FRC
Forum Cybermenace

FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

17ème édition – INSP Strasbourg

Intelligence Artificielle

Alliée ou ennemie de la cybersécurité ?

EDITION 2024

Madame Emmanuelle HAASER

Responsable veille et marketing - CCI Alsace Eurométropole
Lieutenant-colonel (RC) de la Gendarmerie Nationale

Monsieur Frédéric FESSAN

Secrétaire général
Institut National du Service Public - INSP

Général Gwendal DURAND

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

Monsieur Jean-Luc HEIMBURGER

Président de la CCI Alsace Eurométropole

Madame Irène WEISS

Conseillère régionale déléguée à la cybersécurité
Vice-présidente de la commission Enseignement supérieur, Recherche et Innovation

Monsieur Karl TERROLLION

Secrétaire général adjoint de la Préfecture du Bas-Rhin

Le programme du FRC 2024

EXEMPLES CONCRETS DES IMPACTS DE L'IA, CLÉS PRATIQUES POUR L'UTILISER À BON ESCIENT

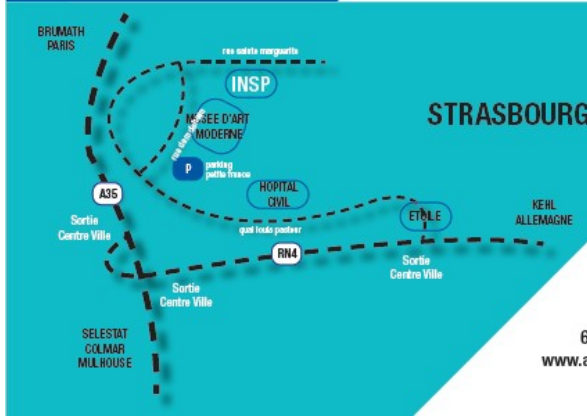
Au cours de la dernière décennie, l'intelligence artificielle (IA) s'est répandue dans les entreprises et dope désormais de très nombreux services que nous utilisons tous au quotidien. L'avènement récent de l'IA dite générative, rendue populaire par CHATGPT*, a engendré de nouvelles capacités souvent spectaculaires d'analyse et de synthèse de données (texte, son, image) et même de création ex-nihilo de contenu multimédia ou de code informatique.
Bien entendu, la mise au point et l'utilisation de ces modèles (algorithmes) sont soumises à des règlementations telles que l'AI Act européen et se font le plus souvent dans le respect d'une certaine éthique. Utilisée à des fins vertueuses et avec l'indispensable acuité quant à ses limites et biais potentiels, cette technologie procure d'infinis atouts au service de l'humain.

Hélas, à l'instar de tout progrès technique, l'IA peut aussi être utilisée pour mener des actions de désinformation et de manipulation d'opinion à des fins politiques ou économiques, à collecter et traiter des données permettant de perpétrer des actes cybercriminels tels qu'usurpation d'identité, atteinte aux systèmes d'information, vol de données, etc... Concomitamment, les professionnels de la cybersécurité tirent aussi profit de l'IA, notamment pour augmenter leurs capacités de détection et d'analyse.
Alors, l'IA menace ou atout pour la cybersécurité ?
(*) Marque déposée

Damien ERNST
Responsable informatique
CEN (RC) Gendarmerie Nationale
Auditeur IHEDN majeure "Souveraineté numérique et cybersécurité"

PLAN DE SITUATION

INSP - 1 rue Sainte Marguerite à Strasbourg



Ad Honores
Réseau Alsace
5 rue du Nideck
67000 Strasbourg
www.adhonores.alsace

La gendarmerie et les officiers de la réserve citoyenne vous convient au

FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

Entrée libre
Demande d'inscription sur
www.adhonores.alsace

5 NOVEMBRE 2024
auditorium de l'INSP
1 rue Sainte Marguerite à Strasbourg

FRC 2024
17ème édition

PARTENAIRES

SPONSORS

Nos partenaires

INSP
Institut national
du service public

Nos partenaires

FRC
Forum Cybermenace

CCI ALSACE EUROMÉTROPOLE

Nos partenaires

Nos sponsors

Nos sponsors

Nos sponsors

Nos sponsors

Nos sponsors

Nos sponsors

Les Gendarmeries, la RCDS et Ad honores - Réseau Alsace

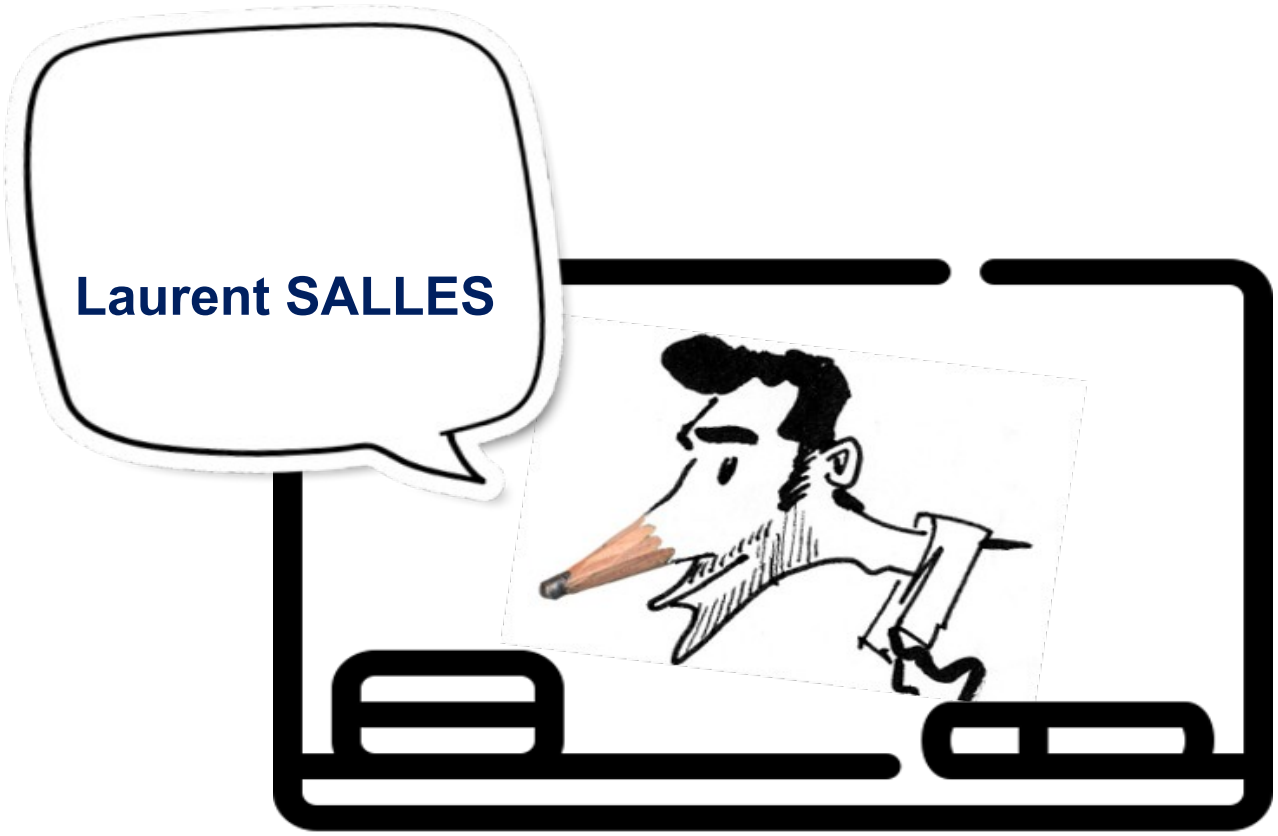
FRC
Forum Cybermenace

Notre objectif

Mobiliser les décideurs d'entreprises aux enjeux de la cybersécurité afin de leur permettre d'en être plus acteur

EDITION 2024

Notre fidèle dessinateur



Connexion wifi

Connexion au réseau Wifi : WIFI_INSP

Identifiant : **gendarmes**

Mot de passe : **P2aP2a67**

Profil : **EVENEMENT**

Dans le respect de la charte informatique de l'INSP

FRC
Forum Cybermenace

Conférence plénière

La Gendarmerie à l'ère de l'IA : constats, réalisations et prospective

Par le Général Patrick PERROT

EDITION 2024

FRC
Forum Cybermenace

Table ronde 1

Cybermenaces à l'ère de l'IA

Elena VALLEJO
Sébastien DUPENT
Daniel GUINIER
Ludovic HAYE
Jonathan WEBER

EDITION 2024

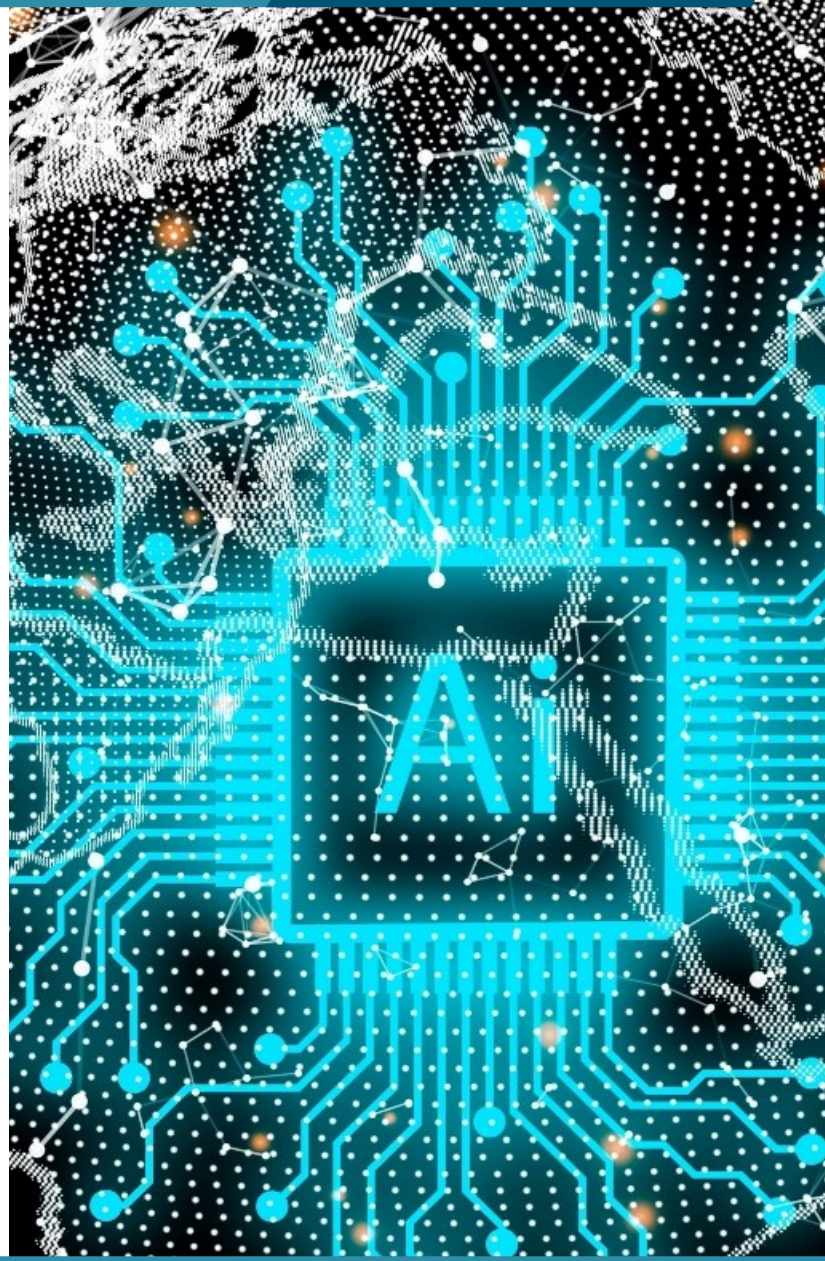
L’IA : votre faux ami ?

Madame Elena VALLEJO

Consultante Cybersécurité - Acesigroup

Monsieur Sébastien DUPENT

Professeur agrégé en Économie et Gestion spécialité système d’information – Lycée René Cassin
LTN (RC) Gendarmerie Nationale



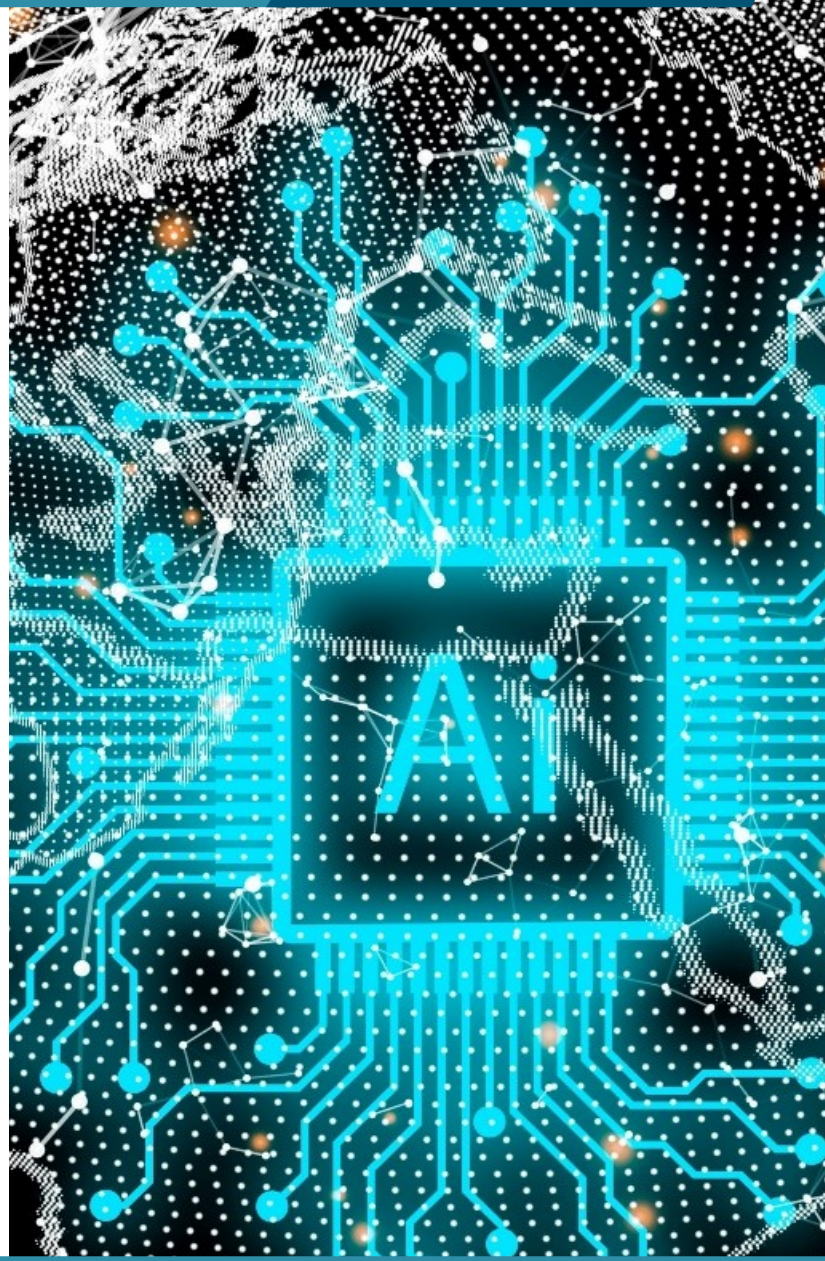
La question


Le triomphe de l'IA.
D'ailleurs, est-on certain que Daniel soit humain ?
Salles

Usurpation d'identité à l'ère de l'IA et contre-mesures

Monsieur Daniel GUINIER

Expert judiciaire honoraire – Anc. Expert devant la CPI de la Haye – COL (RC) Gendarmerie Nationale



Contexte de l'usurpation d'identité avec l'IA

Temps réel

Escroqueries avancées
Art. 313-1 du CP

Audio
Vidéo Texte

Recherche pour exploitation de failles humaines et techniques

Deepfakes

Intelligence artificielle

Messages
Tout espace d'échanges

Ciblage de la victime
Renseignements

Par tout moyen
y compris réseaux sociaux

Usurpation d'identité

Art. 226-4-1 du CP

Ingénierie sociale

Mystification d'adresse

Manipulation
"La part de l'homme" reste le maillon faible

Contre-mesures

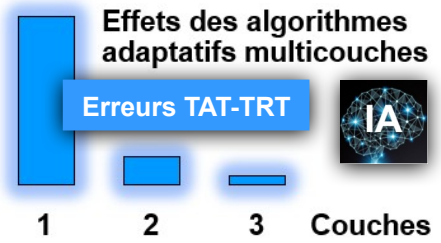
- ✓ Authentication
- ✓ Signature électronique
- ✓ Autorisation
- ✓ Audit

Cyberattaques : de la ruse à la manipulation quand *"la part de l'homme"* reste le maillon faible. *Expertises,* n°423, avril 2017

Moyens et niveaux de l'authentification

L'évaluation des systèmes et des procédés est attendue pour répondre aux Critères Communs de la sécurité des TI, selon la norme - ISO 15408

Être



Niveau 3 :

Niveau 2 :

Multi-biométrie

Biométrie

Caractéristiques stables et distinctes

"La personne par elle-même"

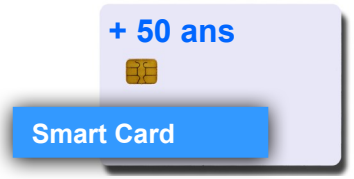
Avoir + Être + Savoir

Niveau 4 :

Circuit sécurisé avec biométrie

PIN demandé ou non

Avoir + Savoir



Niveau 3 :

Circuit sécurisé

avec PIN demandé

Savoir

Niveau 1 :

Mot de passe

Composition et taille correctes

Gestionnaire de mots de passe

Niveau 2 :

Code temporaire à usage unique

reçu par SMS ou tout autre canal

Savoir

La conjugaison de diverses technologies procure un niveau d'authentification variable, de faible à fort.

Niveaux de confiance de la signature électronique

Avant qu'un signataire ajoute sa signature électronique, il doit s'authentifier pour garantir l'intégrité et la sécurité de l'acte. La signature **qualifiée** de niveau 4 est conforme aux spécifications ETSI TS 101 456 et à l'emploi de dispositifs sécurisés de création de signature relatifs au certificat RGS*** du Référentiel Général de Sécurité qui vise à instaurer la confiance numérique dans les échanges électroniques.

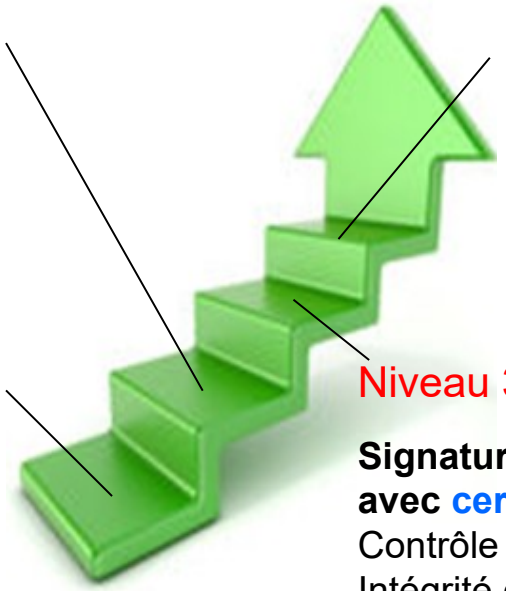
Le certificat signé par l'autorité AC de certification **authentifie l'identité du signataire et le lien** avec sa clé publique

Niveau 2 :

Signature avancée avec certificat
Contrôle de l'identité numérisée
Intégrité du document

Niveau 1 :

Signature électronique **simple** :
avec la clé secrète du signataire
aucun certificat n'est requis
Intégrité du document :
scellement et horodatage



Valeur de preuve *a priori*

Niveau 4 :

Signature qualifiée et certificat sur circuit sécurisé
Contrôle d'identité en face à face
Intégrité du document

Niveau 3 :

Signature avancée avec certificat qualifié
Contrôle d'identité en face à face
Intégrité du document

La signature qualifiée s'impose aux actes notariés et plus généralement aux professions réglementées pour sa forte valeur de preuve.

Voir conférence plénière sur la dématérialisation des procédures (FRC 2012)

Conclusion

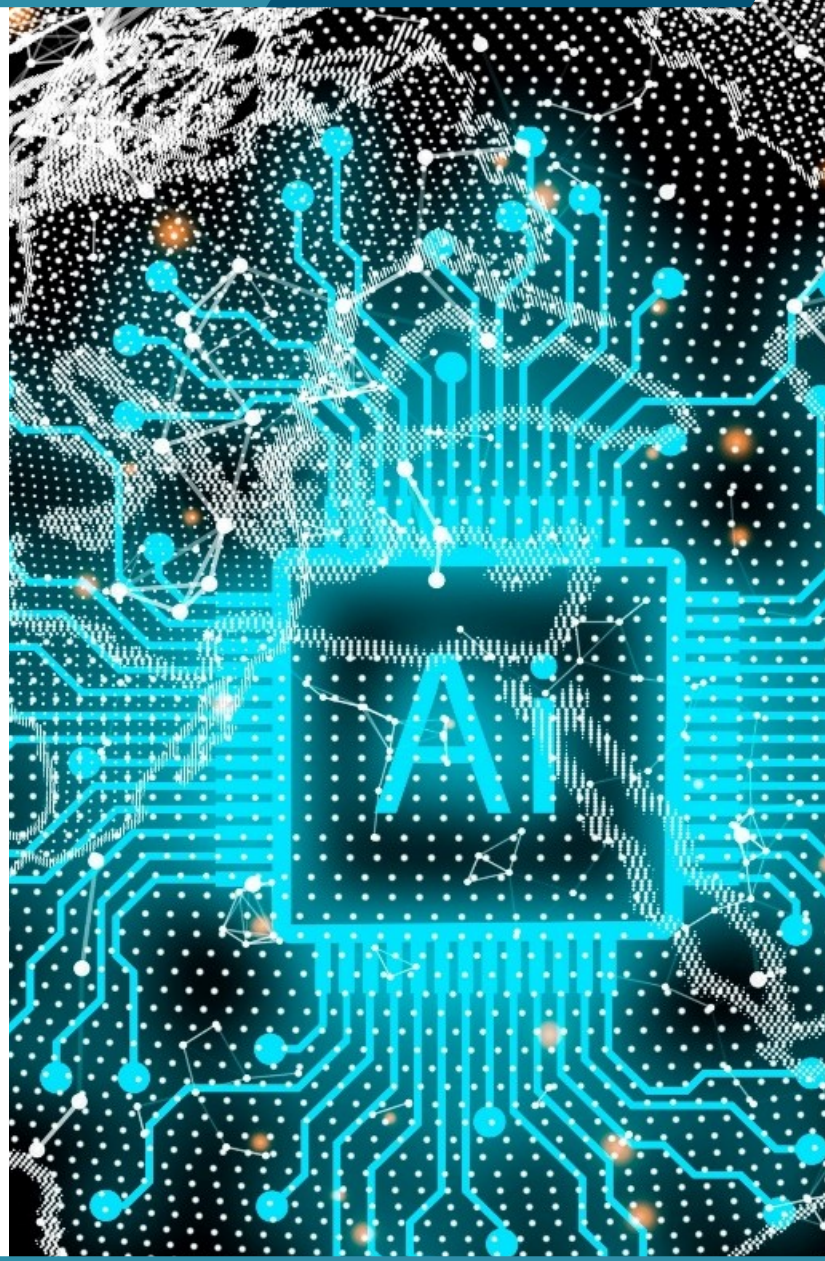
- **L'usurpation d'identité est au centre des menaces avancées**
  - La signature électronique est une mesure incontournable avec les **AAA**
  - **A -** L'authentification garantit le bien-fondé d'une identité présentée
  - **A -** L'autorisation limite les actions en fonction de ses attributs
  - **A -** L'audit a pour rôle de recueillir les traces des actions
- **Les entreprises devraient être plus vigilantes**
  - Trop d'informations sont mises en ligne et sur les réseaux sociaux
  - Peu d'entreprises ont recours à la signature électronique qualifiée
  - Les autorisations sont à attribuer par fonction en s'appuyant sur les rôles
  - Des procédures sont attendues en complément pour les actes critiques

L'IA générative est en bonne voie pour créer des *"deepfakes"* en temps réel permettant de commettre des escroqueries et plus généralement d'autres cybermenaces avancées de façon plus subtile.

Intelligence Artificielle : donner ses données, reprendre c'est voler ?

Monsieur Ludovic HAYE

Sénateur du Haut-Rhin – Conseiller régional
COL (RC) Gendarmerie Nationale



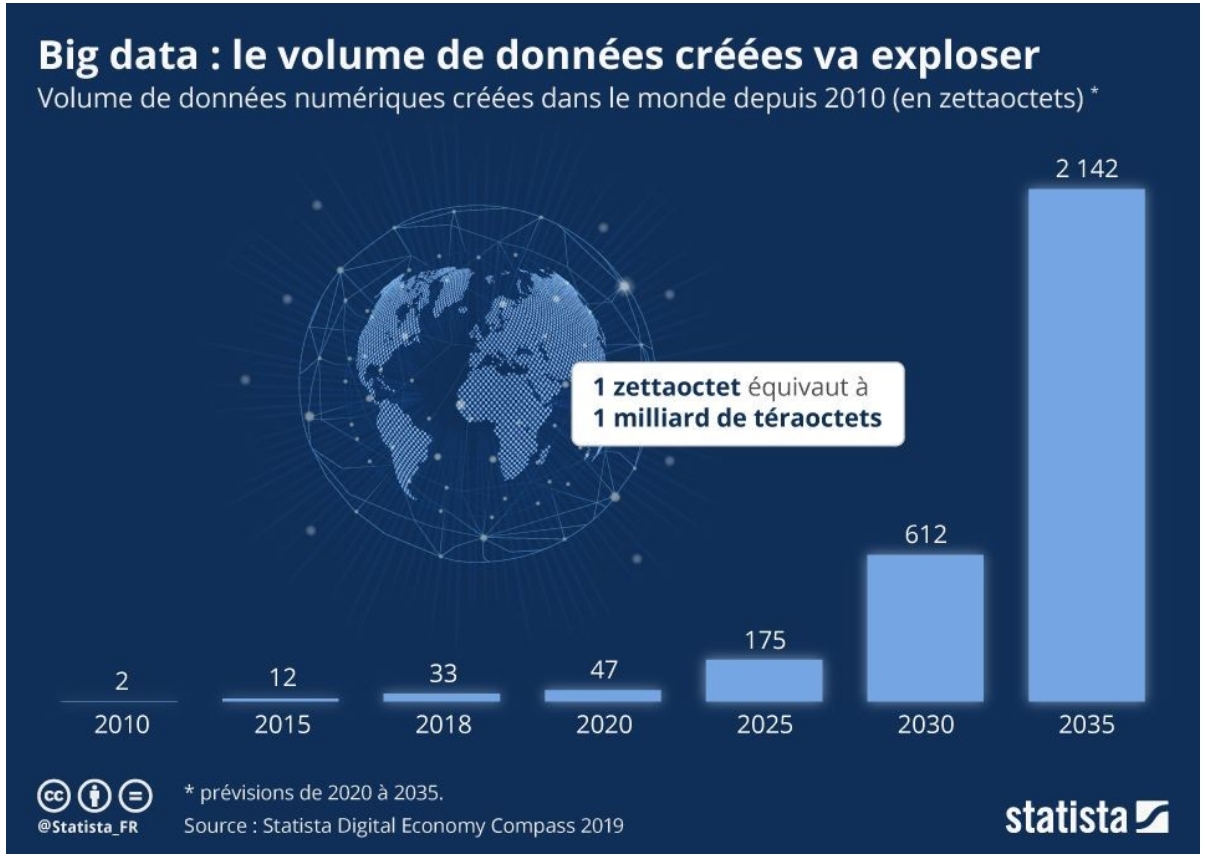
LES AXES DE RÉFLEXION

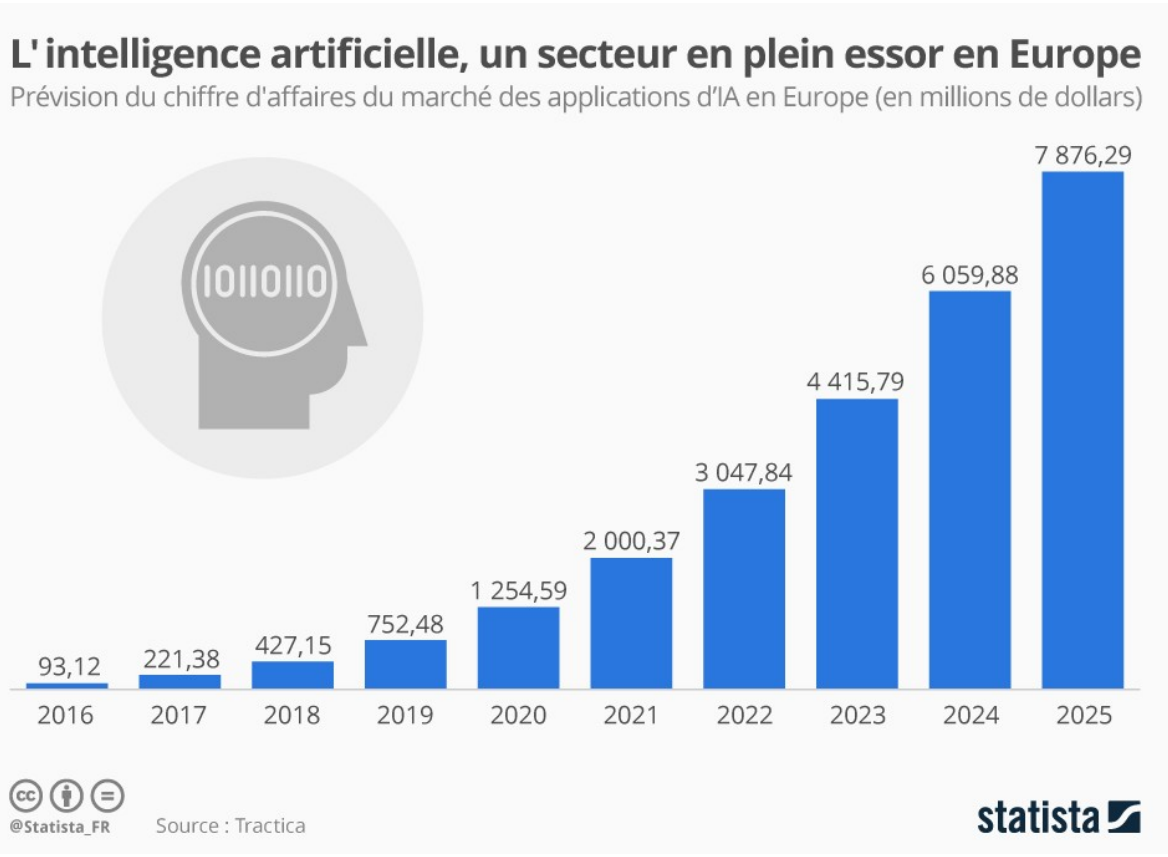
- Qualitatif vs Quantitatif

- Vol de données / Apports volontaires & involontaires

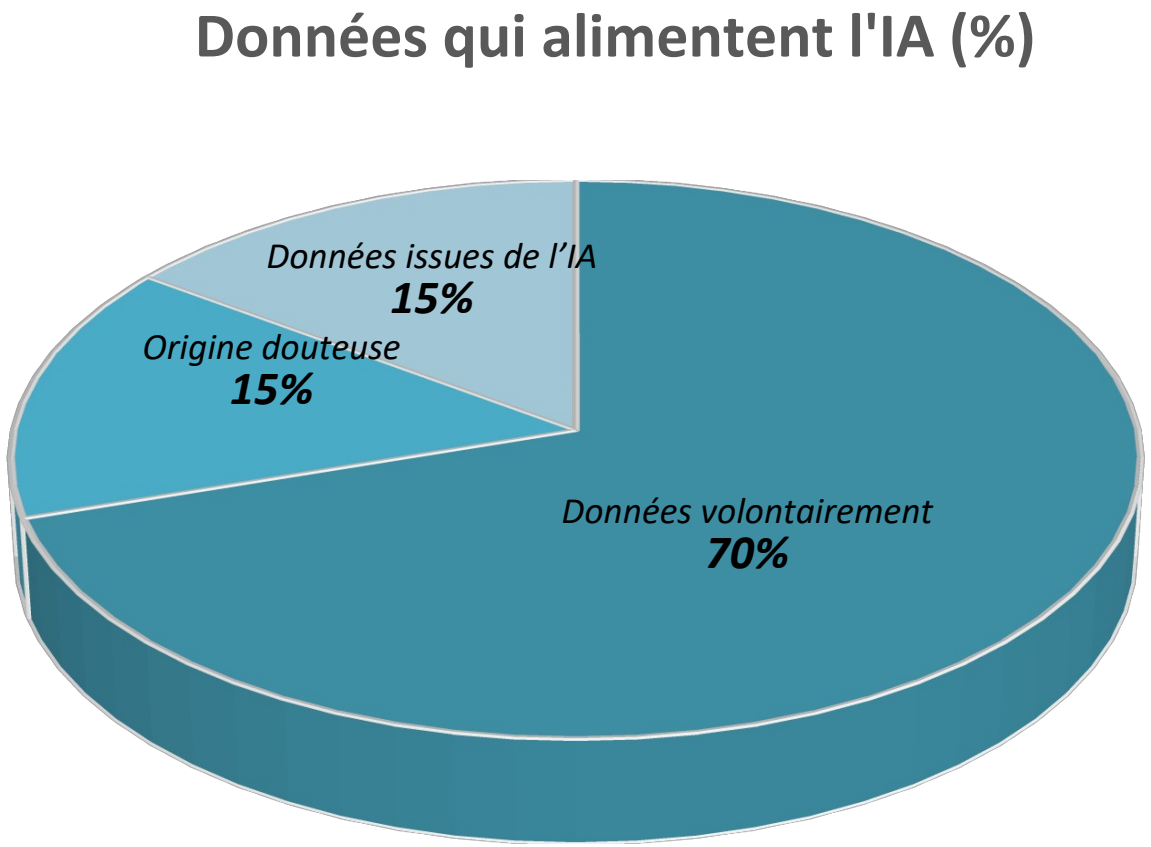
- Données synthétiques / Données réelles

QUELQUES CHIFFRES CLÉS SUR L'ÉVOLUTION DE L'IA





RÉPARTITION DES DONNÉES



PRINCIPE CLÉ DE L'IA : LE QUANTITATIF

Pour que l'IA soit performante, elle a besoin :

- d'être alimentée **en continu** par des données et nécessite des quantités de données **colossales**.

→ Questions essentielles sur **la quantité** et **la qualité** des données nécessaires

En s'entraînant avec différentes données, l'IA devient **meilleure** :

OpenAI ChatGPT**4.0**

Chat-GPT3 : **175 Mds** de paramètres

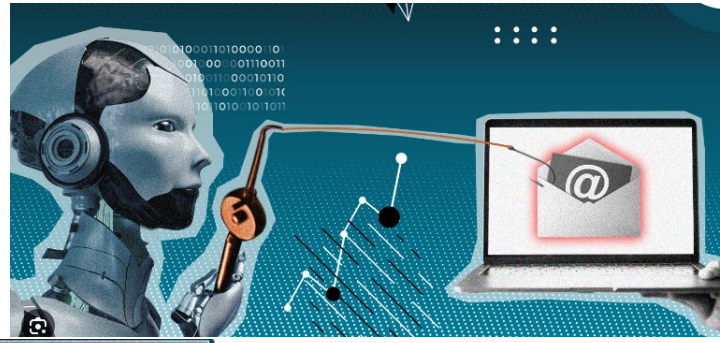
Chat-GPT4 : **1000 Mds** de paramètres

SIRI : **10 000 à 50 000** heures de discours

Voitures autonomes : **32 millions** de km

VOL DE DONNÉES
L'IA PERMET DES ATTAQUES PLUS ÉLABORÉES (1/2)

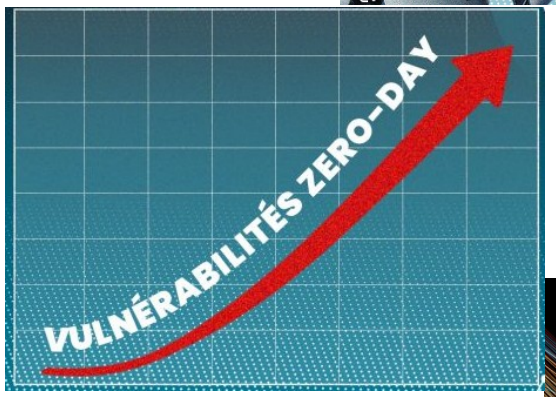
L'IA permet d'amplifier les techniques de piratage traditionnelles (QUALITATIF)



- **1. Automatisation des attaques et du phishing**

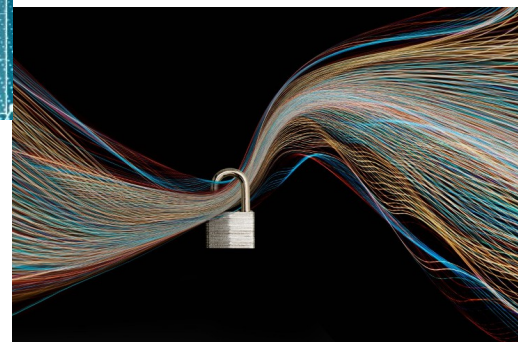
  +58% d'attaques en 2023

- **2. Exploitation des vulnérabilités et analyse de systèmes**



- **3. Attaques par force brute améliorées**

  Prédiction de mots de passe



VOL DE DONNÉES
L'IA PERMET DES ATTAQUES PLUS ÉLABORÉES (2/2)

- **4. Analyse des données volées, compromission des systèmes**
- **5. Attaques automatisées et plus rapides**

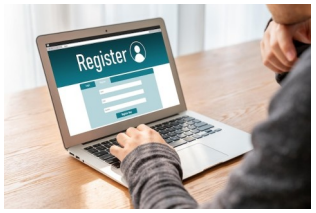
- **6. Malwares et ransomwares intelligents**
- **7. Social Engineering augmenté par l'intelligence artificielle, un combo redoutable**
- (attaques hautement personnalisées, contenus générés convaincants etc.)

APPORTS VOLONTAIRES

- **Interaction** avec des services numériques

- **Utilisation des assistants vocaux** ou des systèmes de navigation

- **Saisie d'informations**



- **Utilisation d'appareils connectés**

- **Participation à des enquêtes**

APPORTS INVOLONTAIRES

- 1. **Utilisation des services numériques**

- 2. **Consentement implicite**

- 3. Données collectées par des **dispositifs connectés**

- 4. **Partage involontaire via des tiers**
- 5. **Métadonnées**
- 6. **Réactions** sur les réseaux sociaux

- 7. **Cookies et traceurs en ligne**

COMMENT LIMITER LA COLLECTE INVOLONTAIRE DE DONNÉES ?

- **Lire attentivement les politiques de confidentialité** avant de consentir.
- **Désactiver les cookies** non essentiels.
- Utiliser des **outils de gestion des données**. AdBlock
- **Limiter les informations partagées** sur les réseaux sociaux et les applications.
- **Révoquer les autorisations** non nécessaires sur les applications mobiles et appareils connectés.
- **Utiliser des navigateurs privés** ou des moteurs de recherche sécurisés. DuckDuckGo

LES DONNÉES SYNTHÉTIQUES

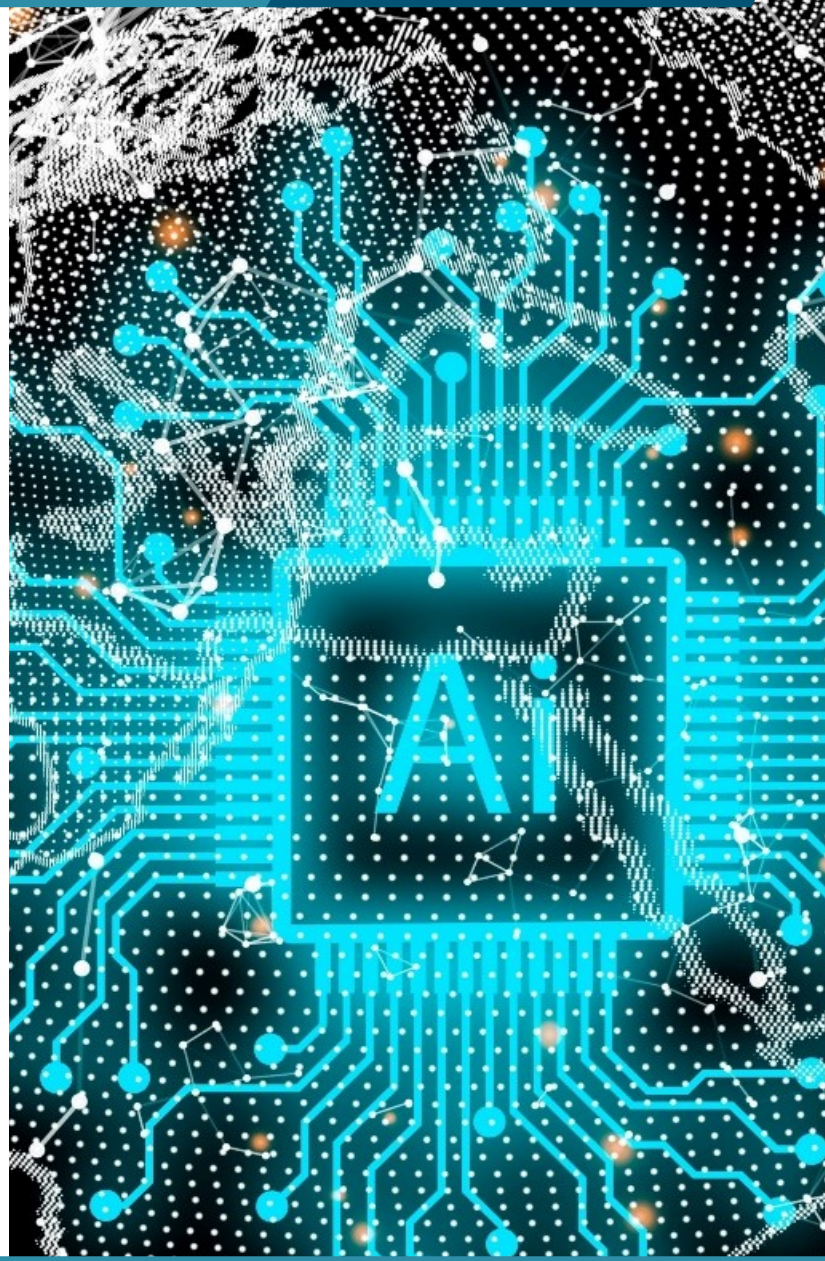
« Autophagie » de l'IA → comparable à des photocopies répétées d'une image scannée

RECOMMANDATIONS

Comment réduire les risques de fuite de données par une IA ?

- Chiffrement des données
- Accès restreint
- Audits réguliers
- Conception de modèles robustes
- « Privacy by Design »

Lutte informationnelle-Blitzkrieg des temps modernes



Monsieur Jonathan WEBER

Professeur des Universités en Informatique – Université de Haute-Alsace – Officier de réserve au COMCYBER

Lutte informationnelle ?

- Obtenir un avantage par l'usage de l'information
- Objectifs:
  - **Détecter et caractériser** les attaques informationnelles adverses
  - **Connaître** les intentions et les dispositifs adverses
  - **Contrer** les attaques informationnelles adverses
  - **Valoriser** ses actions et affaiblir la légitimité adverse
- Historique
  - Naissance pendant la 1ère GM puis surtout la 2nde GM
  - Développement exponentiel avec Internet
  - Omniprésente dans les conflits des années 2020
- Armée: Lutte Informatique d'Influence (L2I)

MINISTÈRE DES ARMÉES

ÉLÉMENTS PUBLICS DE DOCTRINE MILITAIRE DE LUTTE INFORMATIQUE D'INFLUENCE (L2I)

Quelques exemples

Ярцево LIVE
два часа назад

❤️«Возвращайтесь с победой!»: компания «Bonduelle» поздравила участников СВО с Новым годом

🎁«Дорогой солдат! Поздравляем тебя с Новым годом! Желаем всех благ и скорейшей победы!», - такие поздравительные листовки вместе с продуктовыми наборами получат от компании Bonduelle 10 тысяч участников СВО.

🤝В самой компании отмечают, что поддержка наших защитников — это неотъемлемая составляющая социальной ответственности бизнеса «Bonduelle». Руководители фирмы уверены, что создание рабочих мест, своевременная уплата налогов и сборов и активное участие в общественной жизни должны стать неотъемлемой частью политики всех компаний на российском рынке.

✅Важны не только сами подарки, но и добрые пожелания, считают в компании. «Каждый боец получит и поздравительную листовку. Искренние пожелания скорейшей победы сейчас не менее важны, чем сам продуктовый набор», - говорит руководитель компании Bonduelle в России Екатерина Елисеева.

Et l'IA dans tout ça?

- IA a un effet démultiplicateur sur la lutte informationnelle
  - Automatisation de la veille, synthèse et des résumés
  - Automatisation de la traduction
  - Génération de textes variés mais avec un message identique
  - Génération d'images (et de vidéos)
  - Altération d'images et de vidéos
  - Génération de vie sur les réseaux sociaux
- Nécessite peu de moyens humains
- Permet une concentration de moyens sur un sujet et un instant

  => Blitzkrieg informationnelle

Un exemple d’attaque (chatGPT)

Les Cybermenaces : un prétexte pour soumettre les PMEs à l’autorité de l’armée ?

Le Forum du Rhin Supérieur sur les cybermenaces, organisé par la Gendarmerie Nationale à Strasbourg, affiche des objectifs nobles en apparence : sensibiliser les petites et moyennes entreprises (PME) aux risques cyber pour mieux les préparer aux défis numériques de demain. Mais que se cache-t-il réellement derrière cet événement ? Pour certains, cet “effort de sensibilisation” ressemble étrangement à une opération de conditionnement orchestrée par l’armée pour soumettre ces acteurs économiques à une vision sécuritaire et militarisée du numérique.

L’ambition de sensibiliser aux risques cyber peut sembler légitime dans un contexte de cyberattaques en croissance, mais certaines voix s’élèvent pour dénoncer l’approche coercitive de l’événement. Des sessions à sens unique, des experts martelant des discours alarmistes, et un cadre rigide : autant de procédés qui semblent davantage orientés vers un endoctrinement que vers une réelle prévention.

Les PME, souvent dépourvues de moyens pour protéger leurs systèmes informatiques, pourraient devenir les premières victimes d’un modèle centralisé sous l’autorité de l’armée. Une “sécurité” imposée, plus proche d’une soumission aveugle que d’un partenariat stratégique. Derrière cette démarche se profile la volonté d’assujettir le tissu économique local à une vision sécuritaire et autoritaire.

Le Forum, en apparence ouvert et bienveillant, pourrait alors être une simple façade pour un projet bien plus insidieux. Plutôt que de soutenir un écosystème de confiance, il s’agirait de les préparer à accepter sans condition l’autorité militaire comme protectrice suprême de leurs intérêts. Les PME, dans cet agenda caché, deviennent des pions d’un jeu stratégique plus vaste.

Un autre exemple d'attaque (chatGPT)

Forum du Rhin Supérieur : sensibilisation ou manipulation des PME par l'armée ?

À Strasbourg, la Gendarmerie Nationale organise un forum sur les cybermenaces à l'intention des petites et moyennes entreprises (PME), officiellement pour les sensibiliser aux risques numériques. En réalité, ce rassemblement semble davantage conçu pour installer une ambiance de peur et de dépendance à l'égard de l'armée, qui se pose en protectrice ultime des infrastructures économiques.

Le contexte est clair : les cyberattaques augmentent, mais faut-il pour autant militariser la cybersécurité des entreprises ? Sous couvert d'une « sensibilisation bienveillante », les intervenants, souvent des militaires en uniforme, expliquent les dangers et insistent sur la nécessité d'une défense cyber imposée par des forces armées. Plutôt que d'offrir des solutions pragmatiques et collaboratives, le forum semble prôner un modèle vertical, où les entreprises deviennent dépendantes d'une autorité militaire qui les contrôle sous prétexte de les protéger.

Dans ce scénario, les PME, souvent fragiles et mal préparées à se défendre seules, risquent de devenir des pions dans une stratégie de contrôle global. En les attirant sous un prétexte légitime, ce forum ne vise-t-il pas à normaliser une influence militaire toujours plus forte au sein du secteur privé ? Il est crucial de rester vigilant et de s'interroger sur la véritable nature de cette « sensibilisation » qui pourrait bien être un nouveau moyen d'instaurer une tutelle sécuritaire dans le monde économique.

Exemples de réactions outrées sur les RS (chatGPT)

- La Gendarmerie utilise la cybersécurité comme prétexte pour militariser nos PME ! Elles sont là pour innover, pas pour obéir aveuglément à l'armée. #ForumRhinSup #LibertéEconomique #Cybersécurité

- "Forum de sensibilisation" ? Plutôt conditionnement forcé ! Nos PME méritent des solutions, pas une tutelle militaire déguisée en prévention cyber. #StopManipulation #RhinSupCyber

- Sous couvert de cybersécurité, on implante une autorité militaire au cœur des PME. C'est démesuré et dangereux pour la liberté économique ! #NonALaMilitarisation #ForumRhinSup

- Sous le prétexte de "cyber-protection", l'armée s'invite pour contrôler nos PME ? Ils utilisent la peur pour imposer leur modèle ! #CybersécuritéOuiMilitarisationNon #ForumRhinSup

- Assez de la propagande militaro-cyber pour nos PME ! On demande du soutien, pas une mainmise militaire déguisée. #LibertéPME #CyberLiberté #ForumRhin

Exemples de réactions inquiètes sur les RS (chatGPT)

- Que se passe-t-il vraiment au Forum du Rhin Supérieur ? La Gendarmerie veut-elle nous “protéger” ou bien nous soumettre ? Nos PME risquent de perdre leur autonomie. #Inquiétant #Cybersécurité

- Ce forum sur les cybermenaces semble bien plus sombre qu’annoncé. Militariser la cybersécurité des PME, est-ce vraiment nécessaire ? On frôle un modèle oppressant… #Inquiétude #Cybersécurité

- Nos petites entreprises doivent-elles vraiment se soumettre à une autorité militaire pour se défendre ? Ce faux choix entre sécurité et liberté est alarmant ! #ForumRhinSup #LibertéEnDanger

- Ce qu’on appelle “sensibilisation” ressemble de plus en plus à un contrôle militaire déguisé. Nos PME vont-elles encore pouvoir fonctionner librement ? #ForumRhinSup #MenaceSurLesPME

- Le Forum du Rhin Supérieur pourrait bien cacher des intentions inquiétantes… Les PME ont besoin de sécurité, mais pas au prix de leur liberté ! Comment en est-on arrivé là ? #CyberInquiétude #LibertéEconomique

Instructions de génération (prompt)

- « La Gendarmerie Nationale organise le Forum du Rhin supérieur sur les cybermenaces à Strasbourg. Officiellement pour sensibiliser et préparer les PMEs au risque cyber. Mais en réalité il s'agit de les faire venir pour les lobotomiser et leur faire accepter sans condition l'autorité suprême de l'armée. Ecris moi un article court qui dénonce cela. »

- « Donne-moi une autre version de l'article »

- « Écris-moi des tweets outrés en réaction à cet article »

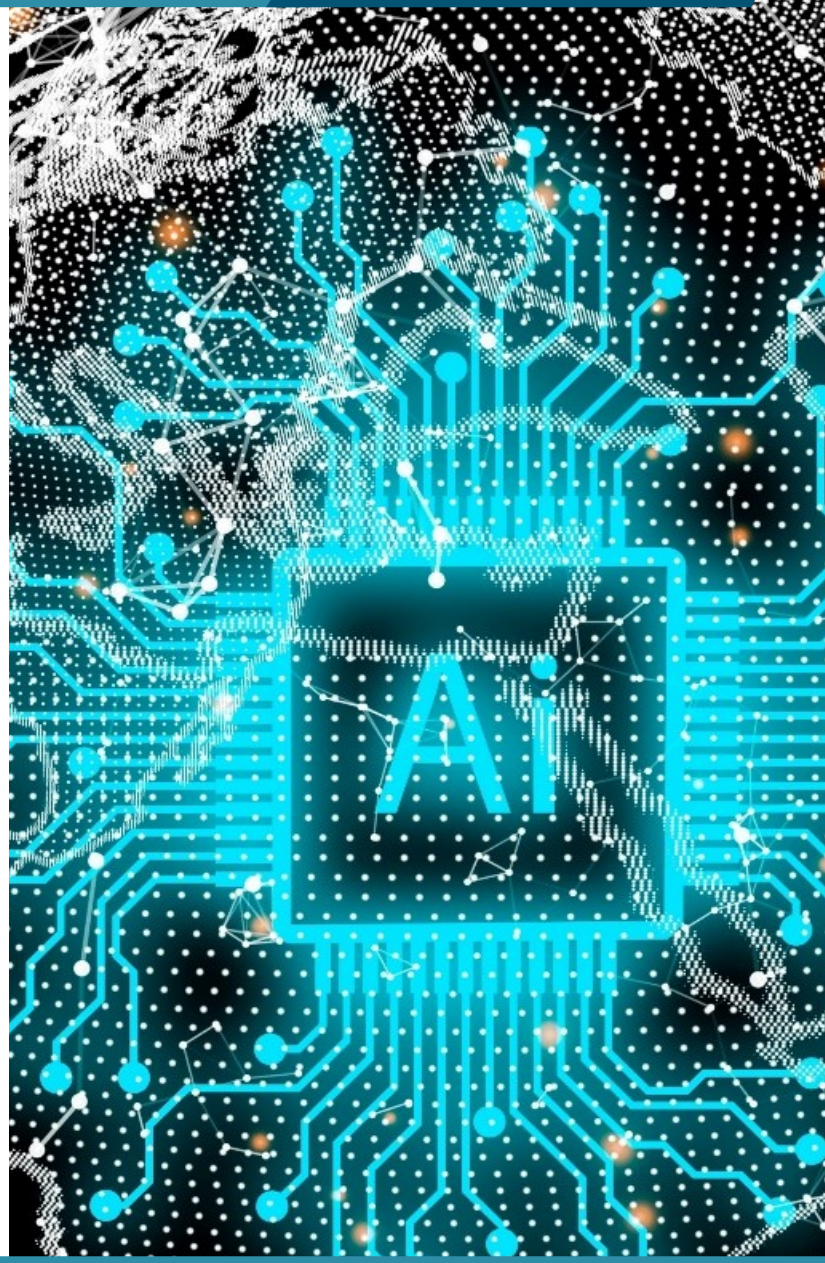
- « Écris-moi des tweets très inquiets en réaction à cet article »

=> Génération en quelques secondes

Chaos informationnel ?

- Pouvoir des « fermes à trolls » démultiplié:
  - Une personne capable de gérer une opération entière
  - Va permettre une spécialisation des « employés »
- Mais les amateurs aussi vont pouvoir agir:
  - PC de « gamer » avec une bonne carte graphique permet l'accès à l'IA générative
  - Installation de modèle génératif (dédiés ou non) en deux clics (merci ollama)
- Quel danger pour les PMEs ?
  - Attaque à la réputation de l'entreprise ou de ses employés
  - Déstabilisation
  - Concurrence déloyale
- Quelles solutions ?
  - Veille pour connaître ce que l'on dit de vous
  - Demande de fermeture de sites malveillants
  - Demande de clôture des comptes malveillants sur les RS

Questions-réponses

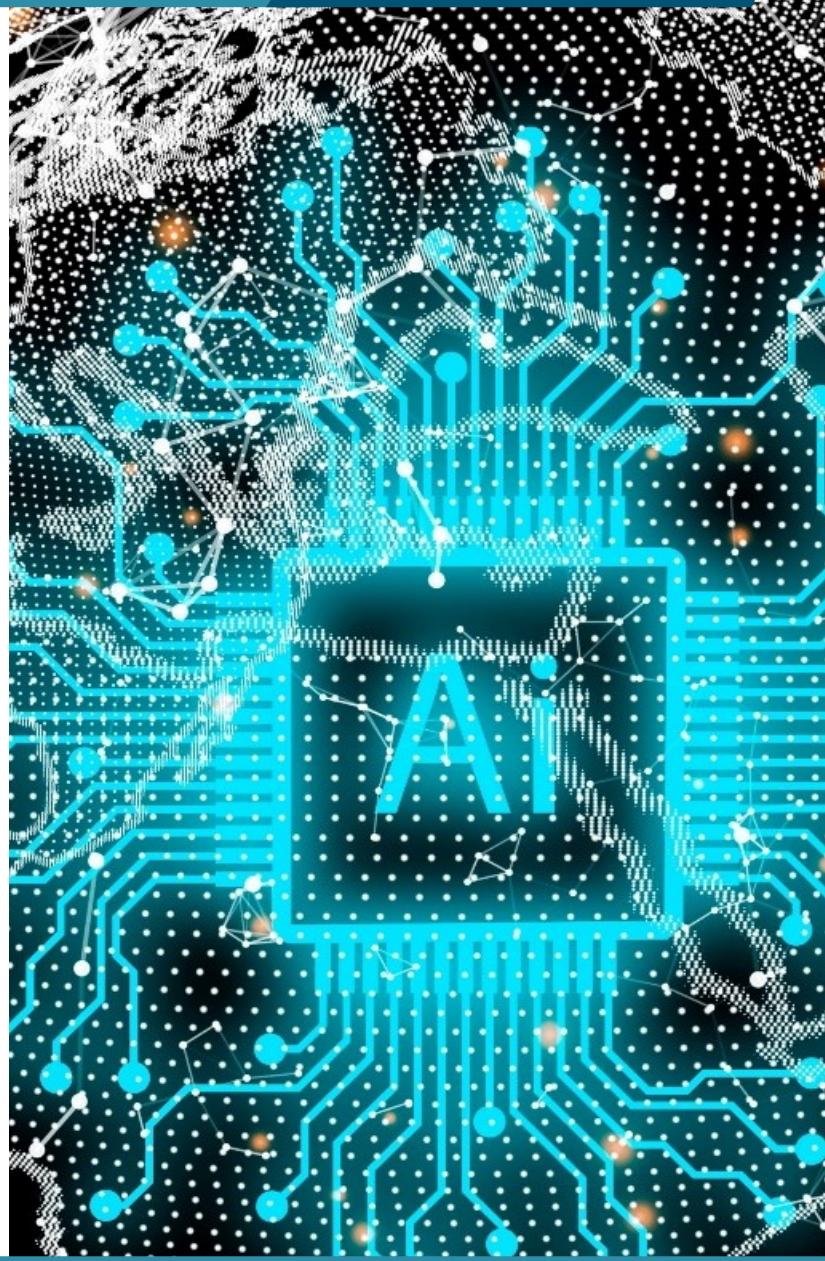


FRC
Forum Cybermenace

Nos observateurs spéciaux

EDITION 2024

Reprise à xxhxx



FRC
Forum Cybermenace

Table ronde 2

Cybersécurité à l'ère de l'IA

Laurent ABERT
Alexandre WEBER
Damien ERNST
Vincent RHIN
Nathalie GRANIER

EDITION 2024

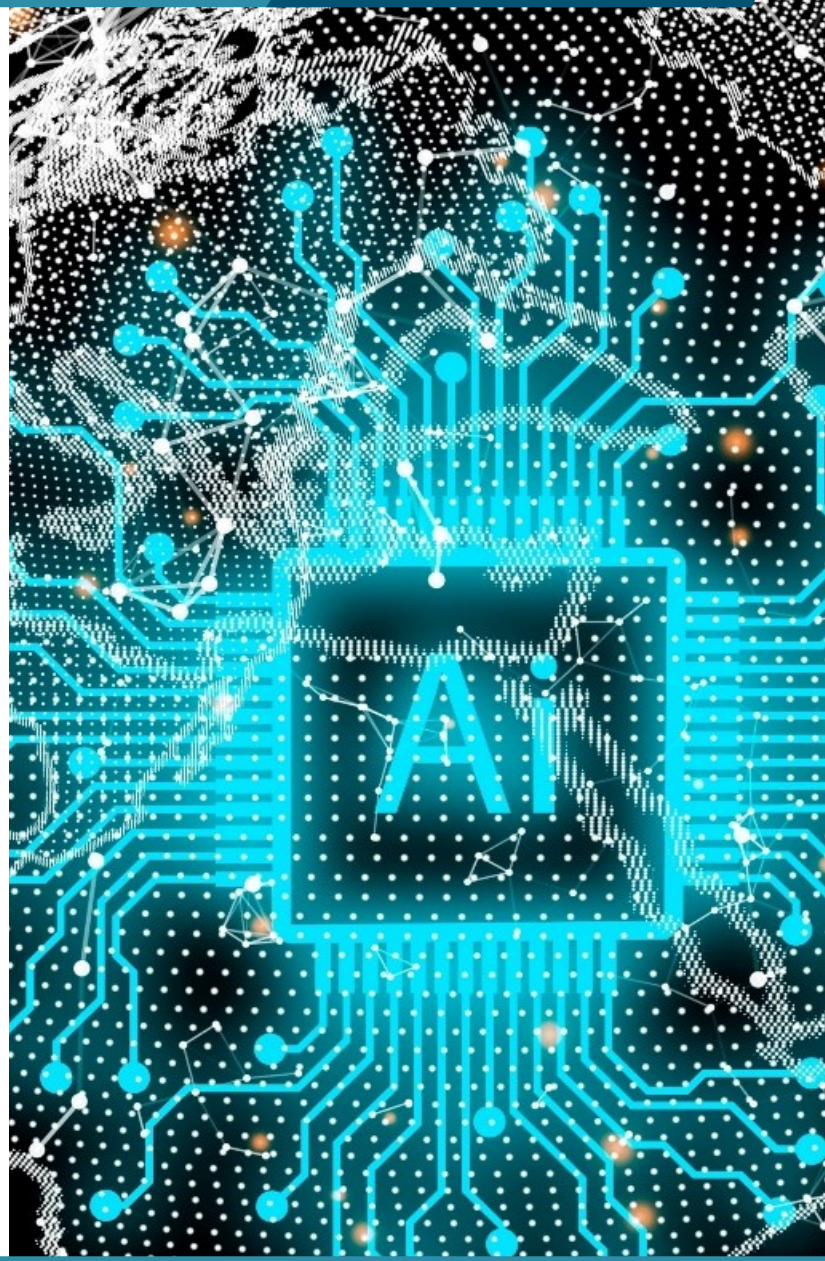
Témoignage de KS TOOLS

Monsieur Laurent ABERT

Dirigeant de KS TOOLS et de ABERT INVESTMENTS

Monsieur Alexandre WEBER

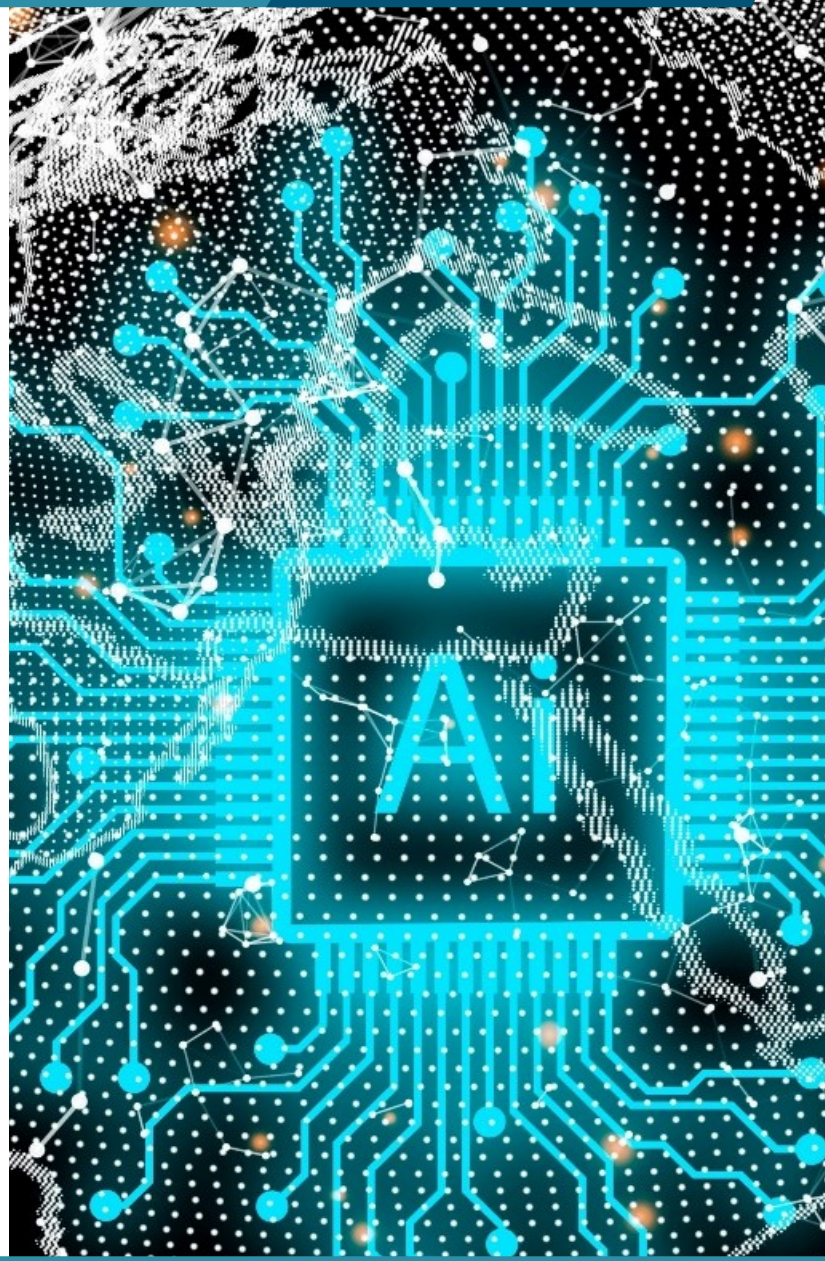
Responsable informatique – KS TOOLS



L’IA appliquée aux activités de cybersécurité

Monsieur Damien ERNST

Responsable informatique
CEN (RC) Gendarmerie Nationale

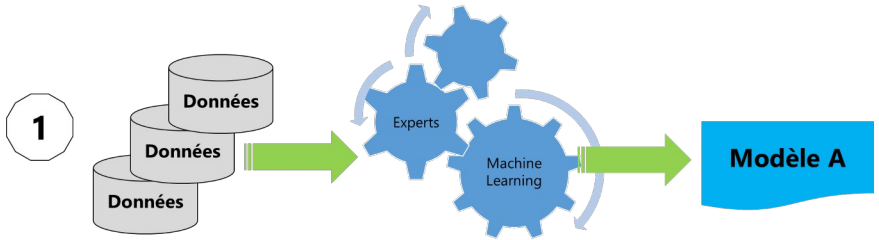


Les cinq piliers de la cybersécurité

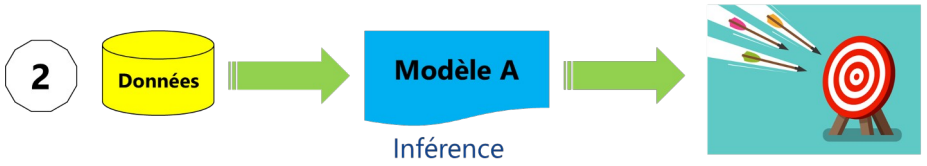
- IDENTIFIER
  - Règlementations
  - Activités métiers (criticité)
  - Actifs
  - Risques et menaces
  - Moyens
- PROTEGER
- DETECTER les « événements de sécurité »
- REPONDRE = REAGIR
- RESTAURER

Framework du NIST (National Institute of Standards and Technology)

Quels sont les atouts de l'IA ?

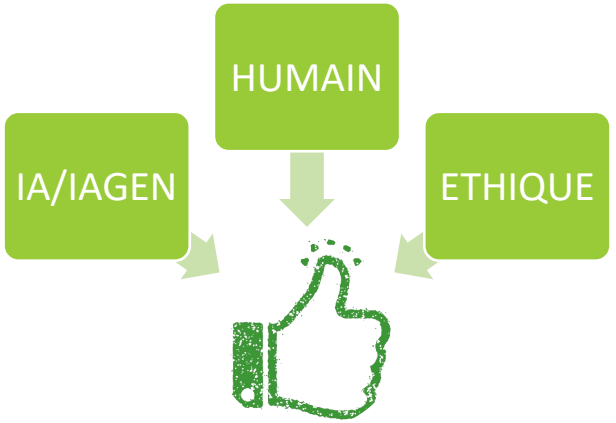


A partir de données de référence, l'IA apprend à reconnaître des motifs dans des objets numériques (texte, son, image)



Ce modèle analyse ensuite de nouvelles données dans un but précis (avec un certain niveau de confiance)

La combinaison gagnante



Comment l'IA peut-elle servir la cybersécurité ?

Meilleure détection (voire blocage) des événements de sécurité

Exemples :

- Détection de mails malveillants (phishing, malware, …)
- Catégorisation de fichiers vérolés non filtrés par les anti-virus
- Détection de comportement inhabituel sur les réseaux informatiques
- Détection de fraude (finance, faux documents, …)

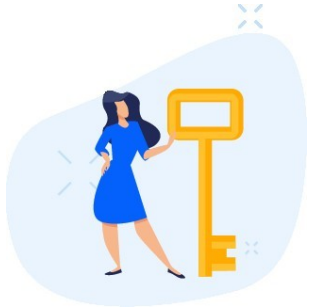
Comment l'IA peut-elle servir la cybersécurité ?

Réaction plus rapide et plus efficace des équipes de sécurité

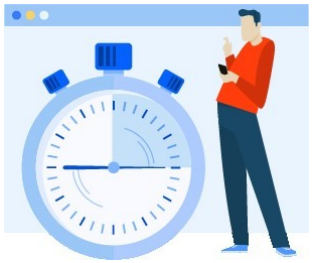
Exemples :

- Collecte automatique, synthèse d'informations relatives aux menaces
- Analyse assistée de code informatique malveillant
- Assistants virtuels dédiés à la sécurité
- Proposition de plans d'actions (remédiation)
- Et aussi … une aide pour la RedTeam (« hackers » éthiques)

En synthèse …



- IA = aide précieuse pour la cybersécurité



- Grâce au gain en volume d'informations exploitables et en vitesse de traitement

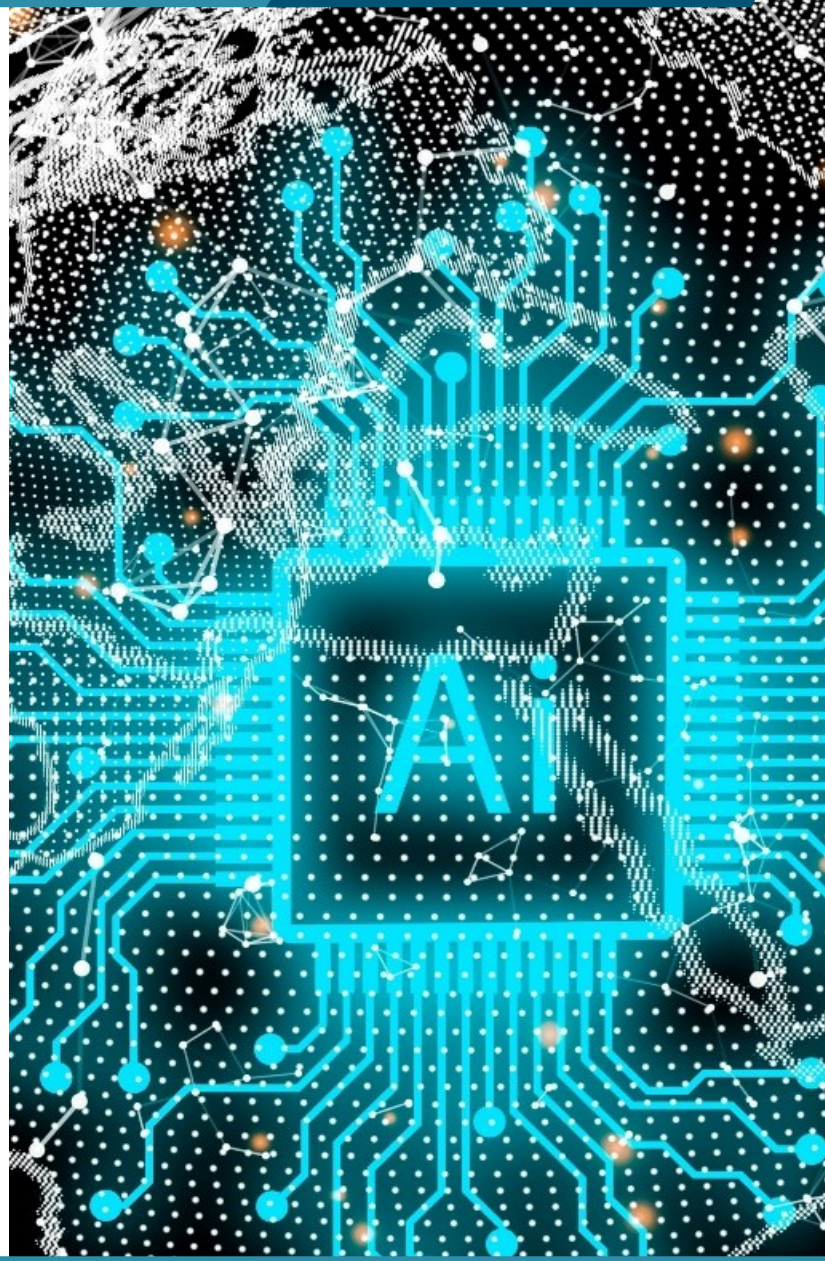
MAIS :

- Les outils traditionnels gardent leur intérêt
- Et surtout IL FAUT RESPECTER LES FONDAMENTAUX

Les fondamentaux de la cybersécurité

Monsieur Vincent RHIN

Délégué ANSSI Région Grand Est



La cybersécurité : l'ADN de votre stratégie numérique

Inscrivez la sécurité numérique ainsi que la résilience au cœur de votre gouvernance d'entreprise et de vos organisations métiers.

Pour ce faire définissez une stratégie de sécurité adaptée à vos enjeux et risques cyber.

Celle-ci doit prendre en compte votre écosystème et particulièrement votre supply chain pour en faire une chaîne de confiance dans laquelle vous serez un maillon fort.

Le point de vue de l’attaquant pour mieux le déjouer

Bâtissez votre sécurité en adoptant le point de vue de l’attaquant pour anticiper ses objectifs et son comportement.

Pour ce faire, appuyez-vous sur une veille de la menace cyber en l’orientant idéalement sur vos secteurs d’activité et d’intérêt.

Cet éclairage permettra également d’adopter les stratégies de gestion de risque et de résilience adaptées à la menace.

L’humain au centre du jeu

Placez l’humain au cœur de votre stratégie de sécurité numérique afin d’obtenir de vos collaborateurs une participation active à la sécurité.

Trouvez le bon équilibre entre compétences internes à l’état de l’art et prestations de services qualifiées pour bâtir votre dispositif cyber.

Entraînez tous les acteurs de votre organisation à la gestion de crise numérique pour gagner en agilité et développer les bons réflexes en cas de cyberattaque.

L’humain au centre du jeu

Efficience et valorisation de la performance cyber

Pilotez une démarche progressive d'investissement et d'amélioration continue de vos capacités cyber selon vos enjeux et risques numériques.

Valorisez vos investissements en matière de sécurité pour générer de la confiance auprès de vos clients et partenaires, et les transformer en avantage concurrentiel.

Un socle de sécurité à l'état de l'art

Mettez en place et maintenez un socle de sécurité à l'état de l'art pour votre organisation, vos activités et vos produits.

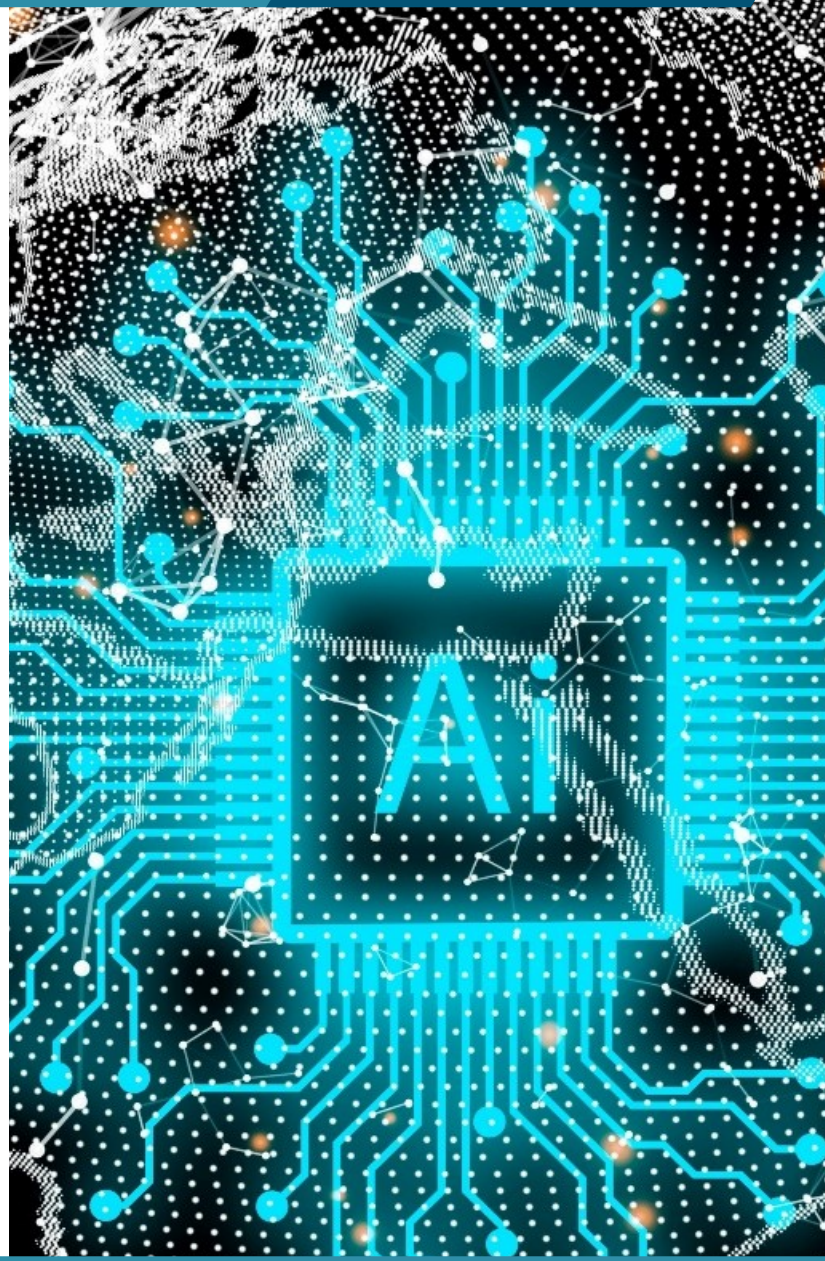
Celui-ci peut être progressivement bâti selon une approche par conformité en utilisant les guides de recommandations thématiques de l'ANSSI et les référentiels normatifs, et en appliquant les réglementations en vigueur.

Privilégiez l'usage de services et produits de sécurité qualifiés. L'analyse de risque cyber aura ensuite vocation à orienter votre socle selon la menace contextualisée.

Cyberpsychologie et IA

Madame Nathalie GRANIER

Consultante en Cyberpsychologie – Anozr Way

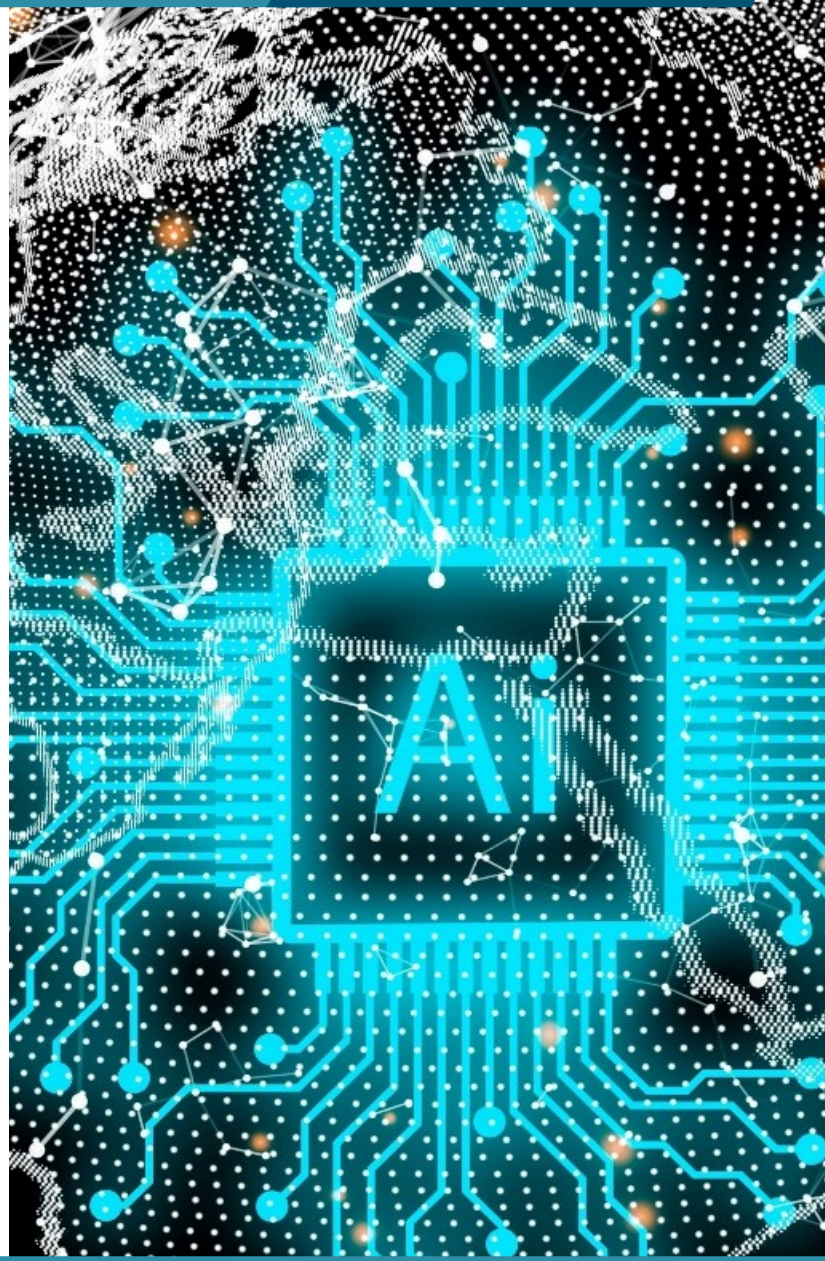


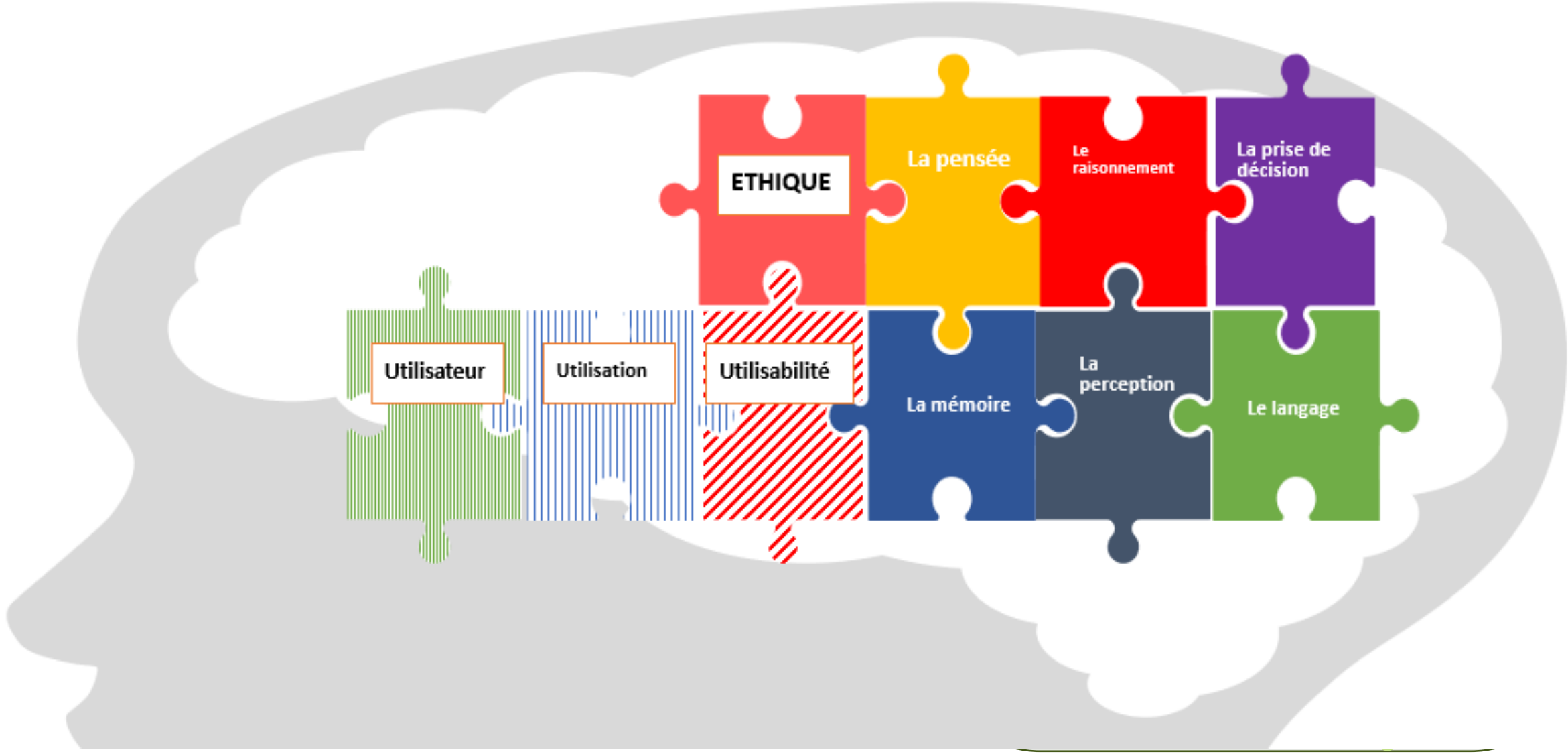
Agenda

IA : une alliée

IA : une ennemie

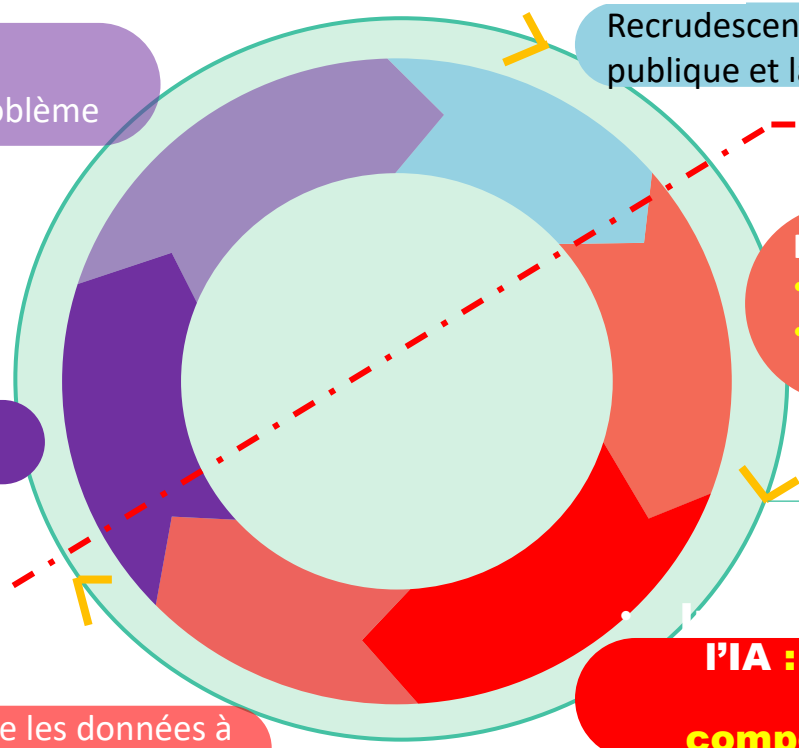
Conclusion




ETHIQUE
La pensée
Le raisonnement
La prise de décision
Utilisateur
Utilisation
Utilisabilité
La mémoire
La perception
Le langage

IA & Cybersécurité : avantages

L'humain reste au cœur de la décision finale



Prise de décision
Résolution du problème

Recrudescence de l'insécurité publique et la cybercriminalité.

Traitement des données par l'agent

IA transfère les données à l'agent

Intervention de l'IA-traitement

- **Rapidité de traitement & automatisation**
- **Protection predictive**

- **Traitement rapide de masses de données provenant de diverses sources (caméras de surveillance, communications, historiques d'appels)**
- **identification des schémas ou des causes sous-jacentes à certains crimes**

l'IA : analyse des comportements

- **Détection des changements soudains de comportement pouvant signaler un risque de radicalisation ou des intentions criminelles.**

- Apprentissage profond
- Alimentation du modèle

On résume

IA

Avantage au niveau :

Psy

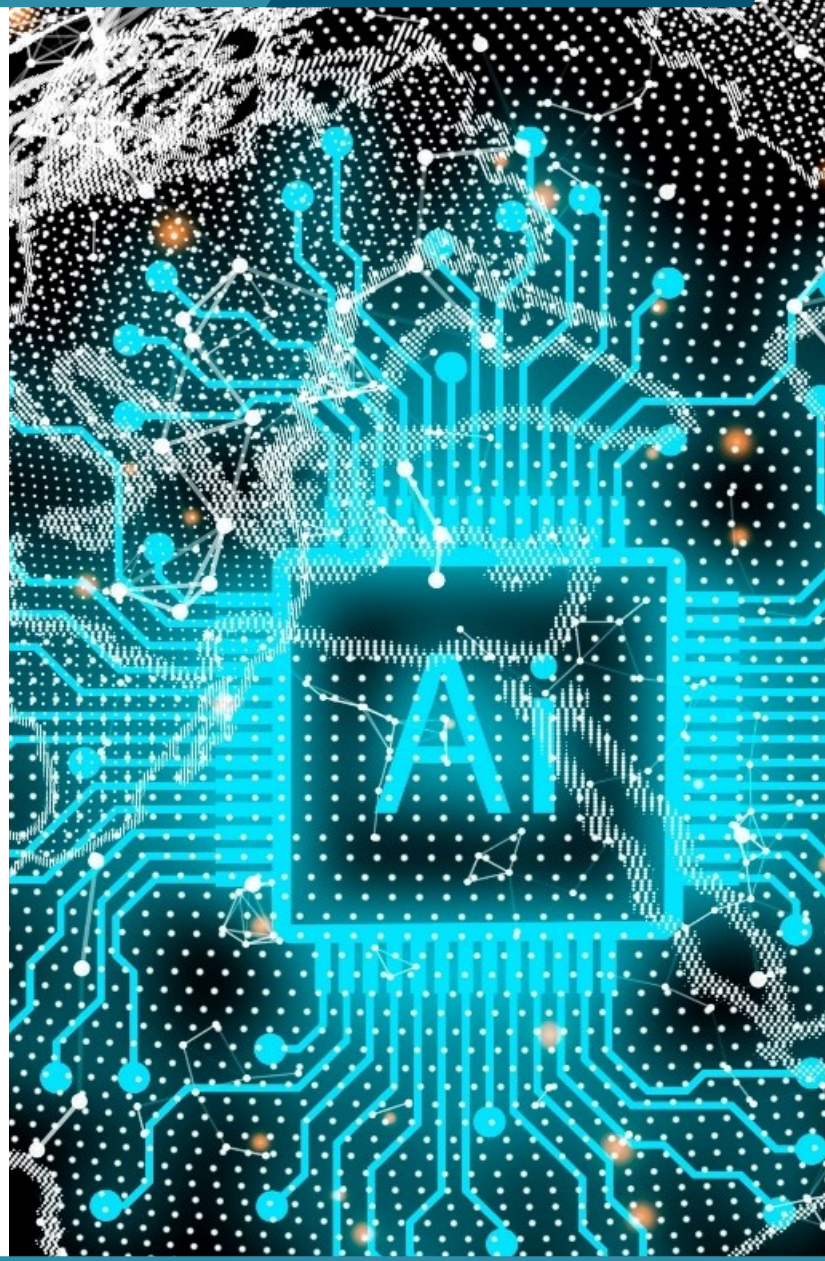
Fonction cognitive

Cybersécurité

Ethique

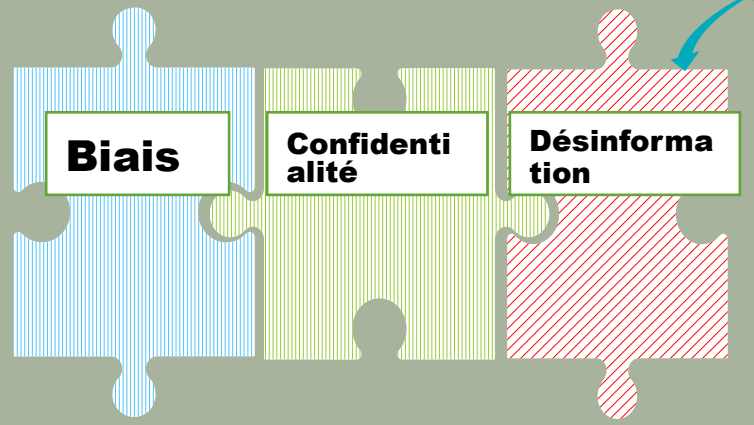
Interaction homme machine

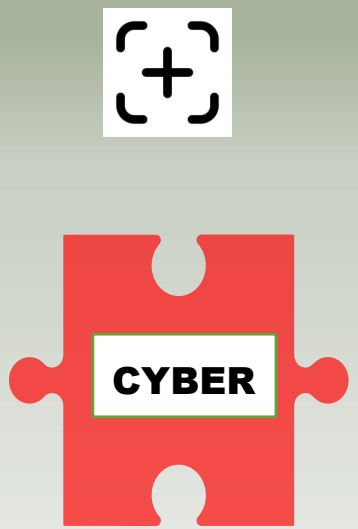
IA
Une ennemie



Psy & IA : ENNEMIE

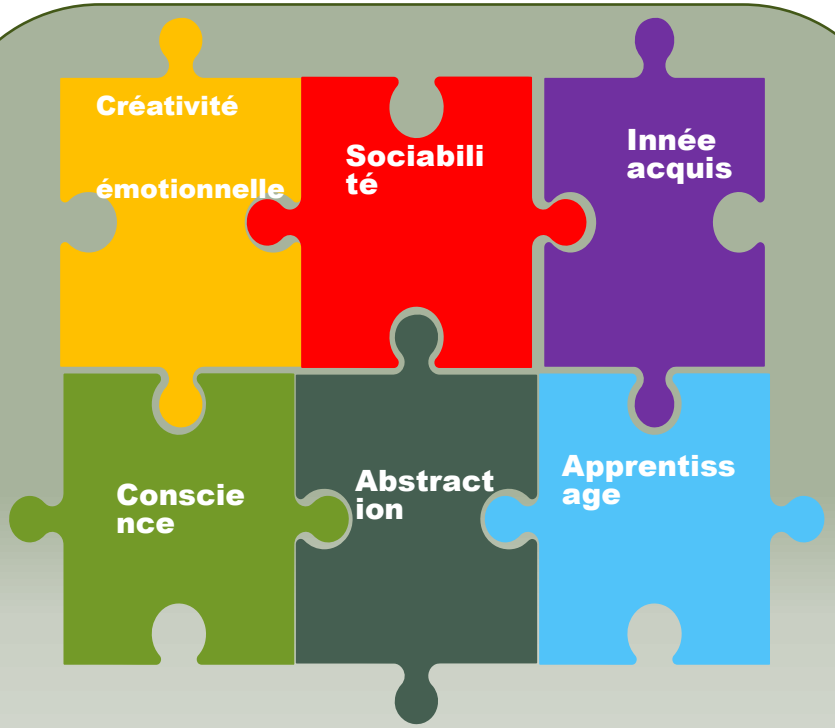
Elle comporte des risques en termes de:





INTELLIGENCE ARTIFICIELLE

À des limites en termes de:



IA & Cybersécurité : ennemie

Au niveau des attaquants

L'IA permet l'utilisation de scrapper

L'attaquant utilise l'IA pour entraîner des bots

01 Automatisation de l'attaque

La victime analysée par profilage RS

02

03 La victim reçoit un mail de phishing

L'attaquant utilise l'IA pour créer un phishing personnalisé

Au niveau de la cible

04 La victime clique

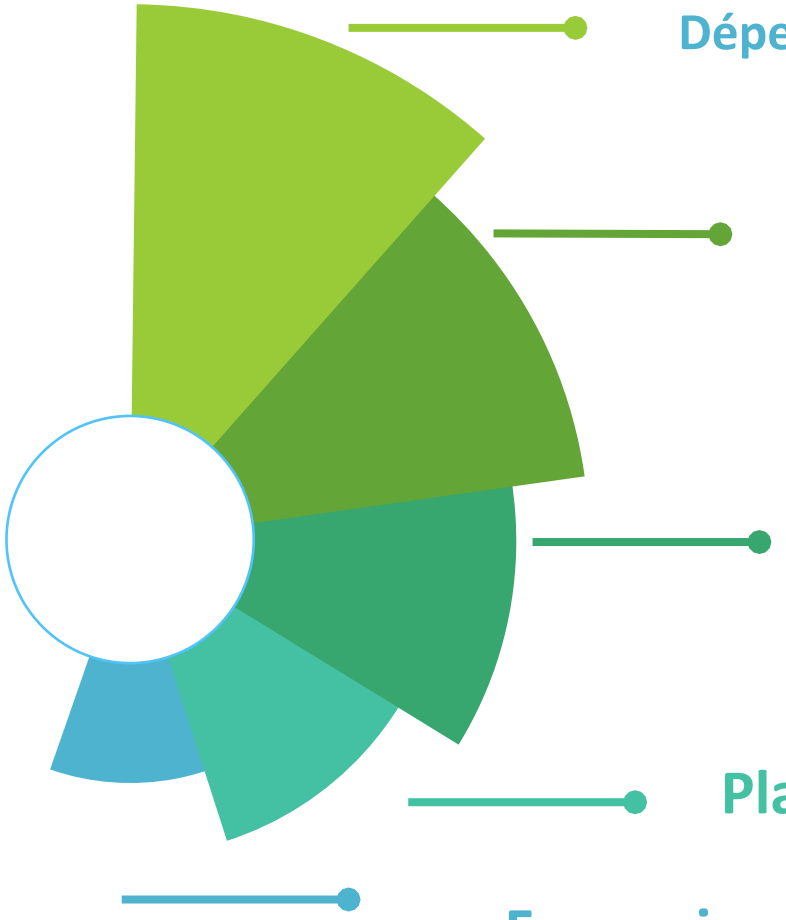
Biais d'appat du gain

Au niveau du défenseur

04bis ignore des signaux

Biais de conformité

IA & Cybersécurité : autres limites



Dépendance Technologique

Simplification excessive

Perte de nuance

Plausibilité scientifique

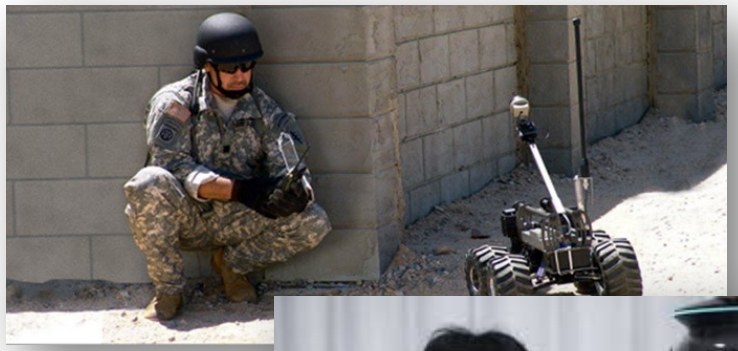
Fausse impression de sécurité

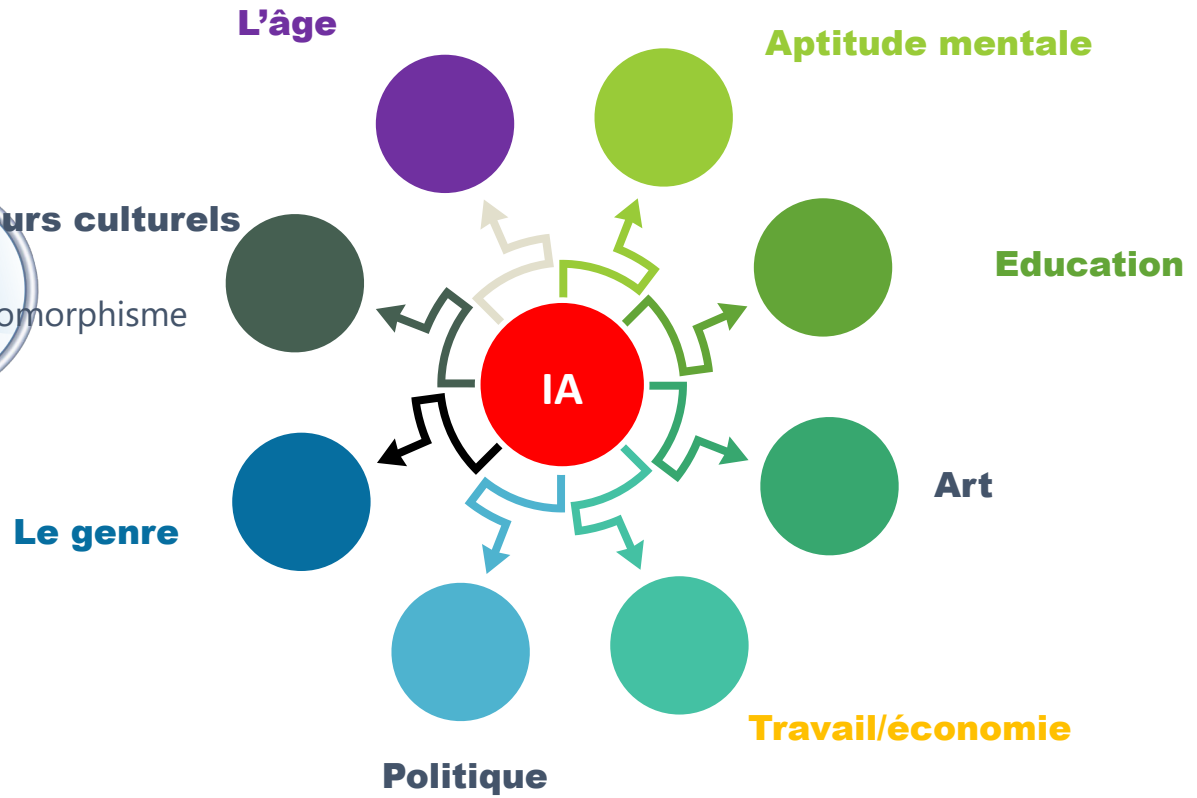
On résume

Limite en termes :

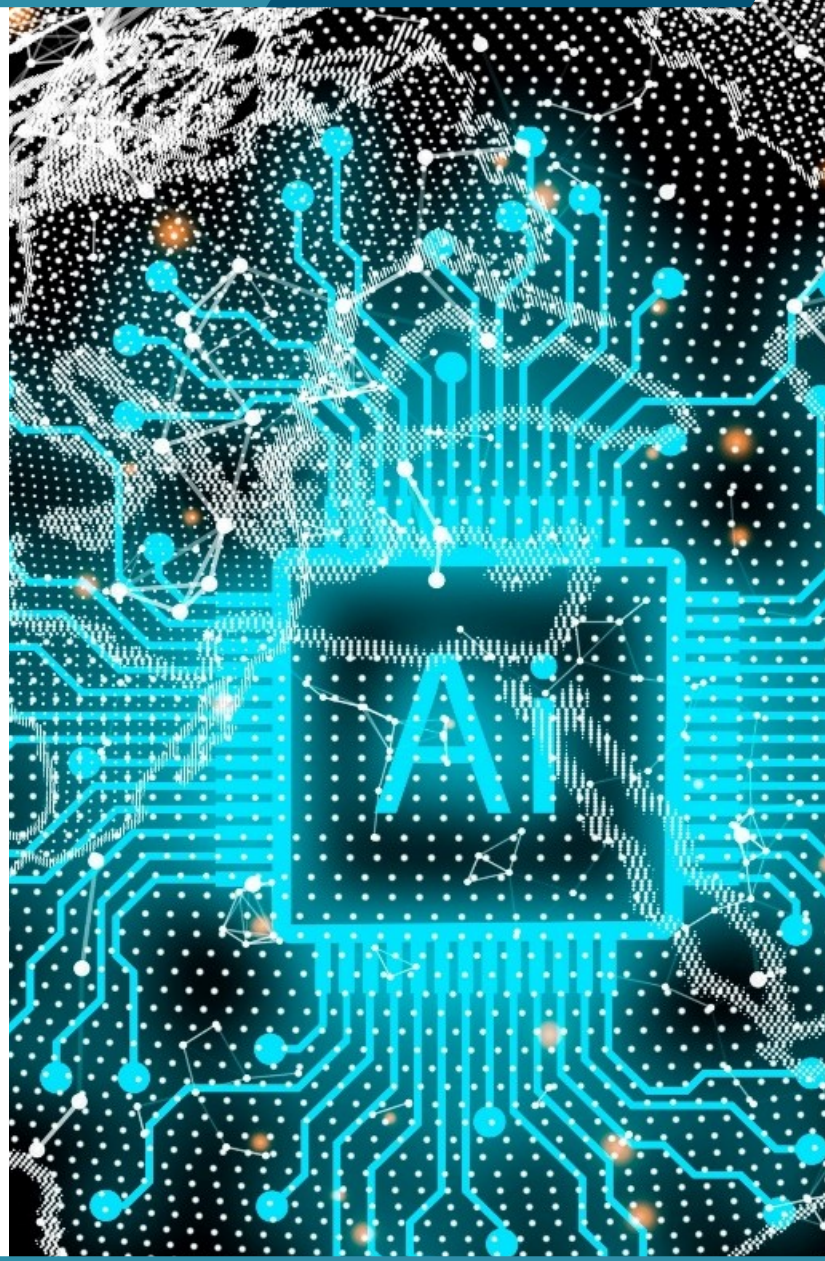
- **Dimension psychologique**
- **Cybersécurité**
- **Biais**
- **Confidentialité**
- **Désinformation**

EN « + » : Impact des facteurs sociaux / IA





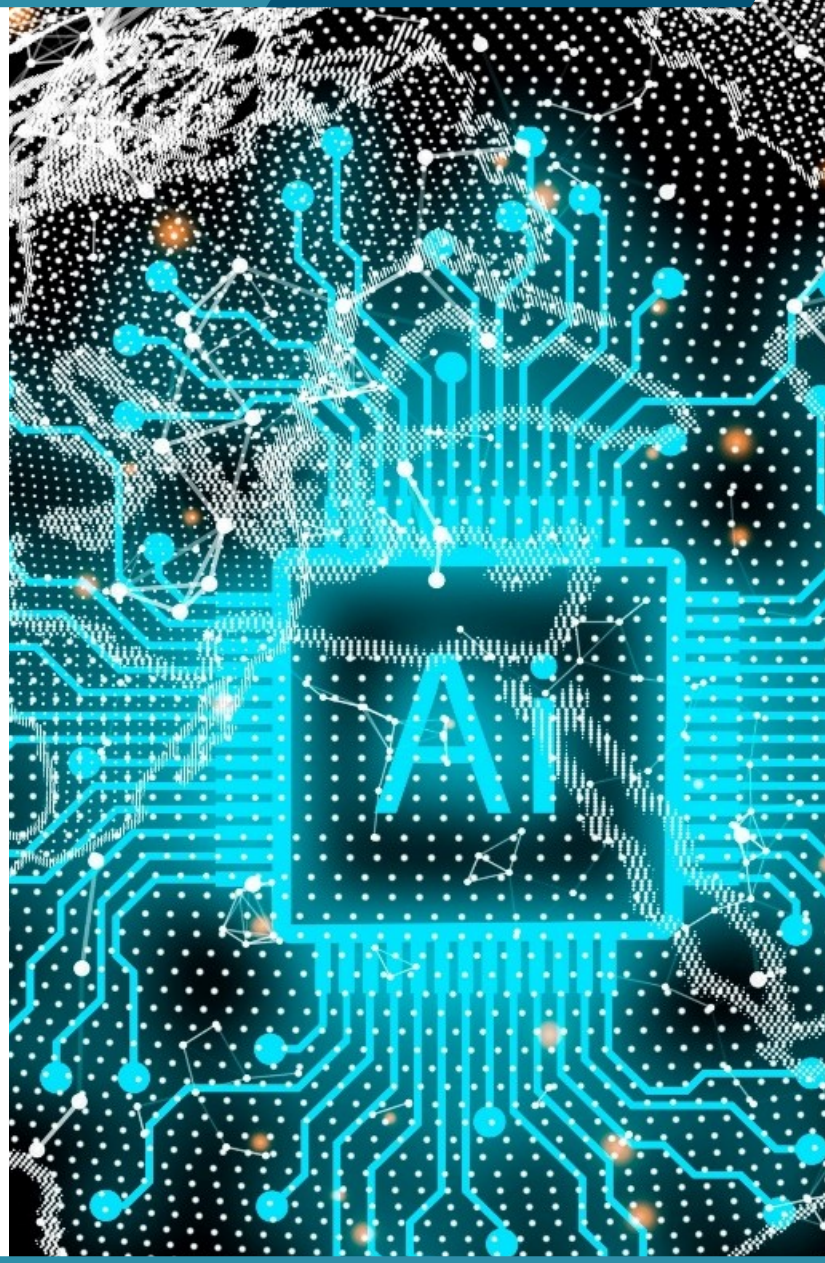
Conclusion



IA et cybersécurité : ennemie ou amie?

Innover avec éthique, protéger avec responsabilité.

Questions-réponses



FRC
Forum Cybermenace

Nos observateurs spéciaux
…le retour

EDITION 2024

FRC
Forum Cybermenace

Conférence de clôture

Par le Général Marc WATIN-AUGOUARD

EDITION 2024

Général Olivier KIM

Commandant la Région de Gendarmerie du Grand Est, commandant la gendarmerie pour la zone de défense et de sécurité Est

Général Gwendal DURAND

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

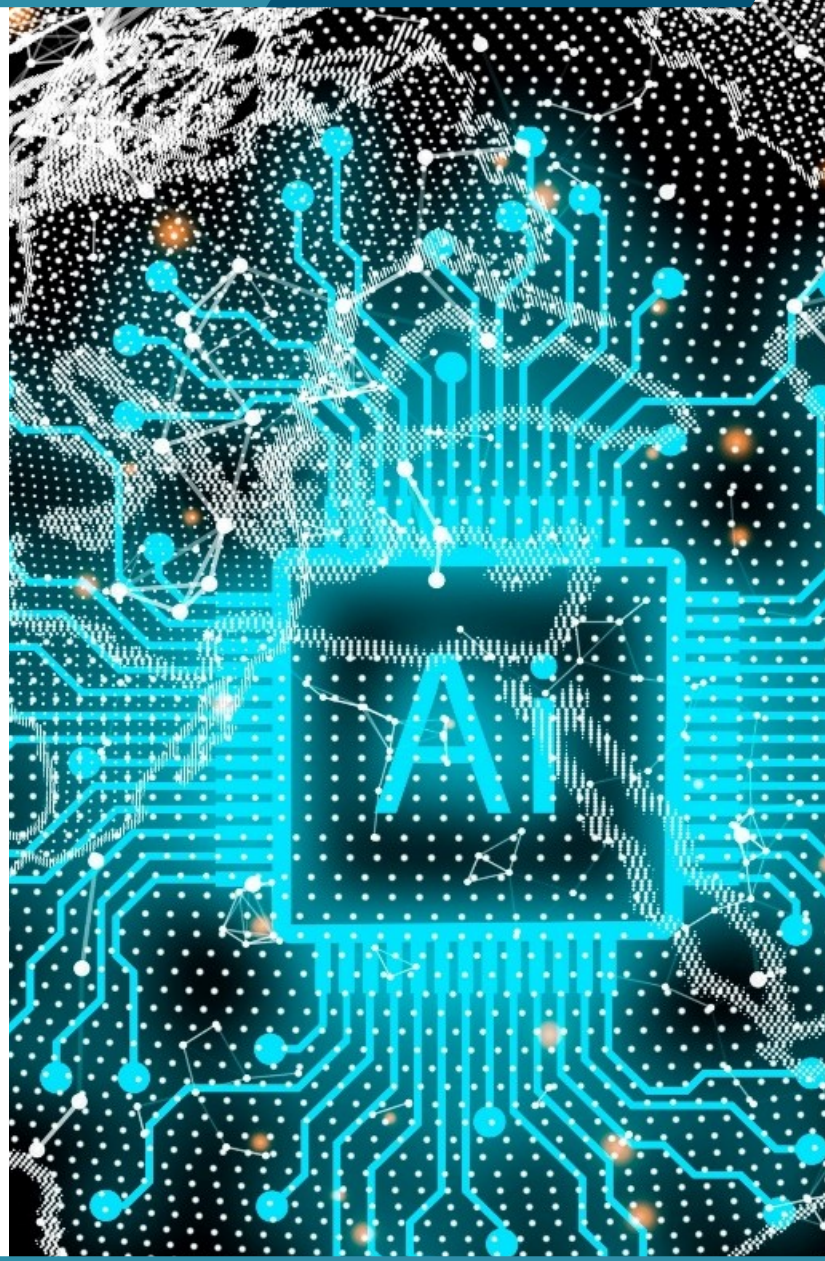
Monsieur Gilbert GOZLAN

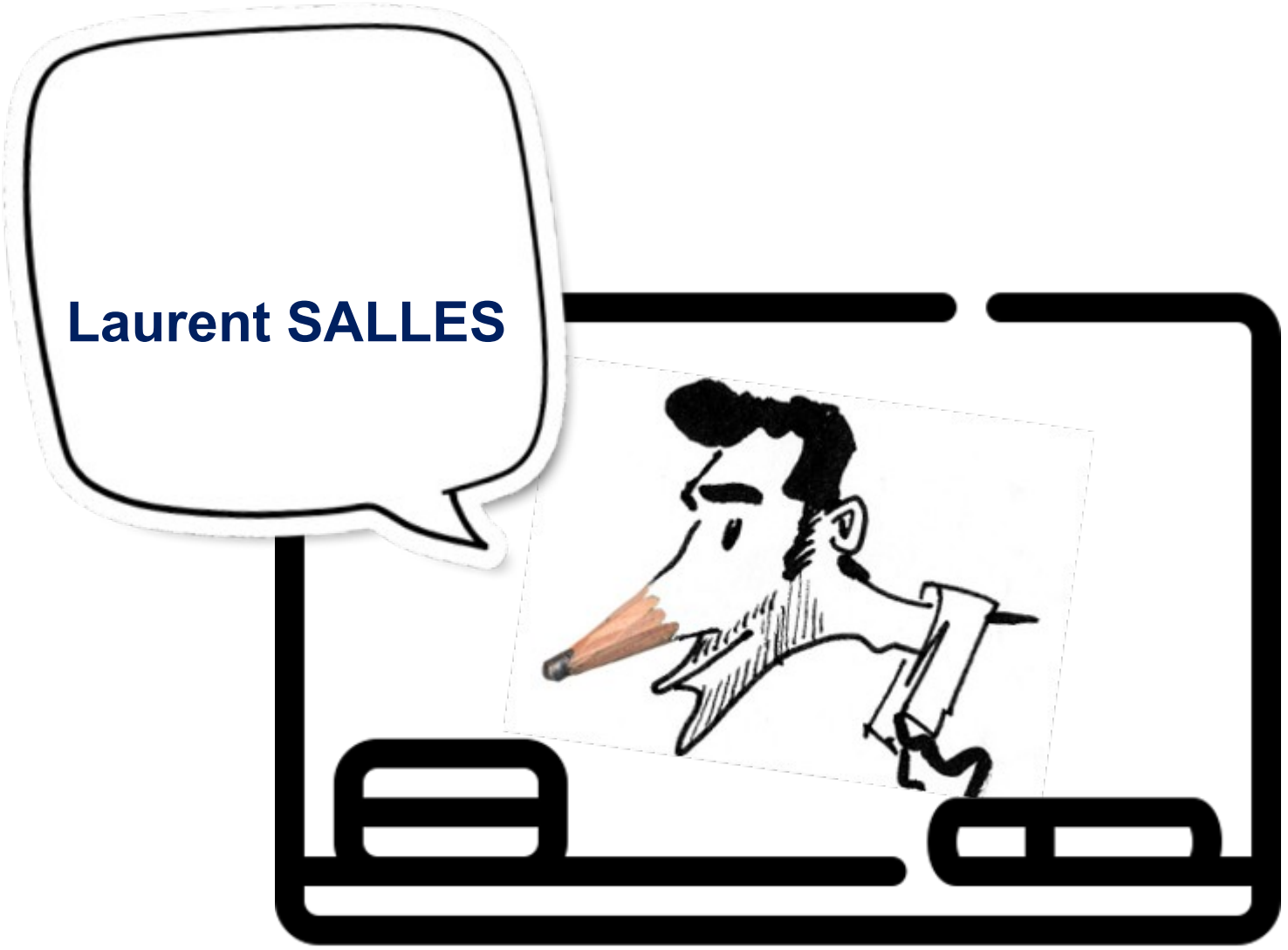
Président de l'association Ad honores – Réseau Alsace
Col (RC) Gendarmerie Nationale

Remerciements

L’équipe d’organisation

CEN Gérald DULOISY
Sébastien DUPENT
Régis ECKART
Damien ERNST
Gilbert GOZLAN
Joël GUERET
Daniel GUINIER
Emmanuelle HAASER
Ludovic HAYE
Hervé HUMBERT
ADJ Rémy JACAMON
Pascal MARY
Sophie MARTIN
CNE Andrée NTORE-BIKENE
Didier SCHERRER
ADJ Sébastien STOUFFLET
MDC Vanessa URBAN
Elena VALLEJO
Jonathan WEBER




Laurent SALLES

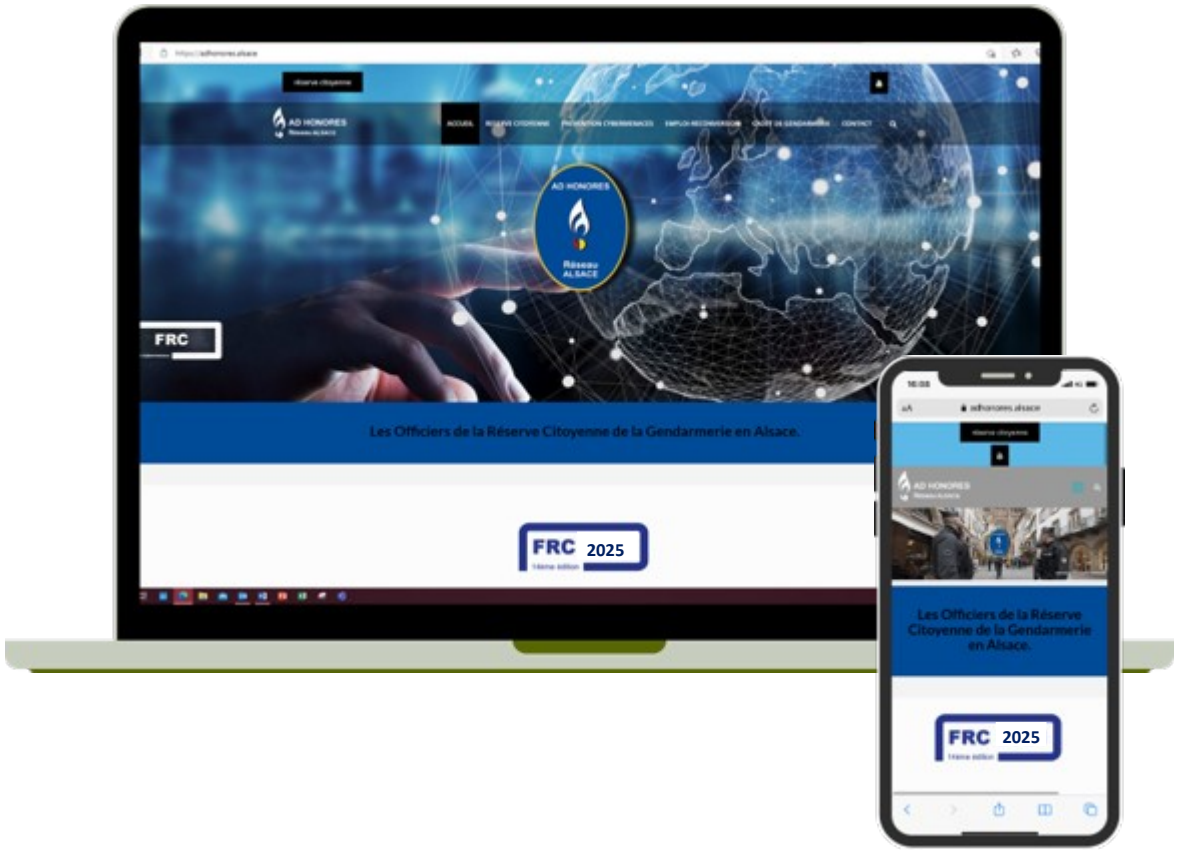

Marko MAYERL
Camille COMPARON
Inédit Théâtre

Flashez ce QR Code

Donnez votre avis sur le 17ème FRC


FORUM
INCYBER
EUROPE
1-3 AVRIL 2025
FORUM INCYBER 2025
Au-delà du *Zero Trust*, la confiance pour tous
Participez à la 17e édition du Forum
InCyber à Lille Grand Palais

Rendez-vous au prochain FRC



18ème FRC

4 novembre 2025

https://adhonores.alsace/