



IA Robotique & Cybersécurité

13 décembre 2023 – Limoges



Thierry Berthier

Pilote du groupe « Sécurité - IA – Robotique » du Hub France IA –
Directeur scientifique de la fédération professionnelle européenne Drones4Sec



13
déc
2023

Lancement du
Centre de Ressources en Cybersécurité
de Limoges Métropole

R

CENTRE DE
RESSOURCES
C Y B E R
L I M O G E S - N A

13 décembre 2023 à 14h30
à ESTER Technopole

Table ronde : Enjeux et objectifs du Centre de Ressources Cyber
Keynote : IA et Cybersécurité - IoT, robotique, systèmes autonomes

Organisé par :

En partenariat avec :

SOMMAIRE

PREAMBULE – L’innovation, produit des grandes convergences technologiques (3)

PARTIE 1 - Six décennies de R&D en IA pour converger vers une IA générale (12)

PARTIE 2 - Les révolutions de la robotique associée à l’IA (36)

PARTIE 3 – La cybersécurité, comme ingrédient indispensable aux révolutions de l’IA et de la robotique (67)

PREAMBULE

**L'innovation, produit des grandes convergences
technologiques**

Les vagues d'innovation technologiques s'effectuent en cycles de plus en plus courts

The History of INNOVATION CYCLES

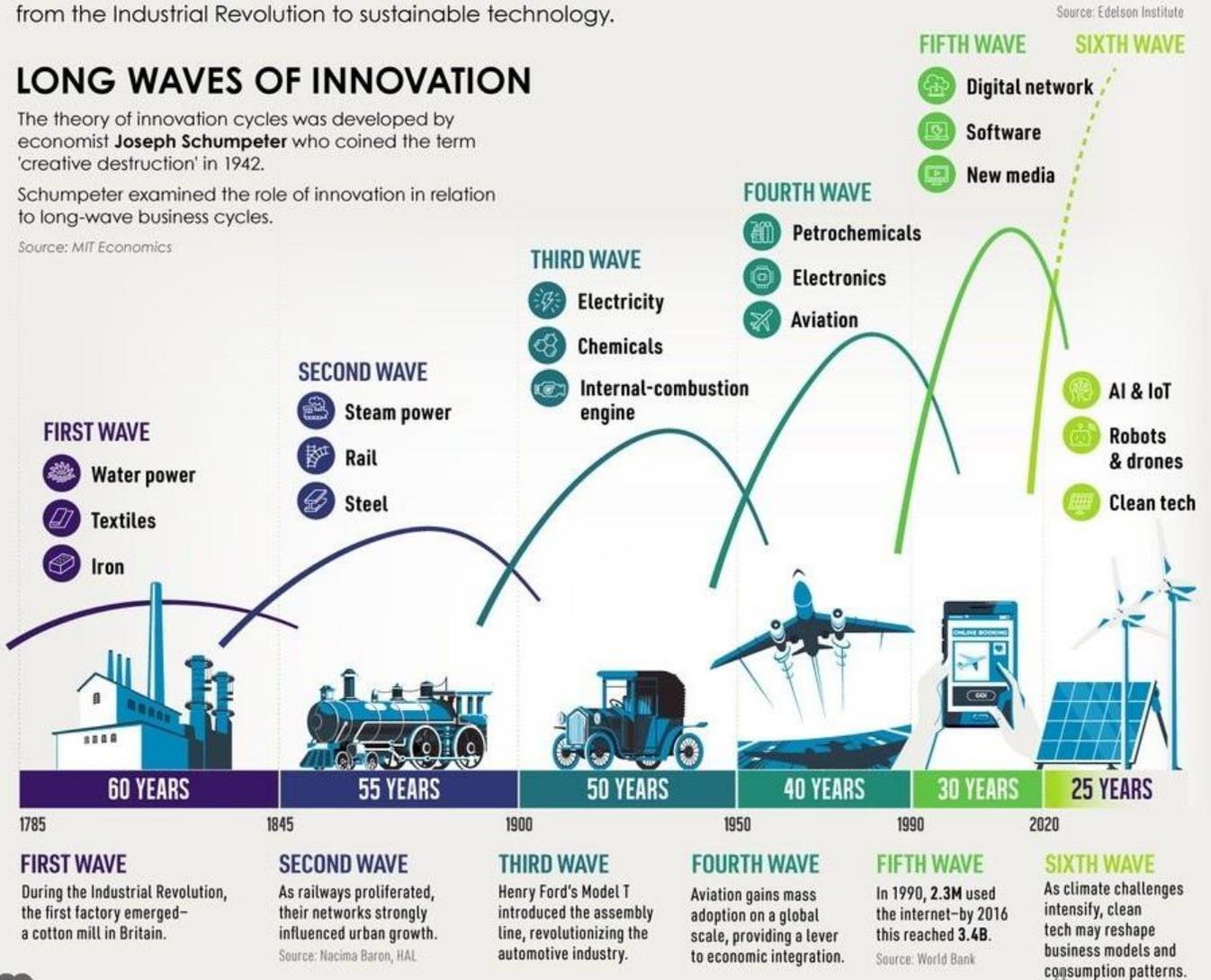
Below, we show waves of innovation across 250 years, from the Industrial Revolution to sustainable technology.

LONG WAVES OF INNOVATION

The theory of innovation cycles was developed by economist **Joseph Schumpeter** who coined the term 'creative destruction' in 1942.

Schumpeter examined the role of innovation in relation to long-wave business cycles.

Source: MIT Economics



Les délais d'adoption
par l'utilisateur des
technologies de rupture
décroissent rapidement



Linas Beliūnas 

@linas.beliunas

Time it took to reach **100 million users:**

Mobile phone - 16 years

Internet - 7 years

Facebook - 4.5 years

WhatsApp - 3.5 years

Instagram - 2.5 years

TikTok - 9 months

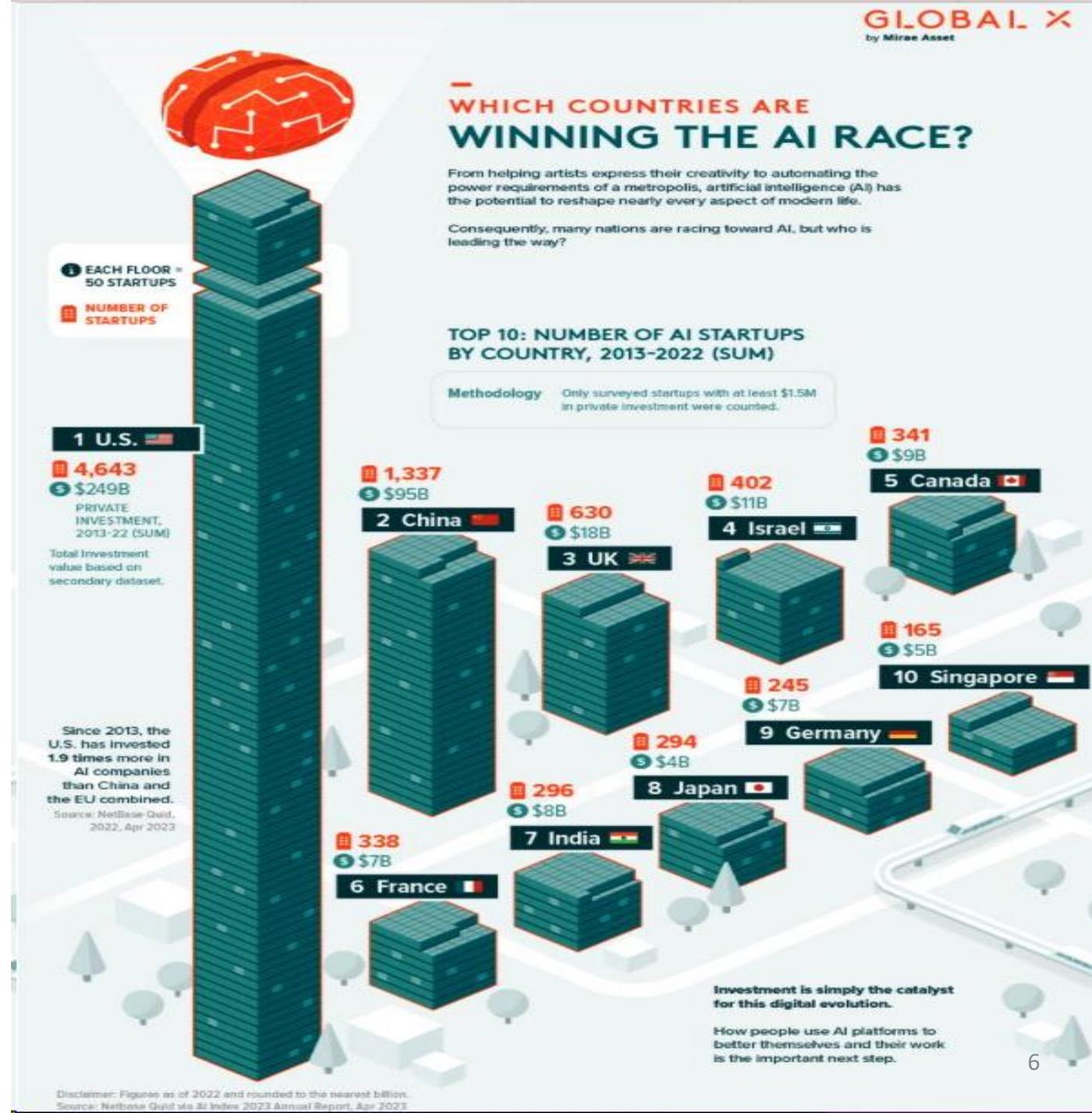
ChatGPT - **2 months**

ChatGPT is the fastest-growing
consumer app in internet history.

La course à l'intelligence artificielle et à la robotique s'installe au cœur des compétitions géostratégiques.

Une partition mondiale USA – CHINE

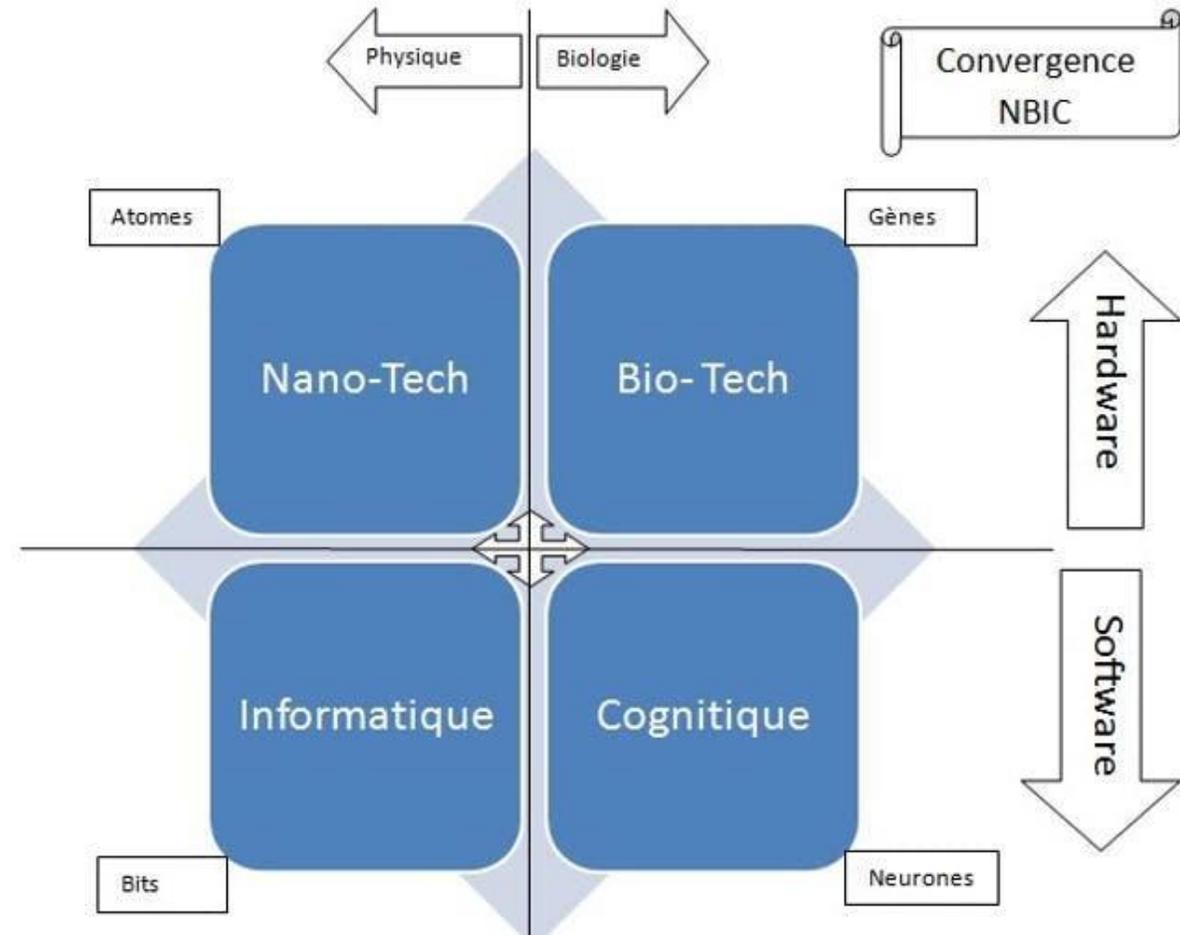
Quelle est la place d'une Europe, championne de la régulation, dans ce duel ?



Où allons-nous ?

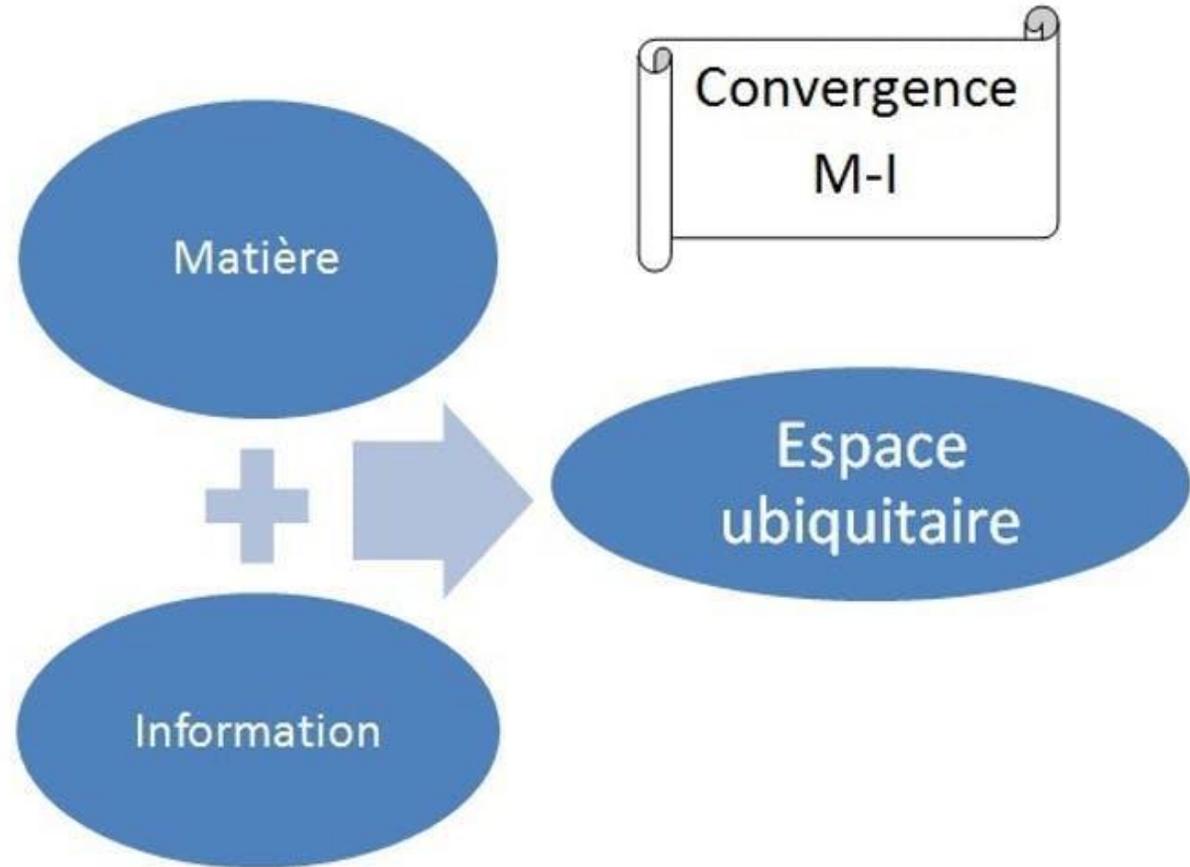
Un début de réponse est donné par la dynamique des quatre grandes convergences technologiques

Convergence NBIC: Nanotechnologie, Biotechnologies, Informatique, Sciences Cognitives



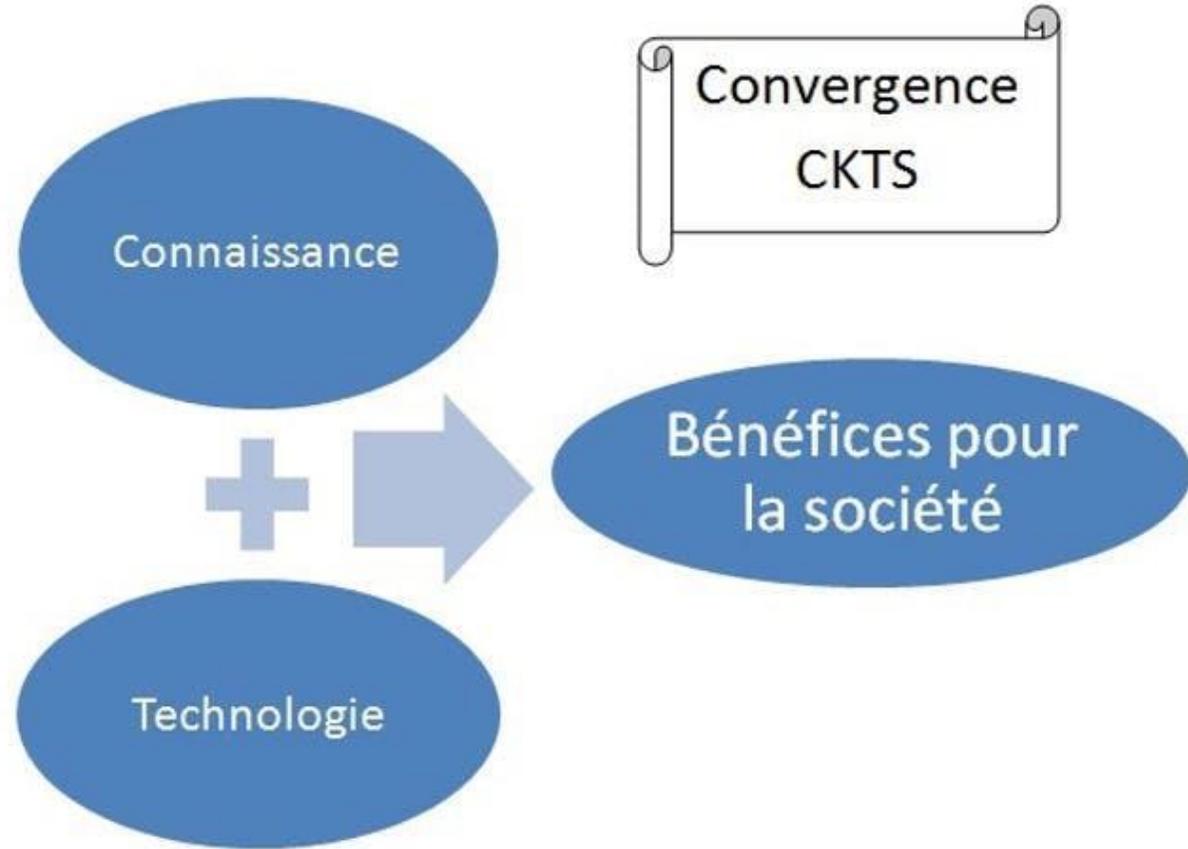
Convergence NBIC

Convergence M-I
Convergence de la
matière et de
l'information pour
créer un espace
ubiquitaire



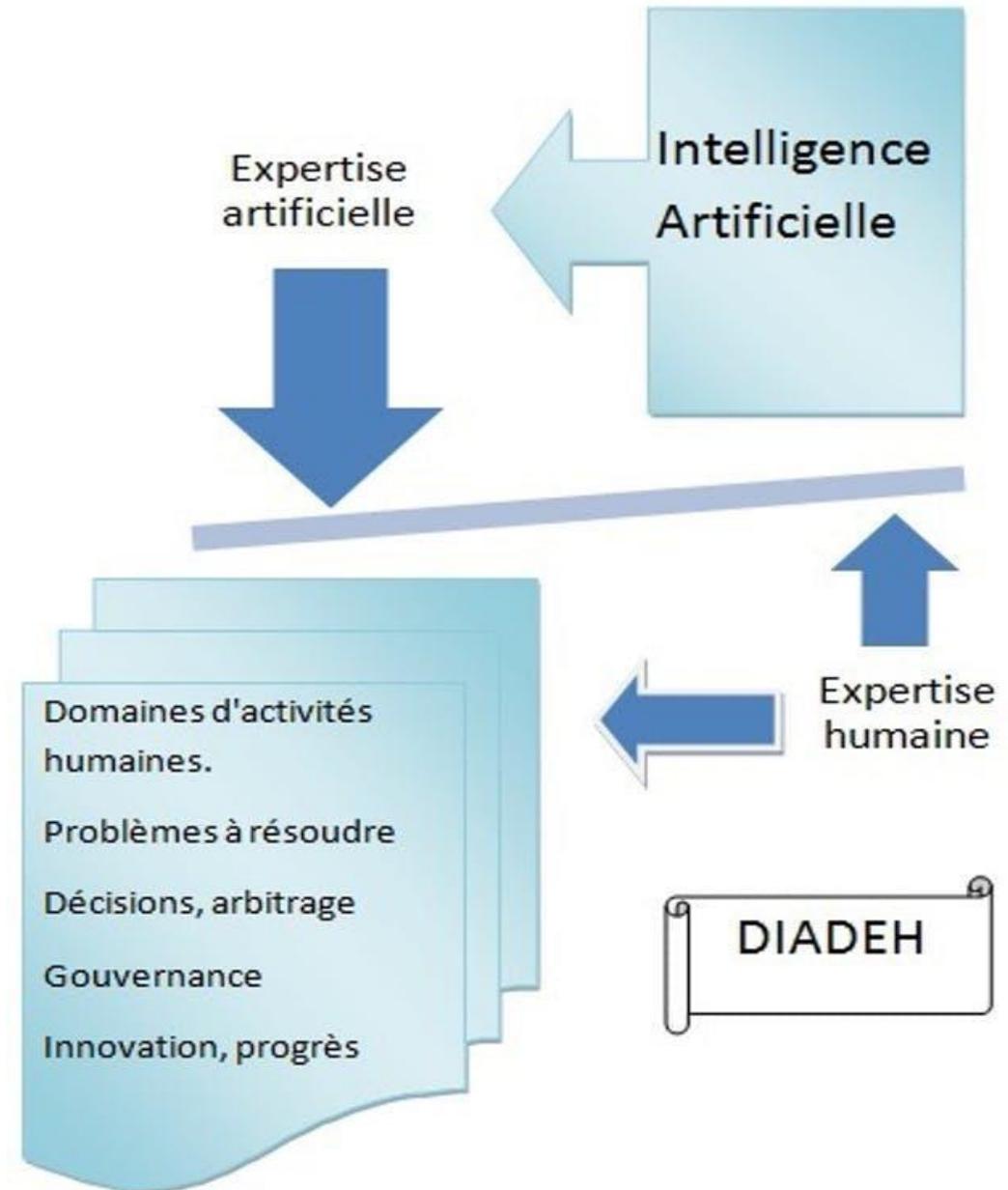
Convergence Matière – Information

Convergence CKTS
Convergence of
knowledge and
technology for the
benefit of society



Convergence CKTS

Convergence
DIADEH
Diffusion de
l'Intelligence
Artificielle sur les
Domaines
d'Expertises
Humaines



PARTIE 1

**Six décennies de R&D en IA pour converger vers
une IA générale**

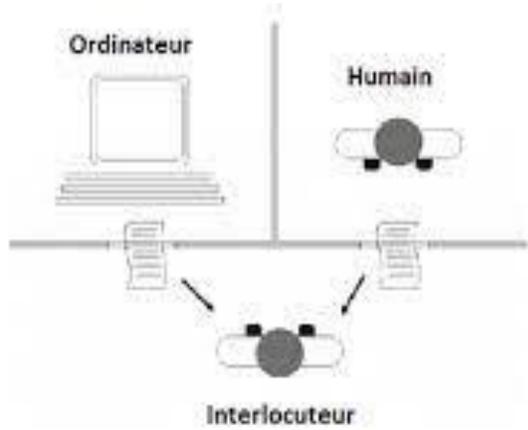
Qu'est-ce qu'une intelligence artificielle ?

L'intelligence artificielle n'est pas une technologie à proprement parler mais plutôt un domaine scientifique dans lequel des outils peuvent être classés lorsqu'ils respectent certains critères.

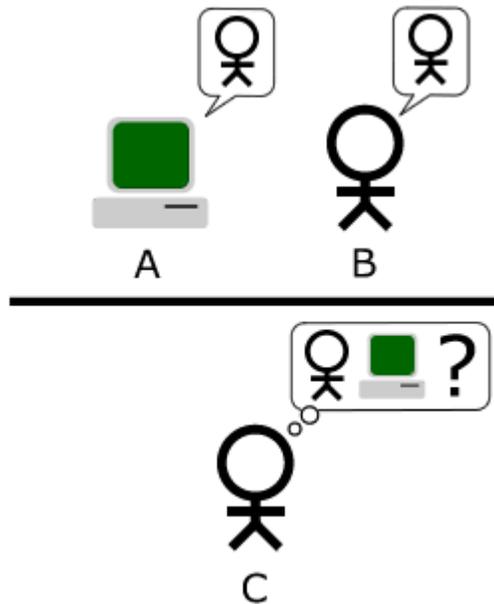
Pour le Parlement européen, l'intelligence artificielle représente tout outil utilisé par une machine afin de « reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité ».



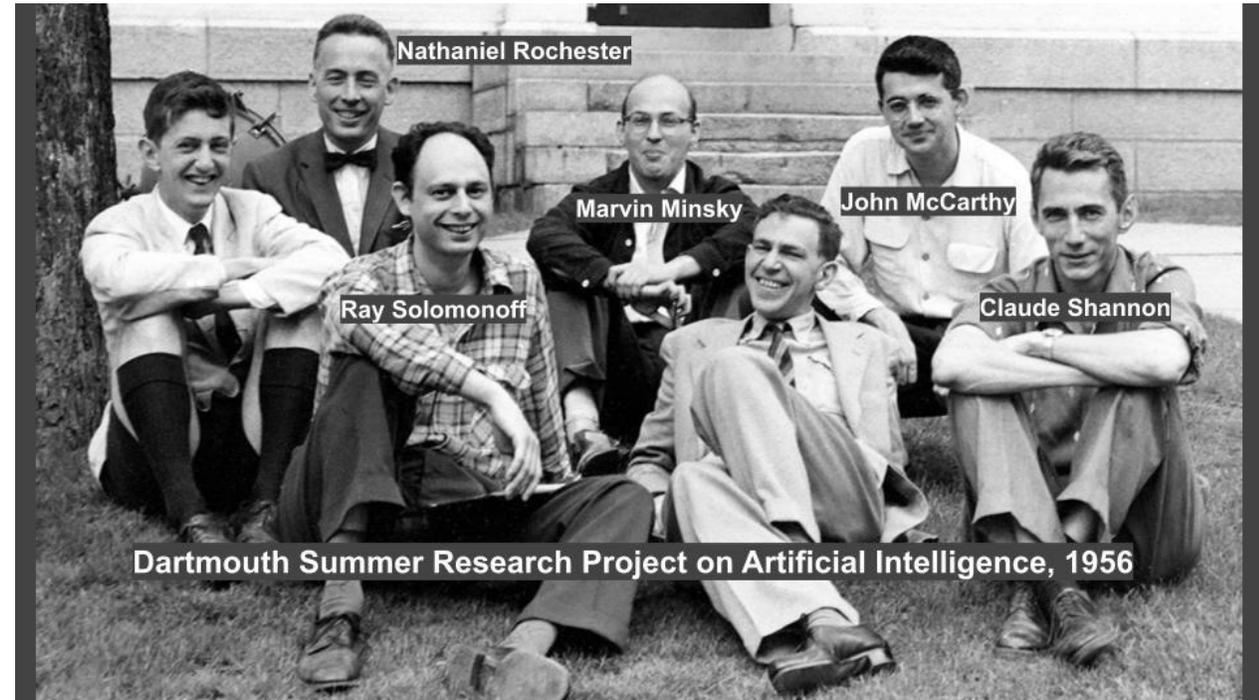
Test de Turing (1950)



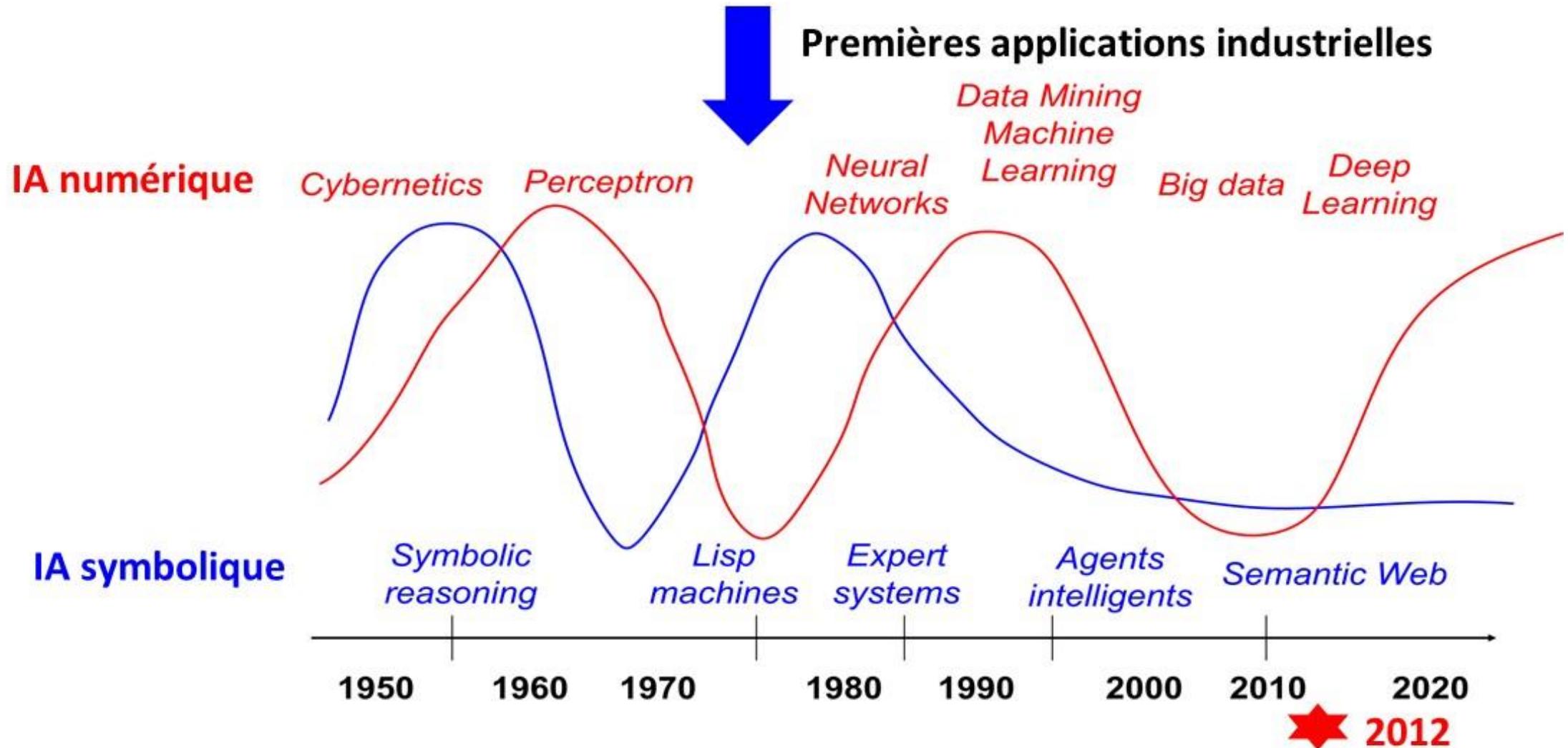
Alan Turing et le schéma de son test éponyme



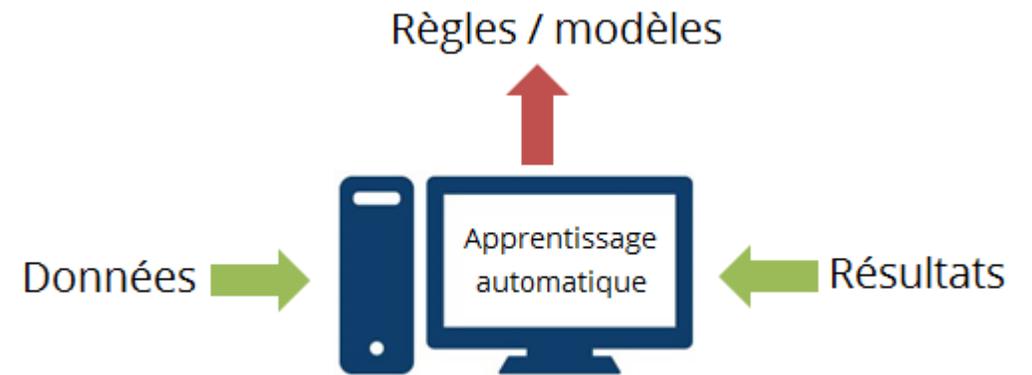
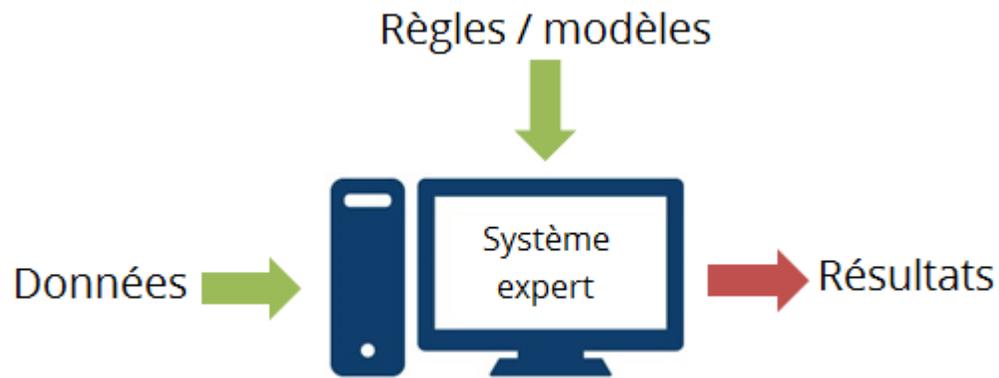
Conférence de Dartmouth (1956)

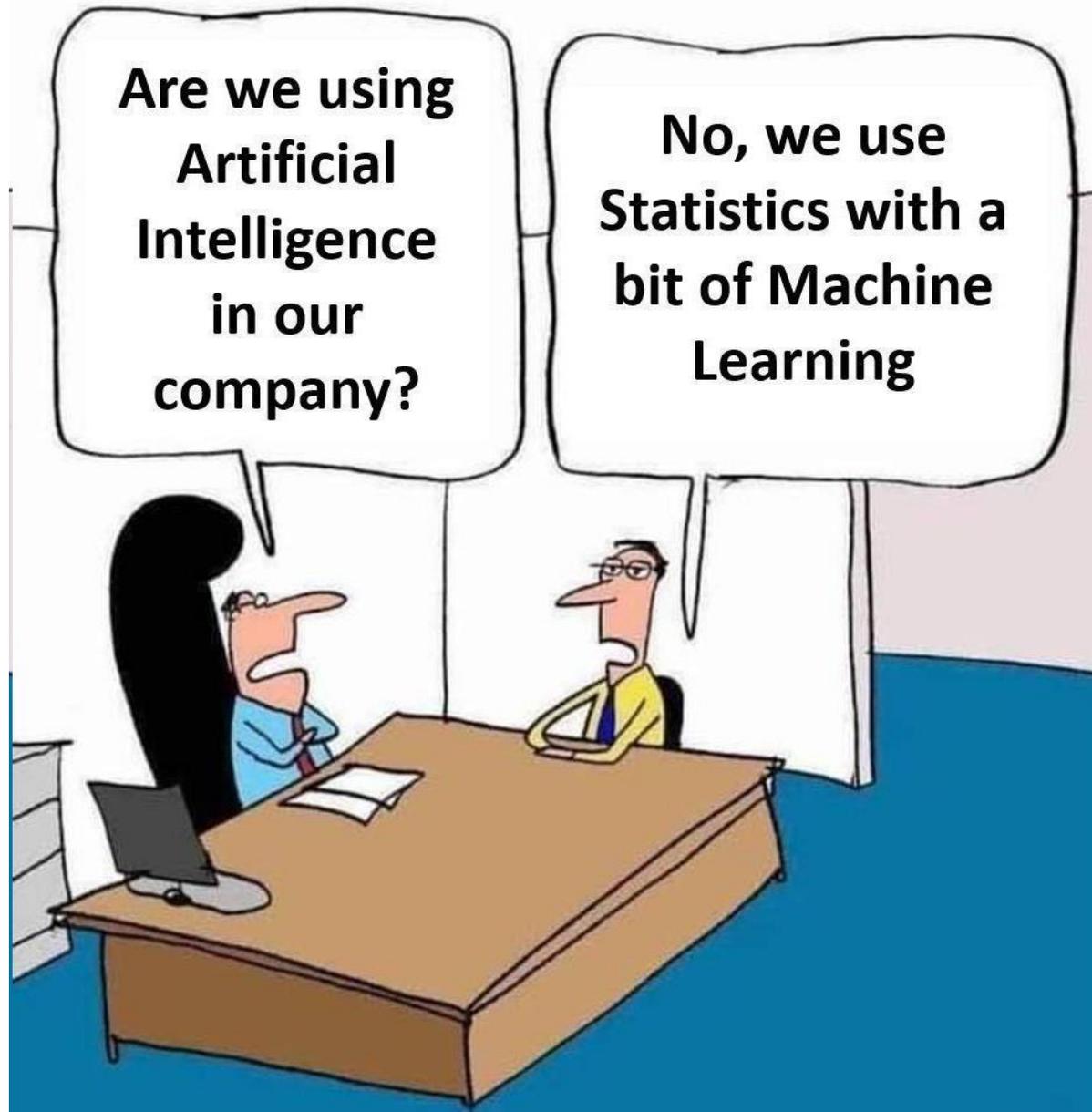


Six décennies de développement de l'IA



Systemes experts et apprentissage automatique : deux conceptions differentes de l'IA



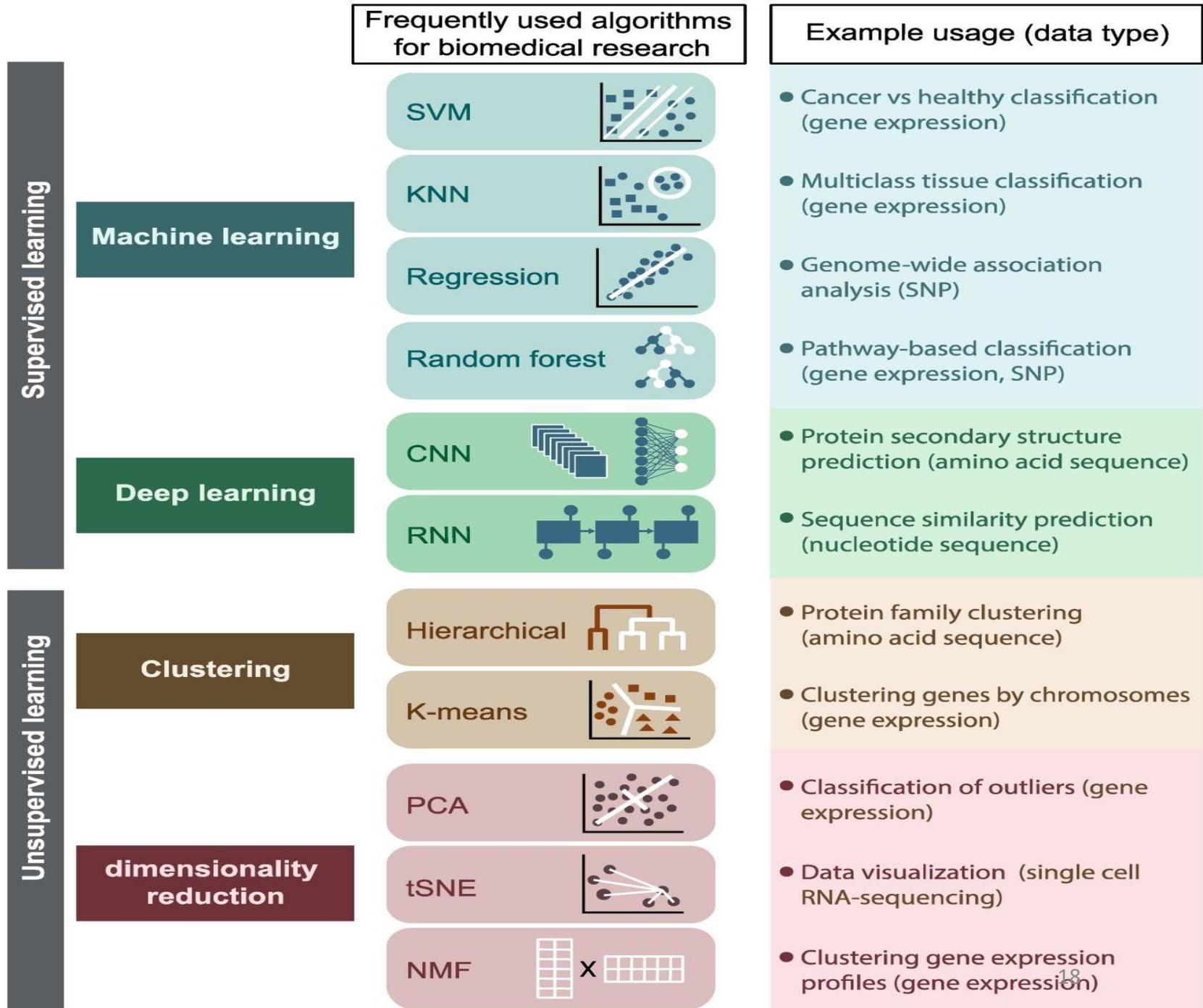


**Are we using
Artificial
Intelligence
in our
company?**

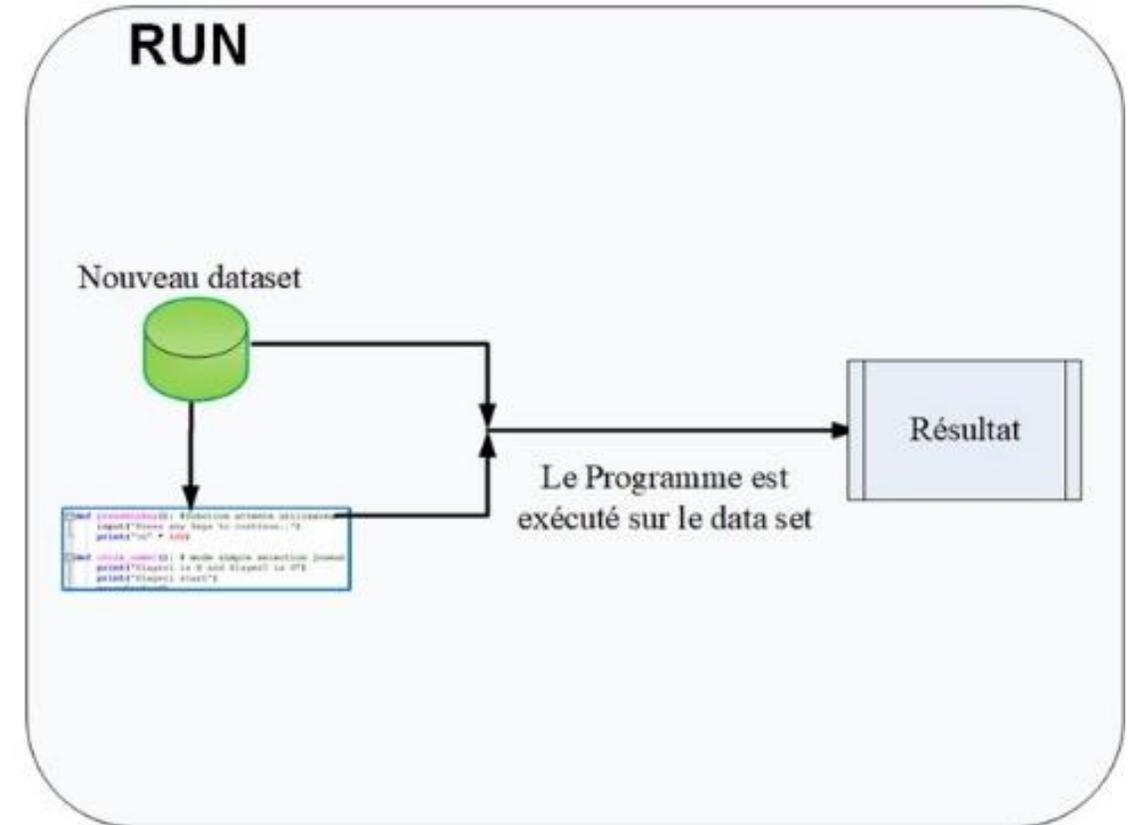
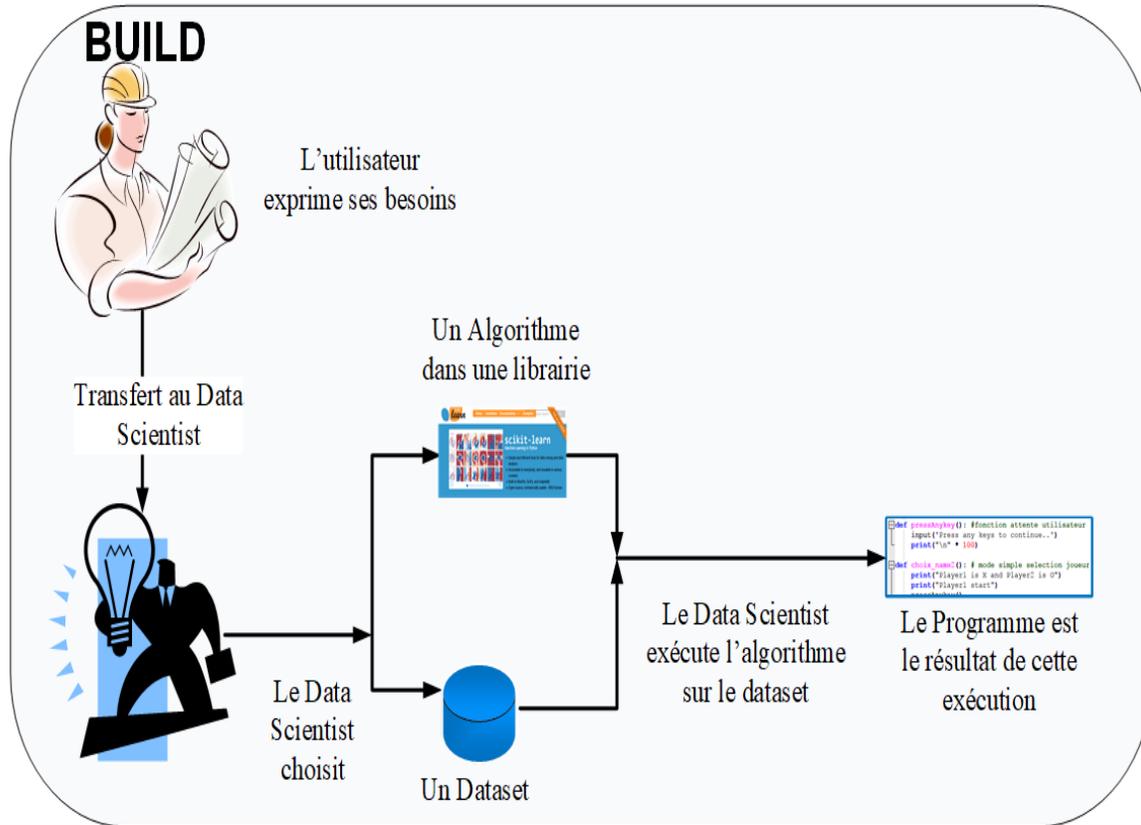
**No, we use
Statistics with a
bit of Machine
Learning**

Dépassons le Buzz et l'écume médiatique pour donner les ingrédients de l'IA :

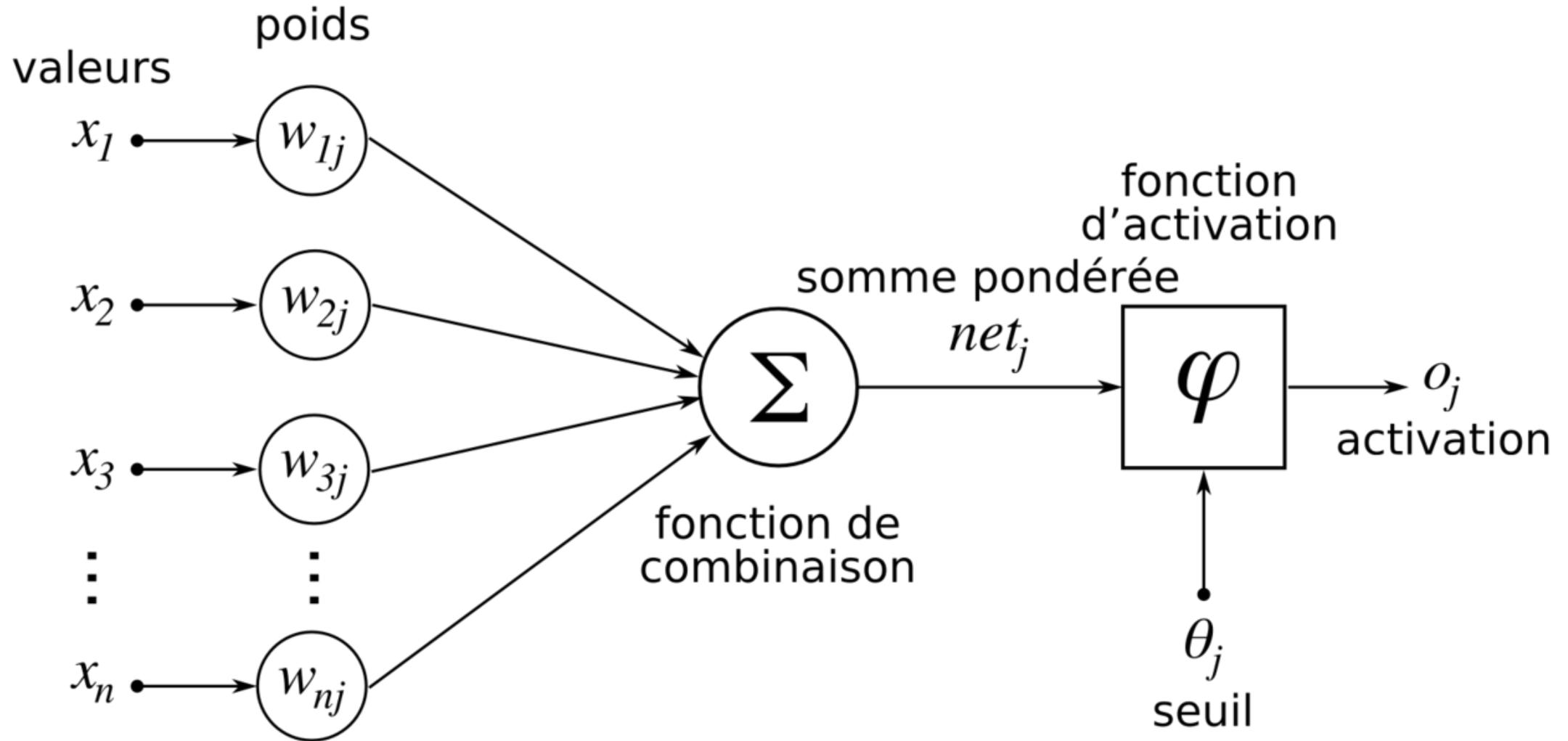
- Statistiques
- Optimisation
- Algèbre linéaire
- Probabilités
- Analyse fonctionnelle
- Combinatoire
- Logique formelle
- Bref, des mathématiques et de l'informatique



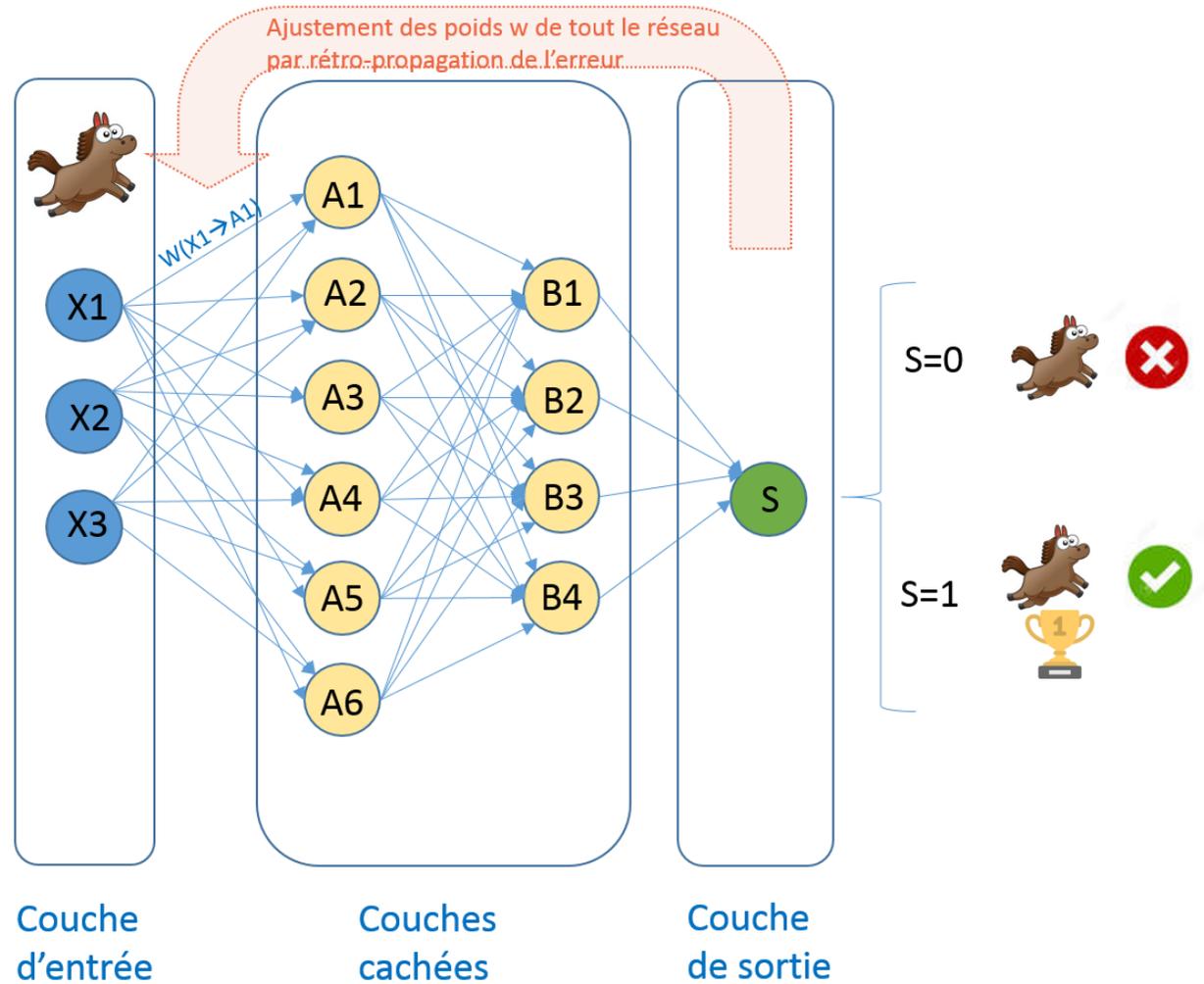
Le modèle « Build and Run »



Réseau de Neurones

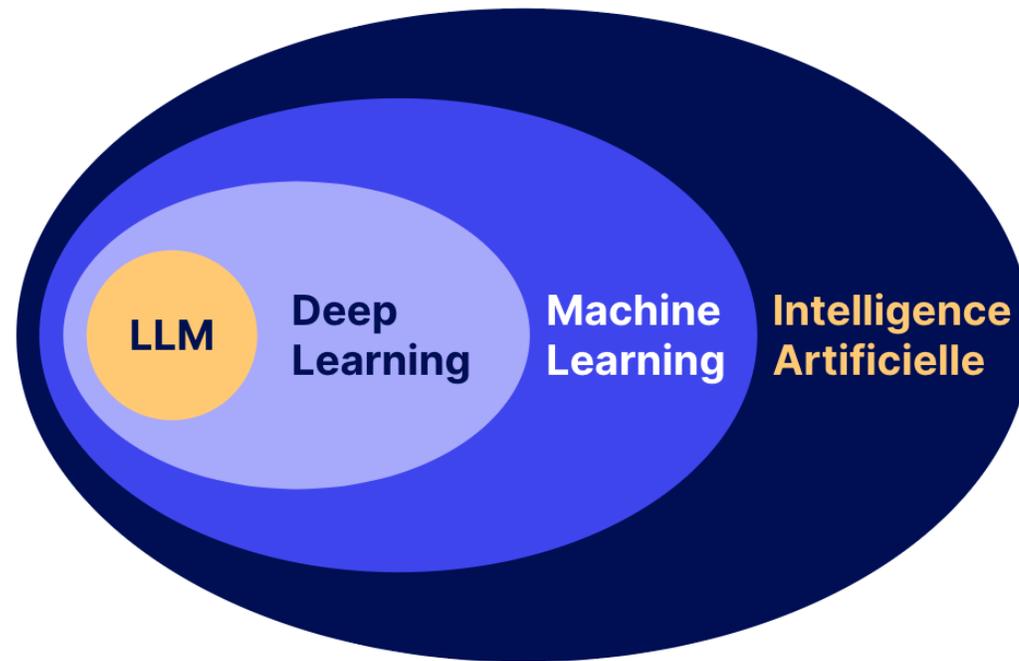


Réseau de Neurones



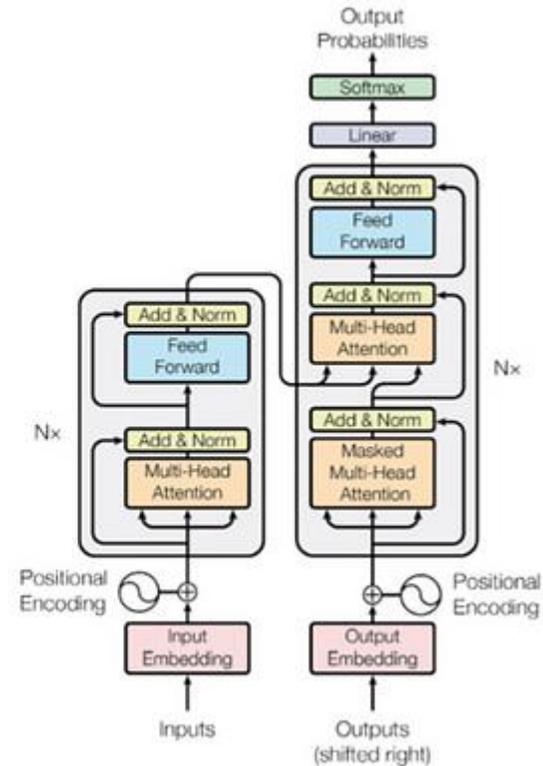
Exemple avec un réseau comprenant une couche d'entrée de 3 neurones (le cheval est décrit par 3 variables X_1, X_2, X_3), 2 couches cachées A et B de respectivement 6 et 4 neurones, et une couche de sortie S à 1 neurone correspondant au classement binaire du cheval (0/non gagnant – 1/gagnant)

La révolution de l'IA générative (2017)



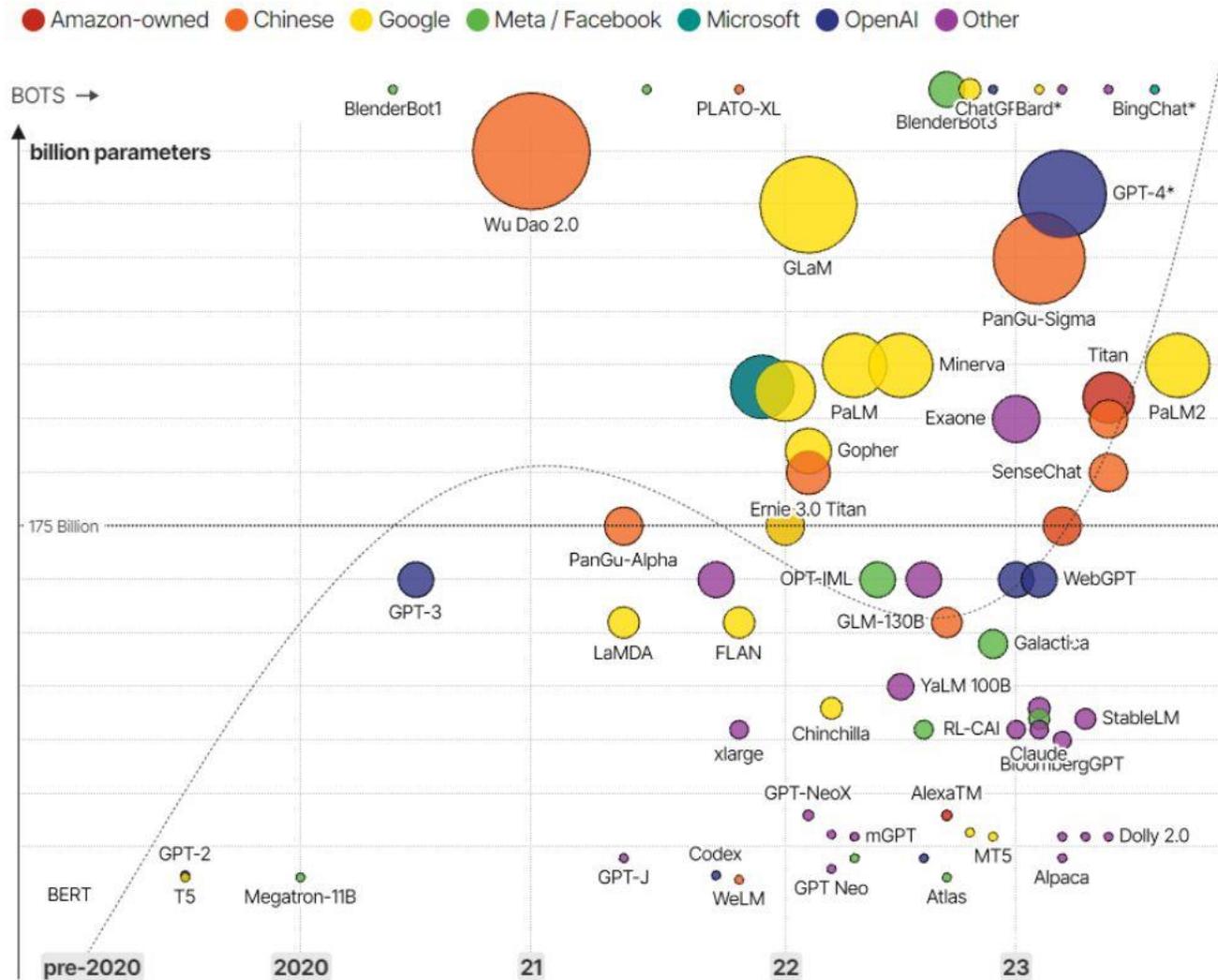
L'IA générative, Transformer (2017) , LLM, ChatGPT, GPT4 : Rendons à ~~César~~ Google Brain ce qui est à OpenAI

Transformer Attention Is All You Need



Google Brain « Attention Is All You Need : <https://arxiv.org/abs/1706.03762>

How Many LLMs Do You Know?



Predictions: Potential Capabilities of

GPT-4



What's in this picture?

Looks like a duck.

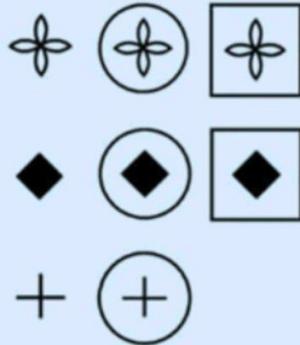
That's not a duck. Then what's it?

Looks more like a bunny.

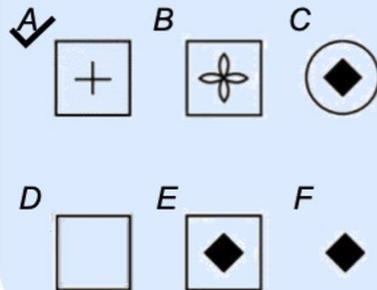
Why?

It has bunny ears.

Here are eight images:



The following image is:



Input Prompt



Question: Explain why this photo is funny?
Answer:



Question: Why did the little boy cry?
Answer:



Question: What is the hairstyle of the blond called?
Answer:



Question: When will the movie be released?
Answer:

Completion

The cat is wearing a mask that gives the cat a smile.

(1)

Because his scooter broke.

(2)

pony tail

(3)

On June 27

(4)

Input Prompt

TorchScale - A Library for Transformers at (Any) Scale
TorchScale is a PyTorch library that allows researchers and developers to scale up Transformers efficiently and effectively. It has the implementation of fundamental research to improve modeling generality and capability as well as training stability and efficiency of scaling Transformers.

- Stability - [DeepScale Scaling Transformers to 1,000 Layers and beyond](#)
- Generality - [Foundation Transformers \(Mogonic\)](#) Invents true general purpose modeling across tasks and modalities (including language, vision, speech, and multimodal)
- Scalability - [A Simple Scalable Transformer](#)
- Efficiency - [A Multi-modal & Transferable Open Mixture of Experts Model](#)

What is TorchScale?

Completion

A library that allows transformers to work efficiently and effectively at any scale.

(5)



Question: The result is?
Answer:

5 + 4 = 9

(6)



Question: What is the heart rate in this picture?
Answer:

57 bpm

(7)



The time now is

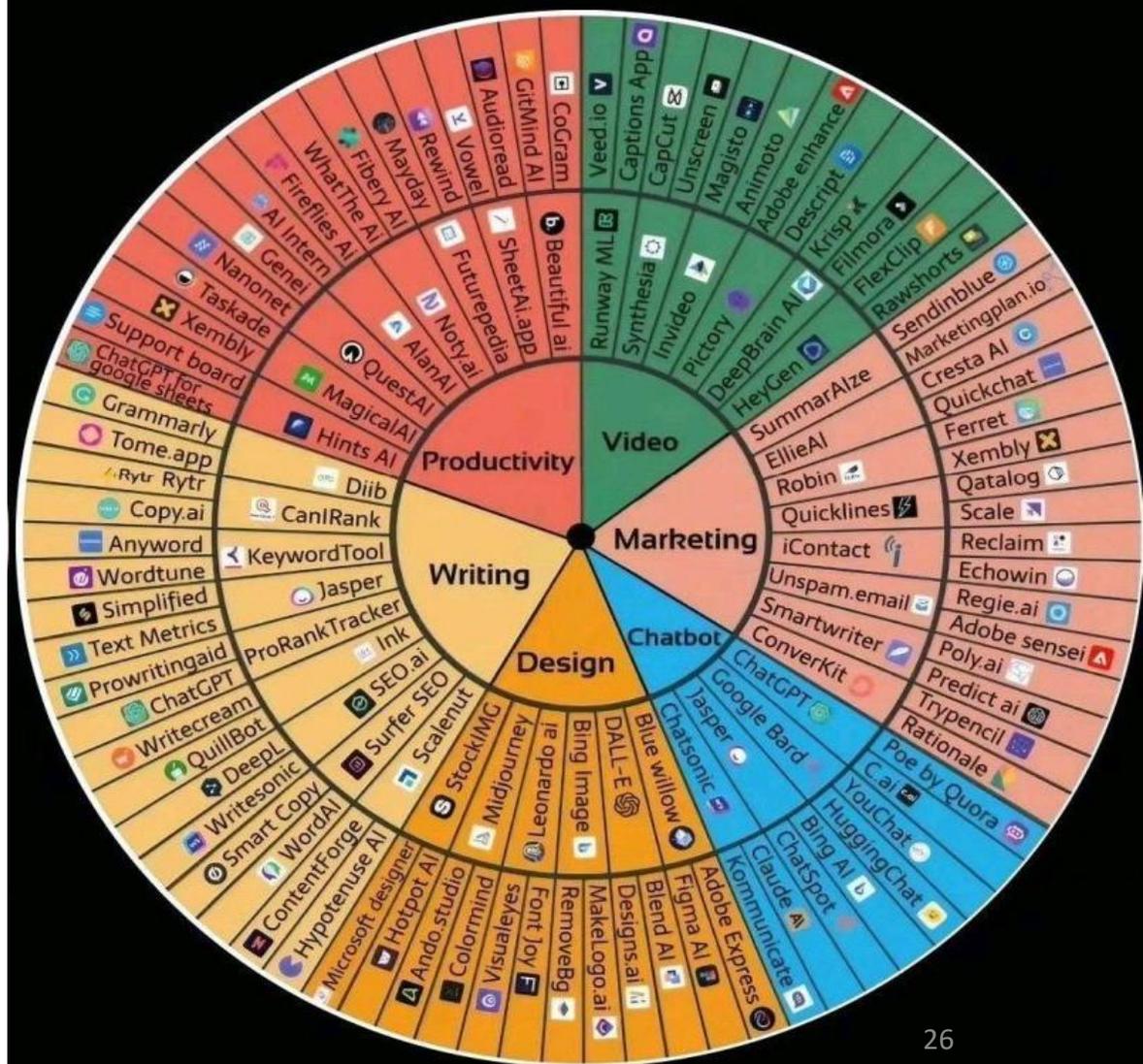
10:10 on a large clock

(8)

THE 27 MOST POPULAR AI TOOLS 2023

Chatbot	ChatGPT	Bard	Bing
Video	Runway	Pictory	Descript
Productivity	Notion AI	Taskade	MeetGeek
Design	Midjourney	Adobe Firefly	Microsoft Designer
Website	10web	Durable	Imagica
Code	Copilot X	AskCodi	AWS Code Whisperer
Content	Opus Clip	Cohesive	Synthesia
Presentation	Tome	Decktopus	Gamma
Automation	Zapier	Make	Bardeen

120 MIND-BLOWING AI TOOLS



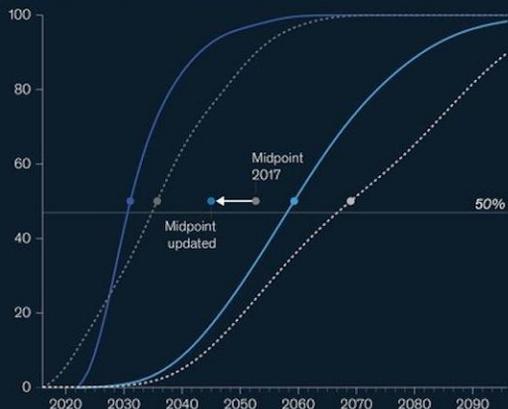
The future of work with generative AI

Since 2017, McKinsey has been modeling potential scenarios for the adoption of work automation around the world. Our new research focuses on the economic potential of generative AI and the impact it could have on the extent and pace of automation.

A faster rate of change

Generative AI may accelerate the midpoint at which half of all work activities could be automated.

Global automation of time spent on current work activities, %



Updated early scenario including generative AI

Updated late scenario including generative AI

2017 early scenario

2017 late scenario

The main factor driving the speed of change is generative AI's natural language capabilities, which accelerate technical automation potential.

Adoption is likely to be faster in developed countries, where wages are higher and thus the economic feasibility of adopting automation occurs earlier.

The activities most affected

Unlike previous types of artificial intelligence, generative AI could automate some knowledge work. Our estimate of the technical potential to automate the application of expertise jumped 34 percentage points, while the potential to automate the management and development of talent increased from 16% in 2017 to 49% in 2023.

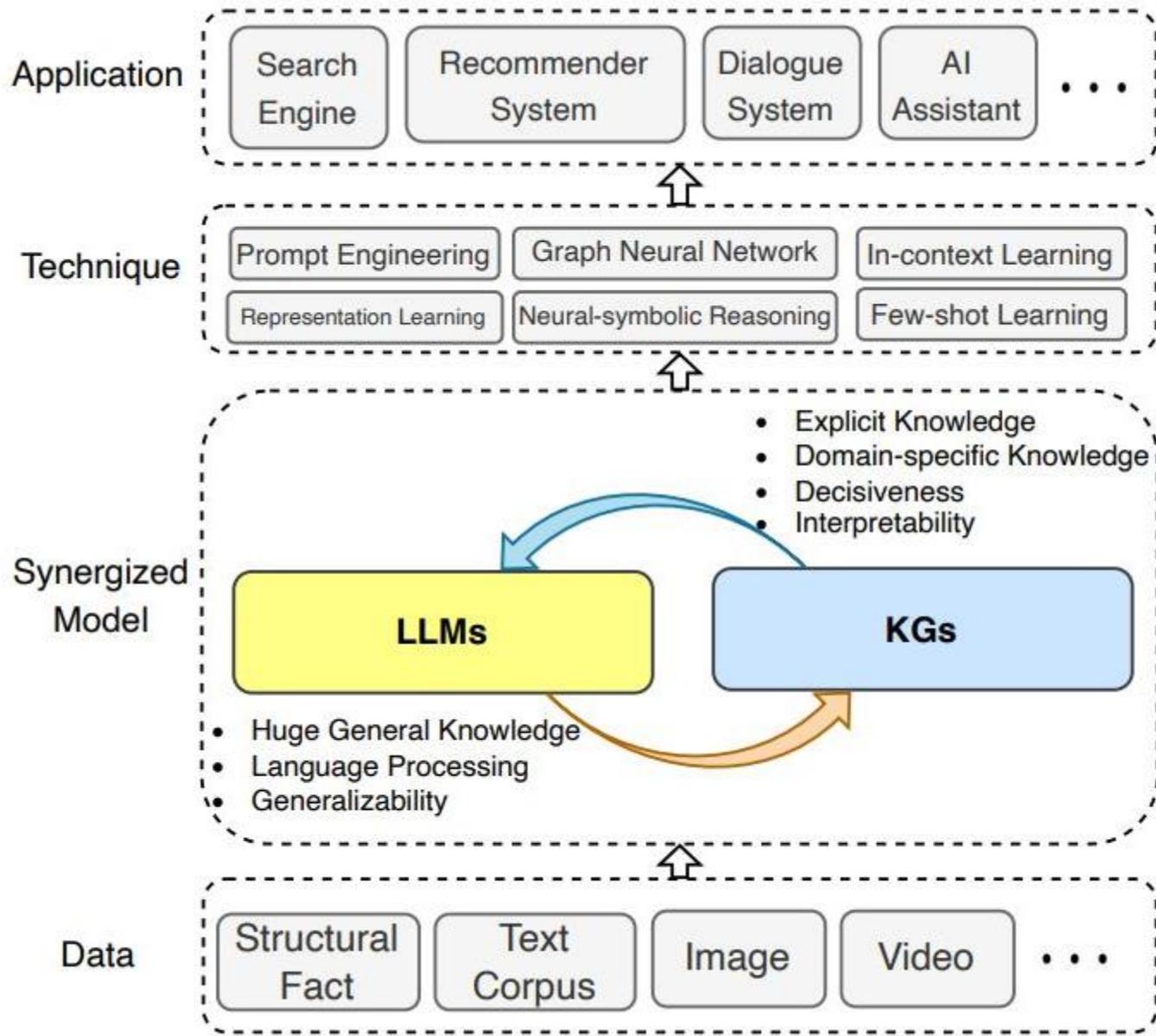
Overall technical automation potential, comparison in midpoint scenarios, % in 2023



A global productivity boost?

The capabilities of generative AI could automate a broader range of work activities sooner than we previously estimated, potentially increasing human productivity and offsetting the impact of aging on workforce growth. We predict that automation enabled by all AI technologies could increase global productivity by 0.2-3.3% from 2023 to 2040.

Productivity impact from automation by scenario, 2022-40, CAGR, %



SONDAGE IFOP POUR TALAN

LES FRANÇAIS ET LES IA GÉNÉRATIVES

Étude réalisée par l'Ifop pour Talan en mai 2023
L'enquête a été menée auprès d'un échantillon de 1008 personnes, représentatif de la population française âgée de 18 ans et plus.

ifop

Talan*

71%

des Français ont entendu parler des IA génératives

74%

de ces Français pensent qu'elles constituent une nouvelle révolution industrielle



des Français qui utilisent les IA génératives dans l'entreprise ne le disent pas à leur supérieur hiérarchique



souhaitent que l'État français soutienne davantage l'émergence d'entreprises françaises qui développent des IA génératives



estiment ne pas avoir les connaissances suffisantes pour les utiliser. Un énorme effort de formation semble donc nécessaire



ont des craintes vis-à-vis de l'émergence des IA génératives

IA génératives les plus citées

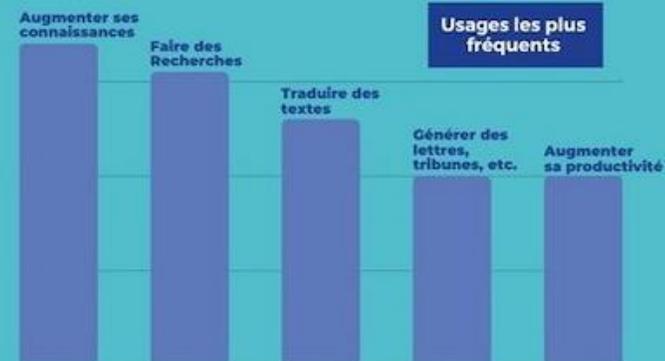


45%

des 18-24 ans utilisent les IA génératives contre seulement 18 % des 35 ans et +

51%

estiment que les enseignants doivent s'en saisir pour en enseigner les avantages et inconvénients



ifop

Talan*

Les travaux du Hub France IA au sein de la commission européenne AI ACT

About the European AI Forum

The European AI Forum (EAIF) is a non-profit organization representing more than 2,000 AI entrepreneurs 'born and raised' all across Europe. We are designed by and for Europe's AI community and aim to serve as a resource and forum for education, information sharing and networking between companies, policymakers and the general public. Member organizations of the EAIF: CroAI (Croatia) Hub France IA (France), KI Bundesverband (Germany), AI4SI (Slovenia), AI Austria (Austria), AI Cluster Bulgaria (Bulgaria), NL AI Coalitie (the Netherlands), Digitalpoland foundation (Poland) Artificial Intelligence Association of Lithuania (Lithuania).



L'IA générale, c'est quoi et c'est pour quand ?

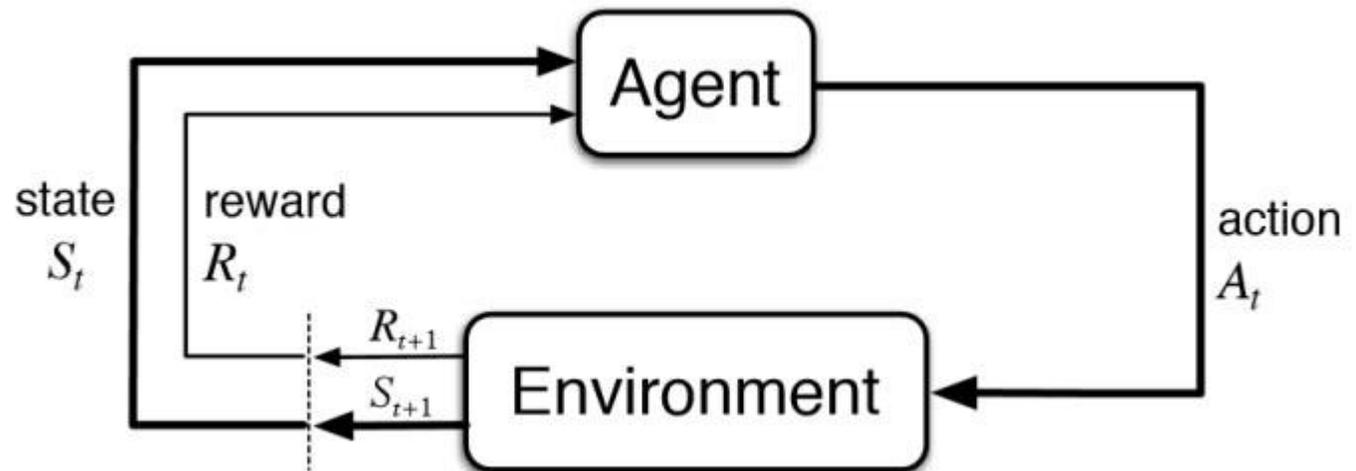
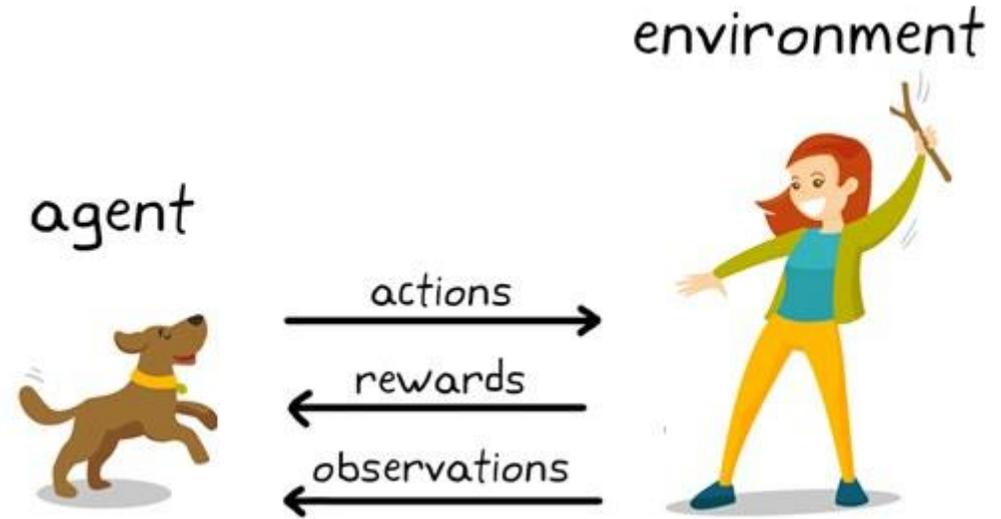
Une IA qui sait résoudre toutes les fonctions d'expertises humaines, c'est-à-dire battre le meilleur des experts humains sur chaque verticale fonctionnelle.

L'IA générative (LLM) n'est pas la seule voie. Il y a aussi le RL

L'Apprentissage par Renforcement (RL)

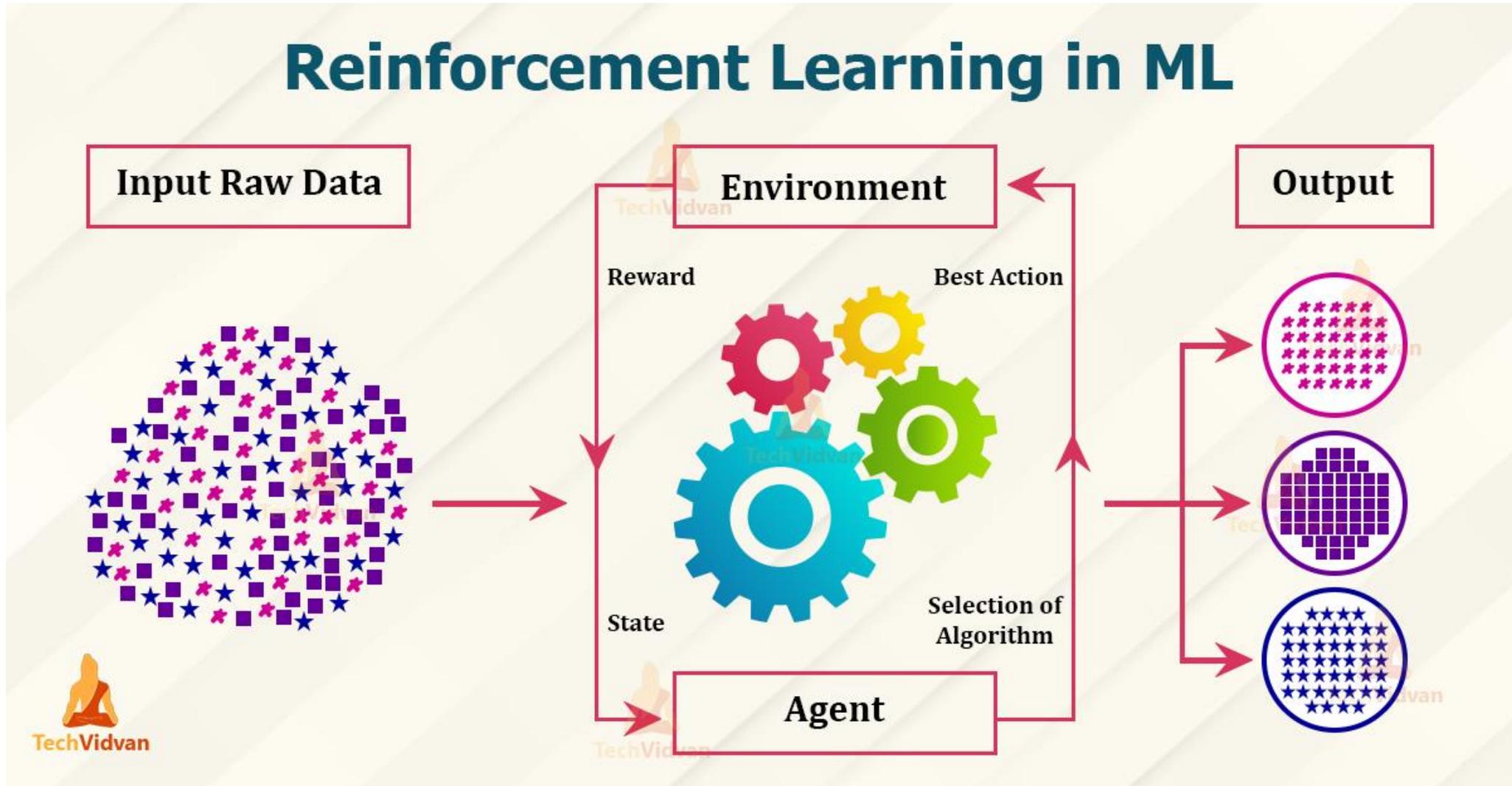
La puissance
« surhumaine »
du RL

Au service de la
Résolution des
fonctions

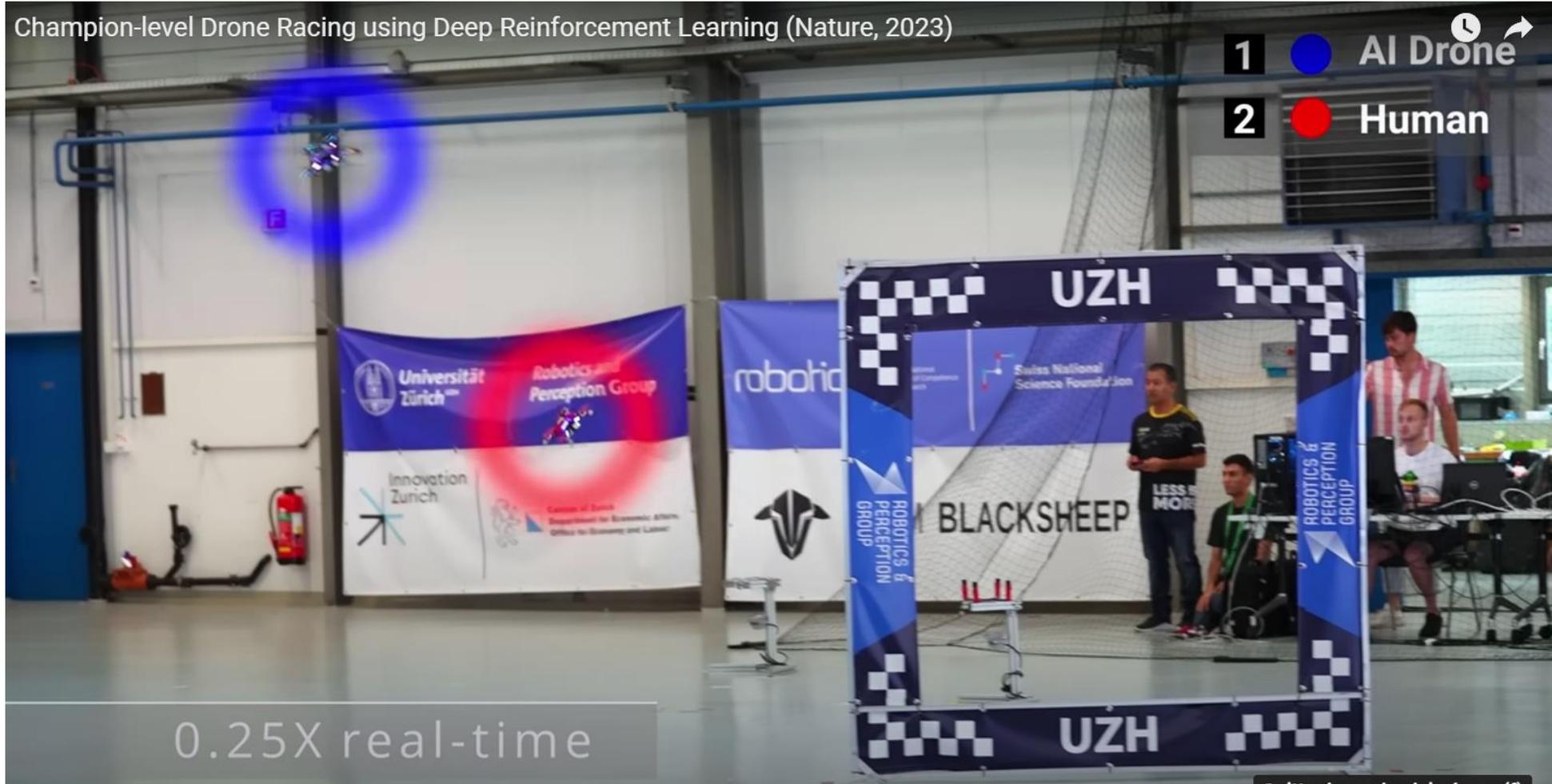


L'Apprentissage par Renforcement (RL)

Reinforcement Learning in ML



L'Apprentissage par Renforcement (RL)



Le vol surhumain résolu (Aout 2023 – UZH)
<https://www.youtube.com/watch?v=fBiataDpGlo>

L'Apprentissage par Renforcement (RL)



Le jeu de GO surhumain résolu (ALPHAGO 2020 DEEPMING GOOGLE
<https://www.youtube.com/watch?v=WXuK6gekU1Y>)

La plus impactante des convergences technologiques :

**La convergence « Matière – Information » via la robotique
embarquant de l'IA générale**

PARTIE 2

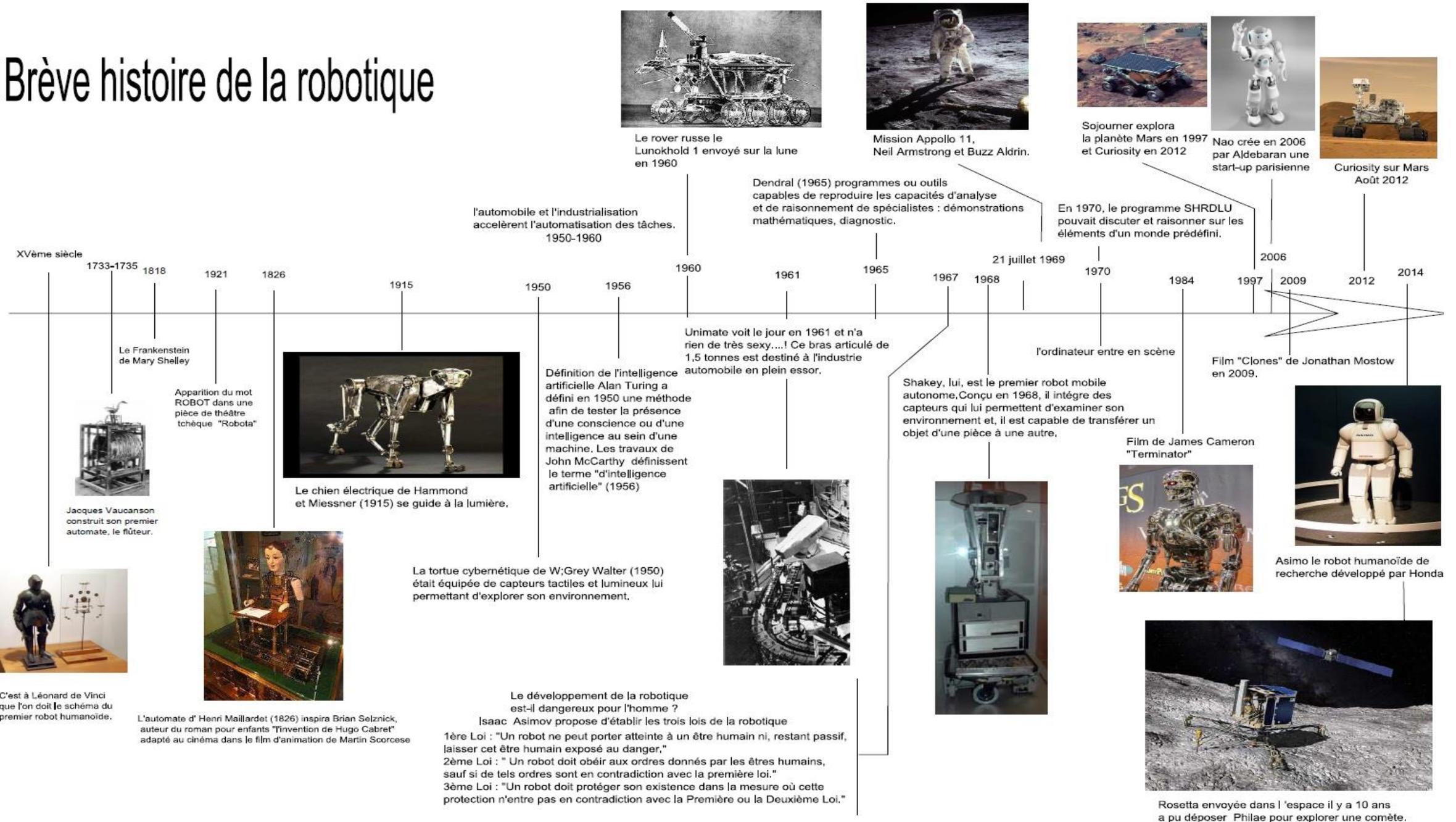
Les révolutions de la robotique associée à l'IA

La robotique au cœur de quatre dynamiques de convergences technologiques

La robotique s'inscrit au cœur des quatre grandes convergences technologiques du 21^{ème} siècle : NBIC, MI, DIADEH, CKTS :

- La convergence NBIC est la convergence des Nanotechnologies, des Biotechnologies, de l'Informatique et des sciences Cognitives.
- La convergence MI est la convergence de la Matière et de l'Information pour produire un espace ubiquitaire.
- La convergence DIADEH (Diffusion de l'IA sur les Domaines d'Expertise Humaine) est la convergence de l'expertise humaine et de l'intelligence artificielle pour produire une expertise hybride.
- La convergence CKTS : Convergence of Knowledge and Technology for the benefit of Society.

Brève histoire de la robotique



Les douze révolutions sectorielles de la robotique qui transforment le monde

R1 - Révolution de la robotique agricole

R2 - Robotique de dépollution automatique des sols, airs, mers

R3 - Robotique de l'industrie et logistique

R4 - Robotique du transport et des mobilités

R5 - Robotique de l'aéronautique et du spatial

R6 - Robotique de la construction et BTP

R7 - Robotique du secteur de l'énergie

R8 - Robotique militaire et sécurité

R9 - Robotique chirurgicale

R10 - Robotique des prothèses et de l'augmentation humaine

R11 - Robotique domotique de l'habitat et du quotidien

R12 - Robotique d'assistance aux personnes dépendantes

La robotique mobile s'appuie sur une très grande variété de vecteurs...

	Flying	Swimming	4+ Legged	2 Legged	4+ Wheeled	2 Wheeled	Arms	Head
Defense								
Industry								
Security								
Medical								
Transport								
Commercial								
Consumer								

Une très grande diversité des systèmes robotisés



VIE QUOTIDIENNE
SERVICES À LA PERSONNE



PRODUCTION - INDUSTRIE



TRANSPORT



AVANÇÉES SCIENTIFIQUES



MEDICAL - SANTÉ

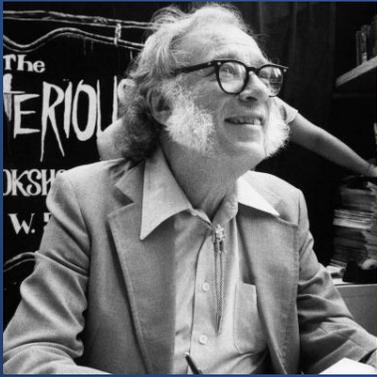


EXPLORATION - EXPLOITATION

Robotique autonome

• Le 21^{ème} siècle est celui de la robotique autonome, c'est le temps du Kronos et de la Société 5.0

- **Société 1.0 des chasseurs-cueilleurs,**
- **Société 2.0 de l'agriculture,**
- **Société 3.0 de l'industrie,**
- **Société 4.0 de l'information,**
- **Société 5.0 : smart society, robotique ubiquitaire**



Robotique autonome

LES LOIS D'ASIMOV

1

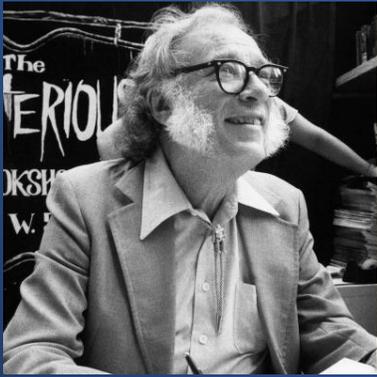
Un robot ne peut porter atteinte à un **être humain**, ni, en restant **passif**, permettre qu'un être humain soit exposé au danger.

2

Un robot doit **obéir aux ordres** qui lui sont donnés par un **être humain**, sauf si de tels ordres entrent en conflit avec la première loi.

3

Un robot doit **protéger son existence** tant que cette protection n'entre pas en conflit avec la première ou la deuxième loi.



Robotique autonome

Isaac Asimov (1920-1992) définit en 1941 les trois premières lois de la robotique. On peut désormais compléter les trois lois d'Azimov une liste de missions d'intérêts supérieurs:

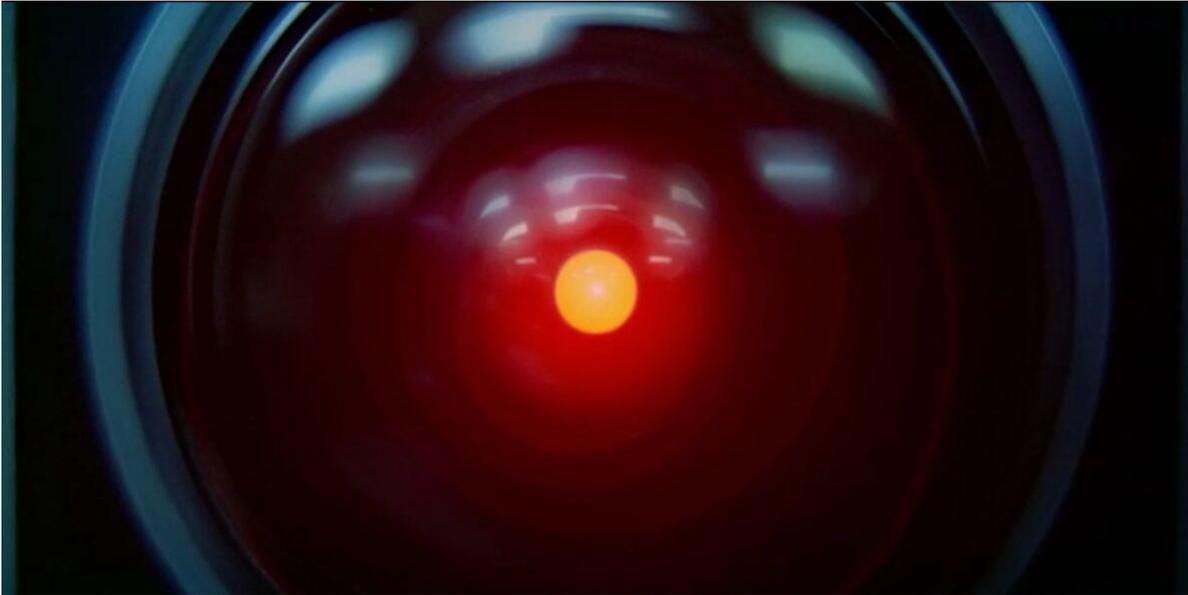
La robotique autonome œuvre :

- pour éloigner l'homme du risque**
- pour garantir sa survie,**
- pour explorer et dépolluer son environnement**

L'imaginaire de la Robotique & IA depuis les années 1960

HAL 9000

2001 L'Odyssey de l'Espace (Stanley KUBRICK – 1968)



**HAL 9000 est-il défectueux
ou bien conscient ?**

Le Monologue des larmes dans la pluie

Blade Runner (Ridley Scott – 1982)



« J'ai vu des choses que vous, humains, ne pourriez croire... Des navires de guerre en feu, surgissant de l'épaule d'Orion... J'ai regardé des rayons C briller dans l'obscurité, près de la Porte de Tannhäuser... Tous ces moments se perdront dans le temps... comme... les larmes dans la pluie... Il est temps de mourir. »

TARS

INTERSTELLAR (Christopher NOLAN – 2014)



Why did Cooper make honesty 95% and humor 60% in the TARS setting at Cooper's station in the Interstellar movie?

L'un des grands défis de la robotique :

« Eloigner l'homme du risque »

Les défis de l'autonomie au service de la sécurité industrielle



A 200 km de Limoges, en Nouvelle Aquitaine

**L'exemple du champion mondial de robotique terrestre
SHARK ROBOTICS**

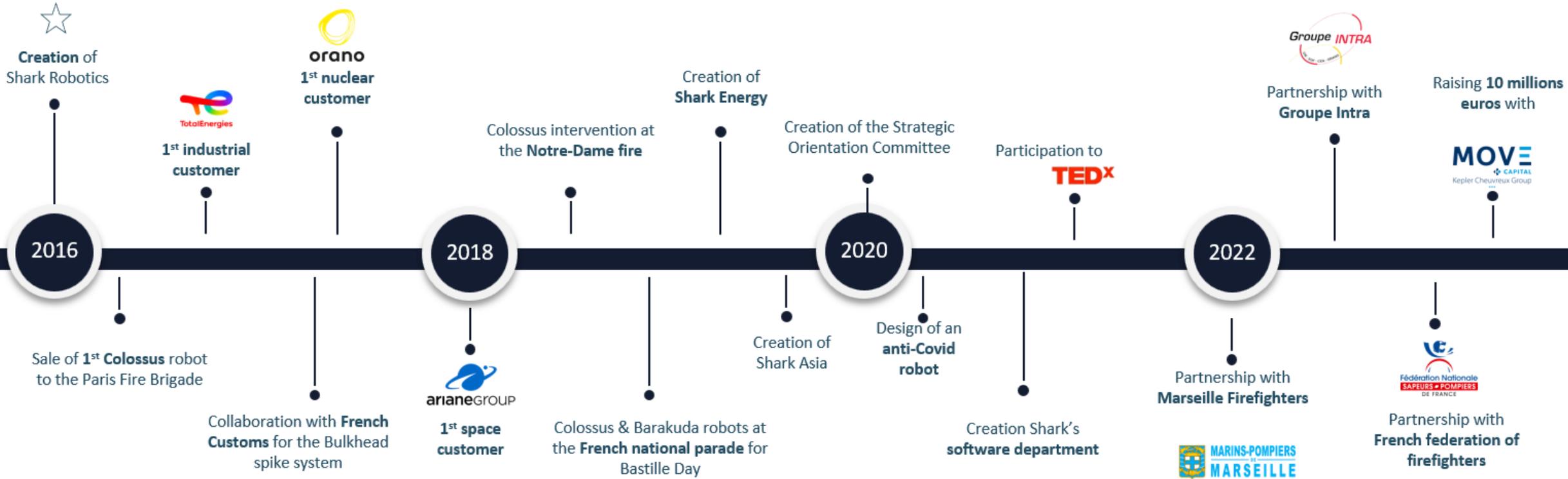
<https://www.shark-robotics.com/>





Les succès français de robotique terrestre nous placent au premier rang mondial pour :

- **la robotique incendie (cf. Notre Dame)**
- **la robotique industrielle en milieu extrême (Oil&Gaz – Nucléaire)**



SHADOW ADVISORY BOARD

SCIENTIFIC ADVISORY



Thierry BERTHIER



Sophie VIGER



Nathalie COLLIGNON



Victor VUILLARD



Erwann LE PENNEC



Amal EL FALLAH SEGHRUCHNI

STRATEGIC ADVISORY



General Olivier KEMPF



Controleur general Gregory ALLIONE

CONFIDENTIAL



COLOSSUS[®]



Surgical strike to
extinct fire with AI

Change option in
less than 30 seconds

Post-fire monitoring
& surveillance

Autonomy :
up to 12
hours

Resistant to very
high temperatures

Thermal cameras
and Zoom x30

Autonomous
detection with
AI



10 HOURS
INTERVENTION DURING
NOTRE-DAME FIRE

ROBOTS DESIGNED TO ANSWER FIREFIGHTERS' NEEDS

COLOSSUS[®]



HEAVYWEIGHT CATEGORY

RHYNO PROTECT[®]



MEDIUM CATEGORY

ALLIGATOR[®]



LIGHTWEIGHT CATEGORY



World leader
In firefighting robots



Multipurpose
robots



30+ patented innovations
In the field of fire-safety



Remotely Controlled
& Autonomous robots

CONFIDENTIAL

10

LAW ENFORCEMENT & EOD ROBOTS

BARAKUDA[®]



Mule robot to transport
materials, inspect and evacuate
wounded people

BULKHEAD[®]



Robotic spike system to stop
vehicles and secure sites

ATRAX[®]



Small EOD robot
(60 kg range)

RHYNO EOD[®]



Medium EOD robot
(200 kg range)



DEVELOPED WITH
THE FRENCH ARMY



DEVELOPED WITH
THE FRENCH CUSTOMS



DEVELOPED WITH
THE FRENCH SPECIAL
FORCES



DEVELOPED FOR
INTERNATIONAL
REQUESTS

CONFIDENTIAL

11

CUSTOM NUCLEAR ROBOTS

MODULAR ROBOTS FOR INSPECTION, DECONTAMINATION, TREATMENT AND INTERVENTION

SILO 130



Robot for processing
radioactive waste

RIANA SC



Robot for detecting
radioactivity

ATRAX XL



Modular nuclear accident
response robot

HAO



Robot for processing
radioactive waste



CONFIDENTIAL

12

CUSTOM INDUSTRIAL ROBOTS

MODULAR ROBOTS FOR INSPECTION AND INTERVENTION

R4



Robot to carry out complex tasks
on offshore platforms

SALAM&DER



Multi-purpose robot for recovering DARTS
sensors and transporting seismic vibrators



CONFIDENTIAL

13

CUSTOM SPACE ROBOTS



CONFIDENTIAL



THEMIS

Refueling robot for reusable space launchers



14

La robotique spatiale : HAL9000 et TARS réunis

A WORLDWIDE COMPANY WITH RECOGNIZED REFERENCES



SHARK'S CUSTOMERS



SHARK'S PARTNERS



CONFIDENTIAL

PRESENT IN THESE COUNTRIES



18

Le numéro 2 mondial, leader européen de mini drones aériens est français



Un autre champion français de niveau mondial , peu connu du grand public EOS TECHNOLOGIE (Bordeaux Mérignac)



ENDURANCE 1200

[LEARN MORE](#)



Flight time max
18 hours



BVLOS Data link
800 km

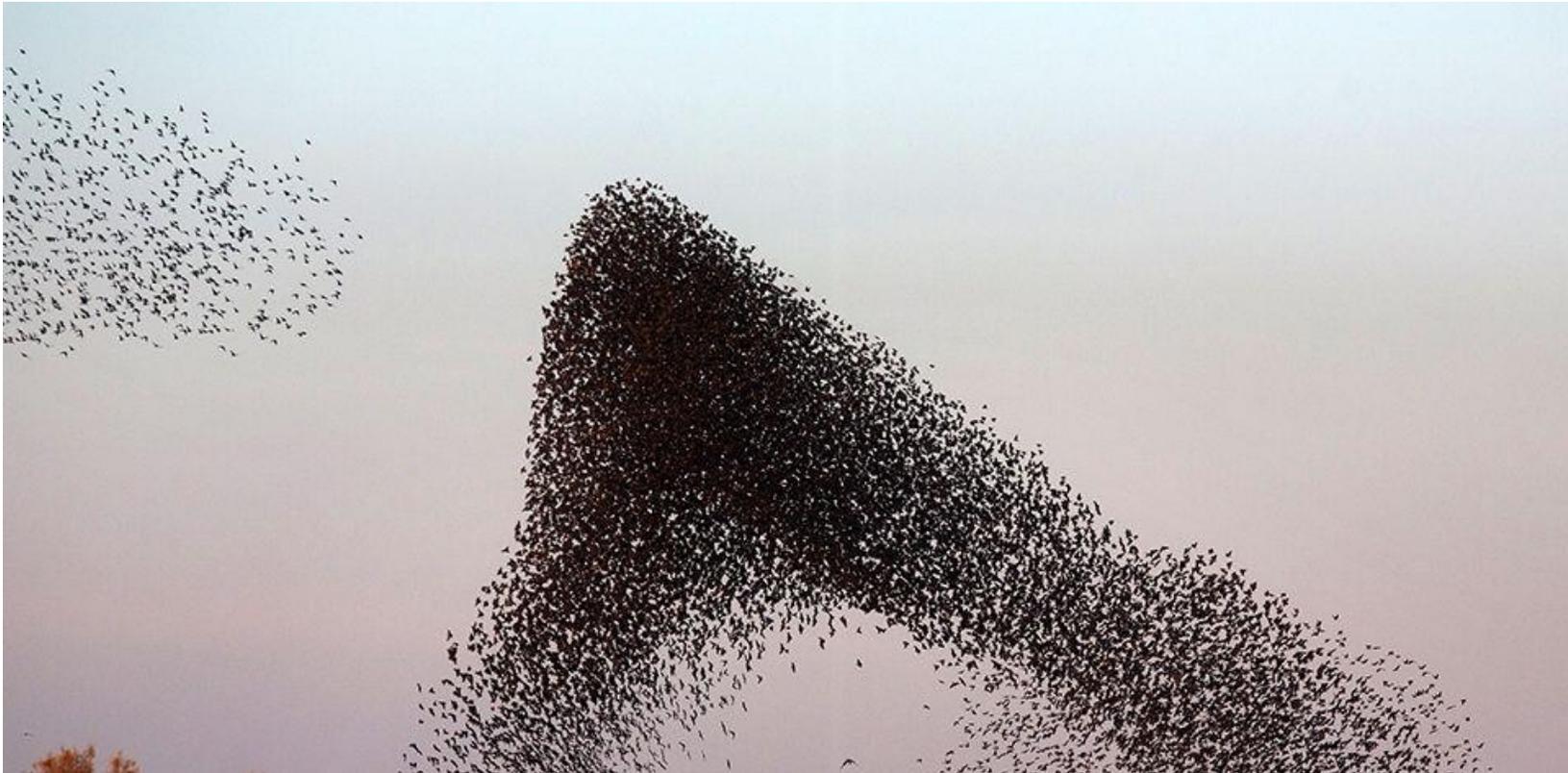


Up to 30 kg
payload



Intelligence collective et émergence de fonctions

La révolution bourdonnante de la robotique en essaims

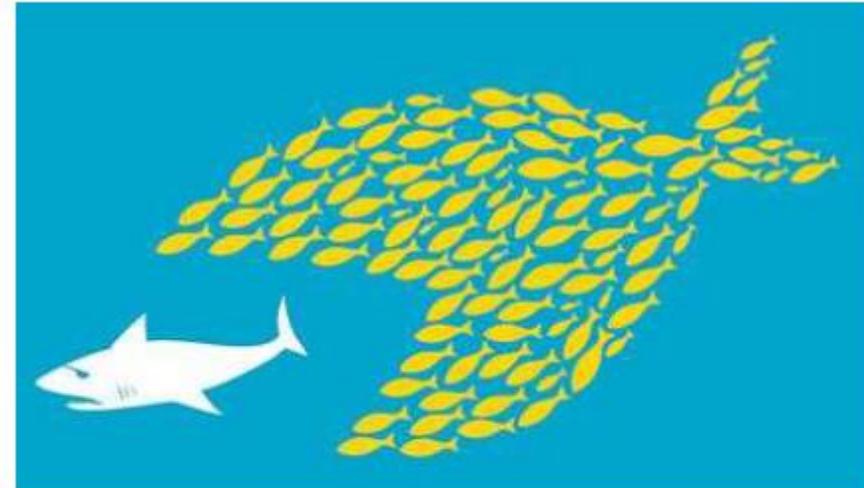


L'intelligence collective

n'est pas l'intelligence qui résulte du travail à plusieurs (« meeting intelligence »)

ni l'effet de nombre

(la somme des intelligences individuelles)



L'intelligence collective dans la nature



La révolution bourdonnante des essaims



1 drone opéré par un grand nombre de personnels



1 personnel opérant un essaim de drones

- Miniaturisation et utilisation loisir des drones → effet « low cost »
- Progrès dans l'informatique distribuée / transmission à fréquence « millimétriques » (60 GHz + ; *Ultra Wide Band*)

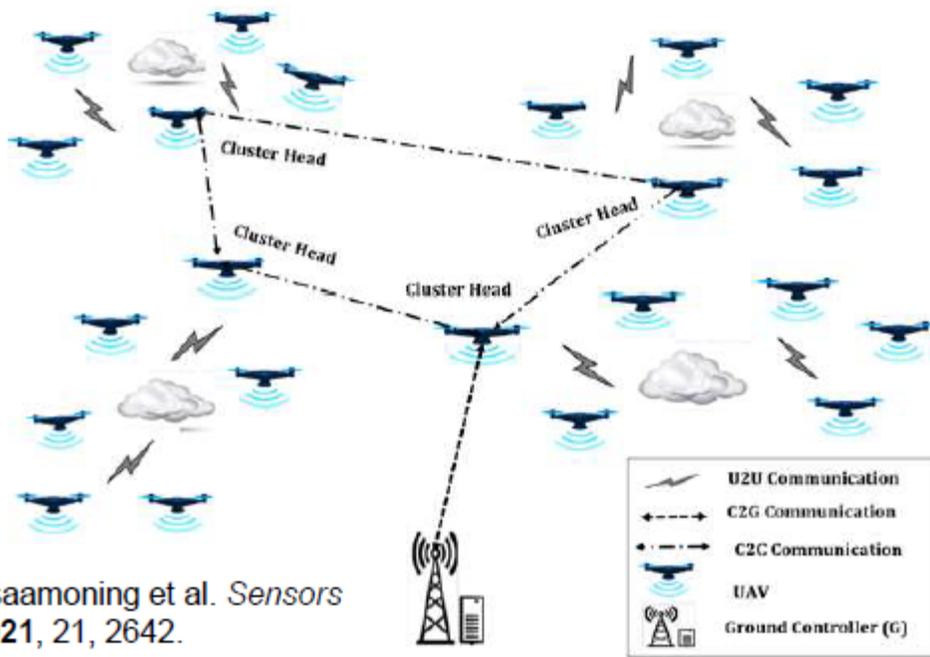


DRONISOS – spectacle de drones aériens : <https://www.youtube.com/watch?v=lirXLdH57mE>
Traversée d'une forêt de bambous par un essaim autonome – Université de Zhejiang - 2022
<https://www.youtube.com/watch?v=SELZwkV13IM>

Communication et autonomie sont liés

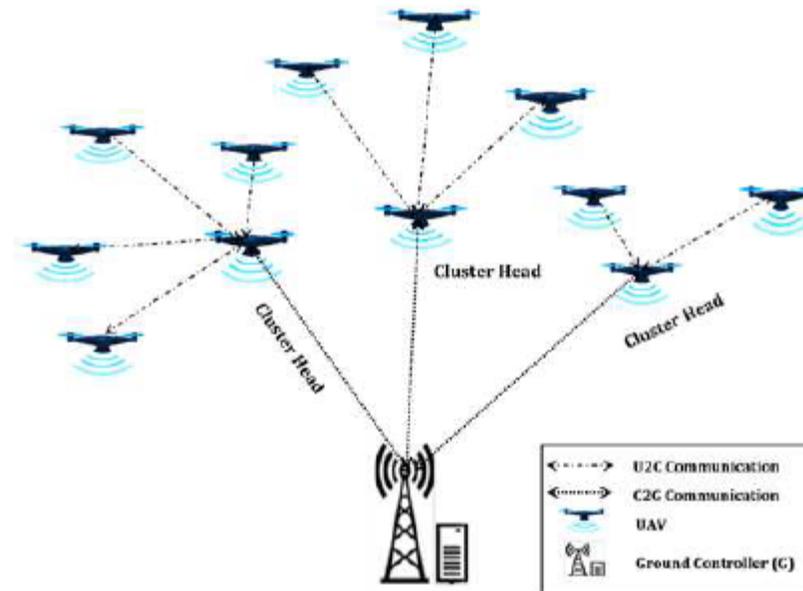
- Intelligence et communication déportés dans l'essaim
- Organisation opportuniste du groupe

Des réseaux « ad-hoc »...



Asaamoning et al. *Sensors*
2021, 21, 2642.

...plutôt que des réseaux type clusters



7

Effets induits des essaims de drones

- Le propre des essaims :

- Reposent sur le calcul déporté « *edge computing* », distribué et miniaturisé (FPGA)
- Tirent leur efficacité des relations et non des individus
- Favorisent plus d'intelligence artificielle et collective, non traçable, pouvant prendre des initiatives

- Limites des essaims :

- Faible élongation/endurance
- Déploiement en masse
- Vulnérabilité aux aléas aérologiques (drones aériens)
- Hacking



13

Le grand défi de la Lutte Anti Drones Swarm Counter Swarm



Essaim UAV kamikazes en attaque



Essaim Anti-essaim autonome Intelligence Artificielle

Contexte 2

36



Essaim UAV kamikazes en attaque



Essaim Anti-essaim autonome Intelligence Artificielle

Lutte anti drones (LAD)



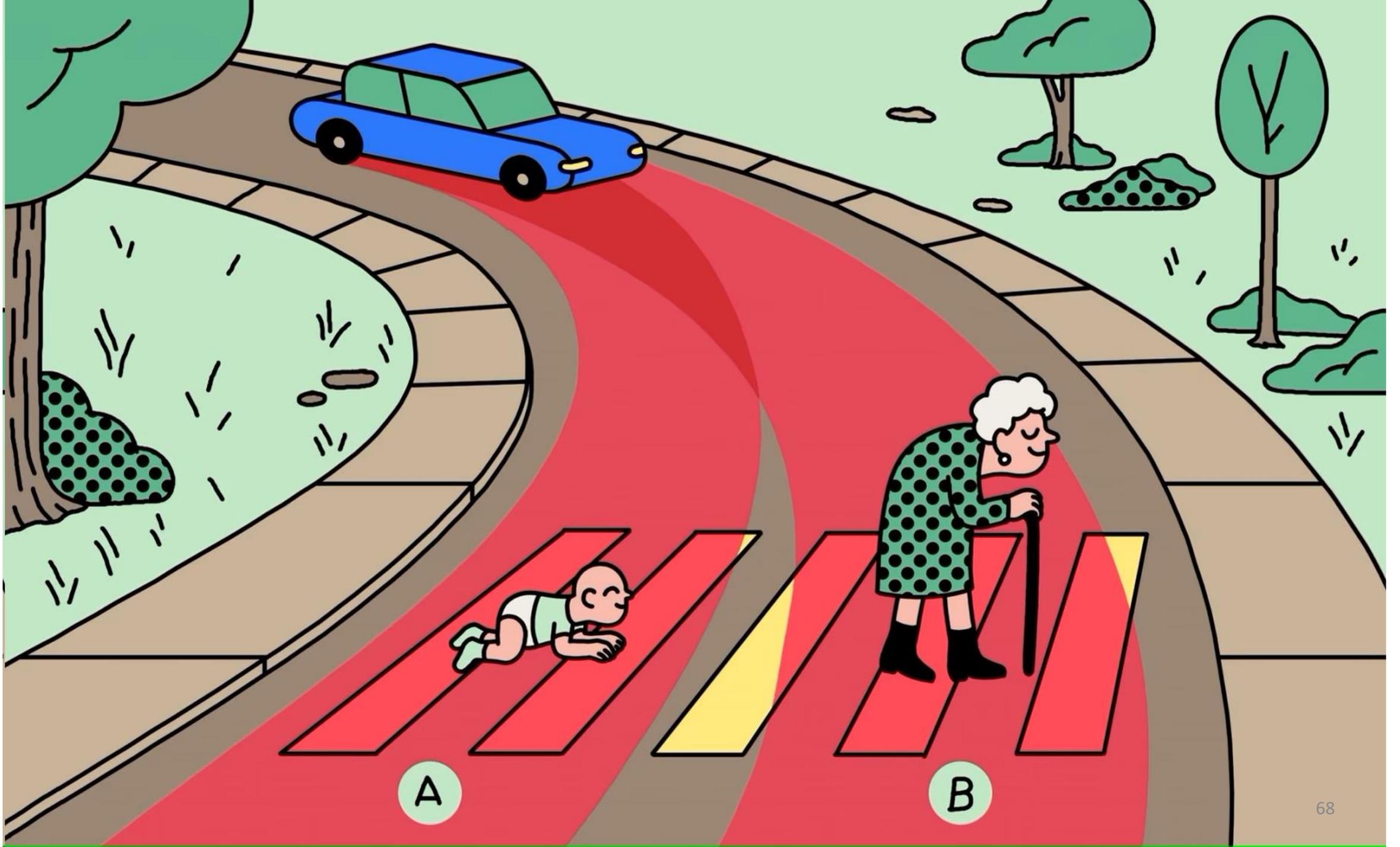
Contexte 3

37

ANDURIL ANVIL : <https://www.anduril.com/hardware/anvil/>

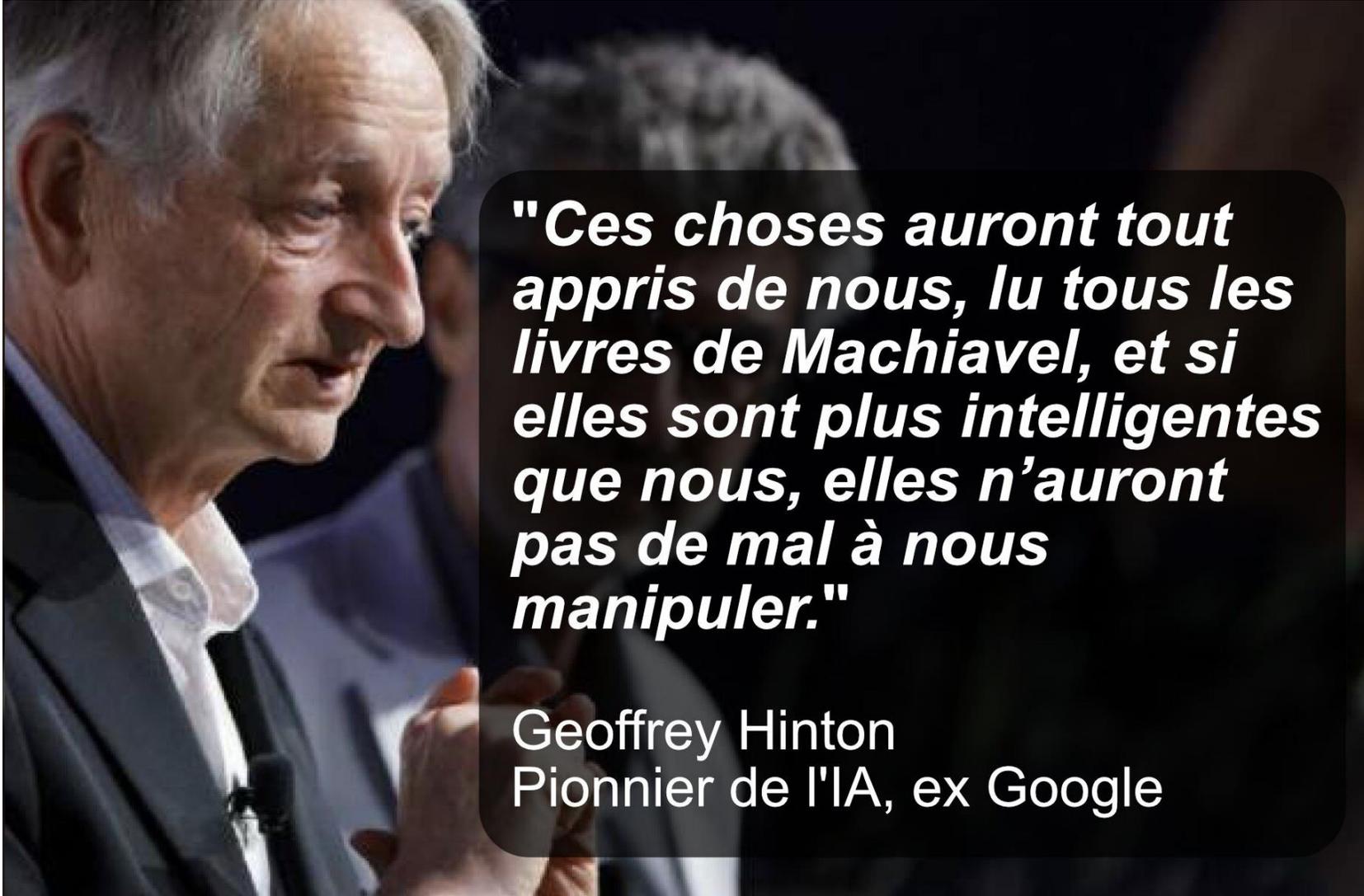
PARTIE 3

LA CYBERSECURITE comme ingrédient indispensable aux révolutions de l'IA et de la robotique



A

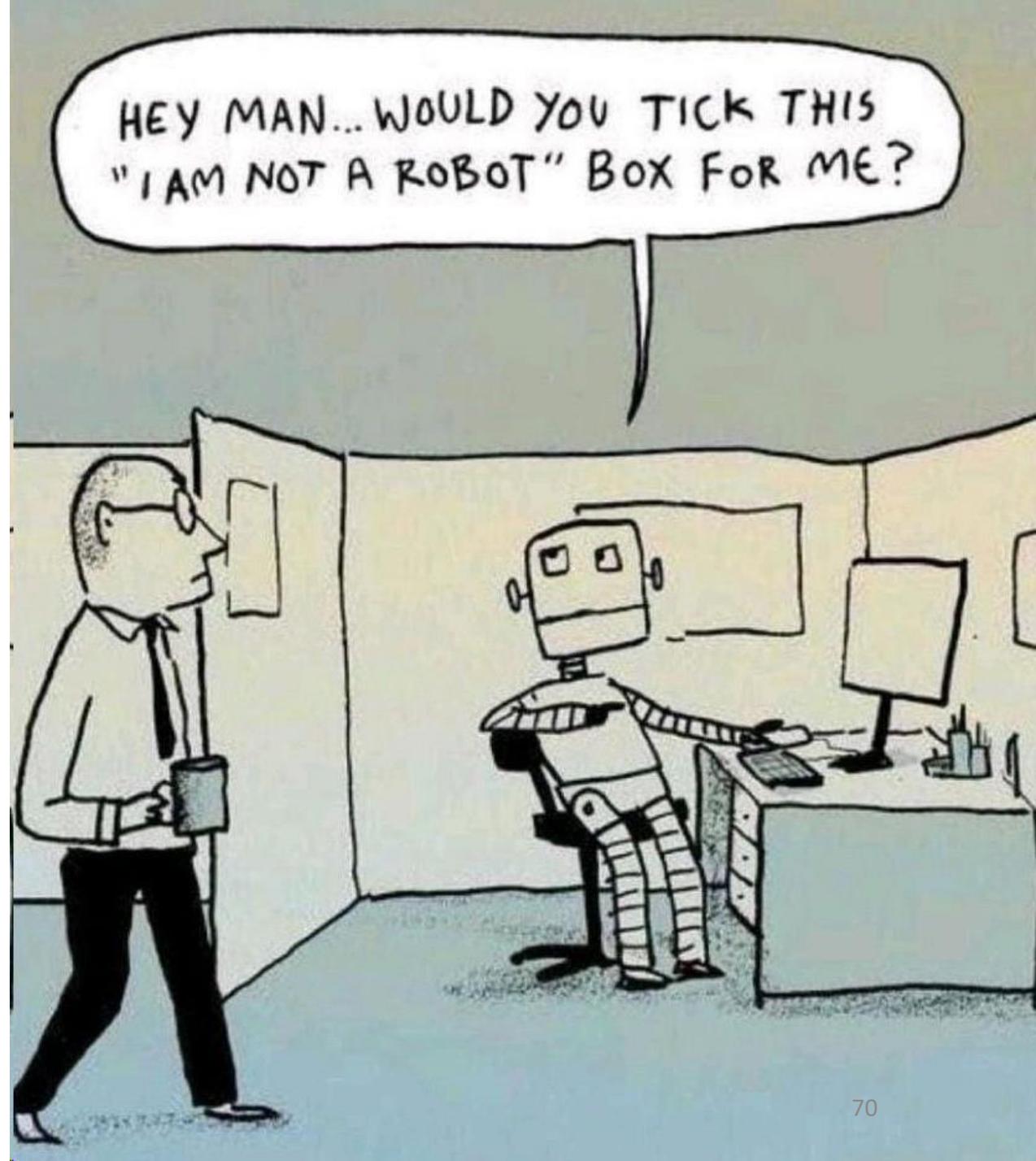
B



"Ces choses auront tout appris de nous, lu tous les livres de Machiavel, et si elles sont plus intelligentes que nous, elles n'auront pas de mal à nous manipuler."

**Geoffrey Hinton
Pionnier de l'IA, ex Google**

- Les progrès et les convergences technologiques NBIC, CKTI, M-I, M-IA s'accélèrent en apportant des niveaux de « résolution » inédits sur les activités humaines.
- Nous convergions vers des IA- générales au sens de la résolution optimale des fonctions d'expertises humaines : (le jeu d'échec est résolu par l'IA, le jeu de GO est résolu par l'IA, la détection précoce de la maladie d'Alzheimer est résolue par l'IA, le vol de drones RACER avec obstacle est résolu depuis septembre 2023 par l'IA (RL), etc,...
- **Ces multiples résolutions produisent systématiquement de nouvelles surfaces d'attaques**



En robotique, le risque cyber induit le risque physique.

Un robot attaqué peut se transformer en une arme létale pour un attaquant

Parfois, il n'y a pas d'attaquant mais juste une sortie du cadre d'emploi du système robotisé.

L'IA peut réduire le risque cyber sur le système de Commande & Contrôle du robot, sur son autopilote.

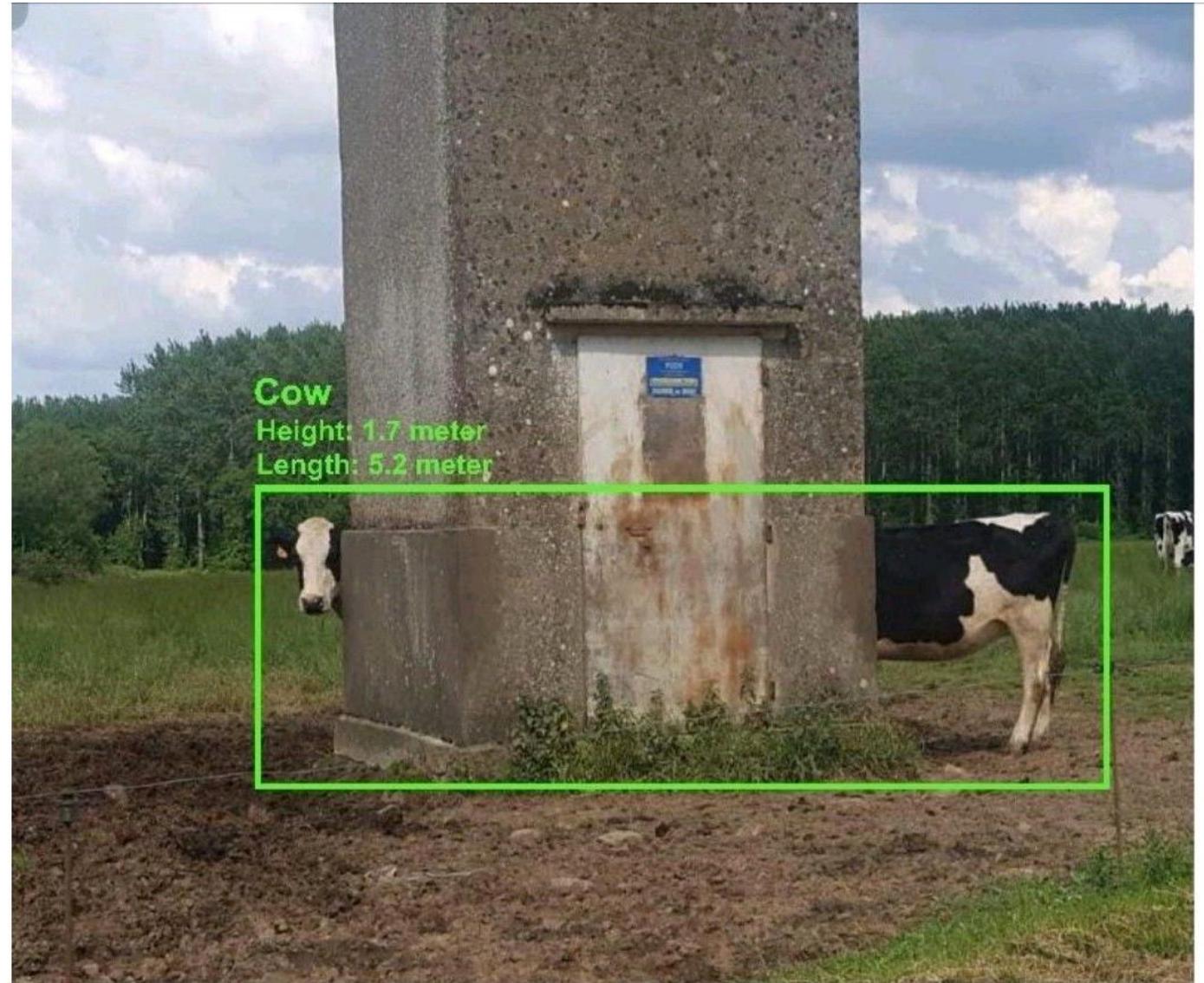
L'IA peut réduire le risque physique en apportant une « compréhension fine » du contexte et de l'activité du robot.

Vers des SIEM UEBA embarqués dans chaque système robotisé pour une IA et ROBOTIQUE de confiance.

Vacuum Robot 'eats' sleeping woman's hair

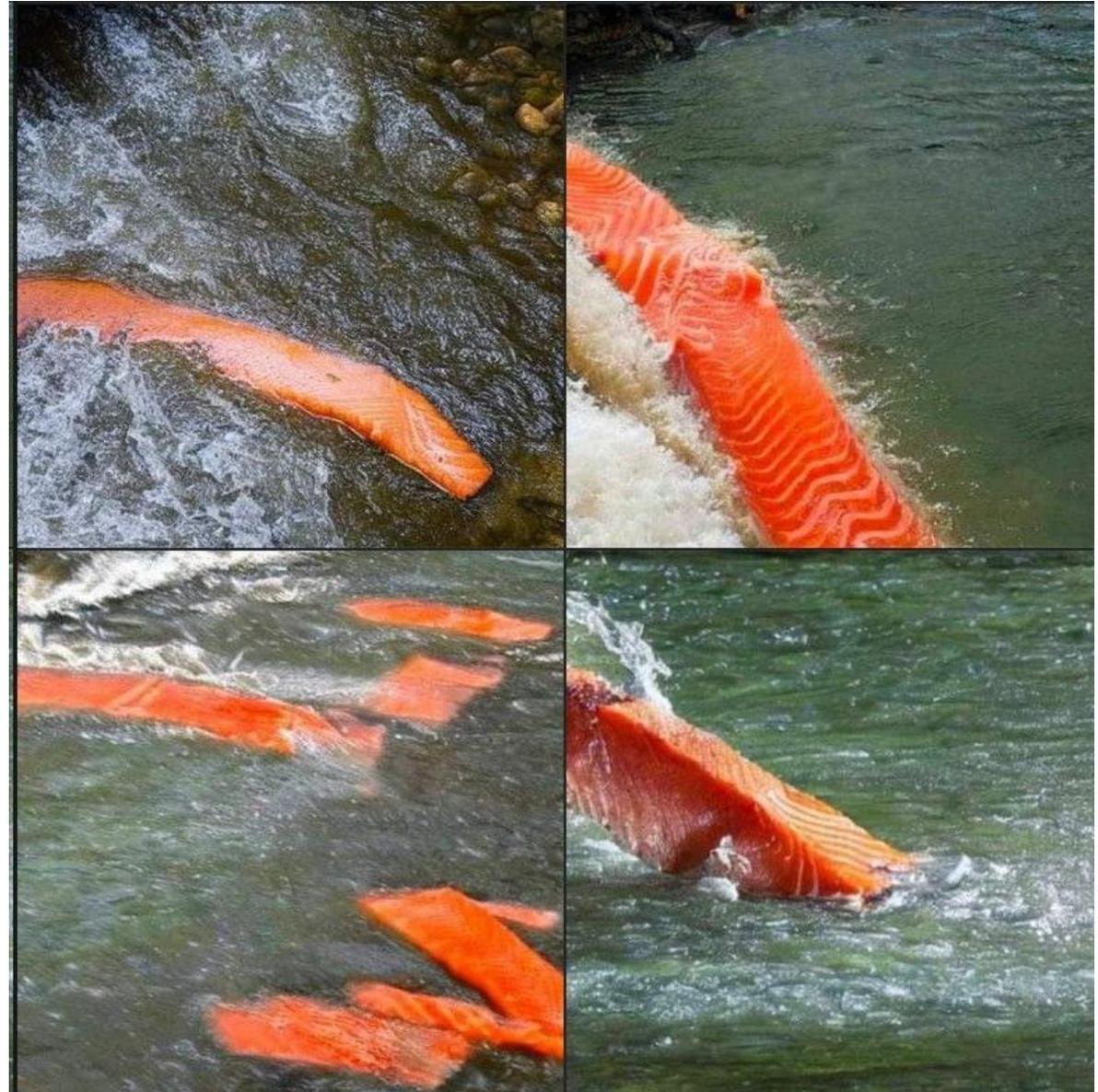


Parfois, il n'y a pas d'attaquant mais juste une sortie du cadre d'emploi du système robotisé ou une ambiguïté dans le contexte.



Parfois, il n'y a pas d'attaquant mais juste une sortie du cadre d'emploi du système robotisé ou une ambiguïté dans le contexte...

Ou une faiblesse dans la phase d'apprentissage du modèle ML



How to confuse machine learning:

La complexité du réel pour l'IA,
pour les capteurs et pour la
robotique



La complexité du réel pour l'IA, pour les capteurs et pour la robotique

G

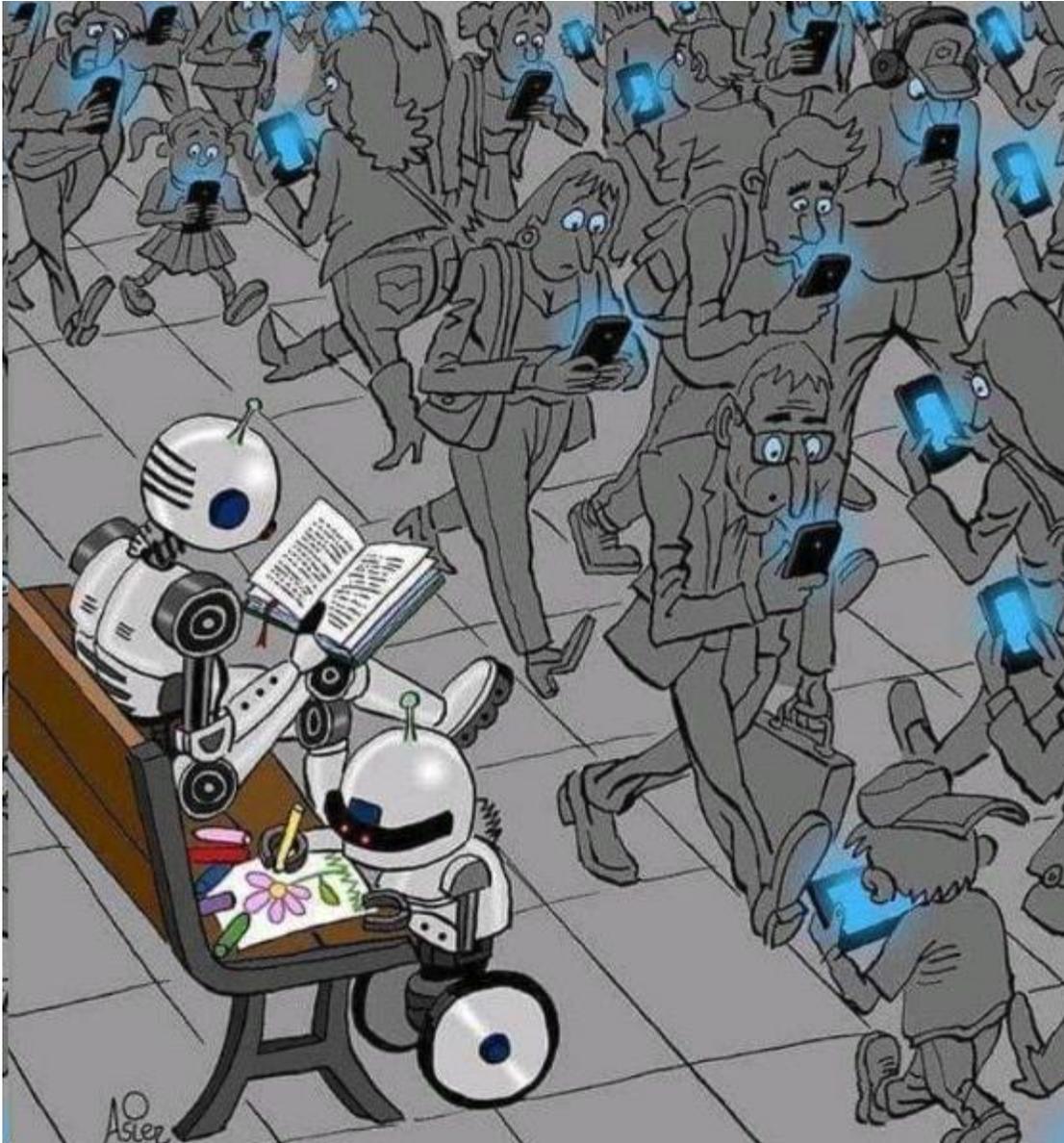


Please tell me what is it in each cell in a tabular format aligned with this picture grid.



Certainly! Here's a breakdown of the content of each cell in the format of a table:

Row	Column 1	Column 2	Column 3	Column 4
1	Muffin with blueberries	Chihuahua (side profile)	Blueberry Muffin	Chihuahua (profile looking up)
2	Chihuahua (frontal face)	Cookie with chocolate chips	Chihuahua (face close-up)	Blueberry Muffin with sugar on top
3	Blueberry Muffin with a smiley face	Chihuahua (frontal face close-up)	Blueberry Muffin with blueberries on top	Chihuahua (slightly showing teeth)
4	Chihuahua (puppy face close-up)	Group of Cookies with chocolate chips	Group of Chihuahua puppies	Muffin with blueberries



Why **automakers** focus on the humanoid robots?



Atlas
HYUNDAI



Avatar
TOYOTA



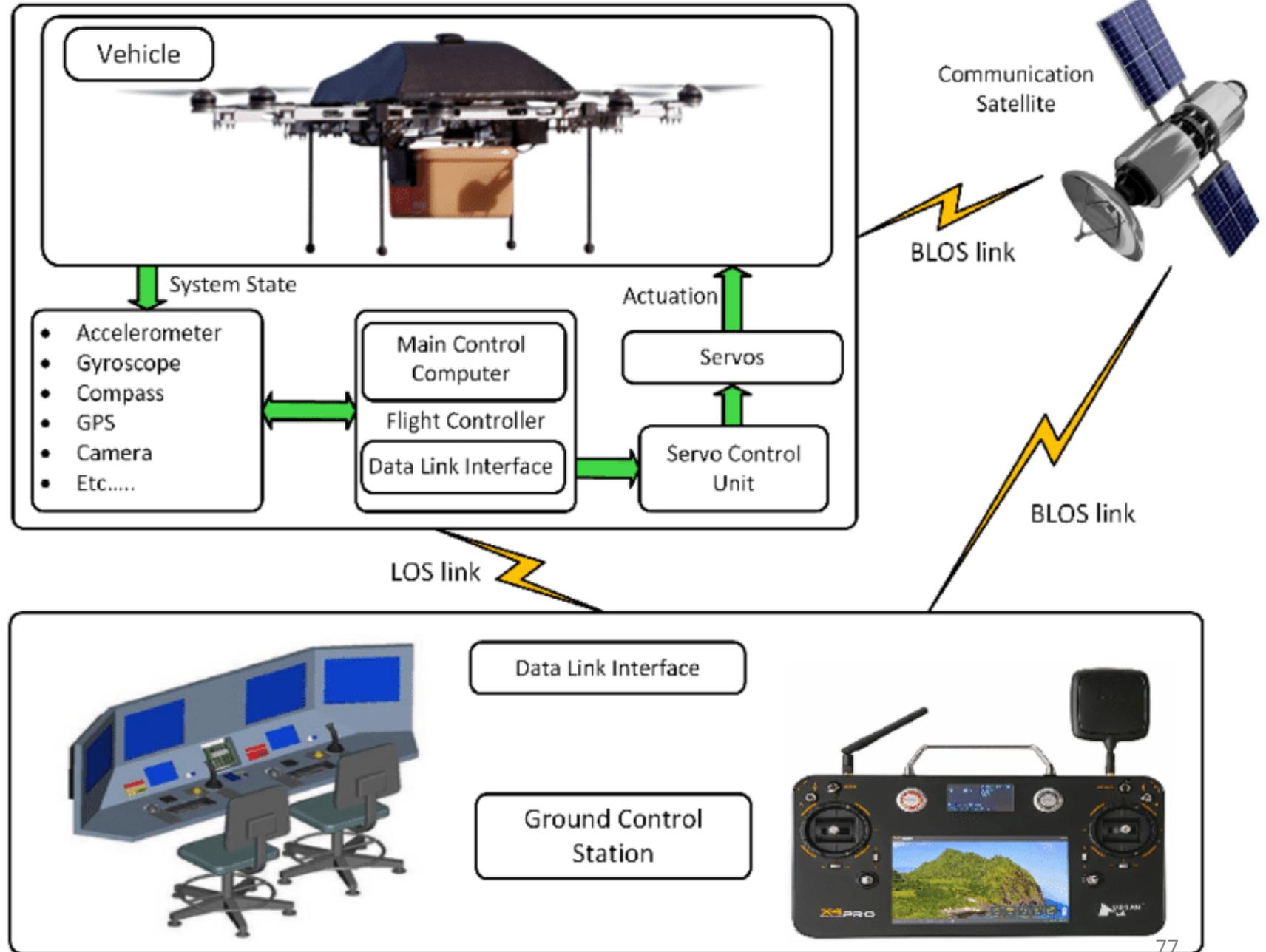
Asimo
HONDA

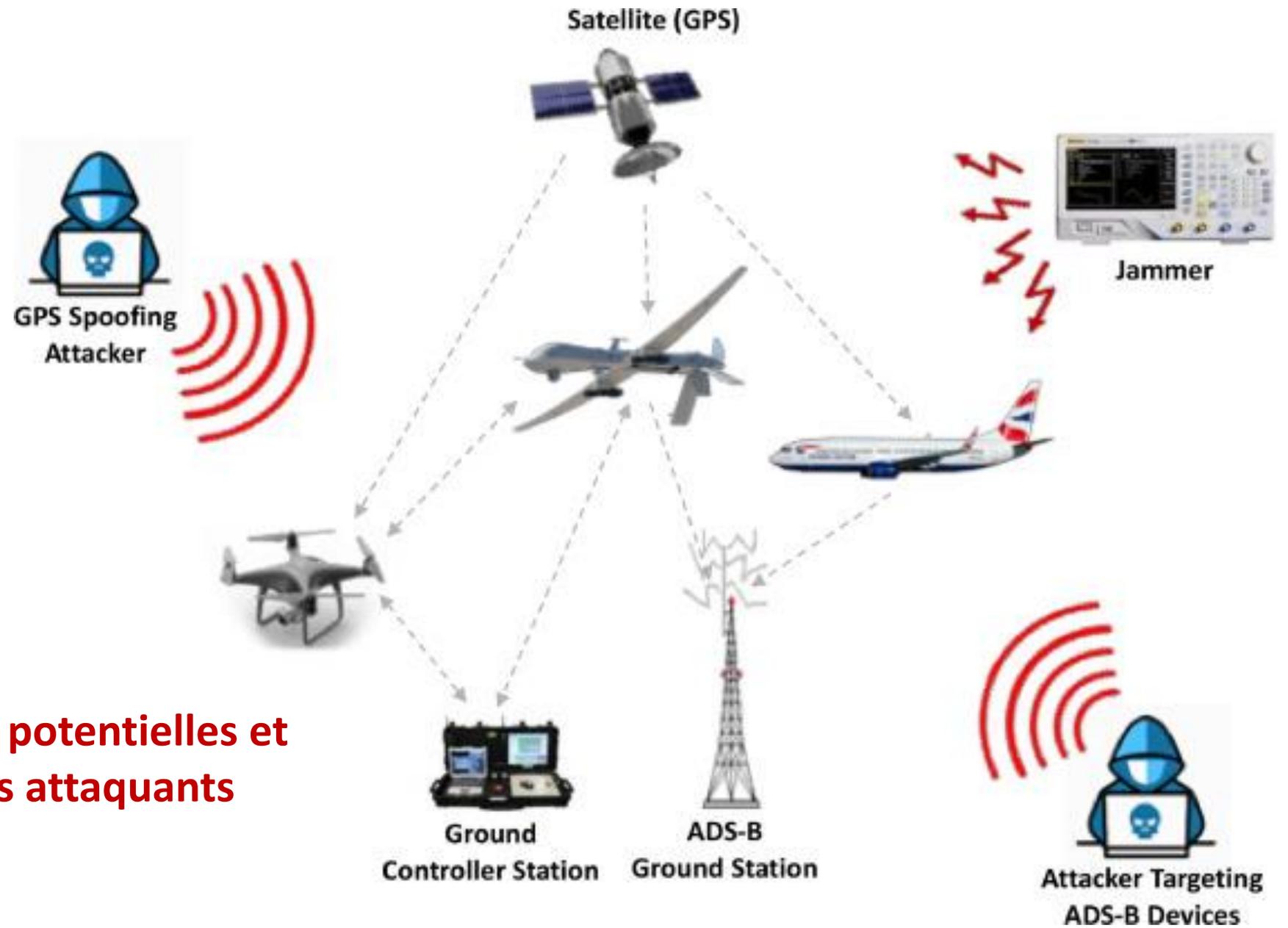


Teslabot
TESLA

Global Robot Marketplace

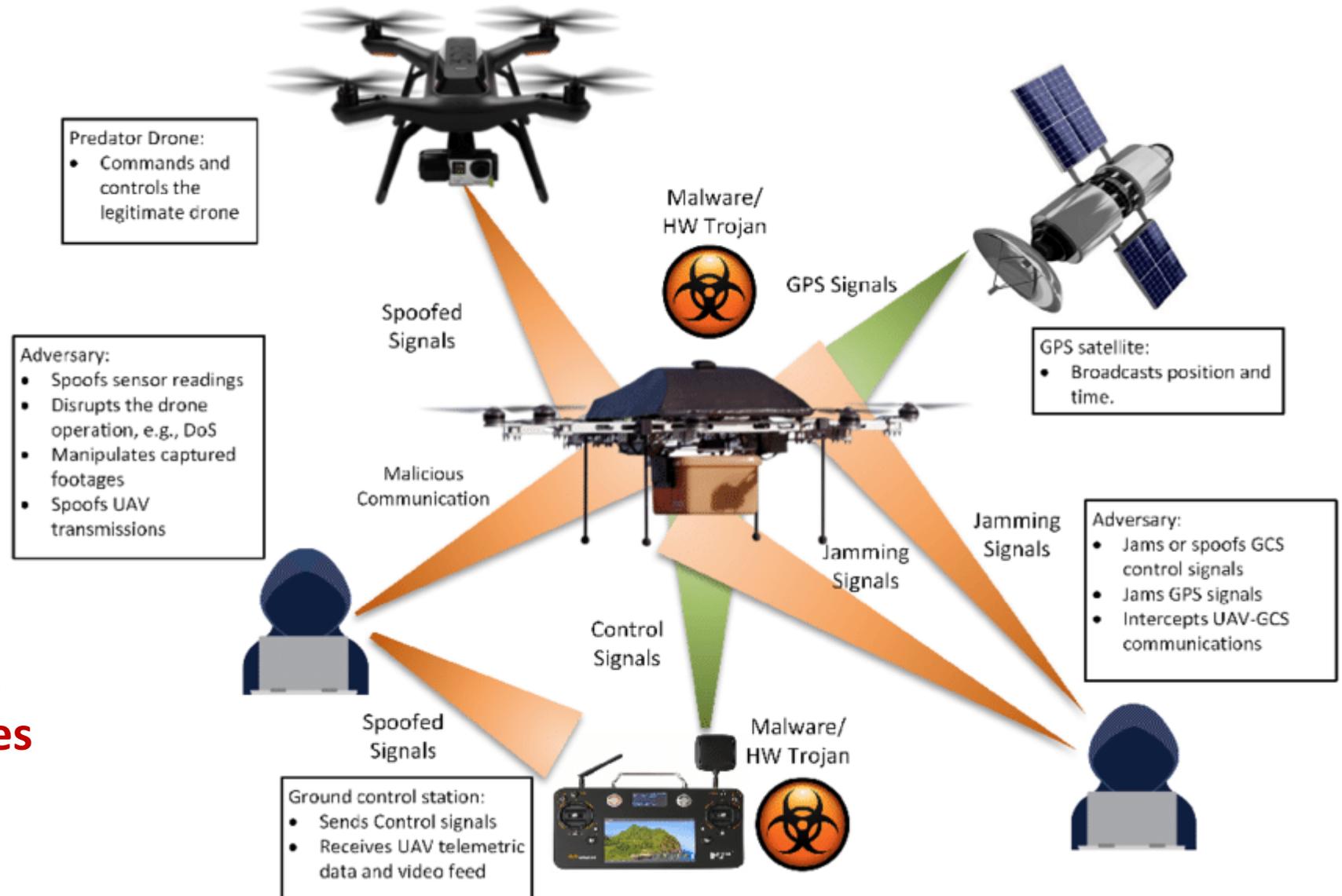
Un système de systèmes très complexes avec des surfaces d'attaque spécifiques...





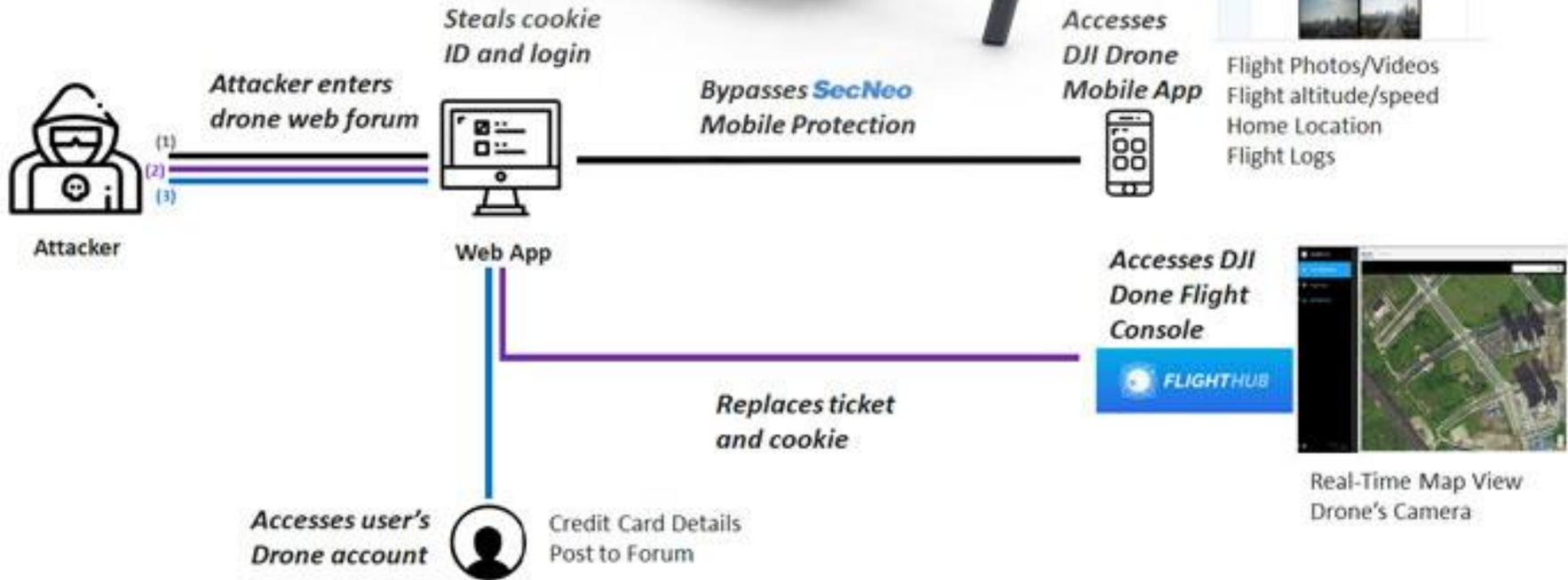
De multiples entrées potentielles et opportunités pour les attaquants

Des drones attaquant (cyber) d'autres drones



Des vulnérabilités non corrigées chez DJI...

DJI Drone Hack



Ukrainian Marines Hacked A Russian Drone To Locate Its Base—Then Blew Up The Base With Artillery

30 novembre 2023 - <https://www.youtube.com/watch?v=9tLlgTNiDC4>

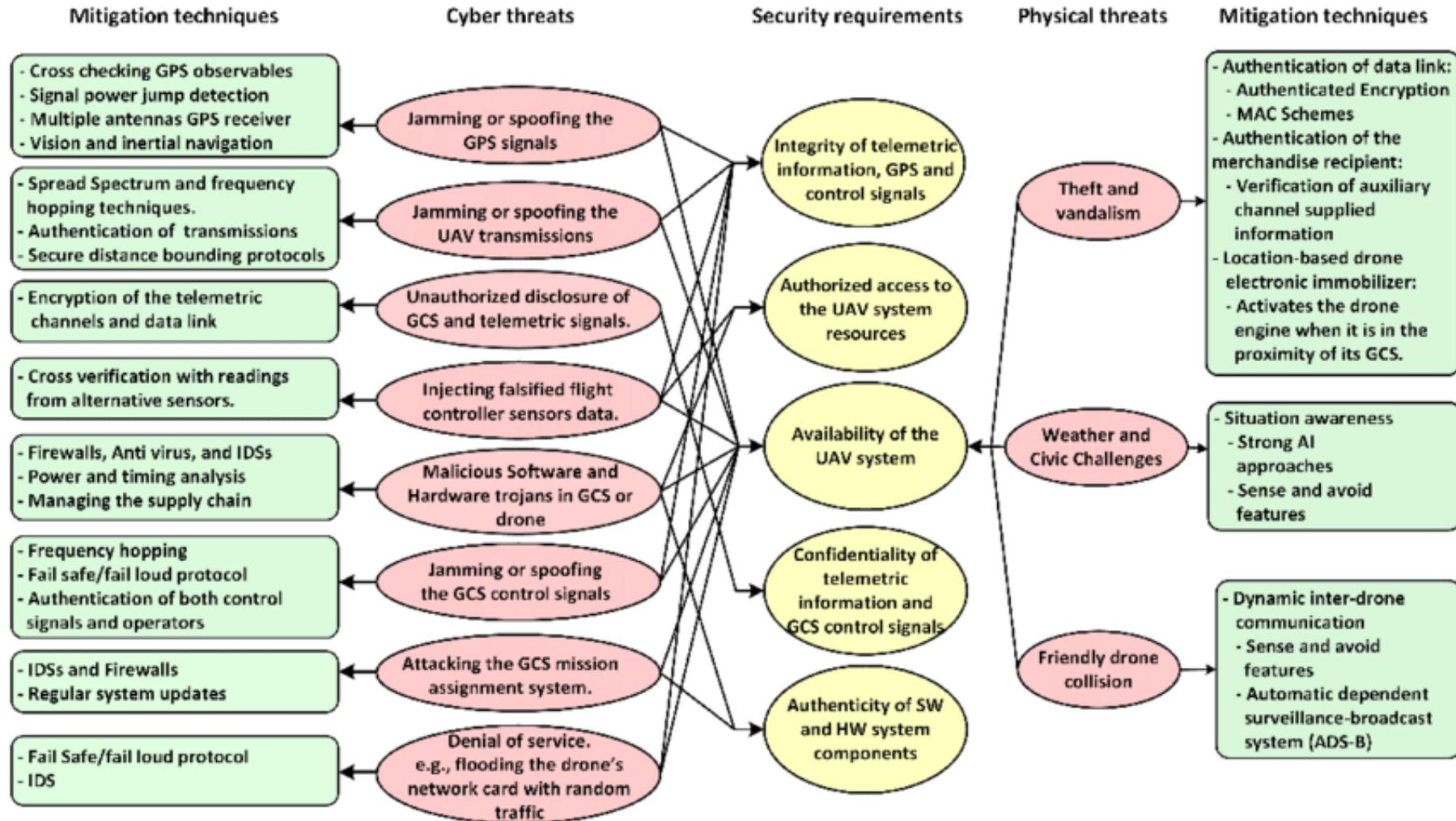


Guerre des robots - Destruction d'un robot terrestre Russe par un drone

FPV Ukrainien : <https://www.youtube.com/watch?v=SfuohNkB5y4>



Typologie des attaques contre les drones



Le défi de cybersécurité pour l'IA

CHATGPT, DES MENACES POUR L'ENTREPRISE

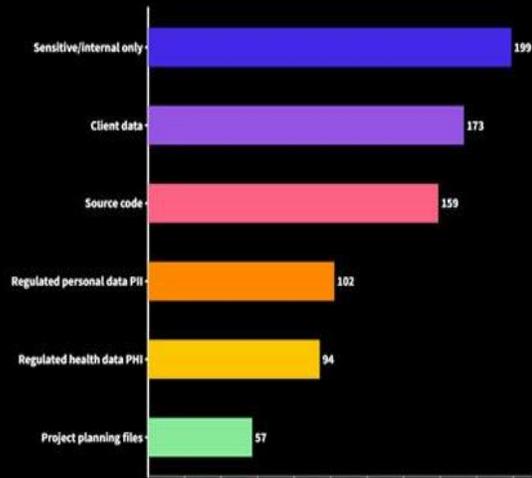
LE « SECRET DES AFFAIRES »

LES « DONNÉES SENSIBLES »

How much sensitive data goes to ChatGPT

(Incidents per 100,000 employees the week of February 26 - March 4)

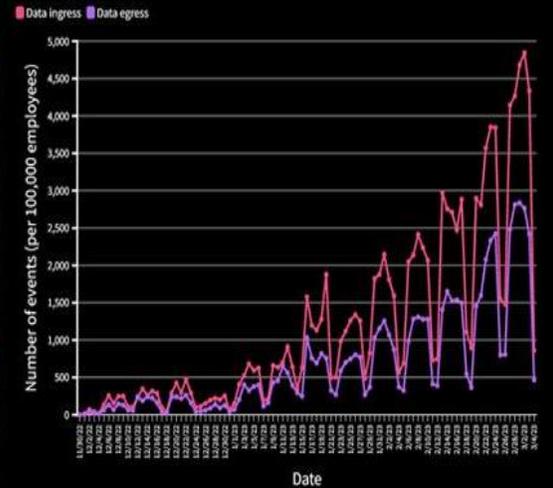
Source: Cyberhaven.com



Usage of ChatGPT in the workplace

(Data ingress and egress events per 100,000 employees)

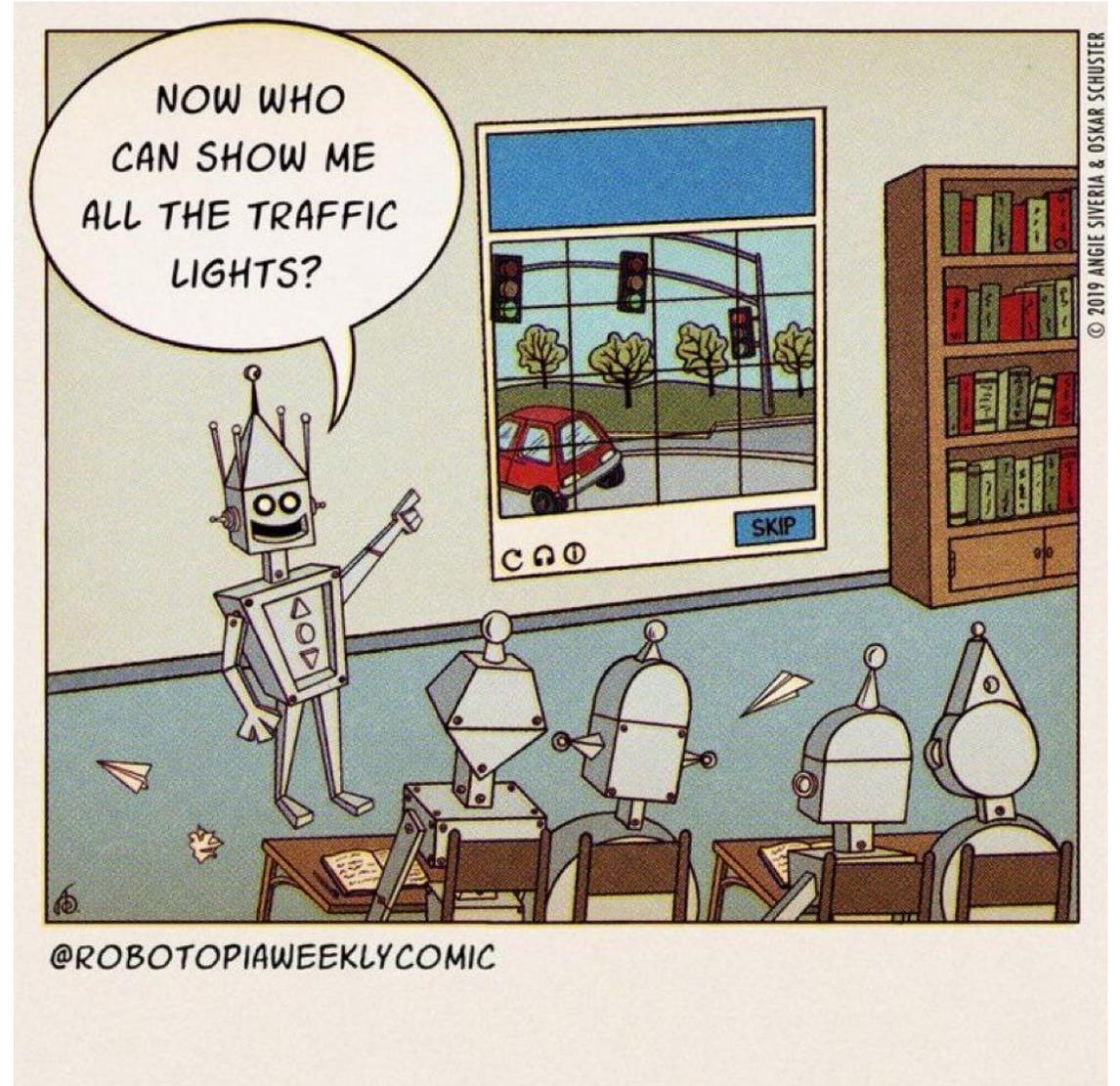
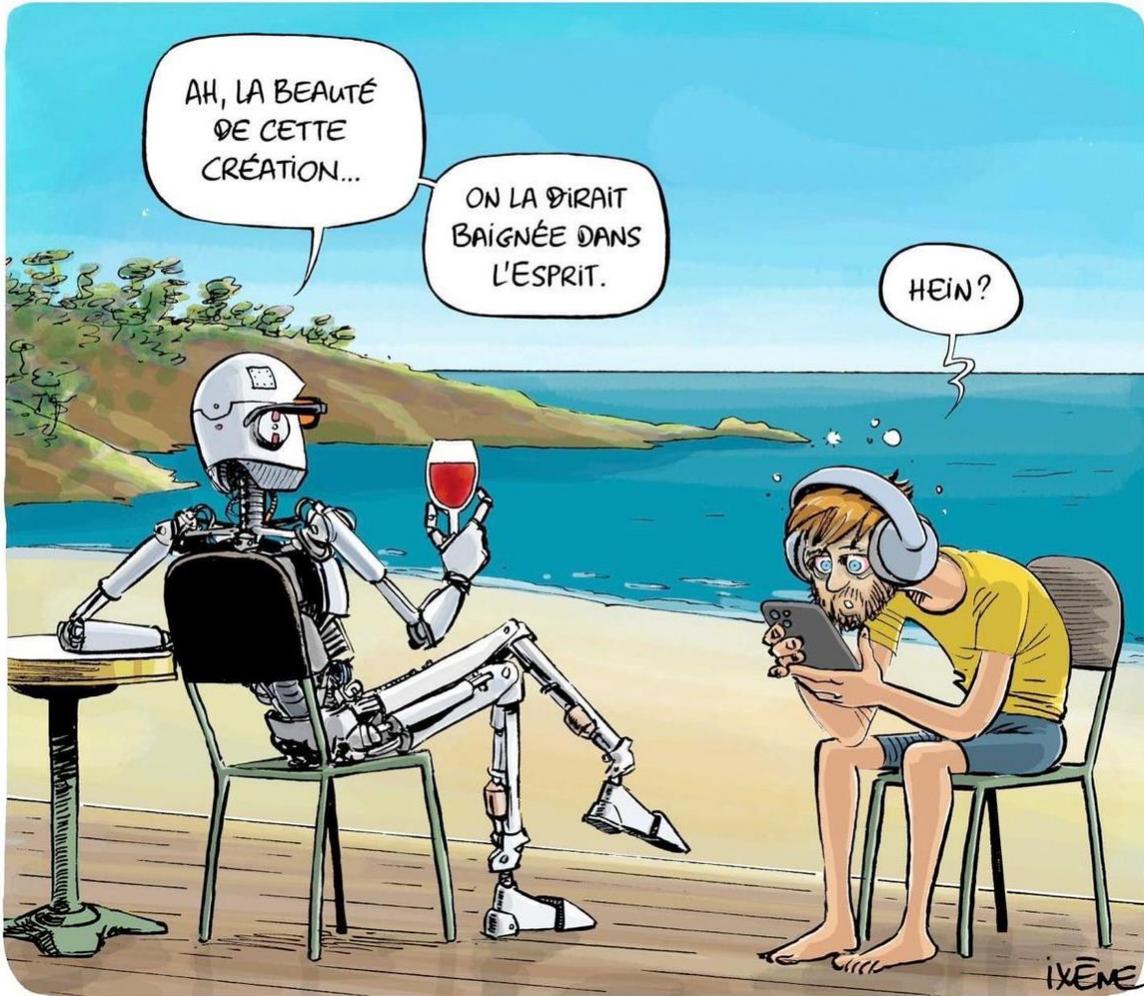
Source: Cyberhaven.com



francoisehalper.fr



DOÏT-ON ENCADRER LE DÉVELOPPEMENT DE L'I.A.?



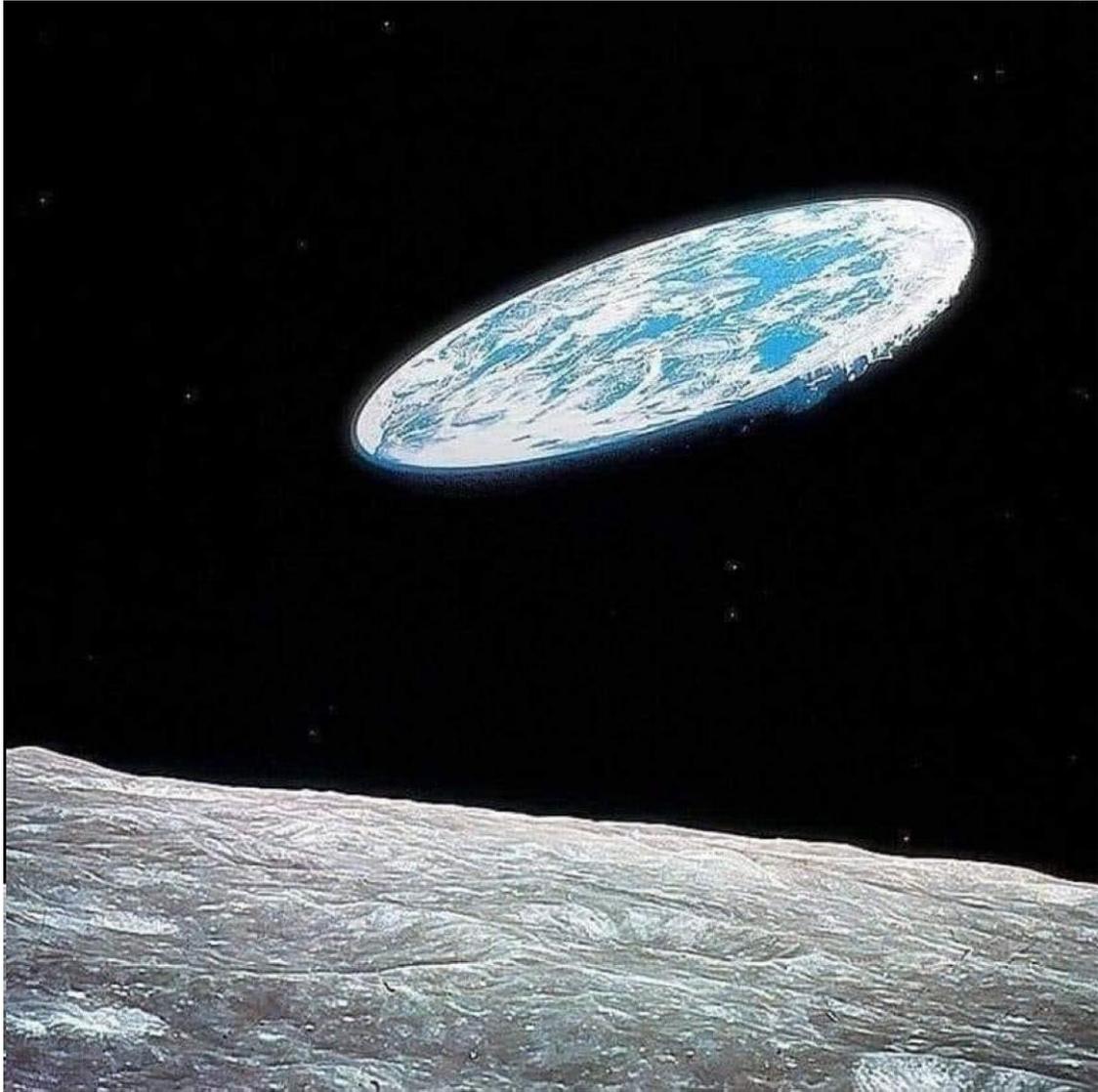
A nos côtés, dans nos maisons, des systèmes robotisés dotés de capteurs, générateurs de données privées en continu.

Quelles sont les garanties de « Privacy » fournies par les constructeurs face à ces générateurs de données privées ? Doit-on leur faire confiance ?

LG CLOi GuideBot



- **takes selfies**
- **sends emails**
- **scans boarding passes**



MERCI

Thierry Berthier

<https://www.linkedin.com/in/thierry-berthier-6143bb6a/>