WISG

Workshop interdisciplinaire sur la sécurité globale

14 & 15 mars 2024 • Couvent des Jacobins **Rennes**

RÉPUBLIQUE FRANÇAISE *Liberté Égalité Fraternité*

anr agence nationale de la recherche — AU SERVICE DE LA SCIENCE

FRANCE 2030

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE *Liberté Égalité Fraternité*

PREMIER MINISTRE *Liberté Égalité Fraternité*

SGDSN

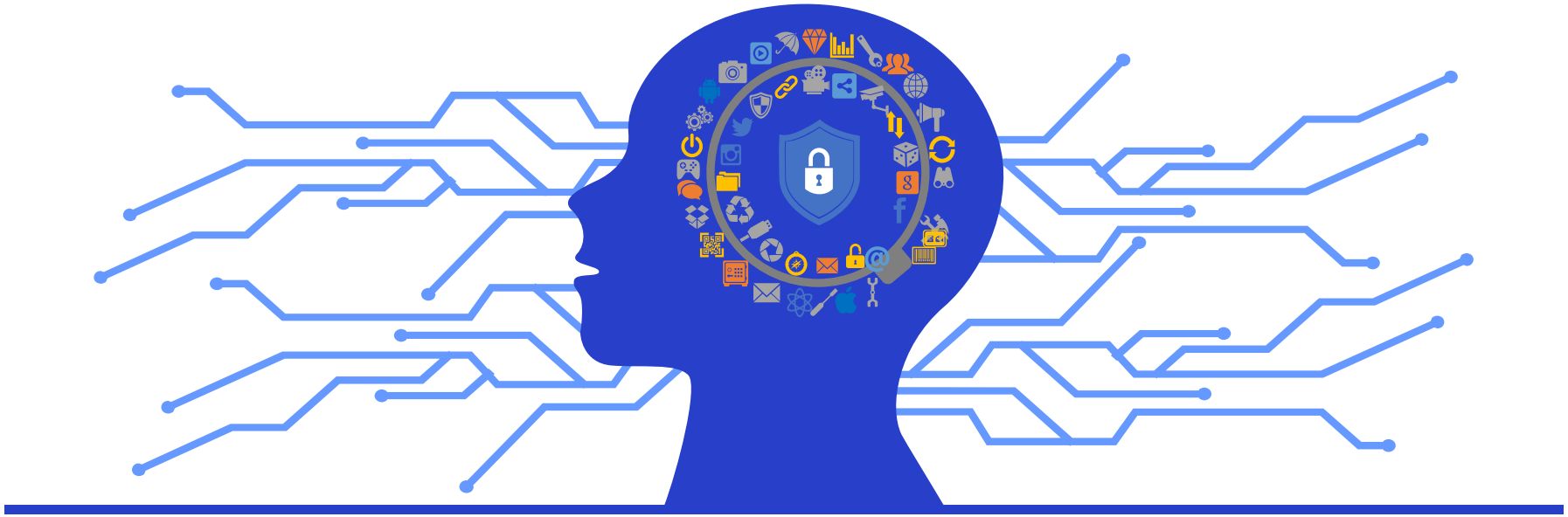
Digitalisation, Risques, Incertitudes et Fragilités des Technologies liés aux Facteurs Humains

DRIFT-FH

Ingrid DUMONT

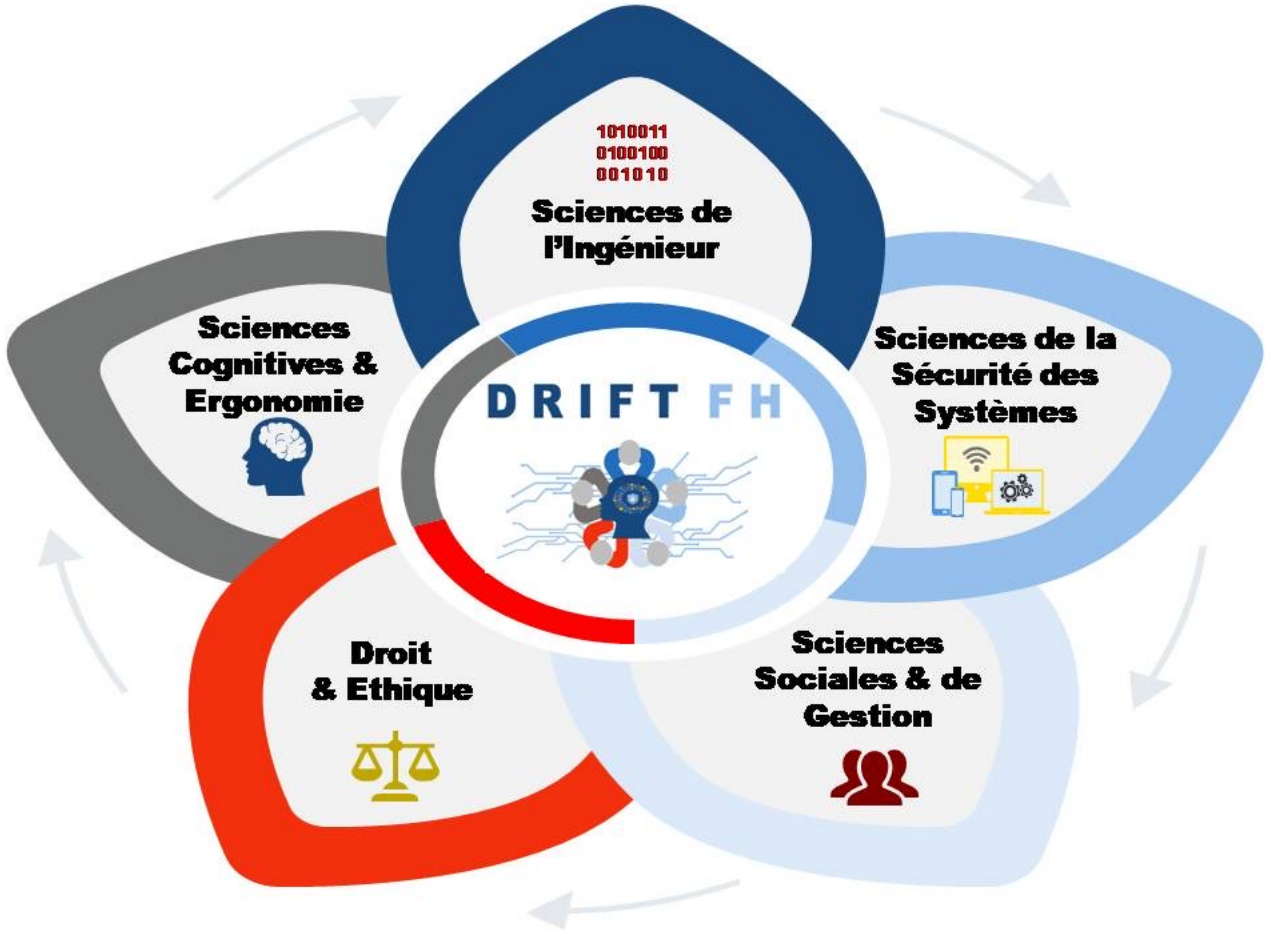
AAPG 2021

Notre ambition



Faire de l'Humain le maillon fort !

Une équipe transdisciplinaire



Objectifs du projet

Axe 1 : Identifier les vulnérabilités associées aux facteurs humains en lien avec les technologies

Axe 2 : Identifier les techniques d'apprentissage pour une prise de conscience des risques (menaces et vulnérabilités)

Secteurs Santé et Défense

SÉCURITÉ DU NUMÉRIQUE

ENVIRONNEMENT (interne et externe)

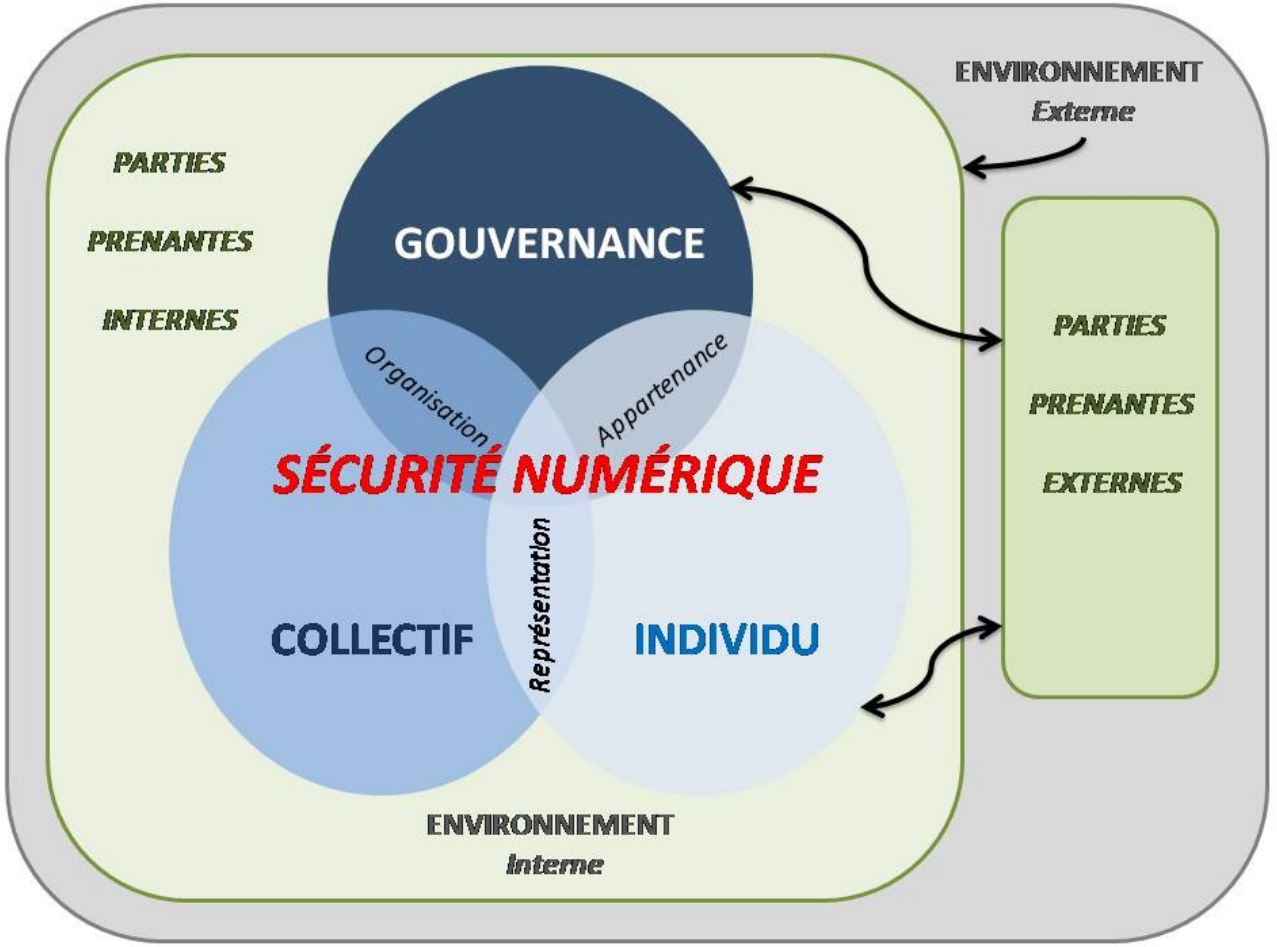
Facteurs Techniques

- GESTION DES RISQUES
- POLITIQUES SSI

Facteurs Organisationnels et Humains

- GOUVERNANCE
- ORGANISATION
- HUMAINS

Axe 1 – Les déterminants de la sécurité numérique

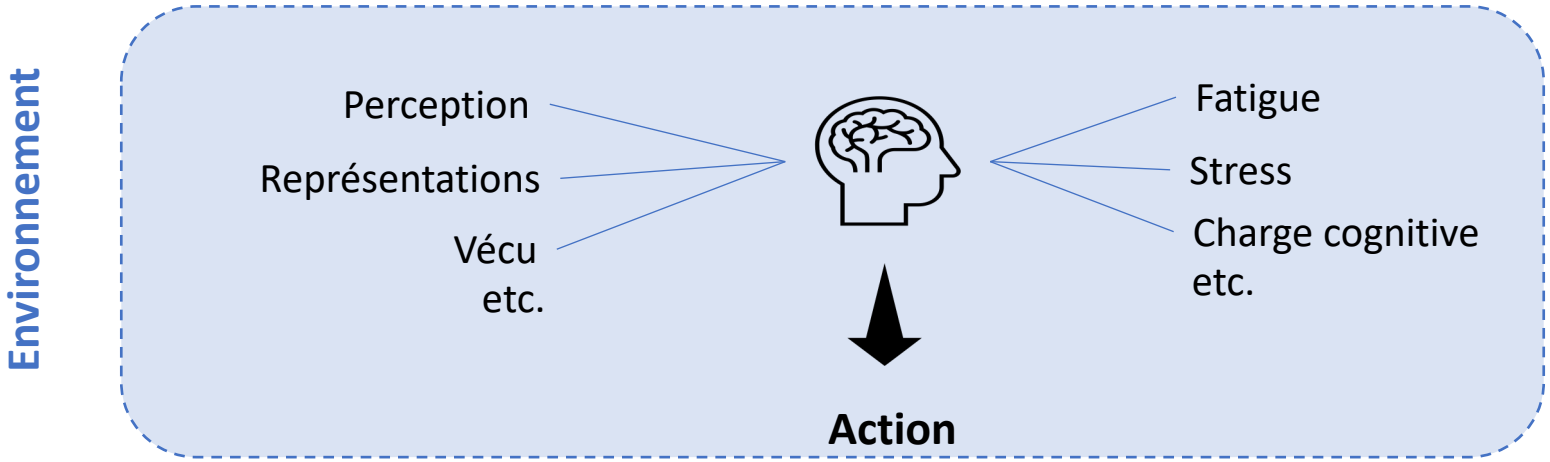


L'individu : un renforcement des capacités individuelles

⇒l'humain n'est pas faible, il a des vulnérabilités => à prendre en compte pour l'équilibre de l'organisation

⇒agit et interagit dans son environnement avec des outils numériques => effets sur la perception et les capacités cognitives

mieux se connaître pour savoir agir, réagir et interagir



Collectif : un renforcement de la fiabilité organisationnelle

La cybersécurité : une opportunité à saisir et non une contrainte pour l'organisation

⇒**Gouvernance** :

⇒la cybersécurité un outil de la stratégie s'appuyant sur la donnée :

- La politique des données
- La gouvernance des données
- L'analyse systémique des risques cyber (et informationnels)

⇒**Les partie prenantes internes : *Mieux les connaître pour savoir agir, réagir et interagir***

⇒encadrement de proximité : la mise en œuvre de la stratégie

⇒les collaborateurs = une somme d'individus => d'une amplification des vulnérabilités (créant des vulnérabilités organisationnelles) à une fiabilisation par le collectif

⇒les partenaires sociaux, les métiers, etc.

Environnement

⇒**Parties prenantes externes** : compétition, coopération, etc.

⇒**Percevoir et identifier les menaces** invisibles et imprévisibles (influences, manipulations, ingénierie sociale,…) => bien connaître son environnement et ses acteurs c'est aussi mieux anticiper et parfois pouvoir prévoir « l'imprévisible »

⇒**Mieux maîtriser la communication vers l'extérieur : (re)prendre la maîtrise de l'information** pour devenir moins vulnérable => limiter les fuites => **trop et mal communiquer, c'est aussi devenir une cible** => réseaux sociaux, publications,…

Mieux les connaître pour savoir agir, réagir et interagir

Axe 2 – Trois temps pour adapter les comportements !

Ancrer la connaissance en cybersécurité

⇒pour une **prise de conscience des risques cyber** en vue d'adapter les comportements des acteurs

⇒par le **raisonnement** : des ateliers associés à une stratégie de communication en continue

⇒par l'**émotion** :

- Simulateur RV
- Appel au connu, au vécu => association d'image pour ancrer la connaissance nouvelle

⇒des interactions humain-machine équilibrées

⇒**éduquer** en évitant la stratégie de la peur

⇒**libérer la parole** pour favoriser l'amélioration continue => sûreté

Retombées attendues

⇒**Intégrer les facteurs humains** dans l'analyse et la prévention des risques cyber tout au long du cycle de vie de l'information => vers une analyse systémique du risque cyber

⇒Publications scientifiques établissant une **fusion des expertises Sciences Humaines et Sociales et Sciences de l'ingénieur**

⇒**Faire de l'humain le « maillon fort » de la cybersécurité** en proposant une **boîte à outils** permettant à l'individu et au collectif de **mieux percevoir** et **prendre conscience** des menaces et des vulnérabilités au sein de leur organisation et de l'environnement afin d'adapter leurs comportements en vue **d'accroître la résilience de l'organisation**

DRIFT FH a su créer sa signature et sa transdisciplinarité fait sa force

pour faire du combattant le maillon fort de la cybersécurité !

Pour en savoir plus :

- Nous contacter : drift-fh@f-sc.org

Merci de votre attention !