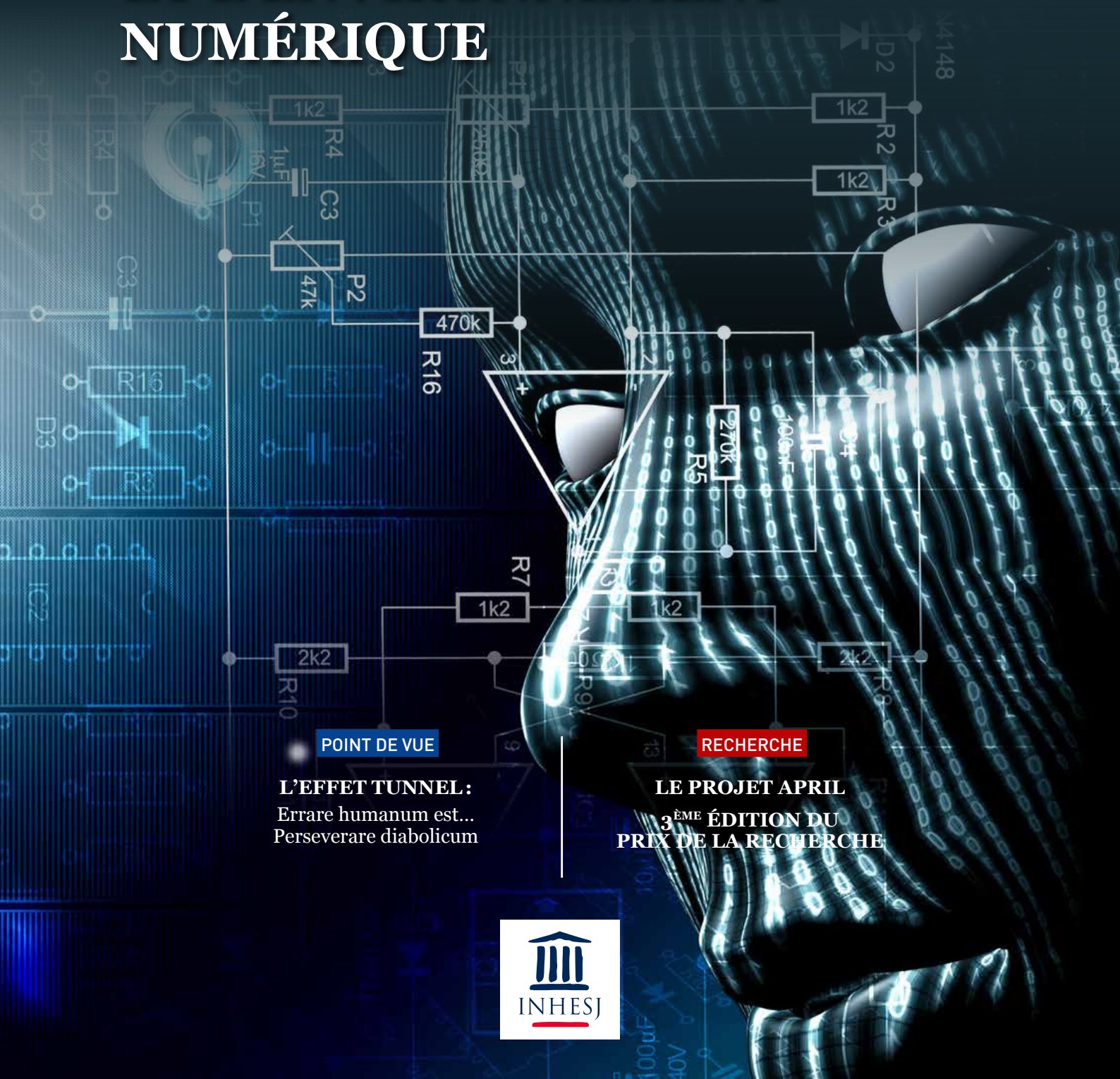
LIREC

Lettre d'information sur les Risques et les Crises

N°59 - MAI 2019

DOSSIER THÉMATIQUE

LES RISQUES ET L'ENVIRONNEMENT NUMÉRIQUE



POINT DE VUE

L'EFFET TUNNEL :

Errare humanum est...
Perseverare diabolicum

RECHERCHE

LE PROJET APRIL

3ÈME ÉDITION DU PRIX DE LA RECHERCHE

INHESJ

LIREC

n°59 MAI 2019

INHESJ

INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

DÉPARTEMENT RISQUES ET CRISES

Le département Risques et Crises de l'Institut national des hautes études de la sécurité et de la justice publie depuis 10 ans la Lettre d'information sur les Risques et Crises – LIREC

Directrice de la publication :
Hélène CAZAUX-CHARLES

Directeur de la rédaction :
Axel SIRVEN

Rédactrice en chef :
Cheila DUARTE COLARDELLE

Pour vous abonner, envoyez-nous un courriel à : **lirec@inhesj.fr**

Vous pouvez nous envoyer des informations concernant un événement, une manifestation ou une proposition d'article à : **lirec@inhesj.com**

Suivez nous :

Les informations contenues dans ce document sont issues de sources ouvertes et ne sauraient être interprétées comme une position officielle ou officieuse de ses rédacteurs ou des services de l'Etat.

ISSN 2265 – 464X

LICENCE OUVERTE
OPEN LICENCE

Photo de couverture :
©carloscastilla - stock.adobe.com

ÉDITORIAL

HÉLÈNE CAZAUX-CHARLES

Magistrate - Directrice de l'Institut national des hautes études de la sécurité et de la justice

Le 59ème numéro de la Lettre d'Information sur les Risques et Crises est consacré à un thème d'actualité : « les risques et l'environnement numérique ».

Les trente dernières années ont été marquées par une profonde transformation de notre société en particulier sous l'impulsion des technologies de l'information et de la communication. En écho à la révolution industrielle du 19ème siècle, le terme de « révolution numérique » a été forgé pour décrire la mutation rapide et profonde de nos sociétés.

Cette révolution bouleverse notre rapport au temps, à l›espace et à l›autre. La complexité des systèmes à l'œuvre et la production de données en masse dont les flux échappent quasiment à tout contrôle posent alors la question des enjeux tant à l'échelle individuelle que collective. Ils percutent l'ensemble des parties prenantes et s'inscrivent quotidiennement au cœur de l'actualité du monde.

Le numérique est un sujet majeur de préoccupations des acteurs économiques, des services de l'Etat et de notre société en général. Il est à la fois vecteur de croissance, de performance et d'innovation mais également porteur de risques. Albert Einstein écrivait déjà : « *Il est hélas devenu évident aujourd'hui que notre technologie a dépassé notre humanité* ». A l'ère du tout numérique, de l'internet des objets et de l'intelligence artificielle, ce constat semble plus pertinent que jamais.

Depuis sa création, la LIREC a pour ambition d'apporter un éclairage pluridisciplinaire sur une approche globale des risques et des crises. Ce 59ème numéro cherche à identifier les risques majeurs et les réelles opportunités qui accompagnent la révolution numérique. Associant experts, leaders d'opinion, décideurs publics, universitaires et chercheurs, ce numéro est intégralement consacré à cette thématique dont chacun s'accorde à reconnaitre aujourd'hui qu'elle occupe une place centrale dans les questions internationales.

J'ai la conviction que nos efforts communs de formation et de recherche permettront de contribuer à la définition de nouvelles stratégies pour faire face aux défis qui nous attendent.

Bonne lecture !

4
BRÈVES

20
POINT DE VUE

• Focus facteurs humains : l'effet tunnel

24
RECHERCHE

• Projet APRIL

• 3ème édition du prix de la recherch

5
DOSSIER THÉMATIQUE
LES RISQUES ET L'ENVIRONNEMENT NUMÉRIQUE

• Cyber-résilience vs business resilience – Francois Tête et Luc Vrignaud

• Open Data, risques et crises – Pierre Chrzanowski

• Risques et nouvelles technologies du monde numérique – Olivier Velin

• Les défis du traitement judiciaire de la cybercriminalité – Jacques Martinon

• L'apport des serious games dans la gestion des risques – Patrick Ruestchmann

26
FORMATION

27
AGENDA

BRÈVES

EN CHIFFRES

Le profil des utilisateurs de l'Internet par âge dans les pays membres de l'OCDE

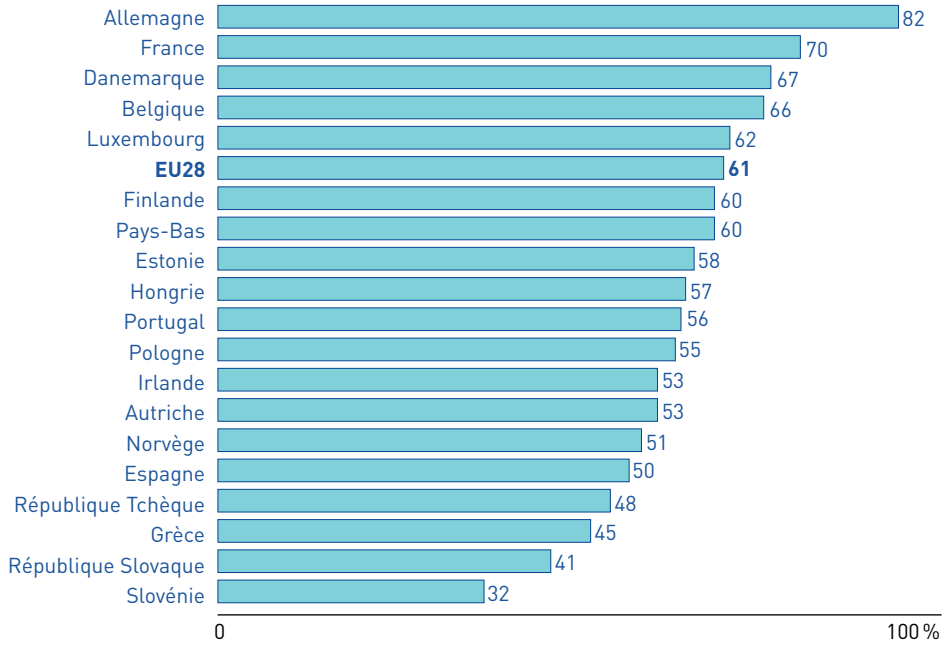
97%
parmi
LES 16-24 ANS

63%
parmi
LES 55-74 ANS

Source : Rapport Digital Economy Outlook 2017, Organisation de coopération et de développement économiques (OCDE)

Une majorité des gens se soucient de la confidentialité en ligne

Réaction d'inquiétude provoquée par la publicité ciblée en ligne (en pourcentage de la population/pays)



Source : Rapport Digital Economy Outlook 2017, Organisation de coopération et de développement économiques (OCDE)

DOSSIER THÉMATIQUE

LES RISQUES ET L'ENVIRONNEMENT NUMÉRIQUE

Cyber-resilience vs Business resilience

par François TÊTE et Luc VRIGNAUD

A PROPOS DES AUTEURS

François TÊTE

François TÊTE, ingénieur, est fondateur et président d'honneur du Club de la Continuité d'Activité (www.clubpca.eu). Il s'est spécialisé dans la continuité d'activité en 1977 à la suite d'un sinistre informatique important dans la banque d'affaires dans laquelle il travaillait comme directeur technique. Il a créé en 1989 un cabinet de conseil TTA spécialisé en qualité et continuité d'activité. Disposant d'une expérience de plus 30 ans dans le domaine de la reprise et continuité d'activité, il est considéré aujourd'hui comme l'un des pionniers de la continuité d'activité en France. Créateur de plusieurs logiciels informatiques de gestion des plans de continuité d'activité (RVR Parad), il intervient en tant qu'expert pour la société Devoteam et anime de nombreuses conférences. Il commet régulièrement en France des formations certifiantes Lead Implemetor et Lead Auditor en lien avec PECB.

Luc VRIGNAUD

Luc VRIGNAUD - Responsable Sécurité & Sûreté du Groupe Macif, 20ieme SNS IE INHESJ
25 ans au cœur des problématiques de sécurité dans diverses entreprises (Capgemini, General Electric, ...) avant d'intégrer le groupe Macif. Partisan d'une approche holistique et résiliente de la sécurité/sûreté impliquant toutes les strates de l'entreprise, il a connu plusieurs crises : cyber, média, et continuité d'activité qu'il partage avec enthousiasme et philosophie.

Cet article se décompose en deux parties. Tout d'abord, il invite le lecteur à réfléchir sur la cyber résilience. De quoi s'agit-il ? Quelles sont ses caractéristiques, ses différences avec les cas d'indisponibilité plus classique des technologies de l'information.
La deuxième partie propose une exploration des réponses possibles au travers de l'élaboration d'un « Plan de Cyber Résilience » intégré aux autres plans du Système de Management de la Continuité d'Activité.
La question n'est plus de savoir quand vous serez impacté, mais de savoir comment vous réagirez, face à trois risques majeurs :

1. *Vos données sont détruites ou corrompues*
2. *Vos activités s'arrêtent brutalement*
3. *Il n'est plus possible de communiquer*

Cet article a été réalisé par deux membres du Club de la Continuité d'Activité :
Luc VRIGNAUD, RSSI1 et RPCA2 du groupe MACIF
François TÊTE, consultant en continuité d'activité et gestion de crise DEVOTEAM

REFLEXIONS SUR LA CYBER-RESILIENCE

Pour certains, la cyber résilience n'est qu'un sous volet de la continuité de l'entreprise : mais si elle en partage de nombreux aspects, elle nécessite une attention particulière car au final ce risque numérique change le paradigme et notre relation à la crise.

Cet article souhaite vous interroger sur ce que vous tenez pour sûr, et qui peut s'avérer d'une toute autre nature nécessitant au final de revoir votre plan de gestion de crise autant que celui de la continuité d'activité de votre entreprise.

Le préfix cyber a envahi depuis une dizaine d'années le landerneau numérique mais force est de constater que c'est la démocratisation du smartphone qui l'a rendu si populaire qu'il nous interroge sur de nombreux plans :

1. sur un plan personnel, quant à l'intégrité de notre identité et a confidentialité de notre vie privée.

2. sur un plan professionnel, quant à la sécurité de notre identité et de notre vie privée (encore ;-) confiée au bon vouloir de l'entreprise ; et la capacité de protection de son RSSI (principalement lié à sa capacité à convaincre sa direction pour obtenir les budgets nécessaires ;-) mais aussi quand au modèle économique de chacune de nos entreprises (savoir, savoir-faire, ...) si celles-ci venaient à se faire attaquer.

Parmi les caractéristiques difficiles à appréhender d'une attaque cyber, on trouve :

✓ sa transcendance géographique : elle se situe hors des frontières informatiques que l'on perçoit, voire que l'on soupçonne ;

✓ son caractère épidémique : la contagion se fait par les proches ;

✓ son impunité relative : elle échappe (pour l'instant ?) à toute forme de protection juridique souveraine, nationale ou autre ;

✓ son caractère furtif : elle n'est parfois découverte que 6 mois après ses effets ;

✓ son caractère destructif : elle laisse parfois l'entreprise sans solution.

Force est de constater qu'elle n'est pas que centrée sur l'activité business, sec-

(1) RSSI : Responsable de la Sécurité des Systèmes d'Information

(2) RPCA : Responsable du Plan de Continuité d'Activité

torielle, mais elle déborde de façon systémique sur tout l'écosystème interdépendant de l'entreprise.

Mais alors que faire ? N'existe-t-il pas une solution de résilience au drame ?

La cyber résilience est souvent définie comme « la capacité attendue d'une entreprise (ou d'un individu) à identifier, prévenir, détecter et répondre aux défaillances technologiques ou de *process issues d'une attaque du cyber espace, et à se rétablir en réduisant au minimum les impacts négatifs pour ses clients, ses préjudices en matière de réputation et ses pertes financières.* »

Vous le savez : la sécurité d'un système d'information doit être multicouche et englober les personnes, les processus et la technologie. « La résilience cyber n'est donc rien sans cyber sécurité[1] » ni stratégie de continuité !

La cyber crise n'est elle pas une simple occurrence de crise d'indisponibilité de SI[2] ? Ou est-elle plus complexe, car plus diffuse ? Nécessite-t-elle de penser autrement : Réfléchir à un plan B, être agile à la crise, voire accepter de perdre une portion de SI au profit de l'ennemi pour protéger l'essentiel voire l'ultime (inacceptable ?)

A la différence du scénario d'indisponibilité SI habituellement traité dans les PCA[3], les crises cyber se distinguent par un niveau de sophistication et une surface d'attaque plus spécifiques. Elles sont plus difficiles à cerner et demandent nombre d'investigations qui ne sont parfois pas compatibles avec les exigences d'activité ou de reprise métiers :

Pour exemples :

✓ un SI fonctionnant peut faire l'objet d'une mesure conservatoire d'arrêt pour protection en cas de compromission partielle (fuite de données, *ransomware*, ...). Mais qui ira négocier avec le métier ? « *business is business* » ...

✓ la remontée des systèmes est aussi plus longue car il convient de s'assurer de l'intégrité exhaustive des services (Pour rappel : l'agent infectieux et/ou l'attaquant peuvent basculer en mode dormant rendant la reprise d'activité sensible).

✓ La cohérence des plaques applicatives et des données est un art compliqué qui est devenu plus complexe en mode distribué.

Il est donc indispensable de réviser ses plans de secours informatique pour être cyber-résilient.

L'élaboration d'un plan de cyber-résilience (PCR) complémentaire au PCA doit donc être demandée aux entités délivrant des services informatiques avec un objectif prioritaire de protection sur les actifs sensibles (critères DICP[4]) et stratégiques de l'entreprise.

Si on regarde l'écosystème des entreprises, l'envahissement des solutions sensibles au risque cyber a explosé depuis plusieurs années : le mode SaaS[5], les développements agiles, les véhicules autonomes, les objets connectés, les technologies disruptives avec leurs algorithmes complexes (blockchain,...), les smart-cities... Tous ces éléments nécessitent un niveau d'expertise dans leur découverte, leur compréhension et donc leur sécurisation en cas d'attaque.

« Le réseau internet n'existe plus : vous êtes internet ». La multitude de solutions d'accès à l'information oblige à repenser les modèles pour que chaque portion, chaque maillon de donnée porte sa propre sécurité.

Ne serait-ce pas cela qu'il faut revoir : prendre le problème à la fois par le tout et par chacune de ses parties élémentaires ?

Si nous revenons rapidement à l'origine écologique du terme, il est intéressant de se rappeler que dans la nature, la résilience[6] s'opère au travers de certaines constantes :

✓ la coopération, qui s'oppose à la compétition

✓ une dégradation de la performance car la priorité va à la redondance

✓ une notion de durée indissociable du moyen voire du long terme

L'histoire est jalonnée de ces partenariats improbables (Apple/Microsoft,...), de solidarité mutuelle, établies pour assurer une viabilité, une persistance de nos structures.

« C'est en protégeant le faible que l'espèce humaine a subsisté et est devenue « supérieure » aux autres car elle a dû mettre en place des stratégies de survie... », il semblerait urgent d'en faire autant en ciblant ces maillons de données si chères à nos préoccupations.

C'est peut–être cela la cyber-résilience ? Un état d'esprit alliant sens et simplicité dans l'art de l'action : préparation, priorisation, agilité et adaptabilité ? Un état qui *in fine* augmente la confiance, l'agilité et donc la capacité des entreprises.

PLAN CYBER RÉSILIENCE (PCR) : UN NOUVEAU PLAN DANS LA FAMILLE DES PCA

La cyber sécurité ne peut pas être totale en permanence. Malgré les efforts permanents faits par la sécurité informatique, il faut définir une stratégie pour assurer le fonctionnement des activités des métiers critiques suite à une cyber attaque. Un des moyens pour s'y préparer progressivement est de développer un Plan Cyber Résilience. Il se décompose en une partie « informatique » et une partie « métiers » se limitant aux métiers déclarés critiques par la Direction Générale.

Comme tous les Plans de la Continuité d'Activité, un Plan Cyber Résilience est prévu pour faire face à un événement perturbateur qui peut être par exemple :

✓ indisponibilité massive des postes de travail et des serveurs suite à une compromission de l'Active Directory

✓ perte d'intégrité des données

✓ attaque simultanée du site de production et du site de secours

.....

(3) https://www.riskinsight-wavestone.com/2017/10/cyber-resilience-plier-pas-rompre-22/
(4) SI : Systèmes d'Information
(5) PCA : Plan de Continuité d'Activité
(6) DICP : Disponibilité ; Intégrité; Confidentialité; Preuve
(7) SaaS : Software as a Service
(8) https://www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2017_02_CGE_SR_Rapport.pdf

SUITE P.8 ...

✓ compromission par une attaque de ressources communes entre le site de Production et le site de secours, par exemple le poste de pilotage unique de la Production

✓ propagation de virus sur le site de secours informatique

✓ perte d'intégrité des données restaurées issues des sauvegardes de recours

✓ perte de l'accès aux applications liées à une technologie (Microsoft par exemple, ...)

✓...

La survenance de ces événements perturbateurs nécessite l'activation d'une organisation de crise cyber chargée, outre de la communication, de coordonner la reprise d'activité de l'informatique et la continuité d'activité des métiers critiques. En fonction de l'attaque cyber, l'organisation de crise peut activer un Plan Cyber Résilience.

Le développement d'un Plan Cyber Résilience nécessite :

✓ Des mesures préventives, avant le constat des effets de la cyber attaque :

- Evaluer le niveau de sécurité de l'IT[9] de façon récurrente sachant qu'il est impossible d'être au top en permanence.

- Déterminer avec les métiers et faire valider par la Direction Générale les activités critiques à continuer impérativement dans un tel contexte ; leur fonctionnement pouvant être dégradé.

- En déduire les moyens critiques pour faire fonctionner ses activités critiques.

- Choisir et faire décider par la Direction Générale une stratégie cyber : mesures de prévention et mesures de protection dont le Plan Cyber Résilience.
  Exemple : doublement de certaines applications hautement critiques développées différemment et exploitées sur un autre site isolé, contrôlées fonctionnellement à plusieurs niveaux par les métiers.

- Augmenter en permanence le niveau de sécurité (mise à jour régulière des logiciels, ...) en renforçant ses processus internes et/ou en investissant dans de nouvelles solutions de parades.

- Surveiller en permanence, qualifier et remonter les incidents.

- Contrôler l'intégrité fonctionnelle des sauvegardes de recours suite à une compromission des données. Elles peuvent embarquer des éléments de compromission : malwares, camps de base, des modifications opérées par les attaquants.

- Mettre en place des sauvegardes ultimes des activités critiques sur un site distant sécurisé ne pouvant pas être compromis. Ces sauvegardes peuvent être utilisées en lecture ou servir à la reprise d'activité sur un autre site de secours. Des logiciels du marché assurent ces fonctionnalités en permettant également de communiquer, quoi qu'il arrive.

- Entrainer par des exercices de validation les cellules de crise et les collaborateurs travaillant dans des activités les plus critiques à traiter des scénarios cyber :

- Travailler sans IT pendant la restauration des sauvegardes de recours.

- Travailler en mode dégradé (faisabilité, durée).

- Se préparer à contrôler un arrêt rapide de l'IT, suite à une attaque cyber.

✓ Après le constat des effets de la cyber attaque :

- Contenir l'attaque : décider rapidement en conscience, avec tous types d'experts (cloisonnement,...).

- Activer l'emploi de moyens critiques : poste de travail apporté contractuellement par un fournisseur, messagerie minimum de secours, ...

- Exécuter des plans préparés et testés régulièrement pour la reconstruction de l'IT nécessaire aux applications critiques : sauvegarde de recours saine, clef USB de chargement des postes de travail, poste de travail dans le Cloud. Des logiciels tels que RVR Parad permettent de créer, maintenir et exécuter ces plans dans le cadre d'exercices et en cas de sinistre Cyber.

Il ne faut pas oublier qu'implémenter ces mesures nécessite de mettre à niveau tout le processus de management de crise et de la continuité d'activité sans oublier de revoir les rôles du Responsable de la Sécurité du Système d'Information, du directeur des risques, du Responsable du Plan de Continuité d'Activité, Responsable de la communication interne et externe, du Responsable juridique, ... Et le rôle de la cellule de crise pendant une attaque cyber.

Il n'existe pas de Plan Cyber Résilience tout fait, universel, il doit être adapté au contexte, à l'organisation de l'entreprise pour assurer *in fine* sa survie ■

QUELQUES RÉFÉRENCES complémentaires pour alimenter vos recherches

→ https://www.symantec.com/content/en/us/enterprise/other_resources/b-a-manifesto-for-cyber-resilience.pdf

→ https://www.us-cert.gov/ccubedvp/assessments#Downloadable%20Resources

(9) IT : Information Technology

Open data, risques et crises

par Pierre CHRZANOWSKI

A PROPOS DE L'AUTEUR

Pierre CHRZANOWSKI

Pierre Chrzanowski est Spécialiste en Développement Numérique auprès de la Banque Mondiale et Consultant Open Data auprès du Global Facility for Disaster Reduction and Recovery (GFDRR). Auparavant, il a travaillé pour l'Ambassade de France à Londres en tant qu'Attaché Scientifique. Il est aussi membre fondateur d'Open Knowledge France, une association qui promeut la diffusion du savoir sur le web. Il est diplômé de l'Université de Technologie de Troyes en Management des Systèmes d'Information et a également suivi une formation à l'Institut des Relations Internationales et Stratégiques.

RÉSUMÉ

Grâce à Internet, nous disposons désormais d'une infrastructure d'information extrêmement performante pour gérer les crises de manière collective. C'est tout l'enjeu de l'open data : assurer que les données essentielles soient disponibles et rapidement accessibles par tous via Internet. Fini le temps du secret par défaut dans la gestion des risques, les organisations doivent désormais savoir distinguer les données qui doivent être publiées de celles à protéger. C'est aussi une question d'outils et de nouvelles méthodes de collaboration à mettre en œuvre.

Le 12 janvier 2010, un tremblement de terre d'une magnitude de 7,0 dévastait Haïti. Les dégâts furent considérables avec une grande partie des bâtiments de la capitale Port-au-Prince détruits, 280 000 morts et plus de 1 million de sans-abris. Les victimes incluaient du personnel clé des institutions internationales et du gouvernement, ceux dont le rôle aurait été de gérer cette catastrophe. Au-delà du bilan humain, des informations critiques pour la gestion de crise et la reconstruction du pays se sont retrouvées sous les décombres du Palais Présidentiel, du Centre National de l'Information Géo-Spatiale (CNIGS) et d'autres bâtiments institutionnels. Ces données, sauvegardées dans des ordinateurs ou des documents papier, incluaient notamment la localisation des établissements de santé et le réseau routier de la ville de Port-au-Prince.

Face à cette situation, plusieurs entreprises de satellites ont pris la décision de publier des images à haute résolution des dégâts, en libre accès sur le web. Digital Globe, SPOT et GeoEye ont ainsi mis gratuitement à disposition leurs images satellites dans un format numérique et une licence qui permettaient leur réutilisation par tous. Cette diffusion de données aériennes a déclenché et rendu possible un effort international de cartographie du pays. En moins de 3 semaines, plus de 600 bénévoles de la communauté OpenStreetMap ont utilisé ces ima ges pour tracer les routes et les bâtiments de Port-au-Prince. Ce qui d'ordinaire représente un travail de cartographie d'une année a été réalisé en 20 jours et pour un coût quasi nul.

Ce résultat spectaculaire devrait interpeller toute personne dont le rôle est de gérer l'accès et le partage de l'information dans la gestion des risques. Traditionnellement, l'information est en effet considérée comme un actif stratégique qui, du point de vue de l'organisation, doit être collectée, protégée, et diffusée à des acteurs identifiées. C'est dans cette vision « attaque défense » que se développent notamment les disciplines de la cybersécurité ou de l'intelligence économique et stratégique. L'application des principes de l'open data permet d'aborder le rôle de l'information dans la gestion de risque d'un autre point de vue, celui de la collaboration et de la mutualisation des ressources et des moyens.

Par définition, une situation de crise est un événement incertain face auquel une multitude d'acteurs différents ont à prendre des décisions pour s'y préparer, y répondre, et si possible l'atténuer. Hors, grâce à Internet, nous disposons désormais d'une infrastructure d'information extrêmement performante pour gérer les crises de manière collective. Encore faut-il que l'information soit disponible sur le réseau, et non pas rangée dans un placard.

C'est tout l'enjeu de l'open data : assurer que les données essentielles à la gestion de crise soient disponibles et rapidement accessibles par tous via Internet. Cela suppose de supprimer ou réduire les barrières techniques, juridiques ou économiques qui entravent l'accès et l'utilisation de l'information. Un jeu de données est ainsi considéré ouvert s'il est disponible en téléchargement sur le web dans un format numérique standard, et dans une licence qui autorise son accès et sa réutilisation gratuitement et sans condition.

De nombreuses initiatives de données ouvertes existent. En France data.gouv.fr est le portail de données de l'État qui héberge et référence l'ensemble des données ouvertes sur le territoire. On y trouve des données essentielles comme le plan cadastral, le registre des entreprises ou les statistiques sur la population. Dans le domaine des risques de catastrophes naturelles, le portail oasishub.co référence des données sur les différents aléas. La plateforme data.humdata.org des Nations Unies est quant à elle utilisée par les organisations internationales pour collecter et partager des données lors de crises humanitaires.

Par principe, l'open data ne concerne que les données d'intérêt général, à caractère public, qui ne peuvent porter préjudice aux individus, aux entreprises ou aux États qui les mettent à disposition. Dans les faits, l'appréciation de la distinction entre données publiques – que l'on peut partager – et données privées – que l'on protège – varie cependant en fonction des intérêts de l'organisation ou de la personne qui en a la charge. C'est la raison pour laquelle le législateur est de plus en plus souvent appelé à trancher sur ce qui constitue une donnée publique, comme

SUITE P.10 ...

ce fut le cas avec les données de référence en France, ou bien plus récemment avec les données à haute valeur ajoutée au niveau de l'Union Européenne. Mais la loi ne saurait considérer l'ensemble des menaces et opportunités associées à telle ou telle information.

Il revient donc également à chaque organisation de se poser ces questions : quelles sont les données essentielles pour mon territoire, mon entreprise, dont la diffusion et la gestion en open data permettrait de réduire le risque ? À l'inverse, quelles sont les données dont l'indisponibilité le jour J accentuerait l'impact d'une crise ? Ou encore : quelles sont les données à protéger et dont la mise à disposition en open data constituerait une menace ? Ces questions doivent aussi être considérées dans un contexte où le public peut accéder à de plus en plus d'information sur le web. On peut ainsi noter que plusieurs pays refusent encore de publier les cartes de leur territoire en open data quand bien même n'importe quel internaute peut accéder aux images satellites via une application comme Google Earth.

La problématique pour le gestionnaire de risque est donc d'abord de bien connaître l'ensemble des données gérées par son organisation, leurs différents attributs, leur niveau de détail, leur mode de production, et de la même façon d'identifier les données produites et mises à disposition par d'autres acteurs et d'évaluer celles qui sont critiques pour la gestion de risque.

Prenons l'exemple d'un établissement qui reçoit du public tel qu'un grand magasin, une gare ou une salle de concert. Est-ce que les données sur les plans intérieurs du bâtiment devraient être accessibles en open data ? Le réflexe serait de répondre non et d'argumenter que ces données, une fois ouvertes, pourraient être utilisées à des fins terroristes ou toute autre utilisation malveillante. Pourtant, les bâtiments qui reçoivent du public ont déjà tous pour obligation d'afficher un plan d'évacuation aux différents étages de leur enceinte. De plus, n'importe qui peut avec son mobile entrer et cartographier cet espace public. À l'inverse, la non disponibilité d'un plan du bâtiment pourrait entraver l'intervention des secours, ou des forces de sécurité. Lors des attentats du Bataclan, les terroristes avaient la carte du bâtiment dans leur téléphone portable, mais pas les spectateurs, ni même les premières forces d'intervention.

Enfin, l'open data ne doit pas seulement être considérée comme une question d'information à ouvrir ou à fermer, mais également en termes d'outils et de mode d'organisation. La gestion d'une crise est un processus complexe qui suppose une coordination forte d'un ensemble d'acteurs hétérogènes qui ne se connaissent pas nécessairement. Ainsi, la réponse de la communauté OpenStreetMap au tremblement de terre d'Haïti ne fut possible que parce qu'une infrastructure technologique appropriée, tirant bénéfice des principes de l'open data et donc utilisable par tous, avait été développée et mise à disposition quelques années auparavant. C'est la principale leçon de la gestion de la crise d'Haïti d'un point de vue informationne : en tant qu'organisation, quelles sont les données ouvertes, outils et plateformes que je dois connaître, utiliser, partager, voire enrichir et améliorer, afin de mieux me préparer à la prochaine catastrophe ?

Suivant ce principe, l'initiative Open Data pour la Résilience (OpenDRI) du GFDRR aide les pays à mieux collecter, partager et utiliser les données essentielles pour la gestion des risques de catastrophes naturelles. Elle appuie par exemple le développement d'outils open source qui utilisent les données ouvertes pour modéliser les scénarios de catastrophes naturelles et leur impact, ou pour mieux communiquer les risques aux populations. L'initiative OpenDRI aide également les États à mieux identifier et publier les données pour la gestion des risques. Ainsi, le site index.opendri.org permet de renseigner pour chaque pays si les données essentielles à la gestion des catastrophes sont disponibles en open data, en accès restreint ou inaccessibles. Ces données concernent les différents risques naturels (tremblement de terre, tempête, inondation, etc.) identifiés et mesurés sur un territoire, mais également les données sur les populations et infrastructures exposées.

En conclusion, voici quelques recommandations afin de mettre en pratique les principes de l'open data dans la gestion des risques :

1. Évaluer votre processus actuel de gestion des risques et caractériser les principaux problèmes ou enjeux pour chaque étape de la gestion de risque (détection, prévention, réduction, préparation, réponse, reconstruction, etc.) ainsi que les solutions associées (outils, méthodes, analyses, données, etc.) ;

2. Identifier et définir les données essentielles nécessaires pour chaque étape. Ces données devraient à minima inclure des données de base, comme les données géographiques, des données permettant de caractériser les aléas et de mesurer les risques, des données sur les populations et infrastructures exposées, ainsi que des données opérationnelles, notamment en ce qui concerne la réponse à la crise (liste des acteurs, localisation des infrastructures d'urgence, etc.) ;

3. Réaliser un inventaire des données ouvertes, ou en accès restreint, collectées par des acteurs externes et répondant aux critères de données essentielles définies dans l'étape 1 ;

4. Réaliser un inventaire des données collectées ou gérées par votre organisation ; évaluer en termes de menaces et opportunités si ces données peuvent faire l'objet d'une diffusion à un groupe restreint ou en open data ; enfin identifier les données dont le traitement est juridiquement contraint (données personnelles qui entre dans le cadre du RGPD, données sensibles ou stratégiques à protéger, données publiques ou d'intérêt général à diffuser, etc.) ;

5. Suite à ces différentes étapes, vous devriez être en mesure de décider plus facilement quelles données collecter, partager, ou utiliser dans le cadre des solutions déterminées afin d'améliorer votre gestion des risques ■

+ SOURCES ET RÉFÉRENCES

→ Open Definition : https://opendefinition.org
→ Open Data Handbook : http://opendatahandbook.org
→ Open Knowledge France : https://okfn.fr/
→ The Data Spectrum, Open Data Institute : https://theodi.org/about-the-odi/the-data-spectrum/
→ Plateforme ouverte des données publiques françaises : https://www.data.gouv.fr/
→ Global Facility for Disaster Reduction and Recovery : https://www.gfdrr.org
→ Open Data for Resilience : https://opendri.org/
→ Open Data for Resilience Initiative Field Guide : https://www.gfdrr.org/en/publication/open-data-resilience-initiative-field-guide
→ Open Data for Resilience Index : https://index.opendri.org/
→ ThinkHazard! : http://thinkhazard.org/

Risques et nouvelles technologies du monde numérique

par Olivier VELIN

A PROPOS DE L'AUTEUR

Olivier VELIN

Consultant senior pour Stratégie GDC, partenaire d'EY (Ernst & Young Advisory), Olivier Velin est expert en gestion des risques, gestion de crise, communication de crise, résilience, continuité d'activité, reprise d'activité industrielle et sécurité. Il accompagne et forme des équipes de direction et des cellules de crise via des simulations de crise spécialement adaptées au contexte de l'entreprise concernée. Concepteur de méthodes innovantes, il a élaboré et mis en œuvre des outils destinés à la gestion de certains risques, notamment le risque d'inondation. Il a réalisé avec succès des prestations chez des clients des principaux secteurs d'activité public et privé, avantagé par sa double expérience opérationnelle de consultant/auditeur externe et d'ancien responsable de centres de profit, qui lui procure une vision plus étendue des contraintes rencontrées par ses clients.
Olivier Velin, membre du think-tank GMAP-Center, a réalisé depuis 2012 des missions opérationnelles avec l'Intelligence Artificielle MILEVA https://www.gmap-center.ch/mileva/. Il est aussi membre du think-tank CyAN (Cybersecurity & cybercrime Advisors Network) http://www.cyan.network/ ; Membre du Corporate Steering Committee de la majeure Systèmes d'Information pour la Finance de Marché à l'Institut Mines Telecom Business School, Olivier Velin enseigne en Masters Spécialisés à l'ESIEA (depuis 2004), à l'Institut Mines-Telecom Business School (depuis 2009) et en Russie (State Government University of Economics & Finance – Saint Pétersbourg) ; co auteur de 3 ouvrages en Gestion de Crise, Continuité d'Activité et Sécurité et auteur de nombreux articles, il est aussi formateur et conférencier.

Contacts :
olivier.velin@strategie-gestion-crise.com
olivier.velin@mileva-ai.ch
olivier.velin@cyan.international

RÉSUMÉ

Le passage à l'ère numérique se caractérise par une rupture dans la place accordée par la société à l'être humain. Au-delà de sa personne physique, c'est son être virtuel constitué par la masse de données sans cesse collectées sur lui, qui s'avère l'objet de toutes les convoitises. Dans ce monde hyperconnecté et mondialisé, les outils technologiques s'avèrent de puissants vecteurs de capture d'information s'affranchissant des frontières et des règlementations locales de protection de la vie privée. Face aux risques encourus, à ses dépends, par la diffusion sauvage d'informations personnelles et sensibles ou leur exploitation à des fins fructueuses voire peu scrupuleuses, l'individu connecté doit accepter d'assumer ses responsabilités, réagir et se montrer circonspect en limitant au strict nécessaire les informations qu'il met à disposition de la société numérique.

Dans notre monde hyperconnecté, tous nos actes, même les plus bénins, sont en voie de digitalisation, de numérisation, pour devenir une masse de données stockées dans des datacenters mondialement dispersés, qui se sont affranchis des frontières géographiques et des contraintes juridiques déterminées par les Etats.
Nouveau cyborg, Homo connecticus, l'individu connecté, s'est ainsi vu adjoindre une ombre numérique personnalisée, constituée par la masse des données recueillies en permanence sur lui, son travail, ses modes de vie, ses échanges scripturaux et verbaux via les technologies de l'information, etc. Une ombre dotée d'une vie propre, sur laquelle homo connecticus n'a que peu, voire aucune, emprise car cette ombre est détenue dans les datacenters auquel il n'a pas accès et contre les propriétaires desquels il n'a que bien peu de recours.
A l'heure du monde datacentré, nous vivons, à l'échelon planétaire, un de ces tournants qui modifient radicalement le cours d'une civilisation. Les références de « l'ancien monde » qui semblaient incontournables, tels les institutions et tiers de confiance, sont progressivement déclassées. Cryptomonnaies, blockchain, mobilité, bibliothèques numériques, uberisation, constituent les briques de construction d'un autre monde qui peut nous paraître inhumain par son caractère virtuel et immatériel étranger au monde réel auquel nous sommes habitués, un monde étrange dans lequel nous sommes condamnés à vivre.

LE « CAPITAL-DONNÉES », CETTE MATIÈRE PREMIÈRE OBJET DE CONVOITISES

Fait unique dans l'histoire de l'humanité, le « capital-données » que représente chaque individu fait l'objet d'une collecte effrénée à laquelle se livrent Etats et entreprises. Consentant ou non, *homo connecticus* est observé, décomposé en catégories, profilé, classé, codifié à des fins parfois nécessaires, parfois peu scrupuleuses mais fructueuses. Aussi, livrer ses données personnelles[1] d'ordre intime, aux réseaux sociaux, c'est prendre le risque qu'il en soit fait un usage abusif et accepter d'en supporter les conséquences. Plus insidieuse, la géolocalisation s'avère aussi un dispositif pour cybersurveiller tous les déplacements d'une personne équipée d'un téléphone mobile[2], allumé ou non.

(1) La Tribune – 17 Mars 2018
(2) Cette remarque s'étend aussi à tout véhicule équipé d'un GPS.

SUITE P.12 ...

Jules Romains[3] l'avait perçu : la courbe de l'évolution technique, en constante accélération, n'est plus en phase avec celle de l'évolution des institutions et celle de la nature humaine. Mais la situation s'est compliquée ; car si les textes règlementaires sont insuffisants à assurer la protection des données personnelles et sensibles, les technologies de la sécurité sont aussi prises de vitesse : malwares, ransomwares, botnets multipliant les capacités des cyber attaquants, cryptominage illicite d'ordinateurs personnels par virus et (bientôt) ordinateurs quantiques briseurs de codes de chiffrement, s'avèrent des armes numériques de destruction massive des données et, ce faisant, d'activités humaines.

LES NOUVEAUX CHEVAUX DE TROIE

Les entreprises, jouant sur la naïveté du consommateur, annoncent comme indispensable tout nouvel objet connecté, qui est présenté sous un jour favorable et sensé procurer confort, simplification de la vie et position sociale (par effet de mode), alors qu'il est avant tout un dispositif d'intrusion dans la sphère privée, en mesure d'observer, d'écouter, de détecter tout ce qui se passe à votre domicile. L'objet connecté est une version moderne du Cheval de Troie, apte à devenir un dispositif de surveillance rapprochée de l'individu. En conséquence, qui choisit d'utiliser de tels objets doit aussi assumer sans (trop) se plaindre l'usage abusif qui peut en être fait. Par ailleurs, du fait d'une conception riche en lacunes de sécurité, ces objets connectés sont des terminaux manipulables à distance via l'Internet, bien adaptés à la constitution de « botnets » (réseaux zombies). Or la quantité d'appareils connectés dans ces réseaux zombies est sans limite. Des botnets de grande puissance se sont constituées en «recrutant» plusieurs millions d'appareils connectés (caméras de vidéo surveillance notamment) et ont été employés pour engager des cyberattaques en déni de service (DDoS), afin de saturer ou bloquer des réseaux de communication à l'échelon d'entreprises, voire de nations.

Par le biais d'injection de virus spécifiques, le cryptominage génère des cryptomonnaies en prenant le contrôle de l'ordinateur d'un utilisateur, dont la puissance est alors détournée au profit cette tâche lucrative.

Ultimes défenses, les dispositifs de sécurité en vigueur pour protéger les données par les techniques de chiffrement DES[4] et RSA[5], cèderont probablement bientôt sous les coups de boutoir de l'ordinateur quantique armés des algorithmes de Grover et de Shor, créant ainsi de nouvelles vulnérabilités jusqu'à conception de nouveaux outils (quantiques ?) de sécurité. Spirale d'un perpétuel recommencement.

De manière plus étendue, l'expansion de l'espace numérique s'est affranchie des frontières géographiques et juridiques. Les textes réglementaires protégeant les données personnelles, notamment RGPD[6], n'ont qu'une portée limitée face aux clauses léonines des contrats d'hébergement qu'imposent, dans un contexte de mondialisation de leurs implantations, les entreprises qui hébergent, stockent et transportent les données qu'elles ont collectées, capturées ou qui leurs sont confiées.

BIG DATA, SCANDALE, ESPIONNAGE ET CHANTAGE

La collecte tous azimuts du « capital-données » de chaque individu est la clef de voûte de cette masse de données déstructurées qui constitue le Big Data. Il trouve une de ses fins dans le profilage[7] des internautes à des fins de harcèlement publicitaire ciblé, l'utilisateur étant perçu comme simple machine à consommer. Un véritable marché du courtage de données personnelles s'est ainsi mis en place, auquel tout un chacun peut s'adresser, pour acquérir des données personnelles que les textes en vigueur interdisent de négocier de manière licite.

Et, bien que plusieurs entreprises[8] aient été prises à partie par les autorités de plusieurs pays, notamment européens, aux motifs du caractère illégal de leurs modes de collectes et de détentions de données dans des bases situées à l'étranger voire de la communication de ces données ou leur vente à des tiers sans l'accord de leur légitime propriétaire, le marché de la donnée n'a jamais été si florissant. Le profil numérique de tout individu s'achète et se vend. Il suffit d'y mettre le prix.

L'une des méthodes les plus insidieuses pour acquérir des données particulièrement sensibles consiste à collecter des informations du ressort de la sphère privée (sports, loisirs, etc.) de dirigeants d'entreprises ou de personnes travaillant dans un secteur hautement concurrentiel ou stratégique. A cette fin, le pirate se met en veille (pratique du «watering hole»), notamment sur le Net, pour récolter des informations sur les thèmes auxquels s'intéresse sa future victime. Lorsque le pirate en a connaissance, il envoie une publicité ciblée relative à de telles activités (par exemple : invitation gratuite à un Salon, Newsletter, etc.) dans laquelle il a inséré un malware (pratique du «malvertising»). En cliquant sur le lien, la victime contamine elle-même ses propres équipements informatiques, le malware se dupliquant sur les appareils synchronisés avec l'ordinateur (smartphones, tablettes, autres ordinateurs, etc.). Toute information stockée ou échangée via ces dispositifs parvient alors entre les mains du pirate.

En s'attaquant à la vie privée ou à la famille de la cible, le pirate s'affranchit des mesures de sécurité mises en place par les équipes de cyber-sécurité du lieu de travail de la victime. Une fois acquises ces données personnelles, le pirate peut aussi se lancer sur la piste de sa victime afin d'avoir sur elle des moyens de pression qui s'expriment en termes de chantage sous peine de dévoiler certains aspects de sa vie privée[9] qu'elle ne souhaite pas voir étaler au grand jour. C'est ainsi qu'un lien qui semble innocent, fait tomber des personnes « clefs » entre les mains d'individus astucieux mais mal intentionnés.

S'introduire dans un cyber-entrepôt de données est d'autant plus intéressant que les données stockées sont volumineuses, sensibles, et s'échelonnent sur une période plus longue. Car obtenir un maximum d'informations sur une personne donne la possibilité de reconstituer tout ou partie de son existence, de ses habitudes, de ses faiblesses, peu importe qu'il s'agisse de problèmes de santé, de moeurs[10] ou d'argent, d'erreurs de jeunesse ou de mouvances politiques considérées comme extrêmes. La faiblesse des dispositifs de protection des données d'un

(3) Romains. J., Le problème numéro un, Plon, p. 230, 1947

(4) DES : Data Encryption Standard

(5) RSA : Rivest–Shamir–Adleman. Nommé par les initiales de ses trois inventeurs : Ronald Rivest, Adi Shamir et Leonard Adleman.

(6) RGPD : Le Règlement général sur la protection des données

(7) Cette pratique du profilage peut être contrariée par la technique de l'obfuscation qui consiste à noyer une recherche utile sur l'Internet, sous un tas d'autres requêtes inutiles qui rendent incohérent et peu utilisable le profilage de l'internaute. Par ailleurs, celui-ci garde tout loisir de « black lister » les entreprises qui le harcèlent via des publicités ciblées.

(8) Notamment Facebook face à l'Union Européenne dans le cadre de Cambridge Analytica.

(9) Des emails réclamant rançon sous peine de voir vos amis apprendre que vous naviguez sur des sites pornographiques circulent depuis quelques semaines. L'accusation, non ciblée, se fonde sur la crainte de l'internaute qui paiera pour protéger sa réputation face à la calomnie (qu'il se soit ou non connecté à de tels sites) ou par auto culpabilisation.

cyber-entrepôt peut conduire à la diffusion, sur la place publique, d'informations sensibles de nombreux utilisateurs, avec des préjudices qu'un dépôt de plainte contre le cyber-entrepôt ne corrigera pas.

LA SURVEILLANCE PLANÉTAIRE, ARME DE LA GUERRE ÉCONOMIQUE

En dépit d'une idée bien implantée, la cyber collecte planétaire n'est pas plus l'exclusivité des GAFA que du secteur privé: les états y règnent en maîtres. Entreprises et internautes sont observés, fichés et profilés, dans l'optique d'une surveillance qui n'est pas uniquement tournée sur l'antiterrorisme[11]. Les données collectées, lorsqu'elles concernent des personnes occupant des fonctions clefs sont d'autant plus précieuses qu'elles permettent d'exercer une pression sur ces personnes, voire de les arrêter dans une optique de « racket planétaire » tel que celui déployé via le FCPA[12] américain. Sur ce plan, les mésaventures survenues à Frédéric Pierrucci[13] (Alstom) ont montré toute la duplicité mise en œuvre par l'Etat américain dans sa guerre économique. Bien que s'appliquant aussi aux entreprises américaines, le FCPA[14], s'exerce surtout contre les entreprises étrangères, notamment européennes, afin de procurer un avantage concurrentiel aux entreprises américaines. La portée de cette loi est planétaire, du moment que la transaction commerciale est libellée en dollars américains ou qu'elle transite par des serveurs informatiques ou un réseau de télécommunications américains.

Cette loi s'est renforcée par le Cloud Act (23 mars 2018), en application duquel les données stockées sur un cloud américain peuvent être communiquées aux services de renseignement ou de la Justice américains. Or, de nombreuses entreprises européennes et bien sûr françaises, qui ont choisi d'externaliser tout ou partie de leur système d'information auprès d'entreprises américaines offrant des prestations de Cloud computing, mettent ainsi leurs données stratégiques à la disposition des entreprises américaines concurrentes sans parler des données personnelles de leurs employés et clients qui, de facto, devraient être protégées par la RGPD mais ne le sont plus, par simple application du Cloud Act. Amazon[15] n'a-t-elle pas été chargée de créer un cloud pour la NSA[16] et la CIA[17] ? On est en droit de s'interroger sur la crédulité des directions d'entreprises, notamment classées OIV (Opérateurs d'Importance Vitale), qui ont ainsi mis à disposition des entreprises et de l'Etat américain toutes leurs informations sensibles ! Et du manque de réaction des services de l'Etat Français qui semblent avoir pris tardivement conscience de la situation. La guerre économique est pourtant bel et bien déclarée.

L'INTELLIGENCE ARTIFICIELLE, PROBLÈME OU SOLUTION ?

Dans ce panorama, l'Intelligence Artificielle (IA) s'avère t-elle l'instrument de tous les dangers claironné par certains ? Ou plus exactement les IAs car toutes ne sont pas conçues pour les mêmes usages. Dans des domaines où les outils traditionnels ont montré leurs limites (complexité, interactions, etc.), l'IA fournit des résultats bruts qui, avant exploitation, doivent être analysés et interprétés[18]. Et ce, afin de s'affranchir de nombreux biais : biais de conception, anomalies et erreurs dans les données collectées et traitées, faux positifs, sous ou sur représentation de certaines catégories de données, corrélations fallacieuses, etc. Contrairement à une idée fort répandue, l'IA n'est pas une machine presse-bouton : il appartient à l'être humain de lui poser les bonnes questions et de se prononcer sur les résultats qu'elle fournit. A défaut, à l'instar d'autres outils (à commencer par l'Internet), l'usage des IAs en se généralisant va entraîner des dérives que des textes réglementaires s'efforceront a posteriori de contrôler avec plus ou moins de réussite.

La protection des données par des moyens technologiques et règlementaires n'obéit pas à un simple désir de dissimuler des informations ou d'en contrôler la détention. Elle doit être en mesure de répondre à deux questions capitales : quelles conséquences aura, dans un futur qui se conjugue au présent, l'effacement de l'ombre numérique d'un individu ? Comment pourra t-il faire restaurer ce clone de lui-même si les données en étaient soudain corrompues ?

Une remarque s'impose cependant : si dans notre monde numérique hyperconnecté l'individu n'est plus en mesure d'échapper au pillage et au commerce de son capital-données, il conserve néanmoins sa capacité à décider s'il veut offrir des informations sur sa vie privée en pâture à qui saura s'en emparer. Face à cette alternative, *homo connecticus* ne peut prétendre se décharger de toutes responsabilités et refuser d'assumer certains risques auxquels il s'expose volontairement ■

BIBLIOGRAPHIE

Big data et cloud - G. Chesnot - Vuibert - 2017

Black box society - F. Pasquale - FYP Editions - 2015

Cybertactique - Conduire la guerre numérique - B. Boyer - Navis - 2014

Gagner les cyberconflits - F.B. Huyghe, O. Kempf & N. Mazzucchi - Economica - 2015

Hacker's guide - E. Charton - Pearson - 2013

Intelligence artificielle - (3 volumes) - Cépaduès - 2016

La face cachée d'Internet - R. Stamboliyska - Larousse - 2017

La grande illusion du monde numérique - C. Aghroum - 2018

La perception des risques - B. Chauvin - de Boeck - 2014

L'empire des données - A. Basdevant & J.P. Mignard - Don Quichotte - 2018

Le renseignement humain à l'ère numérique - T. Zimmer - VA Editions - 2018

Le piège américain - F. Pierucci - JCLattès - 2019

L'hyperpuissance de l'informatique - G. Berry - Odile Jacob - 2017

Ru.net - Géopolitique de l'espace russophone - K. Limonier – 2018

Sécurité et espionnage informatique - C. Pernet - Eyrolles - 2015

Sécurité informatique - Eyrolles - 2016

Sécurité opérationnelle - A. Fernandez-Toro - 2015

The art of invisibility - K. Mitnick & R. Vamosi - Littlbrown.com - 2017

(10) Cf. le piratage des 32 millions de comptes du site Ashley Madison, dont plus de 260 000 adresses emails françaises.

(11) Le Patriot Act (26 Octobre 2001) autorise les agences de renseignement à espionner massivement les entreprises et employés étrangers.

(12) FCPA : Foreign Corrupt Practices Act, loi fédérale américaine de 1977 pour lutter contre la corruption d'agents publics à l'étranger.

(13) Cf. Le piège américain - F. Pierucci et M. Aron – JC Lattès, 2019

(14) Foreign Corrupt Practices Act – 19 Décembre 1977

(15) https://www.01net.com/actualites/amazon-au-service-de-la-cia-et-de-la-nsa-624090.html

(16) NSA : National Security Agency

(17) CIA : Central Intelligence Agency

(18) L'auteur travaille depuis 2012 avec une IA prédictive, la « machine thinking » Mileva – https://www.gmap-center.ch/mileva/

Les défis du traitement judiciaire de la cybercriminalité

par Jacques MARTINON

A PROPOS DE L'AUTEUR

Jacques MARTINON

Magistrat judiciaire, Jacques MARTINON a débuté sa carrière en tant que juge d'instruction (2008-2015). Depuis janvier 2016, il a rejoint la direction des affaires criminelles et des grâces (DACG) du ministère de la justice, afin d'intégrer la mission de prévention et de lutte contre la cybercriminalité, qu'il dirige désormais. Contributeur à la Revue stratégique de Cyberdéfense élaborée sous l'égide du SGDSN, il est intervenu comme formateur à la session nationale « *souveraineté numérique et cybersécurité* » organisée par l'INHESJ et l'IHDEN. Il est enfin titulaire du Diplôme Universitaire de Cybercriminalité de l'Université de Montpellier (Major 2018). Chargé de cours à Science-Po Paris.

RÉSUMÉ

La cybercriminalité couvre traditionnellement les cyberattaques, visant les systèmes informatiques eux-mêmes, mais également les infractions ayant pour vecteur principal ou étant considérablement facilitées par l'usage d'un réseau de communication. Si toutes les juridictions peuvent connaitre de faits de cyberdélinquance, le tribunal de grande instance de Paris bénéficie toutefois d'une compétence concurrente nationale en matière de cyberattaques. Les contours d'une politique pénale de lutte contre la cyberdélinquance sont en voie de consolidation, toutefois les moyens humains consacrés demeurent trop limités et l'organisation judiciaire toujours en quête de maturité.

Seront présentées dans un premier temps les caractéristiques principales de la cybercriminalité avant d'aborder succinctement l'organisation judiciaire actuelle et les relations des acteurs judiciaires avec ceux de la cybersécurité.

UNE CYBERCRIMINALITÉ POLYMORPHE ET DÉLICATE À APPRÉHENDER PAR LE PRISME JUDICIAIRE TRADITIONNEL.

Le périmètre pénal de la cybercriminalité est un véritable défi intellectuel. L'angle traditionnel des qualifications pénales est en effet peu adapté. Par exemple, les atteintes aux systèmes de traitement automatisé de données (STAD) recouvrent en réalité plus d'une dizaine de « phénomènes cyber » différents, tels le cyberespionnage, le cybersabotage, le rançongiel…

En conséquence, les outils statistiques traditionnels sont quasi inopérants pour apprécier les évolutions des phénomènes au cas par cas. Une approche nouvelle, sous l'angle de la classification des phénomènes cyber constatés, semble nécessaire aujourd'hui.

Une cybercriminalité polymorphe et évolutive

La cybercriminalité, qui d'ailleurs recouvre en réalité une majorité de délits, a pour caractéristiques principales d'être polymorphe et très évolutive.

• Une classification délicate

Les phénomènes cyberdélinquants sont traditionnellement classifiés en deux catégories distinguant l'objet de l'infraction.

La cyberdélinquance au sens strict couvre les phénomènes pénaux dont l'objet est l'atteinte à un système de traitement automatisé de données (STAD) et fait l'objet de la première catégorie. La seconde regroupe les phénomènes qui ont pour vecteur principal un STAD ou ont été facilités par son utilisation, il s'agit de la cyberdélinquance au sens large et la plus fréquente.

Infractions ayant pour objet un système de traitement automatisé de données

Ces infractions visent à porter atteinte aux STAD, comme par exemple le cybersabotage. Ces infractions, notamment réprimées par les articles 323-1 à 323-4 du Code pénal, représentent la cyberdélinquance au sens strict. Dans la pratique, cette catégorie est divisée entre :

✓ les phénomènes de haute intensité qui se caractérisent par une atteinte aux intérêts fondamentaux de la Nation, une dimension internationale, une haute technicité, ou un nombre important de victimes avérées ou supposées ; et

✓ les phénomènes de basse intensité qui se caractérisent par l'absence d'atteinte aux intérêts fondamentaux de la Nation ou un degré de complexité moindre.

Infractions ayant pour vecteur principal ou ayant été grandement facilitées par un système de traitement automatisé de données

Elles couvrent l'utilisation d'un STAD qui a grandement facilité la préparation, l'accomplissement ou la tentative d'une infraction principale n'ayant pas pour objet un STAD. Ces infractions mixtes couvrent également la lutte contre les activités illicites sur l'internet sombre (Darkweb).

Cette catégorie, la plus vaste, couvre aussi des phénomènes pénaux classiques mais nécessitant des investigations très poussées dans l'espace numérique.

• Phénomène évolutif : les nouveaux métiers de la cybercriminalité

La cybercriminalité ne semble pas connaître la crise, bien au contraire de nouveaux « métiers » fleurissent régulièrement, faisant naître le concept de « *Crime as a Service* », par analogie avec les services informatiques traditionnels tels que le « *Platform as a Service* » ou le « *Software as a Service* ».

Sans prétendre à l'exhaustivité, on peut citer pêle-mêle les locations/ventes d'infrastructures comme des *Botnets* (réseau d'ordinateurs ou d'objets connectés[1] « zombies », sous le contrôle d'un serveur dit *Command & Control*), de maliciels divers (parfois avec une rémunération au pourcentage sur les sommes dérobées comme certains rançongiciels), des services de *Crypter/Packer* (augmentant la furtivité des maliciels), de *Money mules* (personne qui transfère de l'argent acquis illégalement pour le compte de tiers) ou encore de *Mixer/Blender* (facilitant le blanchiment des cryptomonnaies).

Les cryptomonnaies ont d'ailleurs permis de nombreuses opportunités pour les cybercriminels, que ce soit en les dérobant directement au préjudice des plateformes d'échanges ou des particuliers, mais également en détournant la puissance de calcul de terminaux afin de « miner » des cryptomonnaies au bénéfice de l'attaquant (le *Cryptojacking* étant le plus gros phénomène en 2018).

Plus original encore, il existe des compagnes de recrutement via des annonces d'emploi pour des administrateurs de Darknets, comme ci-dessous pour Liberty Market :

> *« Nous cherchons à recruter un membre, homme ou femme, qui possède une bonne orthographe. Vous devrez être familier avec la gestion ergonomique des pages web. Il faudra que vous puissiez vous connecter au moins une heure et demie, quatre fois par semaine. Vous serez en charge de la correction...*
>
> *...des posts du forum et responsable de leur bonne lisibilité. Vous devrez aussi corriger des douzaines de posts à chaque connexion. Vous aurez votre propre tableau de bord afin que vous puissiez travailler en toute autonomie. »*
>
> *Source : www.ladn.eu*

Dans la même veine, on relèvera un service de type « Tag Telegram », où des personnes sont simplement rémunérées pour réaliser des tags dans des zones urbaines prédéterminées, comprenant des indications techniques pour rejoindre une discussion Telegram d'un dealer : cf. Photo infra.

Les malédictions de la cybercriminalité : chiffre noir, brouillard statistique et phénomène du « going dark »

Le traitement judiciaire de la cybercriminalité est rendu plus difficile en raison de plusieurs facteurs, notamment un nombre important d'infractions qui ne sont pas portées à la connaissance de la justice (**A**), d'une mauvaise évaluation des infractions qui sont connues de la justice (**B**) et enfin des techniques d'obfuscation de plus en plus élaborées, utilisées par les cybercriminels pour se soustraire aux autorités judiciaires (**C**).

• Le chiffre noir de la cybercriminalité

Certains phénomènes cybercriminels de haute intensité, comme le cyber-espionnage ou le cyber-sabotage, sont peu judiciarisés, du fait de leur nature particulièrement sensibles[2]. Surtout, la publicité d'une cyber-attaque réussie à l'encontre d'une entreprise peut porter atteinte à sa réputation et sa santé économique. Le règlement européen pour la protection des données personnelles (RGPD) change la donne, dès lors que les violations de données personnelles conduisent à une obligation de notification dans les 72h à la Commission nationale de l'informatique et des libertés (CNIL)[3].

Concernant les particuliers, les raisons du chiffre noir sont diverses, du fait d'un caractère parfois imperceptible de l'infraction ou d'un sentiment erroné de l'inutilité de la plainte, souvent couplé à de faibles préjudices matériels. Une meilleure sensibilisation semble nécessaire, d'où l'importance du dispositif national d'assistance aux victimes d'actes de cybermalveillance[4].

• Le brouillard statistique de la cybercriminalité

A l'absence de définition juridique de la cybercriminalité de laquelle découle une difficulté à déterminer un champ infractionnel précis, s'ajoute la dispersion des infractions concernées au sein de plusieurs catégories de NATAFF[5], ne permettant pas d'obtenir des données fines quant aux poursuites.

En effet, certaines infractions peuvent certes être identifiées par la NATINF (Nature de l'infraction), permettant l'exploitation des données du casier judiciaire national, mais elles ne seront être isolées au stade des poursuites

Cas ukrainien (15$/jour – SMIC mensuel local 140$)

Source : Trustwave

(1) Un cas célèbre étant le Botnet issu du maliciel Mirai en 2016, ayant servi à des attaques DDos (Distributed Denial of Service) touchant notamment OVH et Dyn, cette dernière affectant une partie critique d'Internet au niveau de la gestion des services DNS (Domaine Name System).

(2) La doctrine américaine est différente à cet égard, au vu de l'activisme récent du Department of Justice (DoJ).

(3) Voir le cas d'Airbus en janvier 2019.

(4) https://www.cybermalveillance.gouv.fr/

SUITE P.16 ...

dans la mesure où l'exploitation des données du SID[6]-Cassiopée[7] s'effectue principalement par le biais de la NATAFF, nomenclature d'enregistrement des procédures à l'arrivée au parquet[8].

La future plateforme THESEE[9] (projet porté par le Ministère de l'intérieur) est susceptible d'améliorer la connaissance statistique pour certains phénomènes de cybercriminalité. La récente loi de Programmation pour la Justice (LPJ) insère d'ailleurs de nouvelles dispositions afin d'encadrer la plainte en ligne[10].

• Le phénomène du « going dark »[11], massif en cybercriminalité

La libéralisation du chiffrement a contribué à améliorer sensiblement le niveau global de cybersécurité, mais a provoqué de manière collatérale des difficultés propres aux investigations judicaires. La banalisation des applications de messageries instantanées chiffrées avec des protocoles particulièrement robustes comme ceux dits *End to end* est un défi actuel pour le régime des interceptions judiciaires. De même, la généralisation du chiffrement de type *full disk* sur les terminaux informatiques, dont les ordiphones, a également rendu délicate l'exploitation forensique. Enfin, les architectures réseaux de type TOR (*The Onion Router*) participent à l'obfuscation des comportements criminels sur les *Darknets*.

Demain, la fusion annoncée entre les applications de messageries et les cryptoactifs ne manque pas d'inquiéter les professionnels[12].

UNE ORGANISATION JUDICIAIRE EN QUÊTE DE MATURITÉ

Seront ici abordés l'organisation judiciaire actuelle ainsi que les relations des acteurs judiciaires avec les acteurs de la cybersécurité.

Constats sur l'organisation judiciaire actuelle

Sans pouvoir détailler ici les multiples compétences territoriales de l'autorité judiciaire en matière de cybercriminalité, il sera souligné le rôle primordial du tribunal de grande instance de Paris bénéficiant depuis la loi du 3 juin 2016 d'une compétence concurrente nationale en matière d'atteintes aux STAD et crime de sabotage informatiqu[13].

Cette réforme a permis de consolider la création en 2015 d'une section dite « F1 » du parquet de Paris dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes. Les effectifs de cette section sont toutefois modestes[14]. Le constat est plus inquiétant au siège avec l'absence notamment de juge d'instruction véritablement spécialisé. Des dépêches de centralisation du traitement de certains phénomènes de cybercriminalité sont à relever, produites par la mission de lutte contre la cybercriminalité de la direction des affaires criminelles et des grâces (DACG) du ministère de la justice[15].

Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment liée à la criminalité organisée[16]. Une réflexion est également en cours concernant la pratique des « cyber-référents » dans les tribunaux.

Relations des acteurs judiciaires avec les acteurs de la Cybersécurité

L'administration centrale Direction des affaires criminelles et des grâces (DACG), via la mission précitée, participe aux travaux stratégiques du centre de coordination des crises cyber (C4), instauré suite à la Revue stratégique de Cyberdéfense de février 2018[17].

La DACG fait également partie du conseil d'administration du GIP (groupement d'intérêt public) ACYMA[18] (responsable du site internet cybermalveillance.gouv.fr), participe à plusieurs évènements de cybersécurité comme le Forum international de Cybersécurité (FIC), et collabore à divers groupes de travail interministériel, en liaison avec l'ANSSI[19].

La bataille contre la cybercriminalité ne peut se gagner seule et tous les acteurs impliqués doivent joindre leur effort. Le levier judiciaire doit gagner en maturité mais des progrès récents sont à souligner. La coopération internationale est aussi un facteur clé de ce succès, avec l'aide d'entités telles qu'EUROPOL, EUROJUST et INTERPOL. Sur le plan de l'accès à la preuve numérique, les yeux sont désormais tournés vers Bruxelles où se jouent en ce moment les négociations des futurs textes européens « E-EVIDENCE » ■

+ POUR EN SAVOIR PLUS

→ Revue stratégique de Cyberdéfense : http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

→ Etat de la menace cyber (rapport DMISC 2018) : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Etat-de-la-menace-liee-au-numerique-en-20182https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Etat-de-la-menace-liee-au-numerique-en-20182

→ Dispositif d'assistance aux victimes d'actes de malveillance : https://www.cybermalveillance.gouv.fr/

→ Plateforme PERCEV@L : https://www.service-public.fr/particuliers/vosdroits/R46526

.....

(5) « Nature de l'affaire » : codification utilisée lors de l'enregistrement au Bureau d'Ordre des tribunaux. L'enregistrement est en général fait par des agents du Bureau d'Ordre, et ne correspond pas à une qualification juridique fixée par un magistrat.

(6) SID : Système d'information douanier

(7) Cassiopée : Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants

(8) Seuls les postes NATAFF B81 *Entrée ou maintien irrégulier dans un système informatique* et B82 *Dégradation, destruction ou vol de données ou de fichiers informatiques*, correspondant aux atteintes aux STAD, sont susceptibles d'être exploités utilement, mais renvoient à une acception extrêmement étroite de la cybercriminalité.

(9) THESEE : Traitement harmonisé des enquêtes et des signalements d'e-escroqueries

(10) Nouvel article 15-3-1 du code de procédure pénale.

(11) Cette expression d'origine militaire fait référence à la perte soudaine des communications de l'adversaire pouvant être analysées, au profit de moyens de communications indétectables.

(12) Voir le lancement du réseau Telegram Open Network (TON) et la cryptomonnaie Gram par l'entreprise TELEGRAM, annoncé pour le dernier trimestre 2019, suite à une levée de fonds de 1,7 milliards de dollars.

(13) Nouvel art. 706-72-1 C. proc. pén.

(14) Actuellement deux magistrats, ainsi qu'un assistant spécialisé et un greffier.

(15) Dépêches des 10 mai 2017 et 22 juin 2018 concernant d'une part la mise en œuvre opérationnelle de la compétence nationale concurrente du parquet de Paris en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et le traitement judiciaire des «rançongiciels», et d'autre part la centralisation du traitement des «fraudes aux réparations informatiques».

(16) Ex : le démantèlement de la Main noire, une plateforme du Darknet.

(17) http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

(18) ACYMA : Action contre la cybermalveillance

(19) ANSSI : Agence nationale de la sécurité des systèmes d'information

ARTICLES ET CONFÉRENCES

Conférences

« *Going dark, going Cyber ? Enjeux et défis de la cybercriminalité et de l'accès aux données* »
16 mars 2018 - Conférence Data Institute de l'université de Grenoble Alpes
→ http://www.msh-alpes.fr/en/going-dark-going-cyber-enjeux-defis-cybercriminalite-acces-aux-donnees

« *Cloud Act, E-Evidence and Cross Border Access to Data* »
Conférence au Forum International de Cybersécurité (FIC 2019).
→ https://www.forum-fic.com/Data/Sites/16/fichiers/ARTOIS-A08-CloudAct.pdf?ts=1549558034

« *L'impact du chiffrement informatique dans les enquêtes pénales* »
Conférence AFDIT Sud-Est 2018, 4ème édition des journées du numériques
→ https://afdit-sud-est.com/videos-2018/

« *Actualités dans la preuve numérique à l'heure du Cloud* »,
Conférence organisée par le Parquet général d'Aix en Provence, 1er juin 2018

Articles parus ou en cours de publication

Article relatif à la conférence précitée du 1er juin 2018 d'Aix en Provence, dans la revue Dalloz IP/IT [en cours de publication]

Article relatif aux conséquences du RGPD au sein du ministère de la justice, dans la revue Dalloz IP/IT [en cours de publication]

Actes du séminaire « Cryptoactifs » organisé le 1er février 2019 (voir infra), revue Dalloz IP/IT [en cours de publication]

« *Les implications juridiques et technologiques post Safe Harbour* »Revue de la gendarmerie nationale, décembre 2016 (p14-20)
→ https://en.calameo.com/read/00271929281c96342ba48

Organisation de séminaire

« *Les Cryptoactifs : la justice pénale à l'épreuve des cryptomonnaies* »,
1er février 2019 (public de 150 personnes, organisation fermée et réservée à des acteurs régaliens)

« *Nanotechnologies, biotechnologies, informatiques et sciences cognitives (NBIC) : généalogie des enjeux de sécurité et de justice* »
Co-organisé avec l'Institut National des Hautes Etudes de Sécurité et de Justice (INHESJ) à l'automne 2017
→ voir p5 https://inhesj.fr/sites/default/files/RA_2017_INHESJ_2017ok.pdf

L'apport des Serious Games à la gestion de crise

Interview de Patrick RUESTCHMANN, président l'association Serious Games Network-France

Patrick RUESTCHMANN

Patrick Ruestchmann préside l'association Serious Games Network-France, organisateur du 1er Forum sur les serious games et le wargaming à l'Ecole Militaire. Il est game designer, participe à des revues françaises et étrangères sur le domaine et favorise l'usage des serious games pour la modélisation de systèmes complexes dans le secteur privé et celui de la Défense.

Il est aujourd'hui DGA du GIP Territoires Numériques BFC et intervient principalement sur le champ des politiques publiques numériques et plus particulièrement de l'open data (OpenData France). Son parcours croise des expériences dans la recherche appliquée (intelligence artificielle), dans les sphères privées et publiques et toujours au moyen de l'innovation par les usages. Il est auditeur de l'IHEDN (session nationale Politique de Défense, 68e).

Définition du « serious game » et du « wargame »

Les « serious games » ont l'ambition de faire travailler les professionnels sur des problématiques adaptés à leur contexte. L'objectif est de les sensibiliser, de les former et d'apporter une aide à la réflexion, souvent stratégique, sur des sujets au cœur de leurs préoccupations.
Il existe plusieurs types de « serious games », notamment les jeux vidéo. Dans les jeux manuels ou jeux de plateaux, on trouve la famille des wargames. Les wargames ont pour vocation de modéliser des conflits souvent militaires avec leurs composantes économiques et politiques. Ces conflits sont utilisés pour travailler les notions de prospection et de rétroaction sur un événement qui a été un combat ou une crise.
Les « serious games » sont des formidables outils d'aide à la formation et d'aide à la réflexion stratégique.

Quels sont les préjugés par rapport aux « serious games » ?

Le premier consiste à minorer leur utilité car ce sont « des jeux » et donc avec une composante récréative. Le deuxième consiste à critiquer la modélisation du problème, qui serait souvent trop simpliste pour être pertinente et permettre de travailler véritablement le sujet en profondeur.

Quelles sont les étapes importantes dans la conception des « serious games » ?

La conception d'un « serious game » commence toujours par les questions suivantes : quel est l'objectif pédagogique du jeu ? Avec qui va t'on travailler ? Pendant combien de temps et sur quel format ? Quel type de résultats attend-on de la modélisation ? On va systématiquement chercher à identifier quel est le bon moteur de jeu. Enfin, des experts mettront en place des scénarii et rentreront ces scénarii dans le moteur de jeu.

Est-ce que les « serious games » permettent de recueillir des data ?

Recueillir des informations, au cours ou à la fin d'un jeu, est une problématique sur laquelle nous sommes nombreux à travailler. Il est particulièrement intéressant de capter les comportements, les décisions ou l'enchainement des décisions des joueurs. En revanche, aujourd'hui on peut considérer qu'on n'a pas encore trouvé des méthodes suffisamment efficaces pour capter ces données efficacement. Néanmoins, les nouvelles méthodes de traitement de langage naturel, les techniques d'intelligence artificielle, pourraient permettre de capitaliser sur ce stock d'information.

Comment sont créés les plateaux de jeu ?

La création d'un plateau ou d'un jeu vidéo relève toujours de la même question : est-ce qu'on va s'adresser à un public du type comité exécutif ou à un public assez jeune dans son métier et qui va chercher des notions d'apprentissage ? En fonction de la réponse à ces questions, on trouvera le bon modèle. La création est assez large en la matière.

Il faut ensuite prêter une attention particulière à l'aspect, la forme, l'ergonomie du jeu qui doivent être attractifs.

Quels sont les acteurs que les « serious games » doivent cibler ?

Ce sont les décideurs qui vont pouvoir tirer le plus de valeur d'une séance, en s'interrogeant typiquement sur une stratégie économique, politique ou militaire.

Prenant l'exemple du Naval War College aux Etats Unis, tous les wargames déployés là-bas le sont au niveau des dirigeants d'une « *task force* », au niveau des amiraux, au niveau de la strate de commandement. Ce sont eux qui vont travailler le sujet d'une campagne ou d'une problématique, comme par exemple la logistique et ensuite tester les différents scenarii, les différentes approches en chambre pour ensuite se servir de cette expérience protégée sous une sorte de bulle, sur le terrain en phase de déploiement réel.

Faut-il proposer ce type de jeu en formation pour un public COMEX ?

Travailler avec un comité exécutif c'est souvent un des buts lorsqu'on crée un jeu pour répondre à une problématique de stratégie d'entreprise. En revanche, il faut convaincre les membres du COMEX de consacrer le temps nécessaire pour les séances. Un des intérêts majeurs des « serious games », est de changer de position ou de posture, de tester ses comportements et surtout de voir comment les acteurs interagissent entre eux. Le jeu permet que chacun sorte de sa zone de confort et de la posture sur laquelle il est attendu.

Faut-il proposer un « serious game » en rapport avec des crises réelles ou plutôt fictives ?

Il est préférable de travailler sur une crise fictive, mais similaire à une situation connue des différents joueurs.

En se projetant dans une crise fictive, il est plus facile de changer de posture. Rapidement, les joueurs laissent libre cours à leurs pensées et à leurs modes d'action sans être prisonniers de l'image qu'ils devraient avoir dans une crise réelle.

Dans « Résilience », un des jeux sur lequel j'ai travaillé, nous avons montré à quel point les politiques publiques que l'on déploie sur une année, ont un impact sur la cohésion sociale et sur la stabilité de la gouvernance. Les événements récents en France, le mouvement sociaux, en sont une bonne résonance. Très récemment, lors d'un forum, les joueurs ont été amenés à créer les cartes de l'évènement qui correspondent à ces mouvements sociaux, en l'occurrence, ici les gilets jaunes pour voir comment ces évènements ont un impact sur la cohésion sociale et sur la gouvernance.

En créant un scénario relativement fictif on peut progressivement y inclure des évènements réels, des évènements quotidiens qui correspondent à une crise. Cela permet à chaque joueur de mieux se rendre compte de l'impact potentiel, de ce qu'on appelle des « *what if* ».

Quelles sont les compétences que les « serious games » permettent de développer ?

Nous observons des comportements qui mettent en jeu des compétences de coopération, compétences d'écoute et des compétences relatives à l'agilité lorsqu'il s'agit de prendre des décisions dans un environnement incertain.

En quoi est-ce que les « serious games » permettent-ils de « penser autrement » ?

Penser autrement, c'est prendre un risque, c'est décaler sa position. Travailler dans une séance de jeu équivaut à travailler dans une sorte de bulle sécurisées laquelle on va prendre des décisions, avoir des interactions, des postures très variées, voir extrêmes par rapport à sa position habituelle, professionnelle. Ces décisions ne vont pas avoir de conséquences au-delà de la fin de la partie. Cette bulle protégée permet de changer probablement de comportement et finalement d'attitude.

Penser autrement c'est aussi changer de rôle. Il s'agit de changer de place et de se mettre dans une position où l'on essaie de mieux comprendre les limites, les contraintes, mais aussi les opportunités de l'autre acteur en face de moi dans la crise. Par exemple, avec l'Ecole de Guerre, nous avons travaillé sur la crise de Notre Dame des Landes. Nous avons demandé à des professionnels du maintien de l'ordre de se mettre plutôt dans la position du politique pour réagir à cette crise. On aurait très bien pu aussi leur demander de prendre la position de ceux qui occupaient la zone, les Zadistes, voir des extrémistes à l'intérieur de ce groupe de Zadistes. Depuis quelques temps, une modélisation du maintien de l'ordre en milieu urbain est d'ailleurs largement testée à l'initiative d'un Colonel de Gendarmerie[1] Ce changement de rôle une valeur très importante et un rendement aussi très important et bien plus efficace que trois heures devant une présentation pendant une conférence.

Une séance de jeu qui développe des compétences, finalement a pour objet d'aider à la prise de décision à chaud mais dans une bulle protégée.

Les « serious games » intègrent-ils la notion d'anticipation ?

Effectivement on peut chercher à travailler sur la prospective, par exemple un durcissement géopolitique (La Corée) ou le durcissement d'une situation sociale croisée avec des opérations de déstabilisation extérieure. La prospective se traduit dans un jeu par la création d'un ensemble de scenarii avec des paramètres qui sont suffisamment compréhensibles pour qu'on puisse inférer et travailler sur ces paramètres et les faire bouger et interagir.

La prospective dans un jeu permet aussi, à travers un scénario, de trouver quels sont les paramètres les plus influents, ceux dont la combinaison va donner des signes avant-coureurs d'une crise à venir.

Les « serious games » intègrent-ils la notion d'incertitude ?

L'incertitude dans un jeu peut prendre des formes extrêmement simples, comme l'aléa, à travers une séquence d'événements semi-aléatoires ou programmés ou l'aléa total, à travers un simple jet de dé. Il faut introduire l'incertitude dans le jeu car les choses ne se passent pas comme on a exactement prévu dans la vraie vie. L'aléa est un point important de toute décision.

L'aléa vient également de la réaction des autres joueurs et de l'interaction que l'on a durant une partie. En pratique, on est amené à prendre des décisions auxquelles on n'a absolument pas pensé, tout simplement parce que l'adversaire ou celui avec qui on va coopérer dans le jeu, prend des décisions que l'on n'a pas prévues. La combinaison de ces événements programmés ou non, l'aléa pur et dur et le déroulé de l'interaction dans la narration du jeu entre les acteurs, crée un ensemble qui traite de l'incertain.

Ce qui est intéressant est ensuite de voir comment la combinaison de ces paramètres peut être analysée. On retombe alors sur la question de la capture de ces données.

Si vous aviez un seul message à transmettre aux gestionnaires de crise, quel serait-il ?

Les crises amènent à prendre des risques et je dirais : « ***prenez le risque d'utiliser ces outils au sein de vos processus formels de formation à la gestion de crise*** ». C'est un complément dont la qualité du résultat est assez formidable ■

Entretien avec Patrick Ruestchmann, 27/11/2018

. . . . .

(1) Colonel Christophe Maresca

POINT DE VUE

FOCUS FACTEURS HUMAINS
L'EFFET TUNNEL
Errare humanum est… Perseverare diabolicum

par **Pierre Raynal,** *Docteur*

RÉSUMÉ

L'effet tunnel associe une focalisation de l'attention à une perte de vue d'ensemble de la situation. Bien connu en aéronautique, il a été incriminé dans de nombreux accidents d'avions. Les professionnels confrontés aux situations d'urgences telles que l'obstétrique, les urgences médico-chirurgicales, le maintien de l'ordre et les conflits armés peuvent également être soumis à cet effet tunnel et à ses conséquences pouvant être dramatiques si non anticipées, repérées et corrigées. Cet article propose de présenter le concept d'effet tunnel, ses conséquences, les théories cognitives associées et les solutions pour en sortir.

L'effet tunnel est appelé « tunnelisation attentionnelle » ou « fascination de la cible » par les spécialistes de l'aéronautique, ou encore « syndrome de persévération » en neuropsychologie [1] [2]. Si les appellations diffèrent, une sémiologie commune peut être dégagée et l'effet tunnel se définir comme « l'allocation de toute l'attention sur une information, une hypothèse particulière, une tâche unique, ceci pendant une durée qui dépasse l'optimal, ce qui entraine la négligence des autres informations, et l'échec d'autres tâches à effectuer » [3].

La persévération résulte d'une focalisation de l'attention sur l'action en cours afin de poursuivre cette tâche et résister aux éléments de distraction de l'environnement. Cependant face à des indices signalant un danger, l'attention doit pouvoir être désinvestie du but poursuivi pour redevenir réceptive aux signaux de l'environnement et mettre en place des comportements flexibles et adaptatifs. La persévération est le résultat de la résistance aux signaux d'alerte émis par l'environnement [4] [5].

Toute intervention humaine peut être associée à un effet tunnel dont les conséquences pourront éventuellement être dramatiques en fonction du contexte (conflits armés, urgences médico-chirurgicales, obstétrique …). L'aéronautique a été une discipline pionnière dans la prise en considération de ce piège cognitif ayant conduit à de nombreux accidents d'avions le plus souvent mortels. Un exemple typique est celui du vol EA401 de la compagnie Eastern Air Lines effectuant la liaison New York-Miami, qui s'écrasa dans les Everglades le 29 décembre 1972. L'incident initial survint alors que l'avion se trouvait en approche de l'aéroport international de Miami. L'équipage sortit le train d'atterrissage mais constata que la lumière verte signalant la sortie et le verrouillage du train était restée éteinte. Deux explications étaient alors possibles : soit le train n'était pas bien sorti, soit l'ampoule était grillée. Les pilotes effectuèrent de nouveau la manœuvre mais la lampe resta éteinte. L'équipage commis l'erreur de consacrer toutes ses ressources à ce seul problème sans se préoccuper de la tenue de vol de l'avion qui perdit progressivement de l'altitude pour finir par s'écraser moins de 10 minutes après la découverte de la lampe grillée. Sur les 176 personnes à bord, 101 périrent dans l'accident. L'enquête conclue en une succession d'erreurs humaines, avec un effet tunnel manifeste. Rares sont les disciplines ayant acquis une telle maturité dans l'analyse et la prise en compte des facteurs humains. Le monde de la santé, et celui de l'obstétrique en particulier, n'a commencé à prendre en considération ces éléments que depuis une petite dizaine d'années. Le monde de l'aviation représente un modèle intéressant dont les autres disciplines peuvent aisément s'inspirer. Ainsi les références au monde de l'aéronautique seront-elles nombreuses dans cet article sur l'effet tunnel du fait de son expérience acquise dans ce domaine au cours des dernières décennies.

BASES COGNITIVES DE LA PERSÉVÉRATION

Les activités telles que le pilotage d'avions, la réalisation d'anesthésie, d'interventions chirurgicales, d'accouchements… sont des activités pour lesquelles le processus évolue en permanence (déplacement des avions, état clinique du patient …), ce qui implique pour l'opérateur d'actualiser sa représentation de la situation en intégrant des données nouvelles, parfois incertaines ou incomplètes. Un des dangers de ces activités, d'autant si elles sont réalisées sous stress ou pression temporelle, est que l'opérateur soit mis dans l'incapacité de réviser de manière appropriée la représentation de la situation et de ses choix d'intervention. Dans ces cas de figure, l'opérateur est persuadé en toute bonne foi, que sa stratégie choisie initialement est et reste la bonne, mais il ne tient pas compte de la globalité des informations qui l'entourent ou il les nie inconsciemment, cela pouvant conduire à une erreur de fixation [6] [7]. La dangerosité de l'erreur de fixation est accrue si elle s'associe à des biais de confirmations consistant pour l'opérateur à sélectionner exclusivement les

informations confirmant son hypothèse tout en leur accordant une importance disproportionnée, et à rejeter celles n'étayant pas sa thèse [8] [9].

Une des explications admises pour expliquer ce phénomène d'effet tunnel avec erreur de fixation est la théorie des ressources limitées qui considère que l'opérateur n'est pas en capacité de traiter toutes les informations qui l'entourent. Seules les données pertinentes pour répondre aux exigences de la tâche seront retenues, les autres devenant des données auxiliaires négligées [10] [11]. Ce fonctionnement à l'économie est le plus souvent adapté et performant, mais il peut se révéler dangereux lorsqu'un opérateur filtre trop d'informations et ne relève pas la pertinence d'un nouveau problème, également lorsqu'il porte une trop grande attention à la résolution d'un problème en oubliant le processus dans sa globalité.

Pour Keyser et Woods, l'erreur de fixation correspond à une gestion inadaptée des mécanismes attentionnels, elle serait favorisée par la pression temporelle, le stress, la fatigue ainsi que la charge de travail [7].

La persévération est également le fruit d'un trouble de l'inhibition. L'opérateur se retrouve dans l'incapacité d'inhiber une stratégie et d'en engager une nouvelle pour répondre de manière adaptée aux sollicitations de l'environnement. Décider reflète d'une aptitude à choisir la meilleure stratégie, et sous-tend une capacité à inhiber celles qui ne sont pas adaptées. La dangerosité de la persévération est liée à son extrême robustesse par absence d'inhibition [12 ; 13].

Le monde de l'aéronautique a été sensibilisé à la problématique de la tunnelisation attentionnelle par le crash du vol AA- 1420 sur la piste de Little Rock en juin 1999 : l'équipage a persévéré dans sa tentative d'atterrissage à trois reprises malgré des orages violents une pluie diluvienne et des vents de côté avec effet de cisaillement, et en dépit d'une capacité en carburant qui permettait de se dérouter sur un aéroport sûr (10 passagers et le commandant de bord trouvèrent la mort dans cet accident). Suite à ce tragique accident, une étude portant sur 2000 approches en condition d'orage pour déterminer si le comportement de ces pilotes correspondait à une tendance généralisée en aviation, a révélé que deux tiers des équipages persévèrent dans un atterrissage en dépit des règles de sécurité, les spécialistes qualifiant ce genre de comportement de "fascination pour l'objectif" (Target Fascination) [14]. Une enquête française du Bureau Enquête Analyse (BEA) a révélé que plus l'incident (panne, dégradation de la météo...) se passe à proximité de l'aérodrome d'arrivée, plus il est difficile pour les pilotes de renoncer à atteindre la destination, c'est-à-dire qu'ils vont persévérer encore plus intensément pour s'y rendre en dépit de la règlementation aérienne [2]. Cette proximité du but terminal est un facteur de persévération et de focalisation qui réduit le champ attentionnel en empêchant de percevoir les informations qui signalent l'inadéquation de la procédure et du but poursuivi [4].

Les résultats du BEA sur la tendance des pilotes à persévérer à proximité de leur destination finale sont en continuité avec ceux de Beauvois et Joules [15] qui révèlent que plus le coût (durée, argent, effort physique ou psychologique) de l'engagement est fort, plus il est difficile de renoncer à un objectif que l'on s'est fixé.

CÉCITÉ ET SURDITÉ INATTENTIONNELLES

Plusieurs auteurs ont démontré le phénomène de « l'escalade d'engagement », qui traduit la tendance que manifestent les individus à s'accrocher à leur première décision même lorsqu'elle est clairement remise en cause par les faits [15-17]. Cependant, il n'est pas toujours possible pour l'opérateur d'avoir une connaissance consciente de ces faits. Des expériences réalisées en simulateur de vol ont démontré que la tunnelisation attentionnelle pouvait conduire les pilotes dans une incapacité à dégager leur attention et ne plus être sensibles aux alarmes visuelles et auditives, et cela dans près d'un tiers des cas du fait d'une cécité et une surdité inattentionnelle [18-20]. Dans un état de tunnelisation attentionnelle, on peut regarder sans « voir », et entendre sans « écouter ».

Ainsi, le signal « proximité sol » n'a pas été écouté par le pilote lorsqu'un Dash 8 de la Lufthansa en provenance de Brême s'est écrasé à l'atterrissage à Roissy en 1993, tout comme ont été ignorées car non écoutées les alarmes de dépressurisation du Boeing 737 qui s'est écrasé près d'Athènes en 2005 [21].

Un autre élément d'explication du phénomène de surdité inattentionnelle est de considérer que les situations critiques mobilisent tellement l'attention de l'opérateur qu'il leur devient très difficile d'intégrer des données supplémentaires comme l'apparition d'une alarme. Une étude menée avec des pilotes d'avion a constaté qu'ils ne percevaient pas en moyenne 30 % des alarmes auditives lorsque ces dernières se produisaient pendant des conditions de pilotage complexe. Ce taux de surdité était d'environ 20 % lors d'un pilotage en difficulté moyenne, et tombait à 3 % lors d'une situation de contrôle simple. Cette étude a par ailleurs bien montré l'incapacité du son à franchir la barrière attentionnelle lorsque le pilote est trop mobilisé par la tâche de pilotage [22-24]. Cette surdité inattentionnelle peut en partie être expliquée par l'existence de mécanismes naturels de sélectivité qui favorisent le traitement des informations visuelles au détriment des informations auditives. La vision focalisée peut « éteindre » ou tout du moins atténuer précocement l'activité du cortex auditif (dans l'exemple d'un freinage d'urgence, il est impossible pour le conducteur de continuer à écouter les passagers ou la radio, il se concentre sur les informations visuelles qui sont les seules pertinentes pour éviter la collision) [23].

LA THÉORIE DE L'ENGAGEMENT

Un mécanisme principal associé au comportement de persévération émerge : l'engagement de l'opérateur dans sa mission. La théorie de l'engagement traduit la tendance pour un individu à « s'accrocher » au premier acte dans lequel il s'est engagé même lorsque celui-ci est par la suite remis en cause par les faits. Le caractère engageant d'un acte est d'autant plus marqué qu'il est publique et répété [25].

ENGAGEMENT ; DÉSENGAGEMENT ; RÉ-ENGAGEMENT : LES CONTRES-MESURES EXISTENT

Pour lutter contre ce phénomène de tunnelisation attentionnelle, des contre-mesures ont été développées pour per-

SUITE P.22 ...

mettre à un opérateur de sortir de sa tâche principale et retrouver une vision globale de la situation. Dans le monde de l'aéronautique, le mécanisme est décrit en trois temps : engagement / désengagement / ré-engagement : le pilote s'engage dans sa mission (engagement) et du fait d'une pression temporelle, d'un stress ou d'une charge mentale importante se retrouve en situation de tunnelisation attentionnelle. Il convient alors de trouver une contre-mesure permettant au pilote de quitter rapidement cet état de tunnelisation attentionnelle (désengagement) pour mieux s'y ré-engager d'une autre façon et obtenir le succès de la mission (ré-engagement).

Historiquement l'approche adoptée par les avionneurs pour lutter contre la focalisation des pilotes consistait à ajouter des systèmes d'alerte ou à augmenter la saillance des alarmes pour mobiliser et attirer l'attention du pilote. Si elle semblait être de bon sens et efficace en théorie, cette démarche s'est révélée contre-productive parce qu'elle a échoué à provoquer le désengagement attentionnel, la charge mentale des pilotes était trop élevée pour analyser de nouvelles informations [23].

Fort de ce constat, des contre-mesures cognitives ont été proposées : supprimer temporairement les informations sur lesquelles se concentre l'opérateur humain pour les remplacer par l'alarme négligée. L'idée est que l'interface utilisateur agisse comme une prothèse cognitive facilitant le désengagement puis le réengagement de l'attention des pilotes. Ce principe a été testé avec succès dans plusieurs expérimentations dans la recherche en aéronautique : un essai impliquait des pilotes de drones qui devaient identifier une cible avec une caméra. Les opérateurs étaient tellement fascinés par leur objectif qu'ils ne percevaient pas une panne de batterie de leur drone pourtant signifiée par trois alertes visuelles. L'extinction de la caméra pendant une seconde avec affichage à la place d'une icône représentant une batterie épuisée a permis aux pilotes de rediriger aussitôt leur attention vers le problème technique et enclenché les actions attendues [23].

Dans le cas d'une intervention sur le terrain (zone de combat, salle de naissance, bloc opératoire) un désengagement peut se faire grâce à l'intervention d'un membre de l'équipe, grâce au collectif. Il convient alors d'annuler la focalisation du regard du professionnel, en interposant un élément entre le regard de l'opérateur et son objet de focalisation (par exemple sa main). Cette intervention rapide et simple permet au professionnel de reprendre une vision globale de la situation, et ainsi se réengager dans sa prise en charge avec une possibilité de décision d'abandon de l'option initiale pour une autre option plus adaptée.

Dans ce cas, le désengagement peut être anticipé grâce à plusieurs mécanismes : en premier lieu une formation des équipes à la connaissance du concept d'effet tunnel, en second lieu par un échange initial systématique (briefing) au sein de l'équipe permettant de partager la même conscience de la situation. Dans le monde de l'aéronautique, les résultats d'une étude dont le but était de déterminer l'impact de la charge de travail sur la performance des équipages en simulateur de vol, ont permis de mettre en évidence que la qualité des interactions entre les membres d'équipages avait plus d'impact sur la performance que les compétences techniques individuelles des pilotes, et que le nombre d'informations échangées était négativement corrélé avec le nombre d'erreurs commises [25]. Plus récemment, une autre étude sur simulateur de vol a permis de montrer que les équipages les plus performants sont ceux qui cherchent à clarifier la situation en posant des questions et qui verbalisent plus fréquemment les actions en train d'être réalisées [26].

Dans le domaine médical, des résultats similaires ont été observés. Dans une étude menée par Halverson en 2010, il a été constaté avant toute formation sur la communication en équipe, 56 erreurs de communication au cours de 76 heures d'activité au bloc opératoire. Ce chiffre est passé à 20 erreurs de ce type sur 74 heures après cette formation [27]. Une étude menée sur 10 interventions chirurgicales complexes a révélé que les erreurs de communication étaient associées à un impact négatif sur la sécurité du patient et sur la performance de l'équipe de bloc opératoire [28]. La majorité des défaillances de communication observées sont la non-transmission d'une information pertinente, la transmission d'une information non pertinente et la transmission trop tardive d'une information pertinente [29].

Par ailleurs, l'effet tunnel se moquant de la hiérarchie, tout professionnel impliqué dans la mission doit avoir la certitude de pouvoir intervenir en cas de constat de dysfonctionnement d'un collègue, et ce quel que soit son grade. Cela suppose au sein de l'équipe une confiance et une approche solidaire. Une telle démarche n'est pas toujours aisée du fait d'un fort gradient d'autorité pouvant exister. Il s'agit là d'un élément de culture et de maturité d'une équipe ayant à cœur d'intégrer les facteurs humains dans la prise en charge des situations critiques. La littérature aéronautique décrit des cas symptomatiques de persévération chez des équipages constitués d'un commandant de bord présentant un égo important, et d'un copilote novice. Dans ces situations le pilote expérimenté commet une erreur grave qu'il s'entête à ne pas reconnaître afin de ne pas perdre la face. De son côté le copilote soumis, soucieux de ne pas critiquer un chef prestigieux, n'osera pas relever l'erreur, ou n'osera pas insister. Cet état de statu quo, s'il n'y a pas l'intervention d'un tiers (le contrôleur aérien) peut se terminer par la perte de l'appareil et parfois de l'équipage [30-32]. Dans le monde de l'aéronautique, du fait de plusieurs accidents dramatiques, ce gradient d'autorité a été efficacement atténué grâce à la mise en place de formations systématiques et obligatoires des équipages au CRM (Crew Ressource Management) [33].

James Reason dit à propos de l'erreur humaine qu'elle est le revers inéluctable de nos processus mentaux [34]. L'effet tunnel illustre parfaitement ce discours, il constitue un véritable piège tendu aux professionnels travaillant en situation d'urgence, de conflits, comme peut l'être le monde de l'armée, celui de l'obstétrique et de la chirurgie. La sortie d'une tunnelisation attentionnelle est complexe et ne peut se faire que grâce à l'intervention d'un autre membre de l'équipe, grâce au collectif. Cette intervention salvatrice ne peut s'envisager que si les professionnels de l'équipe ont connaissance de ce concept, et ont été formés à sa gestion, et qu'une communication pertinente avec briefing et débriefing est culturellement développée. Seule une réelle confiance au sein de l'équipe peut permettre de passer outre un gradient d'autorité, et permettre au professionnel de se désengager d'une stratégie devenue dangereuse pour mieux se réengager dans une autre approche moins risquée et plus adaptée ■

BIBLIOGRAPHIE

[1]. H. Levine, H. Einsenberg, A. Benton
Frontal lobe function and dysfunction. 1991. Oxford University Press.

[2]. Bureau Enquête Accident. Objectif : destination. Technical report. 2000 http://www.bea-fr.org/francais/rapports/rap.htm.

[3]. Wickens. C.D
Attentional tunneling and task management (Tech. Rep. AHFD-05-23/NASA).Savoy, aIL: University of Illinois, Institute of Aviation.2005.Aviation Human Factors Division.

[4]. Richard. J.-F
L'intelligence comme plasticité à l'environnement.
In L. Lautrey & J.-F. Richard (Eds.). 2005. L'intelligence. Paris: Lavoisier.

[5]. Richard. J.F
Editorial.
Psychologie Française 2003;48:1-2

[6]. J. Cellier
L'erreur humaine dans le travail. 1990. In Les facteurs humains de la fiabilité, Leplat J., Terssac G. de (eds). Paris, Octares entreprises.

[7]. D. Keyser, D. Woods
Systems Reliability Assessment, chapter Fixation errors in dynamics and complex systems. 1990. Kluwer Academic Press

[8]. Nickerson, R. S.
Confirmation bias: A ubiquitous phenomenon in many guises.
Review of General Psychology 1998; 2:175-220.

[9]. Fiedler, K.
Voodoo correlations are everywhere - Not only in neuroscience.
Perspectives on Psychological Science 2011; 6:163-71.

[10]. D. Broadbent
Perception and Communication.1958. New York, Pergamon Press.

[11]. Spérandio. J
Phénomènes régulatoires associés aux variations de la charge de travail chez les contrôleurs de trafic aérien. 1975. In L. A. et al. editor, Age et contraintes de travail. NEB, Paris.

[12]. Bourgeon. L
Mécanismes cognitifs et rôle du collectif dans la persévération : gestion d'évènements imprévus dans l'activité de pilotage militaire. 2011. Thèse de doctorat.

[13]. Rhoda. D, Pawlak. M
An assessment of thunderstorm penetrations and deviations by commercial aircraft in the terminal area. 1999. Technical report, M.I.T.

[14]. Beauvois. J, Joule. R
A radical point of view on dissonance theory. In E. Harmon-Jones et J. Mills, editors, Cognitive Dissonance: Progress on a Pivotal Theory in Social Psychology.1999. Washington DC: A.P.

[15]. Festinger. L
A theory of cognitive dissonance. 1957. CA : Stanford University Press

[16]. Heckhausen. J, Heckhausen. H
Motivation and action: Introduction and overview. In J. Heckhausen; H. Heckhausen. 2010. Motivation and action. Cambridge University Press.

[17]. Simons. DJ, Chabris CF
Gorillas in our midst : sustained inattentional blindness for dynamic events. Perception 1999; 28:1059-74.

[18]. Pappas. JM, Fishel. SR, Moss. JD, Hicks. JM, Leech. TD.
Eye tracking approach to inattentional blindness ; Proceedings of the human factors and ergonomics. Society annual meeting 2005;17:1658-62

[19]. Cartwright-Finch. U, Lavie. N
The role of perceptual load in inattentional blindness.
Cognition, 2007;102:321-40

[20]. Durlach. PJ, Kring. JP, Bowens. LD
Effects of action video game experience on change detection.
Military psychology 2009; 21;24-39.

[21]. Dehais. F, Tessier. C, Chaudron. L
GHOST: experimenting conflicts countermeasures in the pilot's activity
2003 Proceedings of the 18th Joint Conference on Artificial Intelligence

[22]. Dehais. F, Tessier. C, Christophe. L, Reuzeau. F
The perseveration syndrome in the pilot's activity: Guidelines and cognitive countermeasures.
Lecture Notes in Computer Science 2010; 5962:68-80.

[23]. Dehais. F, S. Mercier, C. Tessier
Conflicts in Human Operator–Unmanned Vehicles Interactions
Engineering Psychology and Cognitive Ergonomics 2009; 7:498-507

[24]. Dehais. F
Modélisation des conflits dans l'activité de pilotage. Thèse de doctorat de sciences cognitives, Ecole Nationale Supérieure de l'Aéronautique et de l'Espace Toulouse. 2006

[25]. Ruffel-Smith. H. P.
A simulator study of the interaction of pilot workload with errors, vigilance, and decisions (NASA Technical Memorandum 78482). Moffett Field, CA: NASA-Ames Research Center. 1979

[26]. Mjøs. K
Communication and operational failures in the cockpit.
Human Factors and Aerospace Safety 2001; 1:323-340.

[27]. Halverson. A. L, Casey. J. T, Andersson. J, Anderson. K, Park. C, Rademaker. W Communication failure in the operating room. Surgery 2011;149:305-10

[28]. Christian. C. K, Gustafson. M. L, Roth. E. M, Sheridan. T, Gandhi. T. K, Dwyer. K
A prospective study of patient safety in the operating room.
Surgery 2006; 139:159-173.

[29]. Lingard. L, Espin. S, Whyte. S, Regehr. G, Baker.G, Reznick. R,
Communication failures in the operating room: an observational classification of Recurrent types and effects.
Quality and Safety in Health Care 2004; 13:330-334

[30]. Morel. Ch
Les décisions absurdes. Sociologie des erreurs radicales et persistantes.
Bibliothèque des sciences humaines. 2002. Ed Gallimard

[31]. Grau. Y
Aspects médico-psycho-physiologiques des évènements aériens au cours de l'année 1993. Technical report, 1994, IMASSA, Brétigny.

[32]. Grau. Y
Aspects médico-psycho-physiologiques des évènements aériens au cours de l'année 1994. Technical report, 1995, IMASSA, Brétigny.

[33]. Le Crew Ressource Management (CRM) S Nivet - HEGEL [ISSN 2269-0530], 2014, 01, 75-782014 - documents.irevues.inist.fr

[34]. J. Reason
Human error.
1990. Cambridge University Press.

Docteur Pierre RAYNAL

Praticien Hospitalier
Gynécologue/Obstétricien
Référent en Obstétrique
Médecin coordonnateur de la gestion des risques associés aux soins - Médecin médiateur - Centre Hospitalier de Versailles
Formateur en simulation en santé - DU Facteurs Humains en Aéronautique
Expert CRM (Crew Ressource Management) HAS (Haute Autorité de Santé)
Expert RMM (Revue Morbi-Mortalité) ARS IDF (Agence Régionale de Santé Ile De France)

RECHERCHE

PROJET APRIL

Optimiser l'Anticipation et la Prise de décision en situation de crises extrêmes pour maintenir la RésiLience de la société

Confrontés à des situations de crise de plus en plus nombreuses, complexes et hors normes, faisant peser des risques sur les populations et leurs activités, les gestionnaires de crise sont confrontées à un défi majeur : Comment optimiser l'anticipation et la prise de décision en contexte d'incertitude afin de permettre une meilleure résilience des territoires et des sociétés ?

Dans ce cadre, l'Agence Nationale de la Recherche (ANR) a lancé un appel d'offre intitulé : « OURAGANS 2017 : Catastrophe, Risques et Résilience »[1]. Le Projet APRIL a été sélectionné. APRIL est un projet de recherche-action de 36 mois (début 1 Juin 2018).

PARTENAIRES

INHESJ : Institut National des Hautes Études de la Sécurité et de la Justice, représenté par Cheila DUARTE COLARDELLE

BRGM : Bureau de Recherches Géologiques et Minières, représenté par Sophie LECACHEUX

LATTS : Laboratoire Techniques, Territoires et Sociétés, représenté par Valérie NOVEMBER

EFH : Ecole Française de l'Heuristique, représentée par Frédéric LE BIHAN

OBJECTIFS

APRIL poursuivra deux grandes finalités :

1. Capitaliser l'expérience d'IRMA, JOSE et MARIA afin d'apporter des recommandations pratiques visant à optimiser la capacité d'analyse, d'anticipation et de prise de décision des acteurs pendant toute la temporalité d'une crise majeure.

2. Créer des outils d'aide à la décision appréciant les différentes composantes de la vulnérabilité d'un territoire, les incertitudes et permettant d'anticiper des mesures transversales de protection et de remédiations afin d'optimiser la résilience du territoire.

TRAVAIL EN COURS

Une partie de l'équipe APRIL, Cheila DUARTE COLARDELLE et Elie CHEVILLOT MIOT – INHESJ ; Ingrid CANOVAS – LATTS, s'est déplacée aux Antilles entre le 11 Mars et le 14 Avril 2019.
L'équipe APRIL analysera le processus de prise de décision et comportement des acteurs de la sécurité civile et de la gestion de crise. Tous les échelons du dispositif ORSEC seront considérés depuis la commune jusqu'au niveau national interministériel. Les missions terrain se poursuivront en 2020 et en 2021. ■

De gauche à droite : Cheila DUARTE COLARDELLE, Elie CHEVILLOT MIOT et Ingrid CANOVAS – LATTS

APRIL

POUR EN SAVOIR PLUS

→ https://anr.fr/Projet-ANR-18-OURA-0001

POUR NOUS ÉCRIRE

→ april@inhesj.fr

(1) http://www.agence-nationale-recherche.fr/informations/actualites/detail/lancement-de-lappel-ouragans-2017-catastrophe-risque-et-resilience/

3ÈME ÉDITION
DU PRIX DE LA RECHERCHE INHESJ

L'Institut national des hautes études de la sécurité et de la justice, en partenariat avec le ministère de l'Enseignement supérieur et de la Recherche, à lancé la campagne de candidatures pour la 3ème édition du Prix de thèse de l'INHESJ 2019.

Le prix vise à distinguer une thèse en sciences humaines et sociales ou en droit portant sur les thématiques de sécurité et de justice. Il s'inscrit pleinement dans la dynamique de décloisonnement entre le monde opérationnel – notamment des forces de l'ordre et des juridictions – et le monde de l'université et de la recherche.

CALENDRIER PRÉVISIONNEL

1er janvier – 31 mars :
réception des candidatures

1er avril – 15 avril :
détermination des thèses éligibles en conformité avec les modalités de candidature

16 avril – 31 août :
lecture des thèses éligibles par les jurés

début septembre :
réunion du jury – sélection de trois thèses sélectionnées

septembre – novembre :
lecture des thèses sélectionnées par les jurés

fin novembre :
réunion du jury – désignation de la thèse primée

décembre 2019 :
cérémonie de remise du prix

CONTACT

→ prix-recherche@inhesj.fr

POUR EN SAVOIR PLUS

→ https://inhesj.fr/evenements/tous-les-actualites/prix-de-la-recherche-inhesj-2019-appel-candidatures

FORMATION

7e SESSION NATIONALE « MANAGEMENT STRATÉGIQUE DE LA CRISE » 2019 – 2020

La septième session nationale spécialisée « Management stratégique de la crise » débutera en septembre 2019.

Cette formation d'excellence a pour objectif de permettre aux participants de mettre en place dans leurs structures une politique efficace de gestion des risques et de réponse aux crises.

ORGANISATION DE LA SESSION

✓ Des séminaires mensuels

Leur progression vise à couvrir tous les champs du processus de crise, de la prévention au retour à la normale. Cet objectif intègre l'enjeu majeur d'une coopération et d'une coordination entre pouvoirs publics et acteurs privés.

✓ Des grands témoins

Tout au long de l'année, les séminaires associent de nombreux intervenants qui partagent leurs savoir-faire et leurs expériences sur de nombreuses crises nationales et internationales. Ils échangent avec les auditeurs et apportent leurs conseils pour définir des stratégies et mettre en place une culture de crise pérenne.

✓ Des exercices de crise

Les installations techniques du centre de formation à la gestion de crise du département « Risques et Crises » sont utilisées pour les exercices de mise en situation. Les auditeurs sont ainsi immergés dans des situations de crise réalistes permettant d'appréhender les contraintes de la prise de décision en environnement complexe.

✓ Des visites de centres opérationnels

Elles sont organisées dans des structures nationales (ministérielles, régionales...) ou au sein de sièges de grandes entreprises.

✓ Des travaux de groupe

Les auditeurs sont répartis en plusieurs groupes de travail (GDS : groupes de diagnostic et de stratégies).

PUBLIC

Cette formation s'adresse principalement aux cadres d'entreprises ou du secteur public ayant en charge la gestion des crises ou étant appelés à participer au sein des cellules dédiées.

TÉMOIGNAGES D'ANCIENS AUDITEURS

Ecoute, dialogue, professionnalisme, bonne humeur : une véritable pause de bien-être dans un agenda pro.

La mixité privé/ public, donneurs d'ordres/ consultants a été un des facteurs du succès.

Très grande richesse grâce à des profils très différenciés avec des attentes complémentaires et étendues.

INFORMATIONS SUR LE SITE INTERNET DE L'INHESJ

Recrutement sur dossier :

Le dossier de candidature sera disponible sur le site de l'INHESJ

Renseignements et inscriptions :

Alexandre FOUCHARD

→ formationcrise@inhesj.fr

Tél : +33 (0)1 76 64 89 00 - Fax : +33 (0)1 76 64 89 44

AGENDA DU 22/01 → 25/04

Jeudi 13 Juin 2019
9h30

Les 30 ans de l'INHESJ

Colloque
"Prévenir, protéger, juger :
30 ans de sécurité et de justice

Assemblée nationale
Hôtel de Lassay, *Paris 7*

13-16 Août 2019

« Connections 2019 »

Conférences professionnelles
de Wargaming

Army War College in Carlisle, *PA, EUA.*

Pour en savoir plus : https://connections-wargaming.com/

12 et 13 Juin 2019

CoTer Numérique

Conférence francophone pour les acteurs des collectivités territoriales qui s'engagent dans une démarche de « développement intelligent urbain ». Thématique : La Sécurisation des données personnelles »

Troyes

Pour en savoir plus : https://www.business-geografic.com/fr/actualites/evenements/1767-congres-du-coter-numerique-juin-2019.html

03-05 Septembre 2019

« Connections UK 2019 »

Conférences professionnelles
de Wargaming

King's College London, *Grande Bretagne.*

Pour en savoir plus : http://professionalwargaming.co.uk/

18-21 Septembre 2019

La 126e édition du Congrès national des sapeurs-pompiers de France

Vannes - Morbihan (56)

Pour en savoir plus :
https://www.pompiers.fr/agenda/congres-national-des-sapeurs-pompiers-2019-vannes
https://congres2019.pompiers.fr/

23 Septembre 2019

Sommet Climat des Nations Unies 2019 : 'A Race We Can Win. A Race We Must Win'

Siège des Nations Unies, New York

Pour en savoir plus : https://www.un.org/fr/climatechange/

LIREC

ABONNEZ-VOUS À NOTRE LETTRE

www.inhesj.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

DÉPARTEMENT RISQUES ET CRISES