Groupement National pour la Prévention des Risques professionnels dans l'Enseignement Supérieur

Comment anticiper les vulnérabilités liées à la mise en place de Zones à Régime Restrictif : proposition d'un outil d'analyse.

Accélérateur de talents pour l'industrie du futur

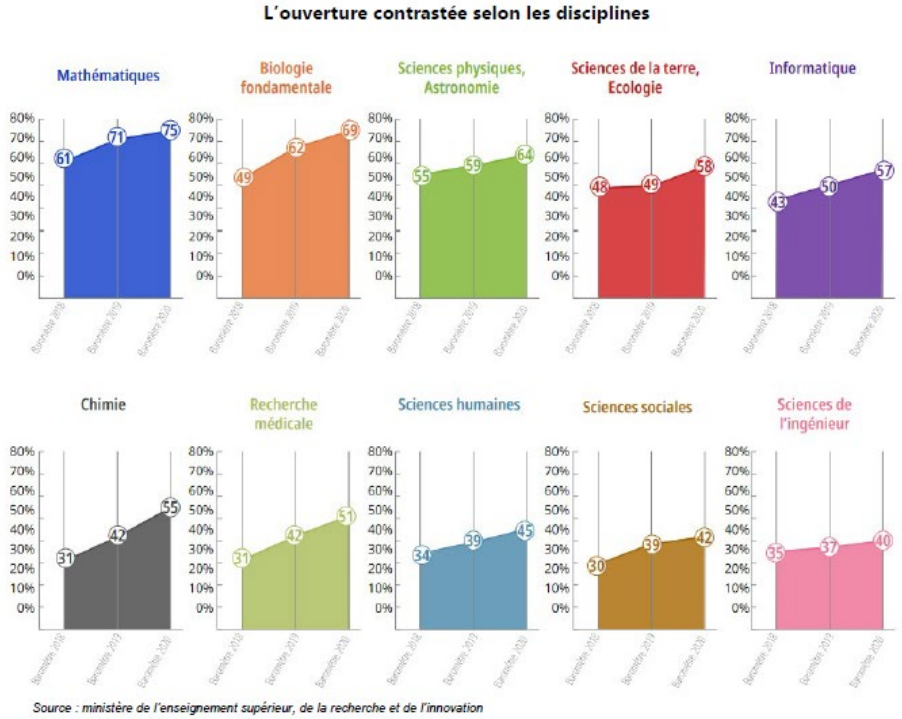
Eric Bertrand – FSD

Arts et Métiers Sciences et Technologies

Sujet de controverse

Arts et Métiers Sciences et Technologies

Science ouverte réaliste, équilibrée et respectueuse de la liberté académique



Dualité… ou force du système ?

Article 410-1 : Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel. **Version en vigueur depuis le 01 mars 1994**

Article L952-2 : Les enseignants-chercheurs, les enseignants et les chercheurs jouissent d'une pleine indépendance et d'une entière liberté d'expression dans l'exercice de leurs fonctions d'enseignement et de leurs activités de recherche, sous les réserves que leur imposent, conformément aux traditions universitaires et aux dispositions du présent code, les principes de tolérance et d'objectivité. Les libertés académiques sont le gage de l'excellence de l'enseignement supérieur et de la recherche français. Elles s'exercent conformément au principe à caractère constitutionnel d'indépendance des enseignants-chercheurs. **Version en vigueur depuis le 27 décembre 2020**

Introduction

Dans un contexte global, mondialisé et très concurrentiel, l'intelligence économique consiste à collecter, analyser, valoriser, diffuser et protéger l'information économique stratégique ou les savoirs, afin de renforcer la compétitivité d'un État, d'une organisation ou d'un établissement de recherche entraînant de ce fait une prise de conscience de l'ensemble des opérateurs sur l'impact de la diffusion de l'information et des savoirs.

Pour mieux protéger notre économie au sens large, l'État, par une circulaire du Premier ministre en date du 15 septembre 2011 (n°5554/SG)2, précise sa nature, ses objectifs et les principales orientations de l'État en la matière, sous la responsabilité de la délégation interministérielle de l'intelligence économique afin de protéger les savoirs et /ou savoir-faire et l'économie en France.

Principaux axes de l'action de l'État :

- Assurer la veille stratégique
- Soutenir la compétitivité des organisations et des établissements de recherche
- Garantir la sécurité économique des organisations et des établissements de recherche

Contexte réglementaire

Circulaire n° 3415/SGDSN/AIST/PPST du 7 novembre 2012

- Économique (risque de porter atteinte aux intérêts économiques de la nation)
- Défense (risque de renforcer des arsenaux militaires étrangers ou d'affaiblir les capacités de défense de la nation)
- Prolifération (risque de contribuer à la prolifération des armes de destruction massive et de leurs vecteurs)
- Terrorisme (risque de favoriser des actes terroristes sur le territoire national ou à l'étranger

L'Arrêté du 30 novembre 2011 portant approbation de l'Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

- la portée et le fondement de la procédure d'habilitation
- les différents types de procédure
- le déroulement des dites procédures
- les décisions qui s'en suivent
- le cycle de vie de la décision d'habilitation,
- et enfin la formation et la sensibilisation de la personne habilitée
- les mesures de sécurité applicables aux personnes morales,
- la sécurité des lieux,
- la sécurité des systèmes d'informations classifiés
- et la gestion des informations et supports classifiés tout au long de leur cycle de vie.

Le **dispositif de protection du potentiel scientifique et technique de la nation** (PPST) qui a pour objectif de lutter contre les tentatives de captation ou de détournement des savoirs, savoir-faire et technologies sensibles ayant trait aux intérêts fondamentaux de notre pays.

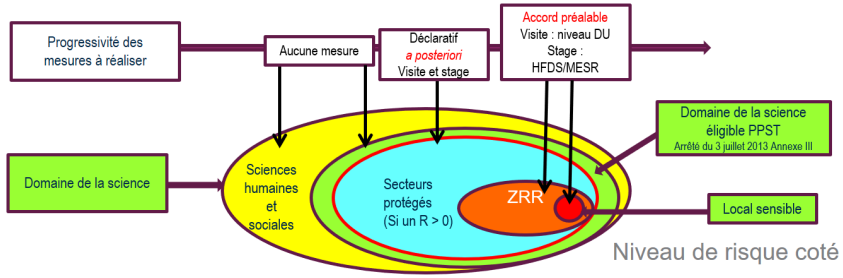
Principes

- Principes de la PPST
  - L'affirmation que la science fait partie des intérêts fondamentaux de la Nation
  - Cadre juridique fort permettant de rendre justice à l'équipe de recherche
  - Permets de protéger les accès virtuels et physiques
  - S'appliquent à toutes les personnes, quelle que soit leur nationalité
  - Concerne aussi toute action de coopération

PRINCIPES DE LA PPST : CRÉER UN ESPACE DE CONFIANCE

- L'affirmation que la science fait partie des intérêts fondamentaux de la Nation
- Cadre juridique fort permettant de rendre justice à l'équipe de recherche
- Permet de protéger les accès virtuels et physiques
- S'applique à tous les personnes quelle que soit leur nationalité
- Concerne aussi toute action de coopération

- R1 = atteintes aux intérêts économiques
- R2 = atteintes aux capacités de défense
- R3 = prolifération
- R4 = terrorisme



Niveau de risque coté de 0 à 3

Source : FSD - CNRS

Nature de la ZRR (par rapport à l'unité de recherche accueillante)	Couverture physique totale	Couverture physique partielle ou morcelée
Couverture thématique totale	unité « ZRR globale »	unité « ZRR intégrale »
Couverture thématique partielle		unité « ZRR partielle »

Objectifs et enjeux

La compétitivité, la notoriété ou l'excellence d'un établissement reposent notamment sur sa capacité d'innovation, ainsi que sur le développement et l'entretien de ses savoirs et savoir-faire.

Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) a pour but de protéger, au sein des établissements publics et privés, ses savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qui concourent aux intérêts souverains de la nation.

Le dispositif PPST offre une protection juridique et administrative fondée sur le contrôle des accès aux informations stratégiques ou sensibles détenues.

Les services compétents des ministères de rattache ment des établissements participent à ces contrôles qui concourent activement à la prévention des risques de captation et/ou de détournement.

Présentation des missions du fonctionnaire de défense (FSD)

Les FSD sont par conséquent des relais fonctionnels du haut fonctionnaire de sécurité défense au sein d'une entité comme un établissement de l'enseignement supérieur ou organisme de recherche.

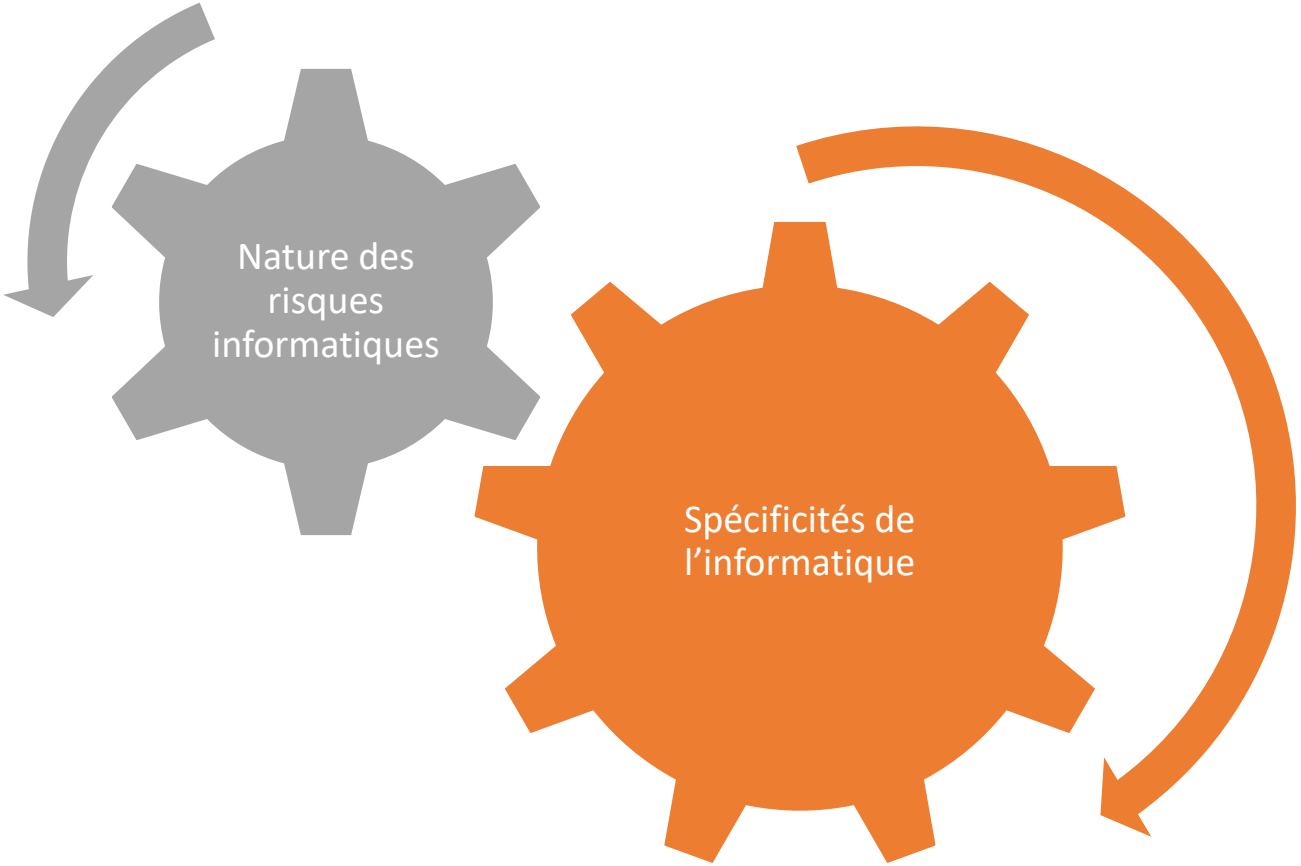
Participer à la protection du patrimoine de la nation et la défense des intérêts fondamentaux de la nation dans l'accompagnement des activités de recherche

Participer à la protection du secret de la défense nationale, qui constitue une cible majeure pour les services étrangers, les groupements subversifs ou les individus isolés cherchant à déstabiliser l'État des institutions ou la société. La protection des informations s'applique à tous les secteurs sensibles de la vie (politique, militaire, diplomatique, scientifique, économique, industrielle…) de la nation

Participer au déploiement des principes d'intelligence économique notamment pour développer en lien avec l'industrie la recherche pouvant avoir un fort potentiel stratégique pour la nation. C'est pour cette raison que le FSD est particulièrement attentif à la valeur économique créée dans les unités de recherche

Participer à la protection des personnes dans le cadre d'avis sur les missions à l'étranger, sur la vie des stages à l'étranger et dans la prévention de la radicalisation

RISQUES INFORMATIQUES

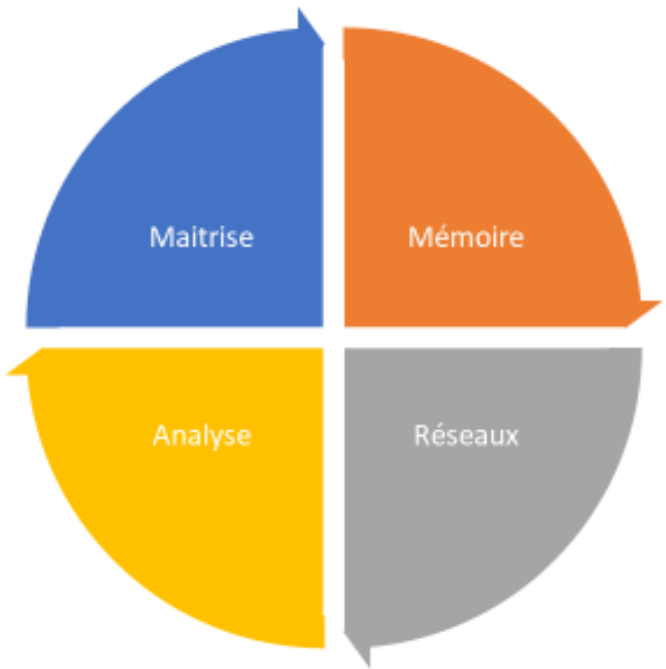


L’intelligence des risques

Vision

Connexion

L’intelligence collective



Action

Quelle est la différence entre digital et numérique ?

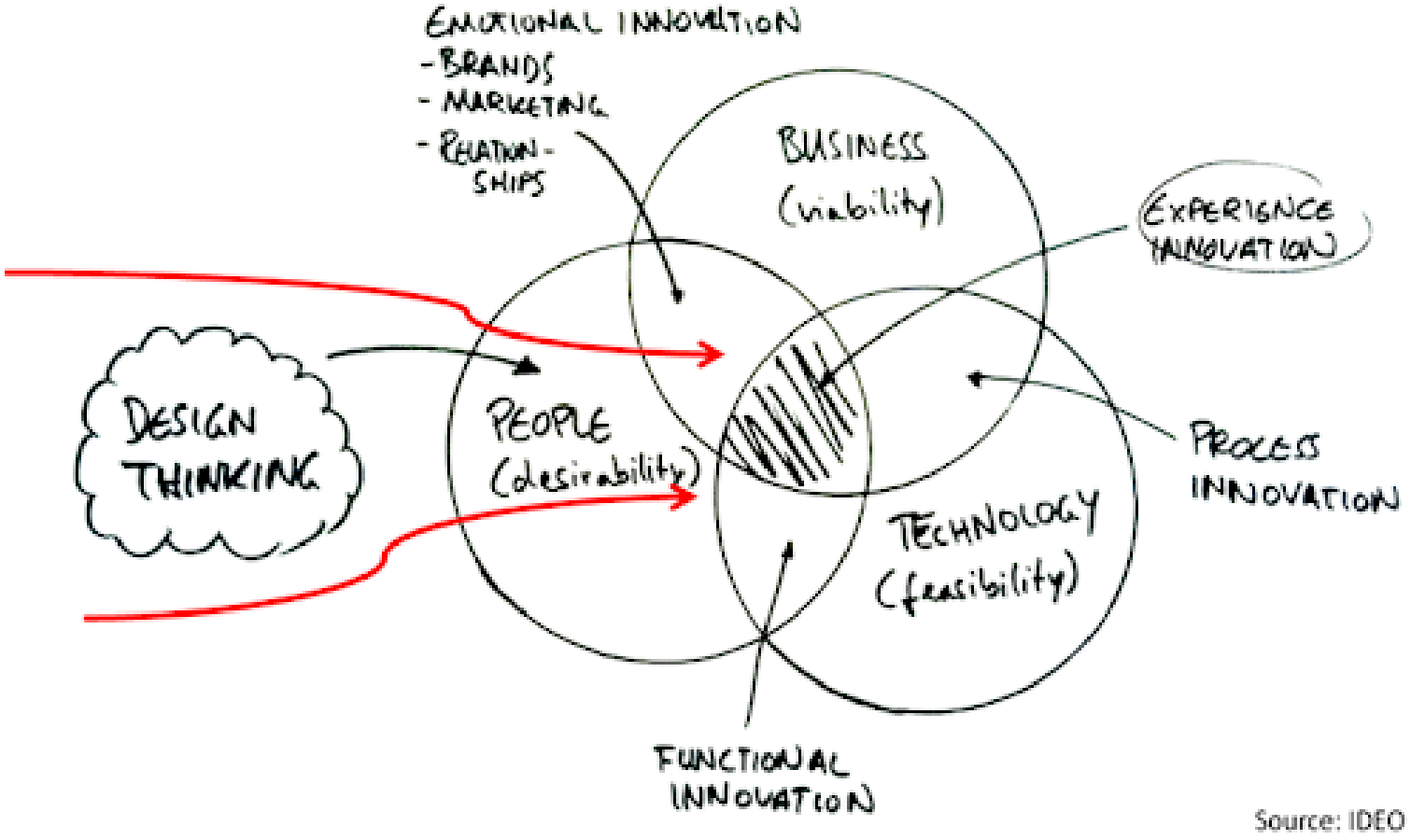
Numérique tend à renvoyer de fait au technologique, à la dimension discrète de la technologie, celle que manipulent les ingénieurs et qui restent intangible.

Digital semblerait concerner plutôt l'usager dans son expérience de cette technologie numérique. Avec digital, on passe de l'autre côté de l'écran (anglicisme formé à partir l'anglais digitalization numérisation, dérivé du nom commun digit, chiffre, du **latin** digitus, doigt.)

Présentation des missions du Responsable de la Sécurité des SI (RSSI)

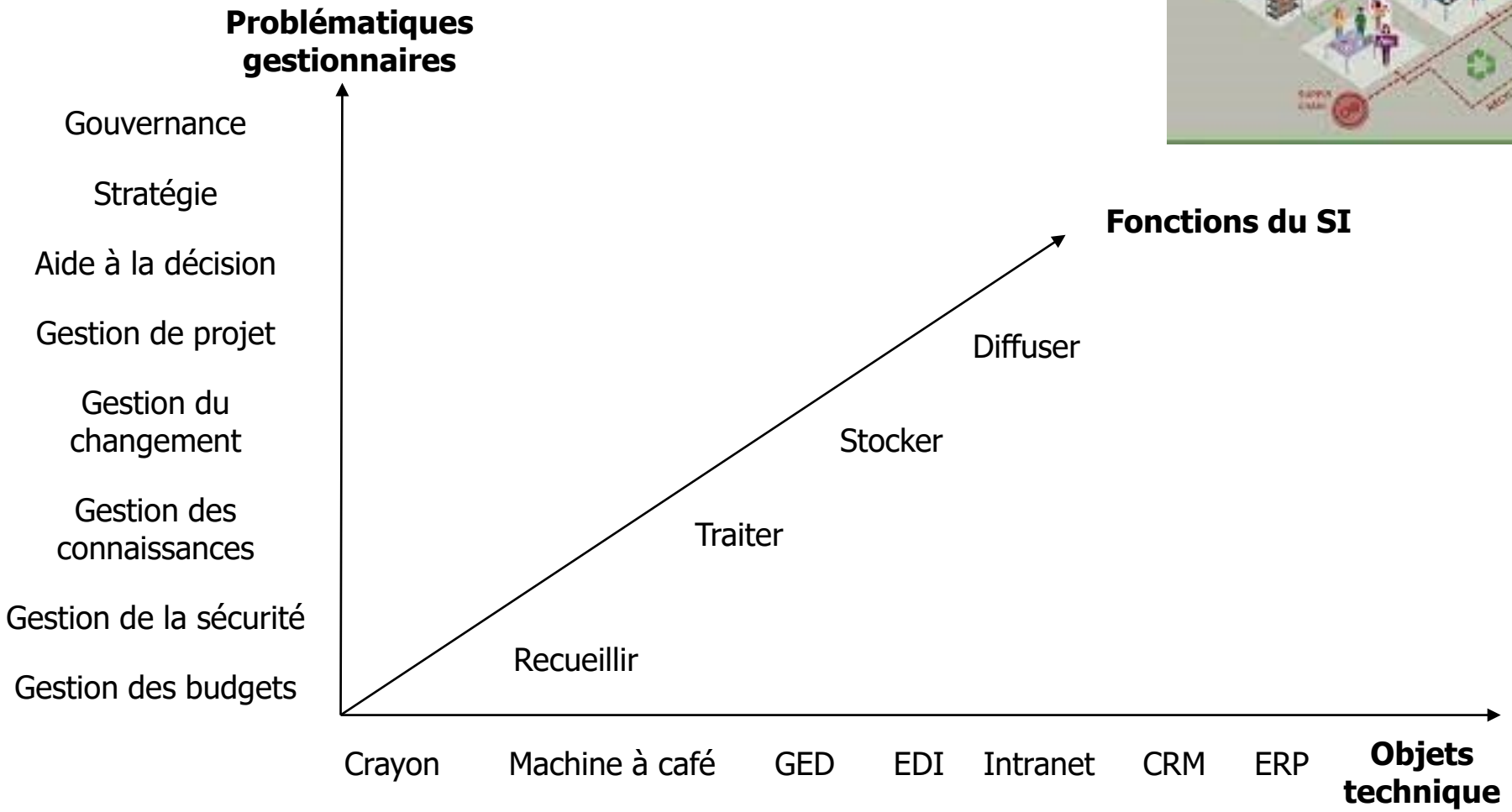
Le RSSI doit agir dans un rôle de concertation et conseil auprès de la Direction Générale, des personnels des Arts et Métiers, et tout particulièrement auprès des personnels de la DSI afin de les accompagner vers une meilleure maîtrise des risques liés à la sécurité des systèmes d'information et à la protection des données.	Participer au groupe de pilotage SI, en ce qui concerne la sécurité du système d'information, dans le cadre de l'élaboration d'un schéma directeur du système d'information ;
	Rédiger ou vérifier les différents documents de sécurité du SI (expressions des objectifs de sécurité, procédures d'exploitation de sécurité, Politiques SSI, Plan d'actions, Fiches Conseils, ...) qu'il soumet pour validation au DSI ;
	Assurer une veille et un suivi par tous les moyens possibles (conférences, Internet, publications, loi...) pour permettre à l'établissement de rester vigilant sur les nouvelles menaces et risques liés au Système d'Information ;
	Donner son avis sur les problèmes d'accès physique des bâtiments et leur contrôle électronique en liaison avec le Responsable Patrimoine ;
	Évaluer et de préconiser le juste niveau de sécurité du Système d'Information, afin de garantir une sécurité adéquate au regard de la réglementation mais aussi des missions et des enjeux ;

Système d'information: c'est complexe...

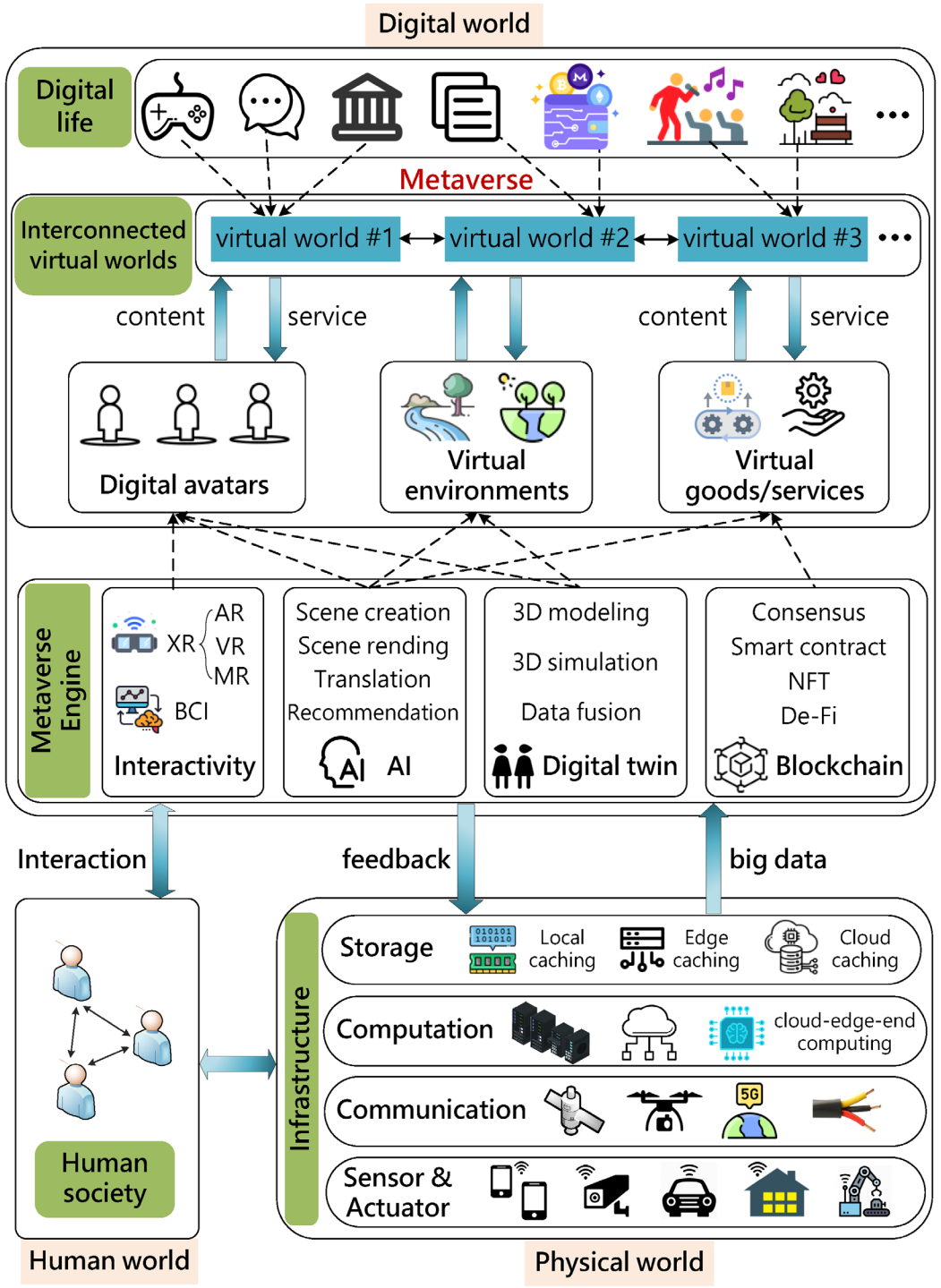


Source: IDEO

Management des systèmes d'information ?



Système d'information: c'est complexe…



Source : A Survey on Metaverse: Fundamentals, Security, and Privacy

Risques et sécurité des systèmes informatiques

Nuisances de nature aléatoire

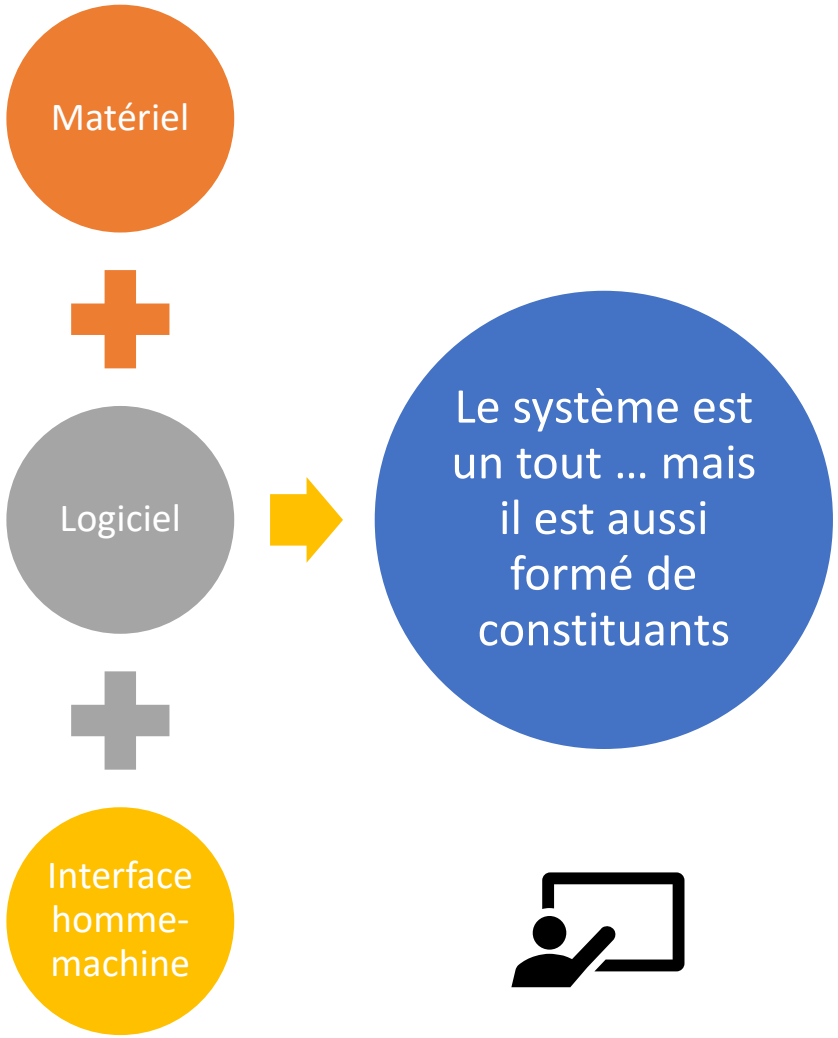
(les dangers) – Sécurité –innocuité

- La sécurité-innocuité concerne l'aptitude du système à ne pas connaître d'événements catastrophiques
- Les dangers sont les défaillances du matériel, les défaillances du logiciel et les erreurs humaines non intentionnelles
- Dans la plupart des entreprises, ces aspects sont traités dans le cadre de la sûreté de fonctionnement du système

Nuisances de nature volontaire

(les menaces) - Sécurité-confidentialité

- La sécurité-confidentialité concerne l'aptitude du système à se prémunir de la manipulation non-autorisée de l'information à des fins malveillantes
- Les menaces sont stratégiques, terroristes, ludiques ou mercantiles
- Dans la plupart des entreprises, ces aspects sont traités dans le cadre de la sécurité des systèmes d'information



Démarche commune de construction de la sécurité

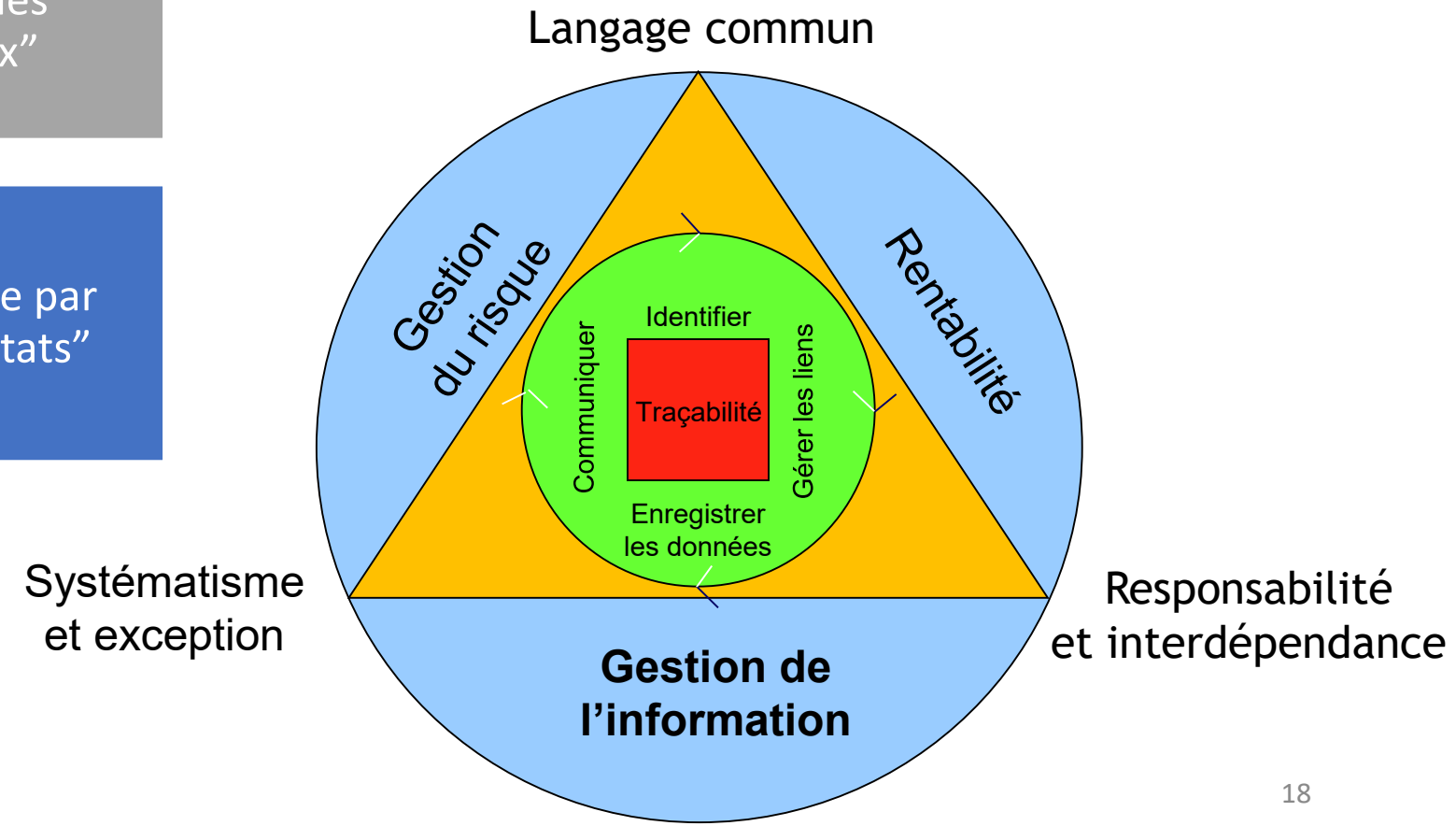
prendre en compte la sécurité dès les premières phases de réalisation du système

être capable de “recoller les morceaux”

savoir le justifier

logiciel passe par plusieurs “états”

Problème général de la traçabilité



Deux types d'exigences de sécurité

Exigences fonctionnelles (ce que fait le produit)

- L'implémentation de ces exigences donne les fonctions de sécurité
- C'est une liste de spécifications de fonctions sécuritaires

Exigences d'assurance (la garantie que le but est atteint)

- Assure la correction de l'implémentation
- C'est une liste de contraintes qui permet d'évaluer le niveau de sécurité que l'on peut atteindre avec l'implémentation fournie

Caractériser la situation → Définir le conflit, le dilemme → Déterminer les parties prenantes et leurs objectifs respectifs → Définir les options raisonnables → Reconnaître les conséquences possibles des choix

Puissance des ordi * 2 tous les 18 mois

Coûts et l'encombrement du stockage des données baissent rapidement

Progrès dans l'analyse des données

Progrès dans les réseaux et les accès peu coûteux via Internet

Cybersécurité en trois mots

Prévention

Protection des actifs de l'organisation (fichiers, données, …)

Détection

Sensibilisation de l'ensemble des acteurs

Diffusion des bonnes pratiques et des codes de conduite

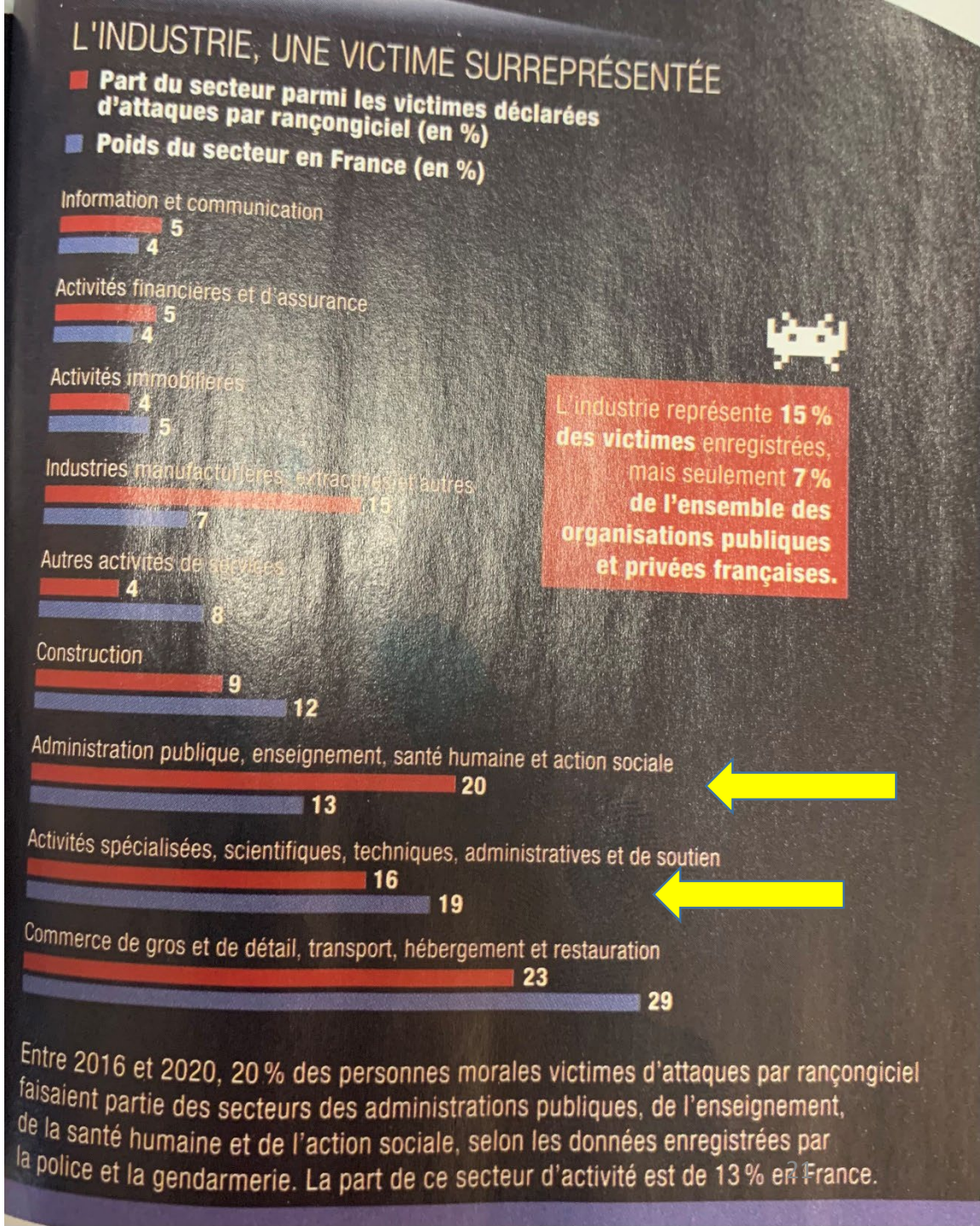
Contre-mesures

Surveillance permanente

Renforcement de la sécurité du système d'information

Les Rançongiciels, le nouveau fléau

La protection de type château fort, où l'on dresse des murailles mais dans défendre l'enceinte, ne fonctionne plus…



Mesures préventives et mesures palliatives

Mesures préventives

- Mesures de sensibilisation et d'éducation
- Mesures de protection (protection technique, organisationnelle, managériale et légale)
- Mesures structurelles (architecture des systèmes d'information)
- Mesures dissuasives (responsabilité, engagement à respecter les mesures de sécurité, surveillance)

Mesures palliatives

- Mesures de récupération (gestion de crise, plan de continuité, retour à fonctionnement normal)
- Mesures de correction et d'optimisation (éviter que les problèmes ne se reproduise)
- Mesures de poursuites judiciaires

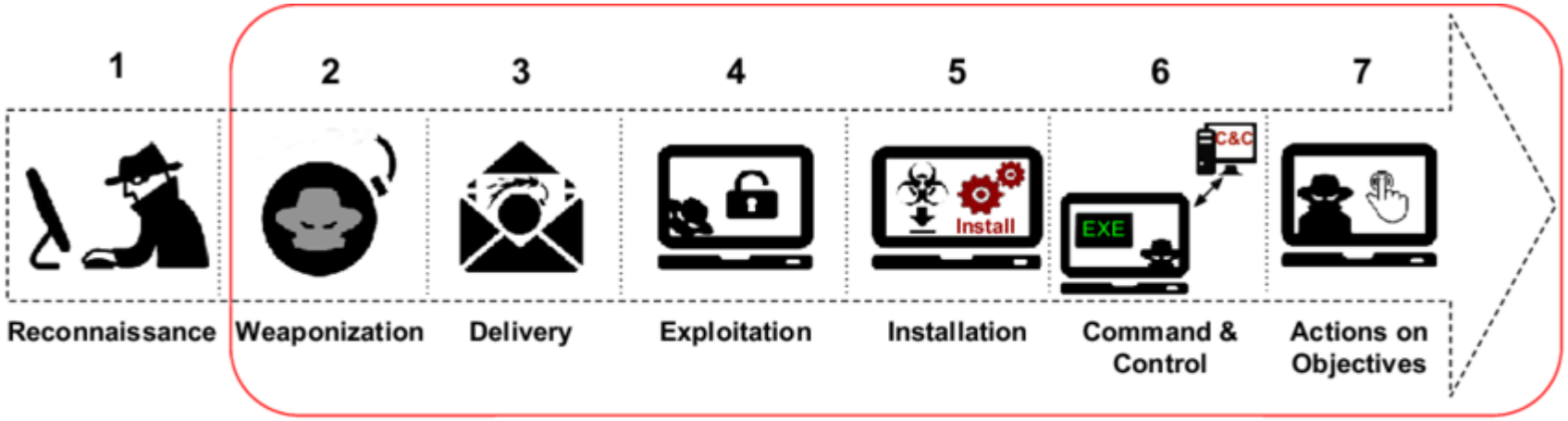
Protection

Réaction

Incident de sécurité

Arts et Métiers Sciences et Technologies

Démarche d'analyse des risques : comprendre ses valeurs pour mieux les protéger



Our considered steps for Ransomware feature taxonomy

Vulnérabilités – Menaces

Valeurs

Risques – Impacts

Appréciation des risques

Prévention – Réactions

Mesures de réduction des risques

Arts et Métiers Sciences et Technologies

Etude de cas : Zones à régime restrictif - Anticiper les vulnérabilités à l'aide d'un outil d'analyse

Zones à régime restrictif - Anticiper les vulnérabilités à l'aide d'un outil d'analyse : Dossier complet | Techniques de l'Ingénieur (techniques-ingenieur.fr)

Accélérateur de talents pour l'industrie du futur

Eric Bertrand – FSD

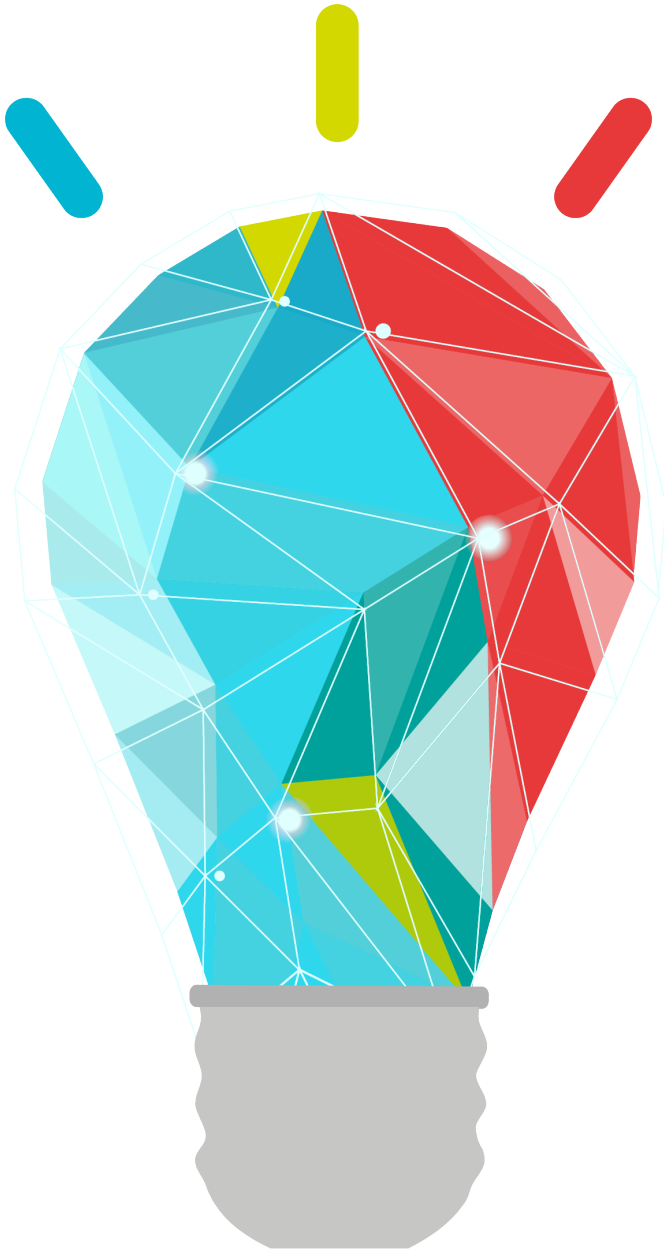
Arts et Métiers Sciences et Technologies

Problématique de recherche

Comprendre les difficultés rencontrées pour la mise en place de zone à régime restrictif ainsi que les vulnérabilités perçues par les directeurs de laboratoire au sein de structures de l'enseignement supérieur, afin de proposer à la fin du mémoire des pistes de solutions pragmatiques d'anticipation adaptées au terrain avec un niveau d'acceptabilité correspondant au cadre réglementaire et à l'aspect sociologique particulier du monde de la recherche et de la science.

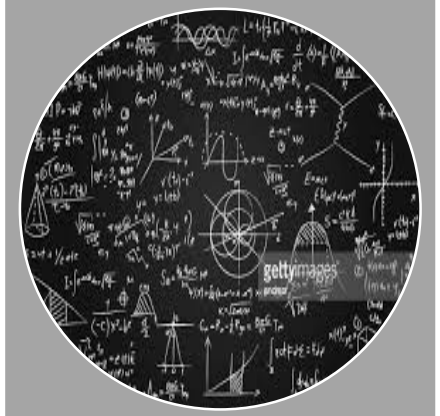
En prenant en compte la dualité entre la science qui doit être partagée au sens ouvert sur le monde et la protection du patrimoine scientifique et technique pour la nation, en ma qualité de fonctionnaire de sécurité défense au sein d'un établissement d'enseignement supérieur.

Cette double tension se traduit par des difficultés physiques ou logiques (digitalisation, numérisation, télétravail, nouvelle organisation, nouvelle stratégie, Covid-19 …) dans la mise en place de zones à régime restrictif au sein de six laboratoires étudiés dans ce mémoire.



Matériels et méthodes - Organisation du projet - Contexte du projet

Le comité de pilotage est composé d'un FSD et de six directeurs de laboratoires de recherche



Les laboratoires de recherche représentent un panel large et cohérent pour l'étude, en regroupant des laboratoires mono ou multitutelles

L'étude a été menée sur une période de cinq mois (de mars à juillet 2020)

Les entretiens ont été réalisés en visioconférence avec l'ensemble des parties prenantes pendant la période de pandémie COVID- 19

Méthode de recueil d'information par questionnaire d'entretien

Le questionnaire a été élaboré à partir du guide méthodologique de la protection numérique du potentiel scientifique et technique de la nation réalisée en partenariat avec le SGDN et ANSSI.

Sensibilisation et la formation des utilisateurs	Connaissance du système d'information	Authentification et contrôle des accès
Sécurisation des postes de travail	Sécurisation du réseau	Sécurisation de l'administration
Gestion du nomadisme	Maintien à jour du système d'information	Supervision, l'audit et la réaction face à des incidents de sécurité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Méthode cindynique

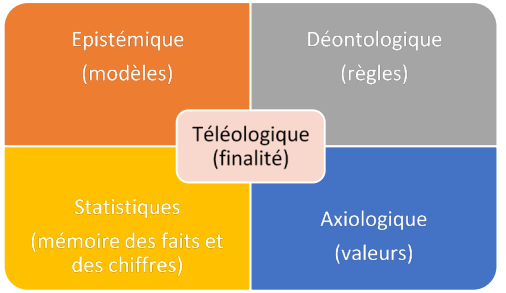


FIGURE 1 - SCHÉMA EXPLICATIF DES AXIOMES CINDYNIQUE

Les déficits systémiques porteurs de dangers ont été répertoriés par :

- DSC1 : Culture d'infaillibilité.
- DSC2 : Culture de simplisme.
- DSC3 : Culture de non-communication.
- DSC4 : Culture nombriliste.
- DSC5 : Subordination des fonctions de gestion du risque aux fonctions de production.
- DSC6 : Dilution des responsabilités. Non-explication des tâches de gestion des risques.
- DSC7 : Absence d'un système de retour d'expérience.
- DSC8 : Absence d'une méthode cindynique dans l'organisation.
- DSC9 : Absence de planification des situations de crise

Sensibilisation et la formation des utilisateurs à la PPST
Verbatim :
☐ DSC1 : Culture d'infaillibilité. ☐ DSC2 : Culture de simplisme. ☐ DSC3 : Culture de non-communication. ☐ DSC4 : Culture nombriliste. ☐ DSC5 : Subordination des fonctions de gestion du risque aux fonctions de production. ☐ DSC6 : Dilution des responsabilités. Non-explication des tâches de gestion des risques. ☐ DSC7 : Absence d'un système de retour d'expérience. ☐ DSC8 : Absence d'une méthode cindynique dans l'organisation. ☐ DSC9 : Absence de planification des situations de crise.

Résultats - Analyse des questionnaires avec verbatim – (individu, collectif et laboratoire)

« Je suis directrice depuis 2018 donc cela fait deux ans sachant qu'il y a eu des évaluations auparavant au laboratoire pour passer en ZRR, mais en tant qu'enseignant-chercheur lambda du laboratoire je n'étais pas au courant… ».

« On est chercheur, chercheur payé par l'État et en théorie notre travail c'est de produire de la connaissance et de la transmettre un public assez large donc c'est un peu antagoniste entre transmettre, publier… pour un chercheur il faut donc publier ! et normalement transmettre au plus grand nombre et en même temps protéger… en tant que directeur de laboratoire c'est un peu compliqué d'être sur ces deux problématiques antagonistes ».

« Le degré de protection de ces différents réseaux (humains et numériques) est la plupart du temps non maîtrisé. C'est-à-dire qu'on n'a généralement pas la compétence ou la possibilité de garantir le degré de sécurité nous-mêmes, nous sommes obligés de faire confiance aux infrastructures qui sont autour de nous pour nous protéger et éviter de nous faire pirater les outils que l'on développe. C'est une problématique dans un laboratoire comme le nôtre de plus en plus importante, nous avons conscience des failles et des limitations.

Résultats - Analyse des questionnaires avec verbatim – (individu, collectif et laboratoire)

« Donc sur le système d'information, je vois trois voies, information informatique donc tout ce qui se passe par le numérique, tout ce qui est écrit, cela peut être de l'écrit informatique, mais aussi de l'écrit papier, et tout ce qui oral. La science… l'information se fait au tout début de manière générale à l'oral ensuite par de l'écrit souvent manuel et ensuite informatique qui passe dans les réseaux, etc. » reposant sur les axiomes qui peuvent être différents en fonction du laboratoire. Il paraît important de souligner que cette connaissance peut être diffuse en fonction de la typologie du laboratoire (multitutelles ou pas) et du type de recherche effectuée par le laboratoire. »

« Il y a cette notion ambivalente entre cette volonté d'ouverture comme un lieu d'échanges et de diffusion de connaissances et la nécessité de protéger certaines données sensibles. »

« Qu'il est de bon ton de travailler avec des gens qui sont à l'autre bout de la planète et de ne pas trop travailler avec son voisin de palier… dans les laboratoires « ce phénomène pervers est encouragé par le système de concurrence interne dans les laboratoires. »

« Je vais tout d'abord parler du réseau des chercheurs dont je pense que ça nous pose un vrai problème, car c'est individuel à chaque chercheur qui vit cela entre la volonté d'avoir une recherche qui soit ouverte vers l'extérieur donc ouvert aussi en paroles avec des collaborateurs qui sont du même laboratoire ou d'autres laboratoires… et parfois nous allons même parler avec d'autres travaux de chercheurs de laboratoire sans leur demander leur accord pour soit effectivement se valoriser ou valoriser le laboratoire ».

« Mon problème c'est que j'ai quatre ou cinq tutelles et voire cinq administrations… c'est à la fois très bien… ça aide à sécuriser des tas de choses… c'est très compliqué et pas forcément cohérent… ».

Résultats - Analyse des questionnaires avec verbatim – (individu, collectif et laboratoire)

« Après nous avons quand même un souci, car nous partageons certaines données et se pose la question du RGPD et parfois on ne sait pas trop se situer par rapport à cela ! » ; cela peut occasionner des impacts individuels. »

« Concernant les personnes et les déplacements en France et à l'étranger dans le cadre de nos activités et de nos objectifs en tant qu'enseignants-chercheurs… culture internationale y est très forte… donc on peut se déplacer partout dans le monde. ». La difficulté est bien la gestion du secret. »

« Une nébuleuse qui serait capable de gérer toutes les activités du laboratoire… »

« Dans la recherche on essaie de faire vite ! Car à partir du moment où on a pensé à rédiger une publication, il y a une ou deux personnes dans le monde qui sont en train de faire la même chose… »

Résultats - Analyse des questionnaires avec verbatim – (individu, collectif et laboratoire)

« Alors théoriquement un ordinateur portable ne devrait pas contenir des choses qui ne devaient pas contenir, mais c'est la théorie, dans la pratique on ne peut peut-être difficilement convaincu à 100 % ! ».

« La notion de protection du savoir scientifique et technologique est très importante. La première particularité très intéressante de notre laboratoire c'est cette dualité : diffusion des connaissances et confidentialité ! C'est-à-dire que nous sommes à la fois sur une logique d'ouverture, c'est la connaissance pour tous et en même temps des travaux plutôt de nature industrielle qui peuvent relever de la notion de secret. »

« Les gens ont bien compris… donc la moitié du labo est dans la démarche de contrôler les accès informatiques avec un changement de mot de passe régulier. Après le reste des mots de passe collectif pour accéder aux machines aux équipements ou des Post-its à des endroits donnés. »

Il y a quand même, une notion de sécurisation pour sécuriser un poste travail numérique. Rien n'est fait pour l'instant et nous allons nous en occuper dans les années à venir, mais cela demande des moyens et des compétences que nous n'avons pas.

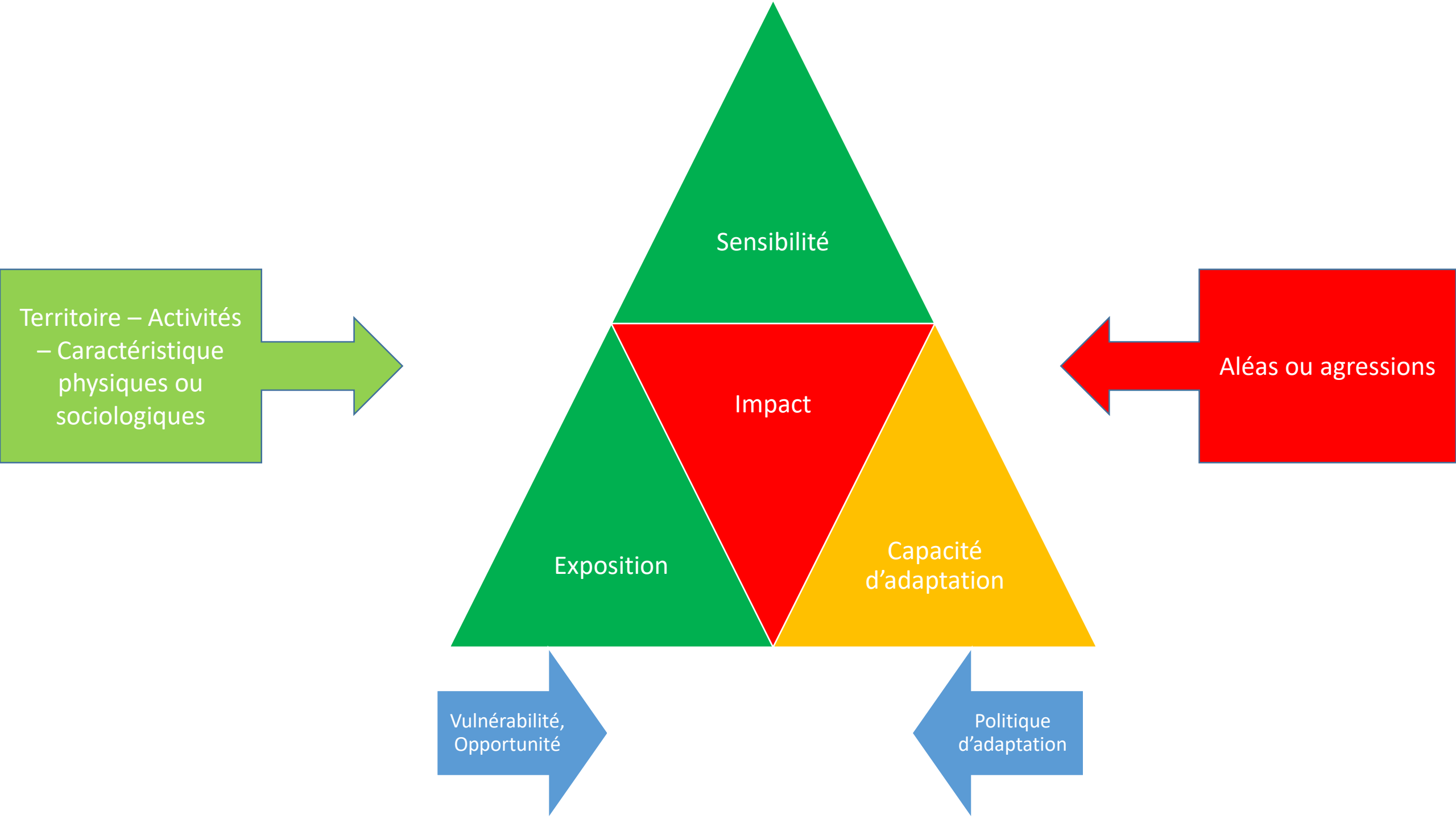
Résultats - Analyse des questionnaires avec verbatim – (individu, collectif et laboratoire)

« Le fait de mettre en place la PSSIE et une ZRR a également un coût informatique très élevé pour lequel nous n'avons pas de financement particulier ni de soutien. »

« Si moi je souhaite sécuriser l'accès à un endroit, il faut aussi que l'école puisse l'accepter aussi. Ou si l'école pour un souci de sécurité demande au laboratoire de se conformer à un certain nombre de règles (respect de la sécurité incendie par exemple) ; le laboratoire doit être en mesure de revoir son périmètre de sécurité et de suivre les préconisations de l'administration. Et sécuriser l'administration pour moi cela veut dire aussi tout simplement que l'intérêt de l'administration soit exactement le même que ceux du laboratoire vis-à-vis de la PPST. »

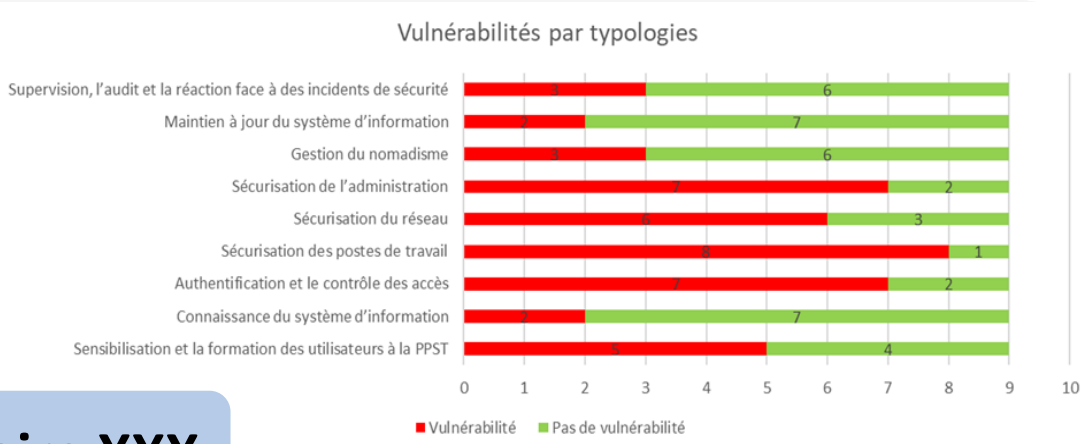
« Sur le voyage lui-même, je pense que 90 % des personnes du laboratoire cherchent toujours la simplicité avant la protection et vont être dans un train en travaillant sans écran de protection, va utiliser le Wi-Fi du train ou des logiciels craqués. »

« Alors pour contrôler tout ça ! C'est extrêmement compliqué ! Extrêmement compliqué… je ne sais pas le contrôler… »

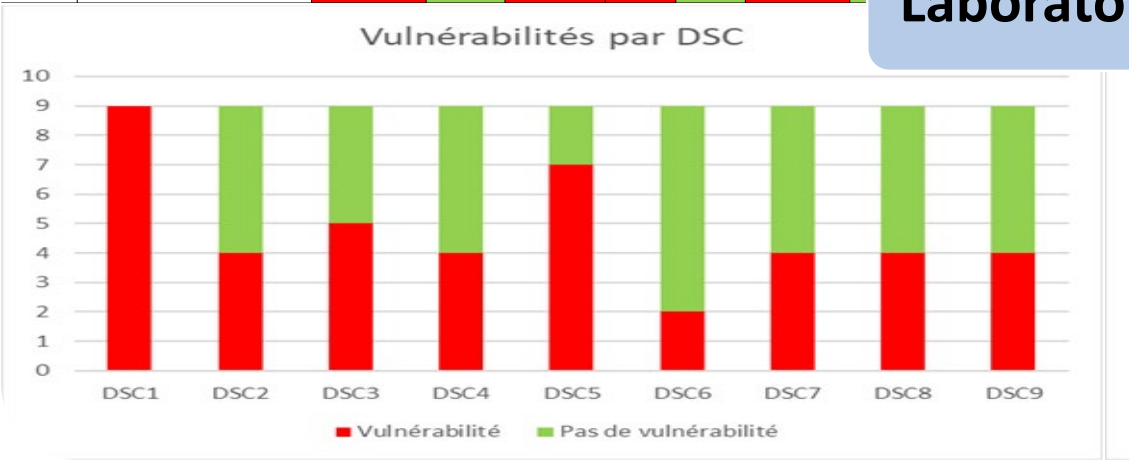

Territoire – Activités – Caractéristique physiques ou sociologiques
Sensibilité
Impact
Exposition
Capacité d'adaptation
Aléas ou agressions
Vulnérabilité, Opportunité
Politique d'adaptation

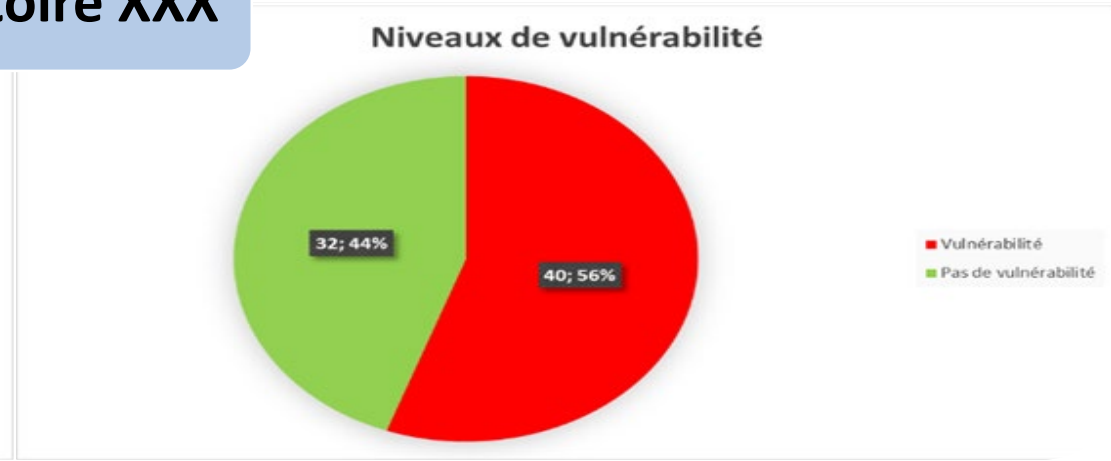
Résultats - Cartographies des matrices d'affinités

	32									
		Sensibilisation et la formation des utilisateurs à la PPST	Connaissance du système d'information	Authentification et le contrôle des accès	Sécurisation des postes de travail	Sécurisation du réseau	Sécurisation de l'administration	Gestion du nomadisme	Maintien à jour du système d'information	Supervision, l'audit et la réaction face à des incidents de sécurité
DSC1	Culture d'infaillibilité.	1	1	1	1	1	1	1	1	1
DSC2	Culture de simplisme.	1	2	2	1	2	1	2	2	1
DSC3	Culture de non-communication.	2	1	1	1	1	2	1	2	2
DSC4	Culture nombriliste.	1	2	1	1	1	2	2	2	2
DSC5	Subordination des fonctions de gestion du risque aux fonctions de production.	2	2	1	1	1	1	1	1	1
DSC6	Dilution des responsabilités. Non-explication des tâches de gestion des risques.	2	2	2	2	1	1	2	2	2
DSC7	Absence d'un système de retour d'expérience.	2	2	1	1	1	1	2	2	2
DSC8	Absence d'une méthode cindynique dans l'organisation.	1	2	1	1	2	1			
DSC9	Absence de planification des situations de crise.	1	2	1	1	2	1			

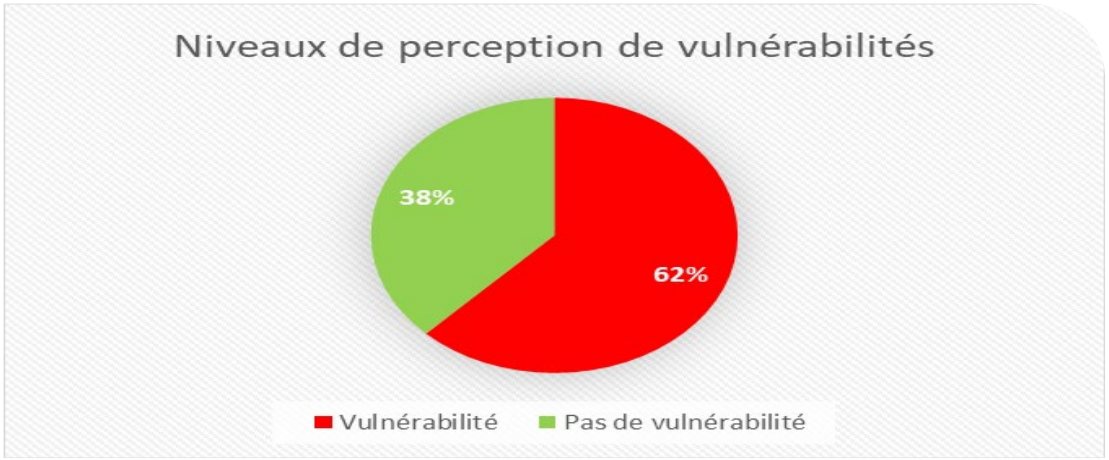


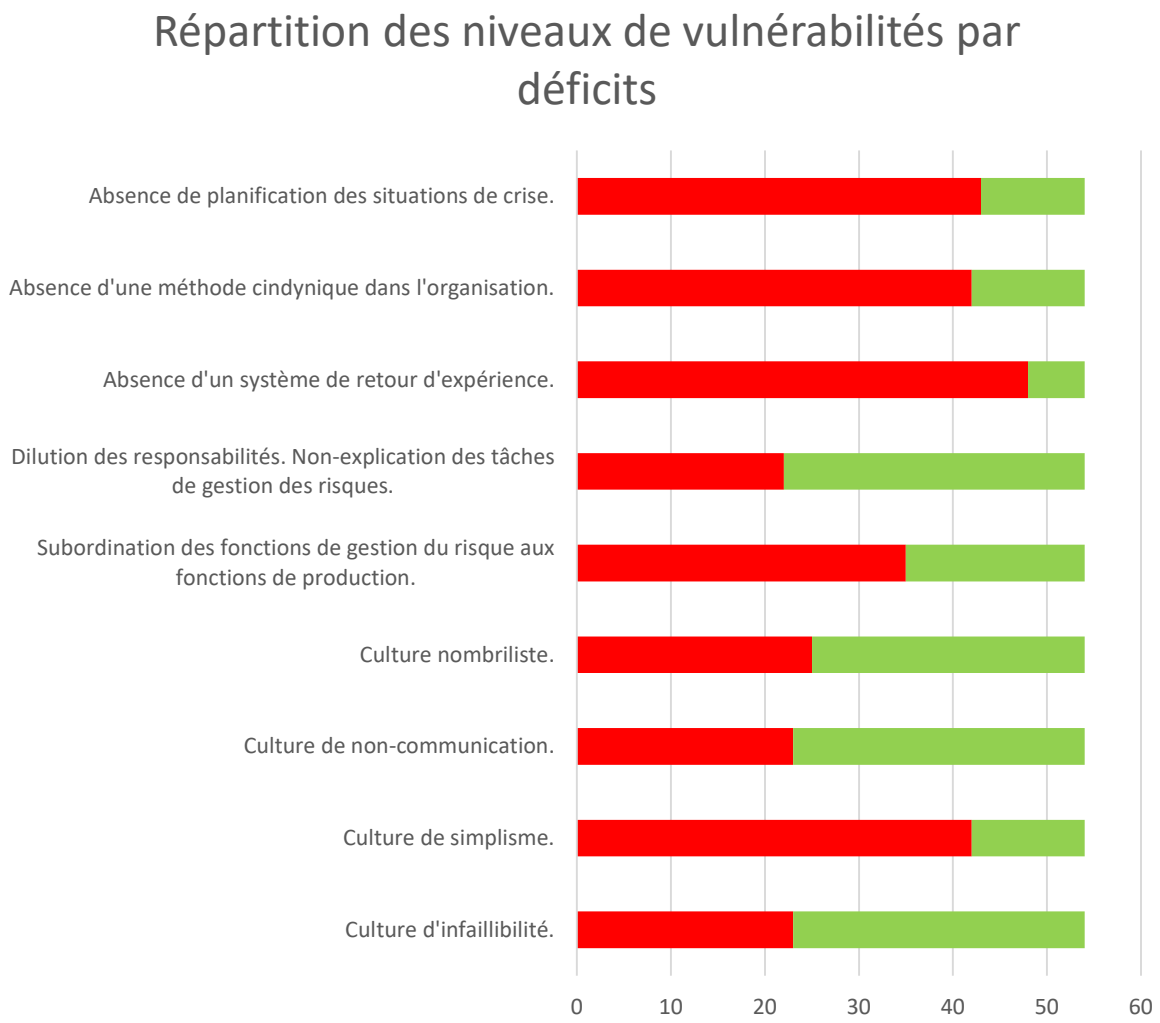
Laboratoire XXX





Résultats - Cartographie par matrices d’affinités globales sur les six laboratoires





Discussion

La complexité « on peut la comprendre, et on gagne à la comprendre » Edgar Morin

- Contraintes imposées par la création d'une ZRR
- Impact de la PSSIE sur la PPST
- La culture simpliste
- Gestion des sphères privée – professionnelle
- Impact de la diversité de la réglementation
- Gestion du nomadisme et des déplacements
- La valeur de la donnée
- Positionnement du directeur de laboratoire
- L'intelligence économique
- Augmentation du risque cyber

Recommandations - Gouvernance

Élaboration de la stratégie : Il serait utile de sensibiliser les autorités nationales à instaurer des procédures de concertation entre les tutelles par exemple pour l'élaboration d'une stratégie globale de gestion des risques, y incluant la définition des objectifs communs, la détermination des contributions respectives sur base de leurs compétences propres et la répartition des ressources (financières et humaines) en adéquation avec celle des responsabilités

Envisager des plans de « sûreté laboratoire » : il serait utile de sensibiliser les autorités responsables en réunissant tous les services compétents autour d'objectifs communs et précisant les actions à entreprendre dans les domaines de compétences respectives, y compris des mécanismes de contrôle

Nécessité de gestion interministérielle (limiter l'effet silo) : il serait utile de sensibiliser les autorités en amont (nationale, régionale, local) de sortir de leurs processus de décision essentiellement verticaux pour en faciliter l'application en aval par les tutelles de gestion

Nécessité de préciser la répartition des compétences : Il est indispensable de préciser les responsabilités pour chaque aspect de la gestion de la sûreté afin d'éviter des lacunes

L'approche stratégique de la gestion de la sûreté : Il serait utile d'envisager l'élaboration d'un document stratégique qui englobe tous les aspects de la gestion des risques et de sûreté et qui comprendrait des volets pour chaque composante (la stratégie, la prévention, la préparation et la gestion, la réhabilitation et l'évaluation) ainsi que par volet des chapitres précisant l'approche spécifique par type de risque dans le cadre de la PPST

Recommandations - Financement

Assurer un financement dédié, sous couvert d'un dossier argumenté pour la mise en place correcte de ZRR. Ce financement comprendrait une partie travaux réalisée pour mise en conformité et une partie dédiée aux systèmes d'information

Mettre en place de façon systématique dans les contrats de recherche une ligne dédiée à la sûreté pour financer les ZRR

Mettre en place un « label France ZRR » pour les laboratoires pour optimiser la sûreté entre les partenaires (industrie, autre laboratoire …) et créer de la valeur durable entre les parties

Sensibiliser les autorités responsables à introduire des analyses des coûts comme critère d'évaluation de l'organisation de la gestion de la sûreté

Recommandations - Audits

Critères d'évaluation : il serait utile de sensibiliser les autorités responsables à définir des critères d'évaluation dans un souci d'augmenter l'efficacité de leurs activités et leur adéquation avec les objectifs à réaliser pour la sûreté des laboratoires

Mettre en place, pour chaque laboratoire disposant d'une ZRR, un audit de bon fonctionnement de la ZRR une fois par an. Cet audit serait réalisé par le fonctionnaire de sécurité défense et le RSSI sur le respect de la PPST de la PSSIE

Revoir annuellement la portée du périmètre de la ZRR en fonction de l'évolution du laboratoire (recherches et partenariats)

Mettre en place des indicateurs en adéquation avec le retour d'expérience des problèmes rencontrés dans le fonctionnement de la ZRR avec une remontée à la direction de l'établissement et au ministère

Mettre en place des diagnostics intelligence économiques de type dièse®

Inventaire et analyse des risques : Il serait utile de sensibiliser les autorités compétentes à tous les niveaux, national, régional et local, de procéder à un inventaire (recensement objectif) et une analyse (évaluation de la probabilité de survenance, estimation des dommages, perception et acceptabilité ...) des risques sur leur laboratoire. Les résultats qui en découlent constitueront la base de leur politique (stratégie) de gestion des risques et de sûreté

Recommandations - Informatique

Mettre en place de façon régulière des « pentests » ou tests d'intrusions pour réaliser tout type d'attaque : reconnaissance, Social Engineering, intrusion informatique ou physique... L'objectif du test d'intrusion est de repérer les potentielles failles et vulnérabilités de votre système. Il permettra de corriger les vulnérabilités afin de sécuriser vos infrastructures,

Mettre en place en systématique des VPN pour les ordinateurs portables et les smartphones,

Mettre en place de façon systématique une supervision par la direction du système d'information locale avec un inventaire complet des matériels et des logiciels utilisés,

Mettre en place de façon automatique un chiffrage des ordinateurs pour chaque laboratoire possédant une ZRR,

Assurer une veille sur les nouvelles technologies comme la 5G qui pourrait être un facteur nouveau de failles.

Recommandations - Environnement

Proposer de façon systématique une stratégie pour réduire le plus possible le périmètre de la ZRR afin de mieux le contrôler

Tenir compte de façon systématique de l'environnement structurel avant la mise en place d'une ZRR

Tenir compte de la place de la pédagogie donc du croisement et du brassage de population dans les laboratoires (mettre en place des schémas spaghettis pour évaluer les flux au sein du laboratoire)

Recommandations - Formation et adhésion

Pour les ZRR ou le laboratoire multitutelles, s'assurer de l'adhésion de l'ensemble des parties prenantes surtout pour la gestion RH (réunion d'adhésion pour les enseignants-chercheurs sur les bonnes pratiques)

Mettre en place une supervision par les directeurs de laboratoire sur le contenu et la zone d'intervention à l'étranger de chaque enseignant-chercheur

Mettre en place un nouveau positionnement pour le directeur de laboratoire avec une posture hiérarchique et non pas fonctionnelle

Former de façon systématique et diplômante les directeurs de laboratoire avant leur prise de fonction sur la gestion, le juridique pour les laboratoires

Positionner le fonctionnaire de sécurité Défense comme un métier à part entière dans les établissements d'enseignement supérieur pour la protection du patrimoine scientifique et technique de la nation et non comme une fonction

Des connaissances à l'aide à la décision : Il est nécessaire de stimuler la recherche pour augmenter nos connaissances sur des phénomènes de plus en plus complexes. Il est nécessaire, en complément au développement des connaissances, et afin de pouvoir efficacement les appliquer, de développer des capacités d'interprétation et de réflexion et des outils d'aide à la décision pour les FSD

Recommandation - Déplacement

Mettre en place une fonction contrôle pour tout déplacement en France ou à l'étranger de personnel issu de la ZRR (contrôler le type d'intervention (support), valider la localisation du voyage en amont.)

Recommandations - Retour d’expérience

Échanger l’information sur les compétences, les bonnes pratiques et les formations – recommandation : Il serait utile de sensibiliser les autorités nationales de centraliser l’information sur les compétences disponibles, les bonnes pratiques PPST et autres, et les formations existantes au niveau national. Il serait utile d’envisager également de mettre les bases de données nationales en réseau pour les FSD

Le retour d’expérience intégré dans la prévention des risques et la gestion des crises : Il serait utile de sensibiliser les autorités compétentes à investir dans le recensement et l’analyse des incidents, accidents et désastres et de développer des mécanismes qui permettent d’intégrer les résultats de ces analyses dans la prévention des risques et la préparation de la gestion des crises

Conclusion

Connaître et penser, ce n'est pas atteindre une vérité absolue, c'est dialoguer avec l'incertitude.
Edgar Morin

La mise en place de ZRR pour un établissement est une organisation complexe avec un enjeu majeur pour la protection du patrimoine scientifique de la nation, mais aussi avec une portée financière, et d'image de marque pour le laboratoire.

Le recours à des outils de diagnostic de vulnérabilités nous permet d'aborder les dysfonctionnements sous l'angle de l'identification de chaque problème et des actions en réduction de risque (prévention et protection) hiérarchisées pour obtenir une consolidation objective et opérationnelle de ce système à mettre en place.

La mise en place de ZRR n'apporte au mieux qu'une modeste amélioration de la PPST pour un laboratoire public de recherche, pour un coût qui est loin d'être nul et souvent supporté par l'entité. Son efficacité reste à être démontrée, en outre par la prise en compte de l'accélération de la numérisation et du digital dans le monde de la recherche.

Les méthodes de la sociologie et de l'ingénieur sont rarement utilisées en simultané dans le monde de l'enseignement supérieur ni dans le monde de l'industrie pour comprendre la problématique et d'y associer des outils adaptés pour maîtriser la mise en place correcte d'une protection du patrimoine scientifique et technique de la nation.

La politique publique menée actuellement en France en matière d'intelligence économique promeut avant tout la sensibilisation de tous les acteurs économiques afin que de simples mesures de précaution élémentaires soient adoptées au sein de chaque organisation française, et ce, quels que soient sa taille et ses secteurs d'activités de produits ou de services.

L'intelligence économique est une boîte à outils, mais c'est aussi un état d'esprit autonome que doit acquérir l'organisation du laboratoire.

Cela permettra à l'organisation de tirer profit des grandes mutations que nous vivons tous en temps réel aujourd'hui face aux crises actuelles et aux crises futures, en prenant en compte le changement de monde qui arrive avec les nouvelles technologies comme la 5G, l'intelligence artificielle, qui aura un impact sur la PPST de demain ?

Pour l'avenir….

Construction d'un processus sécurité et sûreté **commun**

Aide active du FSD et du RSSI

Développement de formation autour de la sécurité dans les systèmes complexes

Prendre en compte les besoins des enseignants dans la gestion des projets de recherche complexes sur le numérique et le digital

Création de zones d'échanges avec l'ensemble des parties prenantes afin de mettre en place une stratégie commune de sécurité

Arts et Métiers Sciences et Technologies

Pour en savoir plus

- Pernet C. Sécurité et espionnage informatique – Connaissance de la menace APT (Advanced persistent threat) et du cyberespionnage. Parus : Editions Eyrolles, 2014, ISBN 978-2-212-13965-5
- Rapport d'information de M. André GATTOLIN, fait au nom de la MI Influences étatiques extra-européennes : **https://www.senat.fr/notice-rapport/2020/r20-873-notice.html**
- Billet V, Liottier M. Survivre à une cyberattaque. Versailles : VA Editions, 2018, ISBN 979-10-93240-42-8
- https://unitracker.aspi.org.au/
- Ghernaouti S. Cybersécurité : analyser les risques, mettre en œuvre les solutions. 6 -ème édition. Malakoff / Editions Dunod, 2019, ISBN 978-2-10-079054-8
- A Survey on Metaverse: Fundamentals, Security, and Privacy
- La répartition du savoir et la diffusion mondiales du savoir
- Agence Nationale de la sécurité des systèmes d'information (Anssi). Guide d'hygiène informatique. Renforcer la sécurité de son système d'information en 42 mesures. Paris, 2017. Accessible à : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
- https://unitracker.aspi.org.au/

Pour en savoir plus

- Code pénal - article 410-1
- Décret N°2011-1425 du 2 novembre 2011 portant application de l'article
- 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
- Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
- Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation.N°3415/SGDSN/AIST/PST du 7 novembre 2012
- PSSI de l'Etat (PSSIE)
- Politique de sécurité des systèmes d'information de l'Etat (PSSIE) – circulaire du Premier Ministre N°5725 [17 juillet 2014] ;
- Instruction interministérielle N°901 relative à la protection des systèmes d'information sensibles [11 février 2015].
- Par ailleurs, plusieurs guides sont disponibles sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI - www.ssi.gouv.fr).

Pour en savoir plus

https://www.ssi.gouv.fr/administration/bonnes-pratiques/

Arts et Métiers Sciences et Technologies

“ Le problème c’est pas le problème. Le problème c’est ton attitude face au problème.”

- Jack Sparrow