O'Reilly, 2016].
Forts de leur capacité d'innovation technologique, et de leur volonté de dérégu-

lation sociale [Morozov, 2014], ces acteurs prévoient d'annihiler les concurrents, vus comme obsolètes. Encore une fois, la capacité de rebond est d'autant plus présente dans les esprits et invoquée qu'une intention de destruction se manifeste (sur le résultat qui semble à constater, d'avoir rendu résilientes les réalités que la Silicon Valley souhaitait *disrupter*, voir [Morozov, 2016]).

Capable de prospérer dans cette sous-culture de prédation, le concept a su se populariser également en Europe, aussi bien dans le domaine technologique (le site *The Pirate Bay* se définit ainsi *The galaxy's most resilient BitTorrent site*) que social, où on arrive donc à le retrouver désormais employé par des acteurs tout aussi lugubres que ceux d'outre-Atlantique : c'est le ministre de l'intérieur qui de toute l'histoire d'un gouvernement démocratique aura le plus œuvré pour la destruction de l'état de droit à louer la résilience des Français [Cazeneuve, 2016] ; ce sont les magazines qui usent de la peur pour tétaniser et capturer leurs lecteurs qui font ensuite des unes sur la résilience, tel *L'Express* en août 2016.

En s'apprêtant à étudier la résilience dans le contexte du système d'information il sera donc préalablement nécessaire de s'interroger sur la pertinence de ce rapprochement : correspond-t-il à l'abus d'un outil intellectuel qui, déjà protéiforme, risque de voir sa signification se diluer et devenir évanescente dans un kamoulox de termes à ramdam?
Ou bien s'agi-t-il d'une expansion ultérieure de la portée sémantique du mot qui serait justifiée et qui permettrait d'enrichir l'analyse portée sur le système d'information et serait par conséquent capable de participer aux outils et méthodes qu'il convient de mettre en œuvre pour le concevoir et l'évaluer?

Partisans de cette deuxième option nous essaierons dans cet exposé de justifier cette position et de montrer comment la résilience peut être envisagée dans le cadre d'un système d'information, quels sont les problèmes qu'elle permet de confronter et dans quelle mesure des solutions résilientes sont déjà employées à ce fins, et cela aussi bien au niveau microscopique que macroscopique.

Un cadre opératoire pour la résilience

Le SI, un cadre d'enquête

La multiplicité des champs d'application du concept de résilience ne facilite certainement pas sa définition, mais la tâche n'est pas pour autant plus aisées lorsque l'on se cantonne à un seul domaine. Comme le montre Serge Tisseron, même en psychologie plusieurs conceptions du phénomène se superposent, expression de courants successifs dans le temps et géographiquement différents [Tisseron, 2009]. En effet, la possibilité d'une perspective globale est d'autant plus malaisée que le travail de conciliation de celles-ci est encore en cours [Aïn, 2007].

Pour ce qui est du domaine à l'intérieur duquel on va étudier la résilience, des différences existent entre les définitions du système d'information données pas les auteurs [Silver, Markus, Beath, 1995], celles-ci sont cependant réduites, et nous pourront ainsi adopter la suivante [Rivard, Talbot, 2004] :

> Un système d'information est [un élément d'une organisation constitué d']un ensemble d'activités qui saisissent, stockent, transforment et diffusent des données sous un ensemble de contraintes appelé l'environnement du système. Des inputs (données) sont émis par une ou plusieurs sources et traités par le système, lequel utilise aussi des données entreposées préalablement. Les résultats du traitement (outputs) sont transmis à une ou plusieurs destinations ou mettent à jour des données entreposées. Pour sa réalisation, un système d'information utilisera des technologies de l'information plus ou moins sophistiquées pouvant aller de la simple calculatrice dans le cas de systèmes très peu sophistiqués jusqu'à des réseaux d'ordinateurs extrêmement puissants, utilisant des interfaces de type multimédia.

Si ici les auteurs prennent garde de souligner la possibilité que le système d'information soit constitué d'une technologie rudimentaire, il est cependant intéressant de remarque que d'autres considèrent que sans « codes sources binaires [sic] les ordinateurs ne fonctionneraient plus, ils ne pourraient même pas s'appeler ordinateurs et il n'y aurait plus de système d'information » ([Lequeux, Challande, 2009]. Une approche tout aussi dépourvue du rôle humain quoique moins simpliste est défendue dans [Wang, 2010]). Cette thèse a certainement le défaut de son caractère axiomatique, accompagné du fait que les auteurs fournissent uniquement une définition en creux du système d'information. Elle a cependant le mérite de souligner l'importance des outils informatiques, quitte à l'exagérer. Si ceux-ci ne sont pas indispensables, il est cependant indéniable que la plupart des systèmes d'information reposent de manière presque inextricable sur un système informatique et que le bon fonctionnement de celui-ci est très souvent un pré-requis pour le système d'information.

Toujours dans ce sens nous devrons bien reconnaître que nombre des fonctions prises en charges par le système d'information ne le sont que par le biais de

l'informatisation des organisations. C'est ainsi, en effet, que des activités, des processus et des tâches deviennent visibles, quantifiables et, surtout, systématisables : morcelés et atomisés ils sont demandés à l'initiative individuelle et transparents au niveau organisationnel.

Le degré d'informatisation du système d'information est donc un facteur déterminant pour son expansion et sa capacité d'être de support à un plus grand nombre de composantes de l'organisation dont il fait partie. Cet aspect est donc directement proportionnel au degré d'ubiquité du système d'information, et, parallèlement, à sa substituabilité. Ces deux indicateurs, il est intéressant de le souligner, font partie des critères qui déterminent le niveau hiérarchique du système d'information dans l'organisation [Lucas 1984].
Ultérieurement intéressant de relever au passage que ces éléments font partie des caractéristiques qui permettent au SI d'avoir une place importante dans une organisation.

Cerner la résilience

Moins évasive que celle de la résilience, la définition du système d'information, en plus d'être assez consensuelle, permet déjà d'identifier des éléments critiques dont il sera important de garantir la résilience.

Mais qu'est-ce donc la résilience?

Si l'on essaie d'explorer le vaste champ que ce concept peut couvrir, on constate qu'à travers les différentes perspectives fournies par la psychologie et par la sociologie au moins huit phénomènes tombent sous cette appellation, Leur identification et classification a été le travail de Arshi Shaikh et Carol Kauppi [Shaikh, Kauppi, 2010]. Néanmoins, chacun de ces phénomènes se voit refuser cette même appellation, soit par les partisans d'autres approches soit à cause d'une vision statique et binaire de la résilience plutôt que dynamique et conjoncturelle.

Travaillant à plusieurs niveaux de profondeur, la résilience psychologique se démontre plus vaste et moins uniforme. Elle est tout d'abord un trait de la personnalité des individus, optimistes, amenés à une interaction positive avec les autres, équanimes, persévérants. Intéressante à un premier niveau d'analyse, cette approche est problématique, en raison de son caractère statique et absolu qui ne permet pas d'envisager un véritable travail de construction de la résilience, notamment à un niveau supérieur de celui de l'individu isolé.
Une deuxième facette de la résilience est celle qui la définit comme la capacité à opérer une adaptation positive dans un contexte de forte adversité ou risque. La difficulté d'appréciation, à la fois subjective et objective de ce qui est un contexte de risque ou d'adversité fait l'objet de nombreuses critiques de la part des chercheurs. Une critique qui aboutit à une troisième vision de la résilience, comme propriété permettant une adaptation positive, ce qui élude le problème de la définition du contexte.
Complémentaire à cette vision, une autre définition de la résilience s'attache plutôt à l'étude des processus dans lesquels des caractéristiques, neutres dans un état de départ, se mettent en relation et constituent un mécanisme d'adaptation. Une approche intéressante et suivie dans le cadre de plusieurs expériences, qui se heurte par contre à la difficulté de modéliser des situations dans lesquelles les facteurs de risque sont multiples, ainsi que les effets des caractéristiques mobilisées.
Proche des définitions qu'on vient d'exposer, une autre qui a été formulée est celle de la résilience comme capacité d'enclencher, lors de l'apparition d'éléments perturbateurs, un processus adaptatif et continu, se prolongeant sur une durée de temps qui permet de les dépasser. La résilience est ici à l'œuvre dans des efforts continus au niveau cognitif et du comportament pour gérer des demandes externes ou bien internes qui sont perçues comme lourdes ou même excessives par rapport aux ressources du sujet en question.
Dans le cadre d'une telle attention à l'expérience de récupération après un

traumatisme, des questions ultérieures se poseraient (on revient de telles expériences plus fort ou pas?) qui ne sont pas sans intérêt.

Moins nombreuses, les définitions dans le domaine de la sociologie se concentrent sur le comportement dans un contexte structurellement hostile. Dans une première définition du terme, la résilience est le fait de constituer une association qui résiste à l'ordre ou aux conditions structurelles auxquelles elle est soumise : une définition qui, à l'image de plusieurs parmi celles du champ de la psychologie, convoque le concept de résistance dans un contexte élargi.
Dernier effort de définition de la résilience est celui de l'adaptation d'un individu à un environnement hostile qui est à même de lui garantir une survie, même si celle-ci peut se payer par une régression. Cette opération peut avoir lieu grâce à des tactiques agressives ou bien à une posture plus sociale : des outils variés qui ont pour résultat le fait de ne pas briser le continuum dans lequel se situe l'individu.

En donnant une synthèse de ce vaste panorama phénoménologique et compte tenu de ces définitions et des critiques auxquelles elles ont donné lieu, nous pourrons nous attacher à l'étude de la résilience en la considérant tout d'abord comme un phénomène pluriel. Celui-ci se construit aussi bien à l'échelle individuelle, microscopique, qu'au niveau du systémique, c'est-à-dire, justement, nos deux niveaux d'enquête.

La résilience est à la fois une caractéristique statique propre aux éléments ainsi qu'un phénomène dynamique conjoncturel.
S'il est vrai qu'elle se définit par rapport à des perturbations de l'environnement, le moment où la résilience entre en jeux peut tout aussi bien être celui de la préparation. Dans ce dernier cas, les éléments convoqués pour constituer le système permettent de mettre en place un environnement qui sera résilient dans la mesure où son fonctionnement normal sera capable d'absorber et contourner, quelque part d'ignorer, des facteurs qui seraient autrement critiques.
Le moment peut également être celui de la confrontation, quand la perturbation se manifeste et risque de compromettre le système, ou bien le moment, plus visible en raison de l'interruption à laquelle il fait suite, de la récupération, quand la perturbation a eu lieu et le système doit gérer ses conséquences.

Ces éléments éclairés, nous pouvons ultérieurement réduire la définition de résilience et nous concentrer sur ce phénomène en l'envisageant comme la capacité statique et dynamique d'un système de gérer, sur un horizon temporel de réponse immédiate ou asynchrone, l'erreur et de le contenir ou reconduire à l'intérieur d'un cadre d'équilibre stable.

L'effet de la résilience sera également conçu de manière large : l'aboutissement pourra aussi bien être la récupération de la situation précédente à la perturbation, un fonctionnement ordinaire, ou bien une amélioration de celui-ci.

Pour conclure notre définition, nous pourrons relever la proximité entre ce do-

maine d'études, tel que nous venons de le définir – et qui a été appelé, sans beaucoup de suite, comme "IS Mindfulness" [BUTLER, GRAY 2006] – et le champ de recherche, plus important que ce dernier, du système d'information robuste. Plus particulièrement, celui-ci

> is achieved by choosing a strategy that yields satisfactory results under all environmental scenarios which are assessed as having an appreciable probability of occurring [El Sawy, Nanus, 1989].

En effet, cette définition touche au cas de « résilience de préparation » ou même « de confrontation ». La résilience telle que nombre de chercheurs s'attachent à l'étudier va cependant au delà de cela ; car il s'agit d'étudier également les situations dans lesquelles le système a été endommagé, au moins partiellement [Wang, 2010], mais, surtout, des situations dans lesquelles le système doit se confronter à une situation qui, contrairement à ce qui fonde la recherche du système d'information robuste, n'a pas été explicitement prévue [Hollnagel, Woods, Leveson, 2006].

> Success belongs to organisations, groups and individuals who are resilient in the sense that they recognise, adapt to and absorb variations, changes, disturbances, disruptions, and surprises – especially disruptions that fall outside of the set of disturbances the system is designed to handle.

Que ceux-ci aient fait déjà l'objet d'études et théorisation nous confirme leur intérêt ; mais, plus encore, le fait de pouvoir les encadrer de manière plus large avec la « résilience de récupération » nous confirme l'utilité d'une approche multidisciplinaire capable d'apporter un questionnement nouveau et enrichissant.

Ce qui n'est pas résilience

Il apparaît maintenant utile de souligner des aspects qui ne rentrent pas dans le champ de la résilience telle que nous l'avons définie tout en présentant des points de contact avec celle-ci.
Comme le soulignent les chercheurs [Hollnagel, Woods, Leveson, 2006], l'horizon dans lequel opère la sécurité est celui des connaissances acquises par l'expérience.

> This is so both in research and in practice, perhaps more surprising in the former than in the latter. The practical concern for safety is usually driven by events that have happened, either in one's own company or in the industry as such. There is a natural motivation to prevent such events from happening again, in concrete cases because they may incur severe losses.

Celle-ci constitue d'ailleurs un prisme qui est à la fois le garant de la possibilité d'observer et comprendre la réalité, mais qui en même temps, en définissant le champs des possibles, active certains parcours cognitifs aux dépends des autres qui, non expérimentés, restent par là inconnus.

> It is practically a characteristic of human nature – and an inescapable one at that – to try to make sense of what has happened, to try to make the perceived world comprehensible. We are consequently constrained to look at the future in the light of the past. In this way our experience or understanding of what has happened inevitably colours our anticipation and preparation for what could go wrong and thereby holds back the requisite imagination that is so essential for safety.

Dans ce sens, la sécurité se définit comme une palette d'outils et procédures pour anticiper ou répondre aux scénarios que l'expérience a donné à connaître. Cependant, l'expérience se renouvelant sans cesse, la sécurité construite pour prévenir les menaces du passé est, tôt ou tard, forcément prise en faille par celles du présent.

> Approaches to safety and risk prediction furthermore develop in an incremental manner, i.e., the tried and trusted approaches are only changed when they fail and then usually by adding one more factor or element to account for the unexplained variability.

Une fois que l'on prend en compte ces précisions, il apparaît donc clairement que la résilience, tout en pouvant inclure la sécurité, vise une approche qui dépasse celle-ci. Elle ambitionne la création d'un système qui ne se construit pas par les échecs successifs, mais qui est capable de se confronter de manière efficiente avec un nombre de problèmes exponentiellement plus vaste que celui des solutions singulières prévues ; un système dont le fonctionnement en équilibre stable permet de ramener les menaces à des archétypes maîtrisables.

Car, en effet, la résilience est une propriété inhérente au système, que celui-ci soit la structure physio-chimique d'un métal ou bien le complexe ensemble d'acteurs qui constitue une organisation sociale.
En tant que telle il est donc clair qu'elle se construit et se prépare, mais la résilience ne peut pas être dictée ou exigée : elle est bien plus complexe qu'une procédure uniquement déclarative. Ainsi un service ne sera pas résilient pas plus qu'un serveur ne sera sécurisé uniquement parce que cela a été affirmé, exigé ou même juré.
Les conditions contractuelles rentrent justement dans ce cas de figure : un système d'information peut tout à fait abdiquer son système informatique et le confier à un tiers. Cela est doit bien évidemment être encadré par un accord précisant quel est le service à rendre et quantifiant de manière précise quel est le niveau minimum demandé. De tels accords seront, de manière inévitable, amputés des circonstances extraordinaires auxquelles en partie la résilience ambitionne à faire face. Pour le restant, ils ont bien évidemment force juridique en cas de manquement des parties, permettent à la direction de pouvoir se délester de responsabilités et l'arment du puissant recours du blâme : celle-ci est une posture très avantageuse en termes hiérarchiques, tout autant qu'elle est improductive [Zwieback, 2015]. Mais, du point de vue qui nous retient dans notre recherche, ces contrats ne construisent pas un système résilient,

tout au plus ils le postulent chez le tiers avec lequel le contrat est passé. Et en parallèle, ils changent le périmètre de résilience qui reste à construire dans son propre système d'information, tout en rendant ce travail plus difficile, car de tels accords amoindrissent la visibilité du système, tout en réduisant les outils et les recours disponibles.

Solutions à des problèmes

Nous avons pu voir comment la résilience se décline en trois moments, définis par rapport au moment où celle-ci intervient pour contrer le facteur de dégradation du système.
Pour ce qui est du niveau microscopique d'intégration d'outils et ressources de résilience, il ne doit pas surprendre de constater comment ceux-ci constituent essentiellement des ressources de préparation ou bien de confrontation.
À ce niveau, en effet, les outils disponibles vont pourvoir la solution à une erreur au même endroit où celle-ci se manifeste ou bien la prévenir là où elle pourrait se produire.

On a pu rappeler comment la place du système d'information dans une organisation est étroitement liée, tant en termes de développement historique qu'au niveau de son bon fonctionnement, à celle de son système informatique. Il n'est donc pas étonnant que nombre des outils de la résilience de celui-ci soient ceux du système informatique ou bien en soient dérivés.

Il s'agit, dans ce cas, de solutions qui ont été mises au point et éprouvées dans une approche à haute valeur intellectuelle ; celle-ci a servi à exemplifier et augmenter la prise de conscience de formulations qui reposent sur des principes de logique générale, mais qui est également très pratique.
Racontée sous la forme de récit, [Blanc, Noor, 2012], l'épopée longue et composite de la création d'Internet [Abbate, 2000] est constituée d'avancées majeures dans la conception d'une structure résiliente [Davies, Barber, 1973], [Davies *et alii*, 1979], infiniment plus aboutie en cela que la constitution du Web, le *cousin populaire* d'Internet.

Parmi les précieuses théorisations accomplies dans ce parcours, prime probablement la mise en garde contre les *Single Point of Failure*, les éléments qui, en cas d'échec, entraînent nécessairement avec eux tout leur système. Le système de la commutation de paquets est riche en remèdes à ce danger.
Première ressource contre ces points bloquants est la redondance : la fonction n'est plus confiée à un élément unique mais partagée entre deux équivalents, l'un étant prêt à assurer la continuité de fonctionnement du système en cas de défaillance de l'autre. Un principe amené également à être décliné sur le plan géographique, en évitant de réunir sur une superficie trop homogène des éléments critiques.
Associées à cette solution, plusieurs s'en ajoutent afin de fournir plus de garanties, telle l'atomisation (également un principe algorithmique dans le cas des traitements effectués par les programmes [Léry, 2013]). Celle-ci permet, dans le cadre de la transmission de l'information via les paquets, de vérifier de manière continue leur bon transit et de remédier à moindre coût à leur égarement.

Bien évidemment connues, ces démarches sont à mettre en regard avec leurs traductions plus récentes au niveau de la gestion des équipes.
L'approche agile est, en effet, attentive aux risques évoqués et a pour cela mis

au point plusieurs procédures. Le risque de disparition d'une personne clé d'une équipe, appellé *Bus Factor*, en évoquant le scénario d'un accident de la route, est une préoccupation prise en compte et que l'on contre, par exemple, par le recours à l'écriture du code par binômes (une approche encouragée dans le cadre *Scrum* et imposée dans celui, plus normatif, de l'*extreme programming* [Coplien, Harrison, 2004]).

Dans la volonté d'atomiser la taille des éléments manipulés (information réduite en paquets ou calculs confiés à des procédures), on peut reconnaître une inspiration utile à la volonté de travailler de manière itérative dans le cadre des approches agiles, chaque approche permettant d'aiguiller et, si besoin, corriger, la trajectoire du travail en cours.

Enfin, d'autres principes président à la mise en place d'un système informatique résilient, tel le recours à des outils de contrôle et correction de l'erreur dans la gestion des données sous le point de vue de leur exactitude formelle, tels les contrôleurs intégrés, à bas niveau, dans l'écriture sur disque [Brewer *et alii*, 2016]. Cette ressource également renvoie à celle employée dans le contexte plus large des équipes du système d'information, c'est-à-dire l'audit, le contrôle des opérations du système et leur alignement avec les buts et missions de celui-ci.
Pour finir, une solution, envisagée déjà depuis de nombreuses années dans les ordinateurs, la compartimentation des application via ce que l'on appelle des *containers* est en constante affirmation et représente à son tour une solution appropriée à la question [Fritsch, 2016]. De manière assez intéressante, nous avons ici un élément de différence entre l'administration du système informatique et le plus large système d'information, dans lequel une attitude analogue avec les personnes est déconseillée et contraire au but recherché de construire de la résilience d'anticipation (voir *infra*).

La résilience à l'échelle macroscopique

On serait tenté de croire, à l'intérieur d'un cadre quelque peu empreint de pensée mécaniste, que la résilience d'anticipation serait capable, à condition de prendre en considération le bon périmètre des phénomènes, de contrer toute erreur, tout dérangement du système.

Faire appel à la vision géographique de la résilience [Dauphiné, Provitolo, 2007] peut aider à contrer et à échapper à ce cadre trompeur. Tout d'abord, elle oblige à se confronter au fait que, telle la crue d'un fleuve bien qu'imaginable et prévisible, le facteur de dérangement ne peut pas être toujours évité, conjuré [Dauphiné, Provitolo, 2007].
Dans un tel cas, nous sommes amenés à saisir la nécessité d'une approche macroscopique, dans laquelle l'erreur qui se manifeste ne peut pas être arrêtée dès sa manifestation, au niveau microscopique, mais sa contention est le fait de l'interaction entre les différentes parties du système.
C'est d'ailleurs cet aspect – la nécessité de prendre en compte le système dans lequel la résilience se manifeste, un système dont les facteurs ont d'ailleurs des effets bidirectionnels – que des chercheurs opposent à plusieurs définitions du phénomène trop pauvres à leurs yeux [Shaikh, Kauppi, 2010]:

> The degree of resilience displayed by a person in a given context is dependent upon the extent to which that context contains elements to nurture resilience. If an individual does not adapt to adverse circumstances, the reason might be that the environment lacks the resilience to negotiate with the individual and to provide what is needed. In such a case, an individual's environment lacks resilience and not the individual per se. Hence it can be said that resilient individuals require resilient families and resilient communities. However, this relationship between individual resilience and the resilience of the families and communities is not unidirectional.
> [...]
> Resiliency cannot be researched by merely focusing on these individual-level factors. Instead careful attention must be paid to the structural deficiencies (e.g., social and economic policies) that might need to be changed in order for individuals, families and communities to become stronger, more competent and better functioning in the adverse situations.

Ce niveau macroscopique peut se constituer d'une systématisation des éléments préparés au niveau microscopique. Tel est par exemple le cas des machines à tolérance de panne : de telles machines font appel aux ressources évoquées précédemment, mises en système, mais aussi à la possibilité, une fois que celles-ci ont relevé un dysfonctionnement, à la possibilité d'altérer le fonctionnement normal, afin de réduire la charge et ainsi ne pas être contraintes à l'arrêt (on reconnaîtra ici à l'œuvre la *résilience de survie* telle que définie dans le domaine

de la sociologie).
La mise en système de ressources de type élémentaire est aussi ce qui donne lieu au PRA, plan de reprise des activités, ainsi que du PCA, plan de continuité des activités [Benassar, 2010]. Ce dernier, encadré par la norme ISO 22301, a pour objectif de permettre de poursuivre l'activité du système informatique sans interruption du service et d'assurer la disponibilité des informations quels que soient les problèmes rencontrés. Le PRA, par contre, décrit les mesures qui doivent être déclenchées à la survenue d'un sinistre ou incident majeur ayant entraîné une interruption de l'activité.

La résilience au niveau systématique peut cependant être aussi autre chose que la réplication à grande échelle des solutions élémentaires, car le recours aux mêmes outils à une échelle différente fait preuve d'une efficacité marginale moindre. En effet, cette logique fractale produit une multiplication des contrôles qui pèse sur la performance du système [DALZIELL, MCMANUS, 2004] ; et celle-ci est d'ailleurs la raison pour laquelle la méthode Six Sigma s'attache à identifier et supprimer ces dédoublements [Tennant, 2001]. Ainsi, observe-t-on désormais une approche différente dans les recherches les plus en pointe.
Exemple de celles-ci, le travail mené par les équipes de Google, sur les disques pour les *datacenters* [Brewer *et alii*, 2016] : parmi les autres souhaits exprimés par l'entreprise figure en effet celui de voir les producteurs de disques durs fournir des produits qui n'intégreraient pas des outils de bas niveau de contrôle des écritures sur disque. Cette suppression va ainsi permettre d'atteindre une plus grande densité des secteurs de mémoire et des temps de latence moindres. D'autre part, la fonction de vérification peut être confiée à un niveau supérieur du système, capable d'effectuer des tests plus complexes et ayant donc un plus grand nombre de niveaux d'efficacité. Dans le cas spécifique, c'est le *file system* qui peut prendre en charge de manière plus efficiente cette tâche, et la qualité accrue du contrôle qu'il peut ainsi effectuer peut être étudiée dans le cas de ZFS, le plus récent parmi les *files systems* parvenant à maturité.
Parmi les nombreuses capacités dont il jouit, celui-ci dispose de la possibilité de contrôler trois (voire plus si besoin) copies des mêmes données. Cela permet au système non seulement de vérifier, comme les systèmes en RAID quand celles-ci ne sont plus alignées – ce qui est l'indice d'une erreur – mais aussi de corriger cette erreur. En effectuant une comparaison non simplement entre deux sources, dont on ne saurait pas identifier celle en erreur, mais entre au moins trois, le système parvient de manière probabiliste à désigner quelle est la copie des données qui s'est éloignée de l'état d'origine [Kadav, Rajimwale].

Exemple illustre de résilience dans leur conception, les réseaux peuvent eux aussi se prévaloir d'outils de résilience intégrés au niveau macroscopique. Dans ce cas également, le niveau supérieur du système prend en charge le contrôle et la vérification de celui-ci, comme illustré dans le projet *ResumeNet*:

> a number of resilience principles are defined, including a resilience strategy, called D2R2 + DR: Defend, Detect, Remediate, Recover, and Diagnose and Refine. […] At its core is a control loop compris-

> ing a number of conceptual components that realize the real-time aspect of the D2R2 + DR strategy, and consequently implement network resilience. Based on the resilience control loop, other necessary elements of our framework are derived, namely resilience metrics, understanding challenges and risks, a distributed information store, and policy-based management.

Comme nous pouvons le relever, le point charnière de ce niveau macroscopique de la résilience est la capacité du système d'examiner son propre fonctionnement: en raison de celui-ci, il pourra activer des parcours d'activités différents, selon le contexte. Ces parcours peuvent être ceux prédéterminés lors de la mise en place du système, mais aussi des nouveaux, organisés *ex novo* lorsqu'ils apparaissent comme nécessaires, par le système lui-même, dans le cadre des systèmes capables d'auto réparation [Keromytis, 2006].
Ce bond, du constat d'état à l'identification de la solution, est rendu possible grâce à la technologie du raisonnement causal, mise au point déjà en 1976 au MIT, technologie qui permet au système d'émettre un diagnostic [Chaudhry, 2014].
Sur la base des cas que le système répertorie, éléments de départ, il organise ensuite de manière dynamique une réponse dont il gouverne lui-même la mise en place, sous un régime de test constant. Ce champ de recherche très avancé produit ainsi les systèmes autonomes envisagés par Turing, dont la complexité serait exponentielle [Chaudhry, 2014].

Stigmergie

La stigmergie représente un nouvel outil intellectuel, né en contraste avec l'approche holistique des communautés, aujourd'hui encore soutenue par le professeur Dario Fontecedro. Ce concept permet de comprendre les mécanismes qui président à l'émergence, la régulation et le contrôle des activités collectives dans les insectes sociaux [Theraulaz, Bonabeau, 1999] :

> Stigmergy (from the Greek stigma: sting and ergon: work) was initially introduced to explain indirect task coordination and regulation in the context of nest reconstruction in termites of the genus Bellicositermes. Grassé showed that the coordination and regulation of building activities do not depend on the workers themselves but are mainly achieved by the nest structure. [...] Stigmergy offers an elegant and stimulating framework to understand the coordination and regulation of collective activities.

Dans ce cadre, les organisations sont caractérisées par une stricte égalité parmi les membres qui agissent de manière absolument autonome, et pourtant parfaitement coordonnée. Le travail réalisé désigne les tâches qui restent à accomplir et les différents individus de la communauté, égaux et interchangeables entre eux, s'en chargent de manière progressive.

La synthèse offerte est assez intéressante et habile pour être relatée en entier [Theraulaz, Bonabeau, 1999]:

> One of the best examples of quantitative stigmergy is the construction of pillars in termites, studied by Grassé. Workers use soil pellets impregnated with pheromone to build pillars. Two successive phases take place. First, the noncoordinated phase is characterized by a random deposition of pellets. This phase lasts until one of the deposits reaches a critical size. Then, the coordination phase starts if the group of builders is sufficiently large: Pillars or strips emerge. The existence of an initial deposit of soil pellets stimulates workers to accumulate more material through a positive feedback mechanism, since the accumulation of material reinforces the attractiveness of deposits through the diffusing pheromone emitted by the pellets. This autocatalytic, snowball effect leads to the coordinated phase. If the density of builders is too small, the pheromone disappears between two successive passages by the workers, and the amplification mechanism cannot work, which leads to a noncoordinated phase. The system undergoes a bifurcation at this critical density: No pillar emerges below it, but pillars can emerge above it.
> This example illustrates three important properties or signatures of the self-organized dynamics associated with quantitative stigmergy: (a) the emergence of spatiotemporal structures in an initially homogeneous medium, that is, a random spatial distribution of soil pellets. The basic mechanism that leads to the emergence of these

> structures is positive feedback (the snowball effect); once the structures are created, they are stabilized through negative feedback, mainly pheromone decay and competition among neighboring pillars. (b) the possible coexistence of several stable states (multistability): Structures emerge by amplification of random deviations, and any such deviation can be amplified, so that the system converges to one among several possible stable states, depending on initial conditions (path dependency). (c) the existence of (parameter-driven) bifurcations, where the behavior of a self-organized system changes dramatically.

Dans ce cadre de mode opératoire, capable de répondre rapidement au changement de contexte et de se réorganiser de manière autonome, il est ensuite possible d'individuer deux types de stigmergie, l'une quantitative, l'autre qualitative (voir [Theraulaz, Bonabeau, 1999]).

Le champ d'application, comme le soulignent les éthologues, est tout simplement immense.

Application aux humains avec la mise au centre du produit de leur travail et sa visibilité selon les paramètres d'adaptation soulignés par [Susi,] et les principes dérivés de la loi de Conway explicités dans [Kwan *et alii*, 2012].

Il est en tout cas frappant de remarquer que, dans une certaine mesure, nous avons atteint un niveau de spécialisation et séparation des tâches qui est largement supérieur à celui décrit pour les communautés concernées et que, donc, nous sommes allés plus loin dans la spécialisation que les insectes eux-mêmes.
Un danger pointé par Robert Heinlein, intellect éminemment scientifique, et capable d'anticiper ce paradoxe avec la sensibilité des gens de lettres [Heinlein 1973]:

> A human being should be able to change a diaper, plan an invasion, butcher a hog, conn a ship, design a building, write a sonnet, balance accounts, build a wall, set a bone, comfort the dying, take orders, give orders, cooperate, act alone, solve equations, analyze a new problem, pitch manure, program a computer, cook a tasty meal, fight efficiently, die gallantly. Specialization is for insects.

Stigmergie *versus* hierarchie

Dans le contexte hautement efficace de la stigmergie, il n'y a pas de structure hiérarchique ou de subdivision du travail, mais une capacité de répondre partagée face à des stimuli communs.
La réduction de l'emprise de la structure hiérarchique est par ailleurs un thème évoqué dans plusieurs contextes, aussi bien ceux qui sont tout à fait attendus sur ce sujet. Il est par exemple assez attendu de la part du fondateur du Parti Pirate [FALKVINGE 2013], qui loue la résilience d'une organisation de telle

sorte, mais il est par contre plus que surprenant qu'un professeur de la London School of Economics invite les lecteurs de la Harvard Business Review à licencier tous les managers [HAMEL 2011].Et cela, dans ce qui n'est pas une provocation improvisée, mais une étape d'une réflexion qui se poursuit dans les années ([HAMEL 2012]).

Il s'agit d'une question d'efficacité et poids organisationnels [HAMEL 2011] :

> A small organization may have one manager and 10 employees; one with 100,000 employees and the same 1:10 span of control will have 11,111 managers. That's because an additional 1,111 managers will be needed to manage the managers.

Mais, au-delà de ce versant, d'autres arguments explorés montrent comme une organisation hiérarchique est fondamentalement anti résiliente:

> Second, the typical management hierarchy increases the risk of large, calamitous decisions. As decisions get bigger, the ranks of those able to challenge the decision maker get smaller.
> [...]
> Third, a multitiered management structure means more approval layers and slower responses. In their eagerness to exercise authority, managers often impede, rather than expedite, decision making.

Ces capacités de renverser radicalement, et de manière brutale, les processus et d'imposer une chaîne de réponses nécessaire tout autant que lente, met à mal la capacité d'une organisation de pouvoir à mettre en œuvre des réponses.
En outre, la nécessité de casser la hiérarchie pour laisser plus de liberté aux acteurs subordonnés est également soulignée dans le contexte des recherches sur la résilience en géographie [Le Blanc, Nicolas, 2013].

Dans les perspectives des avantages et des risques évoquées, comment peuvent se manifester de telles ressources de stigmergie et de prévention des risques d'une organisation rigidement encadrée par les rôles hiérarchiques à l'intérieur du système d'information?

À nouveau, ce sont des éléments de l'approche agile à faire cette transition.
En particulier, dans le cas de l'approche *Scrum*. En plus des aspects déjà évoqués qui vont dans le sens de la création de redondance des ressources humaines, il est utile de souligner l'utilité du recours au Kanban et de la technique du *planning poker* [Coplien, Harrison, 2004].
Le Kanban est un tableau, physique ou bien logiciel, sur lequel sont représentés les tâches accomplies et à accomplir. Introduit dans le système de management de Toyota au cours du siècle dernier, Kanban est, dans sa déclinaison pour le SI, un outil qui permet de matérialiser le travail accompli, ainsi que son degré de progression. Cette technique permet de partager un état des lieux de l'avancement du travail constamment mis à jour à l'intérieur de l'équipe de travail.

Ressource de l'élucidation des exigences, le *planning poker* est une méthode

d'estimation des charges qui, dans le contexte d'une approche agile, devient aussi un outil au service de la stigmergie de l'équipe. En effet, un point de friction dans l'adaptation de ce processus entomologique au contexte des équipes humaines est l'égalité entre les individus, qui est possible à l'échelle des insectes, mais indéniablement absente dans son parallèle.
Face à une pluralité d'estimations, tout choix est sujet à un biais qui risque d'être déterminé par le penchant inconscient de l'arbitre de la question. Dans cet exercice, par contre, le but déclaré est celui de parvenir à une valeur qui soit le reflet des estimations et compétences de la plus grande partie de l'équipe impliquée. Il est ainsi possible d'avancer vers un diagnostic qui effectue un nivellement faisant abstraction des membres hors-norme, et pose ainsi les conditions préalables de l'égalité des différents membres de l'équipe face aux tâches à accomplir.

Mesurer la résilience

Les test d'Augustin-Charles-Marie Mesnager et de Georges Charpy, maintenait codifiés dans des standard (ASTM E23, EN ISO 179-1 et -2, ISO 148-1, -2 et -3) permettent de connaître la résilience des métaux par le biais des simples et rassurantes grandeurs scalaires.

Plus complexe à apprécier, la volonté de mesurer de la même manière la résilience des systèmes donne lieu à un éventail de propositions presque aussi vaste que les possibles définitions du phénomène de résilience lui-même[Wolter *et alii*, 2012].
Ainsi on peu choisir d'évaluer la résilience sur la base de la rédondance et de la fiabilité (comme temps de service entre les pannes) des équipements; à travers un algorithme évolutif qui prenne en compte les nombre de systèmes qui ne seraient pas susceptibles à une panne en cascade, ou encore [Wang, 2010]

> We use the maximum recovery ability to measure the resilience of an enterprise information system. We consider a scenario that an enterprise information system is partially damaged. There are m functions in the system and n categories of resources to recover the functions. The number of resources j (j ¼ 1, 2, . . . , n) needed for the recovery of function i (i ¼ 1, 2, . . . , m) is denoted by r_{ij}. The amount of resources for each category is limited. The process time needed for the recovery of function i is p_i. We assume that functions are not recovered at the same time. This assumption implies that the recovery may take a particular order among a set of recovery tasks. For function i, there is a completion time, denoted by c_i. It is noted that the completion time c i is different from the process time p_i in that the completion is the sum of the starting time for function i and its process time.

Ces approches sont cependant marquées par une forte empreinte mécaniste, et de manière non surpenante limitent leur champ d'analyse au système informa-

tique.
Proche de la gestion de risque, la résilience nécessite également d'une partie d'évaluation subjective afin d'apprécier, par exemple, les paliers de services à viser dans le cadre d'un fonctionnement réduit. Il est important donc de prendre en compte la nécessité de pondérer de telles mesures en fonction des buts et missions du système d'information spécifique qui effectue cette évaluation. Ceux-ci sont en effet nécessairement fonction du contexte de l'organisation dans laquelle le système d'information est intégré.

Même avec cette mise en garde, il est cependant à relever comment ces approches oublient que le concept de résilience est aussi le produit d'une réflexion des sciences humaines. On peut donc choisir de faire appel à la résilience géographique, qui mesure la présence dans un système de centres d'attraction gravitationnels capables de canaliser les phénomènes sortant des parcours prévus.
Enrchissante, cette approche ne permet cependant pas de prendre en compte que le système d'information a justement une composante humaine.
Or le facteur humain dans un système est souvent vu comme pourvoyeur de désordre, cause d'erreur en raison de la trop large variabilité potentielle de son comportement: lorsque l'on constate des accidents, on peut souvent remonter à une erreur humaine. La recherche sur la sécurité a cependant pu relevere que lorsque l'on s'attache également à *ce qui n'arrive pas*, aux accidents évités, l'humain a là aussi une place importante [Hollnagel, Woods, Leveson, 2006]:

> When researchers in the early 1980s began to re-examine human error and collect data on how complex systems had failed, it soon became apparent that people actually provided a positive contribution to safety through their ability to adapt to changes, gaps in system design, and unplanned for situations.

Capable d'adaptabilité face à l'inattendu, l'humain représente un facteur de résilience à l'intérieur d'un système que les mesures jusqu'ici proposées manquent de prendre en compte, ce qui d'ailleurs est peut-être impossible de faire. Car en effet s'il était possible de prévoir l'action humaine celle-ci serait calculable et donc remplacée, justement à cause, entre autre, de la vision de l'humain comme source d'erreurs.

Conclusion

> The construct of resilience has captured the imagination of researchers across various disciplines over the last five decades. [Shaikh, Kauppi, 2010]

Cette panoramique essaie de convoquer une pluralité d'horizons disciplinaires afin de montrer l'intérêt de cette approche.
Nous avons vu ensemble comment des éléments de celle-ci diffusent dans le système d'information, aussi bien via des méthodes qui ont fait leur preuves et sont désormais des piliers organisationnels incontournables, ainsi que par le biais de solutions bien plus récentes.
On pourrait par conséquent considérer que les concepts de résilience ainsi que celui, ici présenté comme subordonné, de stigmergie ne font que réunir un ensemble d'outils et pratiques déjà couramment adoptés, existants, conçus ou bien souhaités, bien que dans des domaines différents et distants. Cette remarque est sans doute vraie, tout en considérant que l'éventail des expériences de la résilience offre une palette d'outils encore plus variée, que le raisonnement analogique doit encore finir de saisir et de transposer.
Car, justement, le fait de les encadrer conceptuellement – dans leur buts communs, dans leurs modalités et leurs parentés – n'est pas anodin : c'est ainsi qu'on peut les connaître comme éléments non plus isolés, mais participant d'une même réalités, des facettes différentes du polyèdre qu'elles participent à construire. Tel Adam prenant possession de la création par le fait de nommer les espèces, nous transformons le constat de l'existant en un puissant outil épistémologique, nous renouvelons notre capacité gnoséologique, notre regard.

En concluant il est intéressant de souligner comment la résilience d'un système d'information constitue à la fois une des caractéristiques qui lui permettent de prendre une place de relief dans l'organisation à laquelle elle appartient ([Lucas 1984]) ; mais aussi comment la fréquente dynamique d'externalisation de services, qui touche actuellement bon nombre de systèmes d'informations, met en péril la possibilité de construire cette capacité.

Face à cette contradiction, à ce tiraillement, on pourrait enfin se poser la question de l'intérêt de la résilience : pourquoi la rechercher, la prévoir et la bâtir ?

L'idée qu'il soit important de concevoir des systèmes qui fonctionnent apparaît tellement de bon sens qu'il serait possible de mener toute une enquête à ce sujet, sans jamais la questionner et c'est d'ailleurs ce que nous risquions de faire.

La multiplicité des domaines dans lesquels ce thème a été étudié montre l'intérêt qu'il suscite et à quel point celui-ci est en adhérence avec une aspiration fondamentalement humaine. Caractérisé par une partie des éthologues comme l'animal qui forge, garde et améliore ses outils, l'humain trouve dans la résilience l'éclat de sa première étincelle, le parachèvement de la révolution néolithique :

non plus fabricateur, non plus concepteur d'outils, l'humain entrevoit dans ce cadre la possibilité de devenir le concepteur de l'outil ultime, capable de transformer tout autre instrument en l'instrument adéquat. La résilience, pierre philosophale de la conception intellectuelle.

S'il n'est pas né par les ordinateurs, en ceux-ci le système d'information trouve toutefois son parangon et relègue de plus en plus l'humain à un rôle ancillaire. En effet, on peut reconnaître qu'un système informatique résilient vise, tout de moins dans bon nombre d'approches, à rendre l'humain superflu. Complètement résilient, une fois programmé, et capable de se réparer de lui-même et d'augmenter ses capacités de réponse en fonction des évènements passés via une fonction d'apprentissage, celui-ci est parfaitement autonome. Dans une situation paradoxale, c'est uniquement l'incapacité des humains à réaliser un tel système qui les rends nécessaires et indispensables : leur utilité est une conséquence directe de leurs erreurs. Tandis qu'on essaie de les éliminer du système des machines, les failles des humains sont l'élément qui continue à garantir leur place.

Au-delà d'une curiosité intellectuelle, le paradoxe se révèle encore une fois une ressource de la pensée très profonde. Loin d'être un simple sophisme, celui-ci libère les nœuds ontologiques que les apparences ne peuvent pas saisir : si, poussés à programmer leur futilité, les humains se découvrent utiles simplement grâce à leurs erreurs, cette équation révèle l'inhumanité d'une telle ambition et dénonce, par conséquent, un danger. Dans le cadre d'une telle recherche – qui, si elle est en accord avec les aspirations humaines de complétude et d'amélioration, se révèle néanmoins être fondamentalement contraire aux principes de l'humain – le risque est alors, une fois de plus, que les conséquences soient bien plus profondes qu'on ne sait l'anticiper : les erreurs propres à l'homme rentrent encore une fois en jeux et, après avoir suscité la recherche de la résilience, invitent à l'approcher avec vigilance.

Cette critique a d'ailleurs déjà été formulée, à un moment où les outils informatiques étaient encore dans un état primitif. Dans un contexte intellectuel qui ne s'interdisait pas de critiquer la validité des choix pris par la hiérarchie et des réponses automatiques, *Fail Safe* est une histoire qui explore les conséquences d'une procédure conçue pour être résiliente – dans l'acception de l'exclusion des facteurs de dérangement externe – et pleinement automatisée. Celle-ci va, de ce fait, déclencher un carnage thermonucléaire.
Écrit par Eugene Burdick et Harvey Wheeler en 1962, ce roman a été, deux années plus tard, transposé au cinéma par Sidney Lumet. Reproposée au public par Stephen Frears en 2000, sous les aspects d'un vieux noir et blanc et l'inactuel contexte de la guerre froide, l'histoire cache le thème fondamental de la possibilité de débrancher les machines et arrêter les processus.

À l'heure de la surveillance planétaire, de la gouvernance algorithmique, des réseaux neuronaux profonds, des assassinats confiés aux drones, des failles informatiques qui ciblent les centres de recherche nucléaire, la mise en place de systèmes résilients impose une nouvelle approche. Les femmes et les hommes

impliqués dans de tels projets se doivent d'en évaluer la retombée éthique, de prendre en compte la possibilité de faire objection de conscience et ne pas les mettre en œuvre. Il est désormais impératif de relever un autre défi et de considérer que la mise en place de systèmes capables de contourner l'erreur et d'assurer un fonctionnement virtuellement pérenne peut être une faute.

Bibliographie

[Abbate, 2000] Jane Abbate, *Inventing the Internet*, MIT Press, 2000.

[Aïn, 2007] Joyce Aïn, *Résiliences : Réparation, élaboration ou création*, Erès, 2007.

[Benassar, 2010] Matthieu Benassar, *Plan de continuité des activités et système d'information: vers l'entreprise résiliente*, Dunod, 2010.

[Berleur, David Hercheui, Hilty, 2010] Jaques Berleur,Magda David Hercheui, Lorenz M. Hilty, *What Kind of Information Society. Governance, Virtuality, Surveillance, Sustainability, Resilience*, Springer, 2010.

[Blanc, Noor, 2012] Sabine Blanc, Ophélia Noor, *Hackers : Bâtisseurs depuis 1959*, OWNI, 2012.

[Boin, McConnel, 2007] Arjen Boin, Allan McConnell, Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience, *Journal of Contingencies and Crisis Management*, 15(1) :51-59, 2007.

[Branscomb, Gazis, 1977] Lewis M. Branscomb, Denos C. Gazis, Resilience, Hypotheticality and Computers-Designing Social Systems under Uncertainty, *Proceedings of the American Philosophical Society*, 121(5) :346-349, 1977.

[Brewer *et alii*, 2016] Eric Brewer *et alii*, *Disks for Data Centers White paper for FAST 2016*, h ttp://research.google.com/pubs/pub44830.html, 2016.

[Bucharles, 2008] Charles Bucharles, Les "Notes" de Oxford de Herbert G. Thomson, *Bulletin du DTHA*, 27 :4-8, 2008. [Butler, Gray, 2006] Brian S. Butler, Peter H. Gray, Reliability, Mindfulness, and Information Systems, *MIS Quarterly*, 30(2) :211-224, 2006.

[Camarinha-Matos, Bénaben, Picard, 2015] Luis M. Camarinha-Matos, Frédérick Bénaben, Willy Picard, *Risks and Resilience of Collaborative Networks*, Springer, 2015.

[Caragiannis *et alii*, 2013] Ioannis Caragiannis *et alii*, *Euro-Par 2012: Parallel Processing Workshops*, Springer, 2013.

[Cataldo, Hersleb, 2013] Marcelo Cataldo, James D. Herbsleb, Coordination Breakdowns and Their Impact on Development Productivity and Software Failures, *IEEE Transactions on Software Engineering*, 39(3) : 343-360, 2013.

[Gazeneuve, 2016] Paris Normandie, *Bernard Gazeneuve : « Les Français font preuve de résilience et de fraternité* https://web.archive.org/web/20160803181600/http://www.paris-normandie.fr/region/bernard-cazeneuve–les-francais-font-preuve-de-resilience-et-de-fraternite-XK6480505.

[Chaudhry, 2014] Junaid Ahsenali Chaudhry, *Self-Healing Systems and Wireless Networks Management*, CRC Press, 2014.

[Christensen, 2013] Lars Rune Christensen, Stigmergy in human practice: Coordination in construction work, *Cognitive Systems Research*, 21 :40–51, 2013.

[Comfort *et alii*, 2001] Louise K. Comfort *et alii*, Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments, Journal of Contingencies and Crisis Management, 9(3) :144-158, 2001.

[Comfort, Boin, Demchak, 2010] Louise K. Comfort, Arjen Boin, Chris C.

Demchak, *Designing Resilience: Preparing for Extreme Events*, University of Pittsburgh Press, 2010.
[Coplien, Harrison, 2004] James Coplien, Neil Harrison, *Organizational patterns of agile software development*, Wiley, 2004.
[Cresti, 2014] Simona Cresti, *L'elasticità di resilienza*, http://www.accademiadellacrusca.it/it/lingua-italiana/consulenza-linguistica/domande-risposte/l-elasticit-resilienza.
[D'Atri, De Marco, Casalino, 2008] Alessandro D'Atri, Marco De Marco, Nunzio Casalino, *Interdisciplinary Aspects of Information Systems Studies*, Physica-Verlag, 2008.
[Dauphiné, Provitolo, 2007] André Dauphiné, Damienne Provitolo, La résilience : un concept pour la gestion des risques / Resilience: a concept for risk management, *Annales de Géographie*, 116(654) :115-125, 2007.
[Davies *et alii*, 1979] Donald W. Davies *et alii*, *Computer networks and their protocols, Computing and Information Processing*, John Wiley & Sons, 1979.
[Davies, Barber, 1973] Donald W. Davies, Derek L. A. Barber, *Communication networks for computers*, John Wiley, 1973.
[El Sawy, Nanus, 1989] Omar A. El Sawy, Burt Nanus, Toward the Design of Robust Information Systems, *Journal of Management Information Systems*, 5(4) :33-54, 1989.
[Falkvinge, 2013] Rick Falkvinge, *Swarmwise, The Tactical Manual to Changing the World*, CreateSpace Publishing Platform, 2013.
[Fontecedro] Dario Fontecedro, https://www.youtube.com/watch?v=4r7C3P_4NoA.
[Fritsch, 2016] Joerg Fritsch, *How to Secure Docker Containers in Operation*, Gartner, 2016.
[Hamel, Breen, 2007] Gary Hamel, Bill Breen, *The Future of Management*, Harvard Business School Press, 2007.
[Hamel, 2011] Gary Hamel, First, Let's Fire All the Manages, *Harvard Business Review*, :2-13, December 2011.
[Hamel, 2012] Gary Hamel, *What Matters Now*, Jossey-Bass, 2012.
[Häring, 2015] Ivo Häring, *Risk Analysis and Management: Engineering Resilience*, Springer, 2015.
[Heinlein, 1973] Robert A. Heinlein, *Time Enough for Love*, G. P. Putnam's Sons, 1973.
[Hollnagel *et alii*, 2011] Erik Hollnagel *et alii*, *Resilience Engineering in Practice. A Guidebook*, Ashgate, 2011.
[Hollnagel, Woods, Leveson, 2006] Erik Hollnagel, David D. Woods, Nancy Leveson, *Resilience Engineering Concepts and Precepts*, Ahgate, 2006.
[Hyslop, 2007] Maitland Hyslop, *Critical Information Infrastructures. Resilience and Protection*, Springer, 2007.
[Kadav, Rajimwale] Asim Kadav, Abhishek Rajimwale, *Reliability Analysis of ZFS*, http://pages.cs.wisc.edu/~kadav/zfs/zfsrel.pdf.
[Keromytis, 2006] Angelos D. Keromytis, *Characterizing Self-Healing Software Systems*, Ashgate, 2006.
[Kwan *et alii*, 2012] Irwin Kwan *et alii*, Conway's Law Revisited: The Evidence For a Task-based Perspective, *IEEE Software*, 29(1), 2012.

[Konsynski, 1984/1985] Benn R. Konsynski, Advances in Information System Design, *Journal of Management Information Systems*, 1(3) :5-32, 1984/1985.
[Le Blanc, Nicolas, 2013] Antoine Le Blanc, Thierry Nicolas, « Politiques et pratiques de la résilience », *EchoGéo* [Online], 24, http://echogeo.revues.org/13451, 2013.
[Lequeux, Challande, 2009] Jean-Louis Lequeux, Jean-Francois Challande, *Le grand livre du DSI. Mettre en oeuvre la direction des systemes d'information 2.0*, Eyrolles, 2009.
[Léry, 2013] Jean-Michel Léry, *Algorithmique. Applications en C, C++ et Java*, Pearson, 2013.
[Lucas 1984] Henry C. Lucas, Jr., Organizational power and the information services department, 27(1) :58-65, 1984.
[Moisand, Garnier de Labareyre, 2009] Dominique Moisand, Fabrice Garnier de Labareyre, *CobiT pour une meilleure gouvernance des systèmes d'information*, Eyrolles, 2009.
[Morozov, 2014] Evgeny Morozov, *Our Naive "Innovation" Fetish*, https://web.archive.org/web/20160310094927/https://newrepublic.com/article/116939/innovation-fetish-naive-buzzword-unites-parties-avoids-policy-choice.
[Morozov, 2016] Evgeny Morozov, *Silicon Valley was going to disrupt capitalism. Now it's just enhancing it*, https://web.archive.org/web/20160825201017/https://www.theguardian.com/commentisfree/2016/aug/07/silicon-valley-health-finance.
[O'Reilly, 2016] Courtney Nash, *5 ways to make your operations more resilient in 2016*, https://www.oreilly.com/ideas/5-ways-to-make-your-operations-more-resilient-in-2016.
[Olshansky, 2011] Robert B. Olshansky, Designing Resilience: Preparing for Extreme Events, *Journal of Comparative Policy Analysis: Research and Practice*, 13(2) :233-235, 2011.
[Omer, Mostashari, Lindemann 2014] Mayada Omer, Ali Mostashari, Udo Lindemann, Resilience Analysis of Soft Infrastructure Systems, *Procedia Computer Science*, 28 :565-574, 2014.
[Payet, 2015] Linda Payet, *Cartographie du Syst'eme d'Information*, mémoire MIMO, 2015.
[Piccinini, 2010] Gualtiero Piccinini, The Resilience of Computationalism, *Philosophy of Science*, 77(5) :852-861, 2010.
[Rak, 2015] Jacek Rak, *Resilient Routing in Communication Networks*, Springer, 2015.
[Ridley, 2011] Gail Ridley, National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience, *Journal of Business Ethics*, 103(1) :111-125, 2011.
[Riolli, Savicki, 203] Laura Riolli, Victor Savicki, Information system organizational resilience, *Omega*, 31 :227-233, 2003.
[Rivard, Talbot, 2004], Suzanne Rivard, Jean Talbot, *Le développement de systèmes d'information : une méthode intégrée à la transformation des processus*, Presses de l'Université de Québec, 2004.
[RP] *The Resilience Project*, http://resilienceproject.com/.
[Shaikh, Kauppi, 2010] Arshi Shaikh, Carol Kauppi, Deconstructing Resilience:

Myriad Conceptualizations and Interpretations, *International Journal of Arts and Sciences*, 3(15) :155-176, 2010.
[Silver, Markus, Beath, 1995] Marc S. Silver, M. Lynne Markus, Cynthia Mathis Beath, The Information Technology Interactive Model: A Foundation for the MBA Core Course, *MIS Quarterly*, 19(3) :361–390, 1995.
[Smith *et alii*, 2011] Paul Smith *et alii*, Network Resilience: A Systematic Approach, *IEEE Communications Magazine*, :99-97, July 2011.
[Smith *et alii*, 2014] Michael W. Smith *et alii*, Resilient Practices in Maintaining Safety of Health Information Technologies, *Journal of Cognitive Engineering and Decision Making*, 8(3) :265-282, 2014.
[Susi, Ziemke, 2001] Tarja Susi, Tom Ziemke, Social cognition, artefacts, and stigmergy: A comparative analysis of theoretical frameworks for the understanding of artefact-mediated collaborative activity, *Journal of Cognitive Systems Research*, 2 :273-290, 2001.
[Tennant, 2001] Geoff Tennant, *SIX SIGMA: SPC and TQM in Manufacturing and Services*, Gower Publishing, 2001.
[Teoh, Yeoh, Zadeh, 2015] Say Yen Teoh, William Yeoh, Hossein Seif Zadeh, Towards a resilience management framework for complex enterprise systems upgrade implementation, *Enterprise Information Systems*, :1-25, Septemeber 2015.
[Theraulaz, Bonabeau, 1999] Guy Theraulaz, Eric Bonabeau, A Brief History of Stigmergy, *Artificial Life*, 5 :97–116, 1999.
[Tisseron, 2009] Serge Tisseron, *La résilience. Que sais-je?*, Presses Universitaires de France, 2009.
[TLFi] *Trésor de la langue française informatisé*, http://atilf.atilf.fr/dendien/scripts/tlfiv4/showps.exe?p=combi.htm;java=no;.
[TPB] *The Pirate Bay*, https://web.archive.org/web/20160125114847/https://thepiratebay.se/.
[Wang , Gao, Ip, 2010] J. W. Wang , F. Gao, W. H. Ip, Measurement of resilience and its application to enterprise information systems, *Enterprise Information Systems*, 4(2) :215-223, 2010.
[Weyns, Van Dyke Parunak, Michel, 2007] Danny Weyns, H. Van Dyke Parunak, Fabien Michel, *Environments for Multi-Agent Systems II*, Springer, 2006.
[Weyns, Van Dyke Parunak, Michel, 2007] Danny Weyns, H. Van Dyke Parunak, Fabien Michel, *Environments for Multi-Agent Systems III*, Springer, 2007.
[Wolter *et alii*, 2012] Katinka Wolter *et alii*, *Resilience Assessment and Evaluation of Computing Systems*, Springer, 2012.
[Zhang, Watts, 2004] Wei Zhang, Stéphanie Watts, Knowledge Adoption in Online Communities of Practice, *Systèmes d'Information et Management*, 9(1) :81-103, 2004.
[Zwieback, 2015] Dave Zwieback, *Beyond Blame, Learning From Failure and Success*, O'Reilly, 2015.