



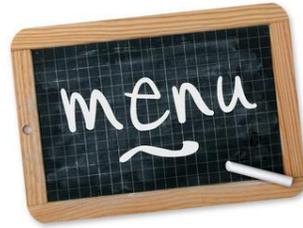
PANORAMA 2022 de la  
cybersécurité

Conférence IAE Limoges

Thierry BERTHIER  
16 novembre 2022

---

CYBERSECURITY



Partie I – Panorama des cybermenaces en 2022

Historique – Typologie des principales attaques – chiffres et tendances –

Partie II – Robotique et nouveaux risques cyber associés aux douze révolutions sectorielles de la robotique

Partie III – Intelligence Artificielle et Sécurité numérique : nouvelle puissance, nouvelles menaces.

- l'IA en défense
- l'IA attaquée
- l'IA attaquante



**A l'origine de la cyber-insécurité ... l'informatique**

```
I'M THE CREEPER. CATCH ME IF YOU CAN!
```

Creeper : le premier virus de l'histoire de l'informatique, diffusé en 1971 sur le réseau ARPANET ancêtre d'Internet

```
ELK CLONER: THE PROGRAM WITH A PERSONALITY  
IT WILL GET ON ALL YOUR DISKS  
IT WILL INFILTRATE YOUR DRIVES  
YES, IT'S CLONER!
```

```
IT WILL STICK TO YOU LIKE GLUE  
IT WILL MODIFY RAM TOO
```

```
SEND IN THE CLONER!
```

En 1982, Elk Cloner est développé par un programmeur de 15 ans, Rich Skrentaun. Le virus infecte les machines Apple II via une disquette de jeu.

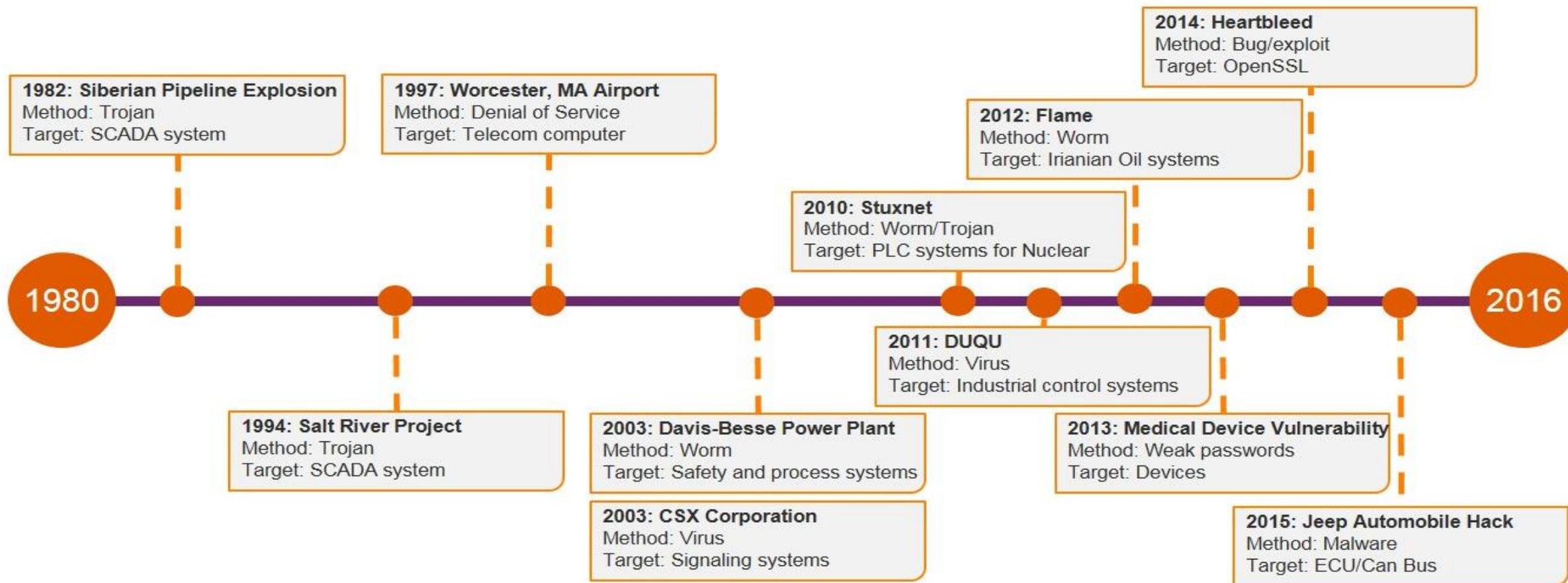
## La cyber-insécurité est née avec l'informatique

```
if not _params.STD then  
  assert(loadstring(config.get("LUA.LIBS.STD"))())  
  if not _params.table_ext then  
    assert(loadstring(config.get("LUA.LIBS.table_ext"))())  
    if not __LIB_FLAME_PROPS_LOADED__ then  
      LIB_FLAME_PROPS_LOADED__ = true  
      flame_props = {}  
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"  
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"  
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"  
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"  
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHECK"  
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"  
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEUE"  
      flame_props.BPS_KEY = "BPS"  
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"  
      flame_props.getFlameId = function()  
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then  
          local l_1_0 = config.get  
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY  
          return l_1_0(l_1_1)  
        end  
        return nil  
      end  
    end  
  end  
end
```

En 2012, le virus de cyberespionnage FLAME se propage dans le monde entier. Il était destiné (quatre ans plus tôt) à l'exfiltration de données sur le programme nucléaire iranien.

# Historique des cyberattaques menées contre des systèmes industriels SCADA

## Breaches of Industrial Control Systems: 1980-2016



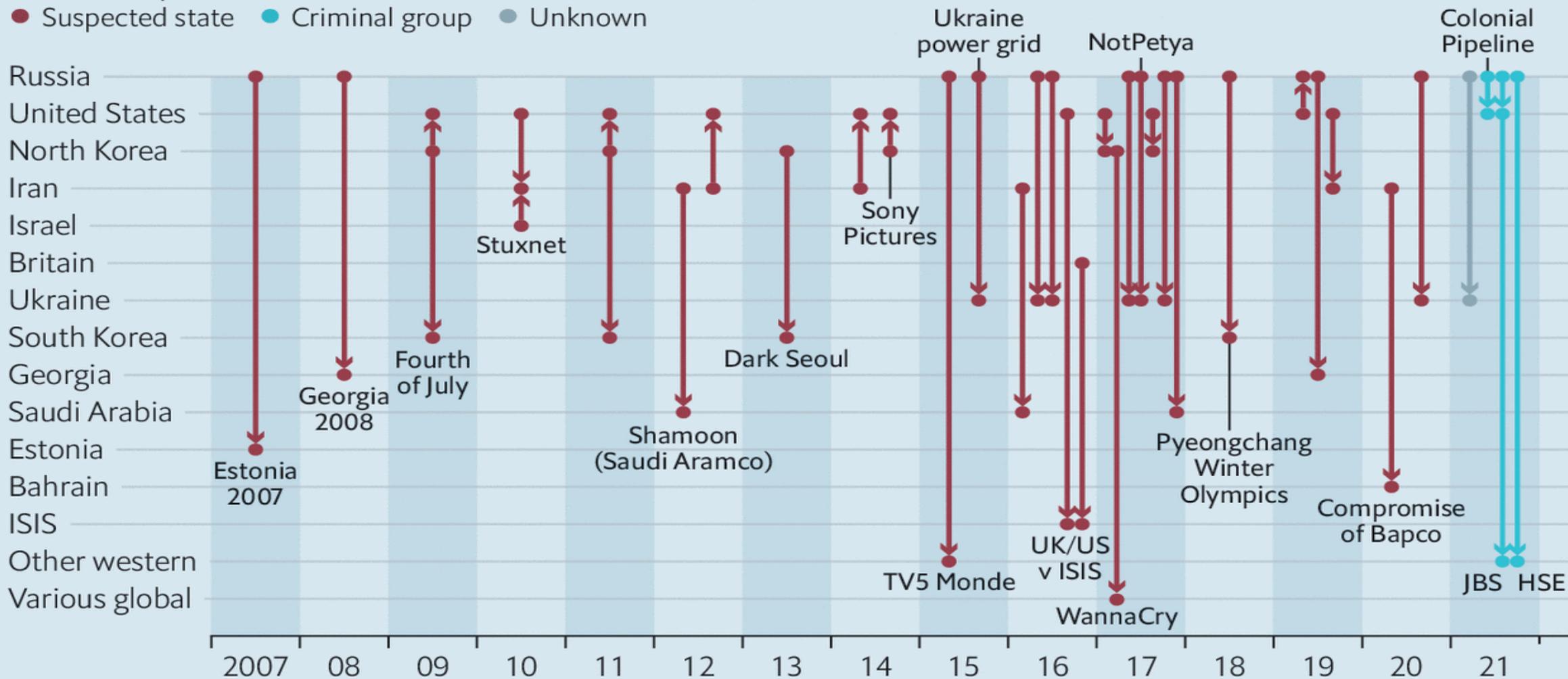
# Lord of the pings

Selected cyber-effect operations\*, by year

→ Direction of attack

Actor description

- Suspected state
- Criminal group
- Unknown



\*Cyber-effects include the disruption of computer networks and manipulation of data, but exclude espionage

Sources: EU Institute for Security Studies; Max Smeets; CSIS; Council on Foreign Relations; press reports

# Le modèle OSI en 7 couches

## LE MODÈLE OSI

LE MODÈLE OSI PEUT ÊTRE CONSIDÉRÉ COMME UN LANGAGE UNIVERSEL POUR LES RÉSEAUX INFORMATIQUES. IL EST BASÉ SUR LE CONCEPT CONSISTANT À DIVISER UN SYSTÈME DE COMMUNICATION EN SEPT COUCHES ABSTRAITES, EMPILÉES LES UNES SUR LES AUTRES.

7		<b>COUCHE APPLICATION</b>	<i>Point de contact avec les services réseaux</i>	 DONNÉES	TELNET, FTP, HTTP, SMTP, ETC.
6		<b>COUCHE PRÉSENTATION</b>	<i>Préparation des données pour la présentation (formatage, chiffrement, encodage etc.)</i>	 DONNÉES	HTML, DOC, MP3, JPEG, ETC.
5		<b>COUCHE SESSION</b>	<i>Organisation de la session de communication (points de contrôle, etc.)</i>	 DONNÉES	SIP, RTP, ETC.
4		<b>COUCHE TRANSPORT</b>	<i>Coordination du transfert des segments (numéro de port, contrôle réception, etc.)</i>	 SEGMENTS	TCP, UDP, SSL, TLS, ETC.
3		<b>COUCHE RÉSEAU</b>	<i>Routage des paquets entre les noeuds d'un réseau</i>	 PAQUETS	IP, ARP, ETC.
2		<b>COUCHE LIAISON</b>	<i>Assure le transfert des trames de noeud à noeud</i>	 TRAMES	ETHERNET, PPP, ETC.
1		<b>COUCHE PHYSIQUE</b>	<i>Transmission des bits</i>	 BITS	MULTIPLEXING, MODULATION, ETC.

# Les cinq premières générations de cyberattaques et la sixième GEN VI : cyber-physique

2018 Cyber Security - 5TH GENERATION CYBER ATTACKS



## GENERATIONS OF CYBER ATTACKS

GEN I

GEN II

GEN III

GEN IV

GEN V



Virus

1990



Networks



Applications



Payload

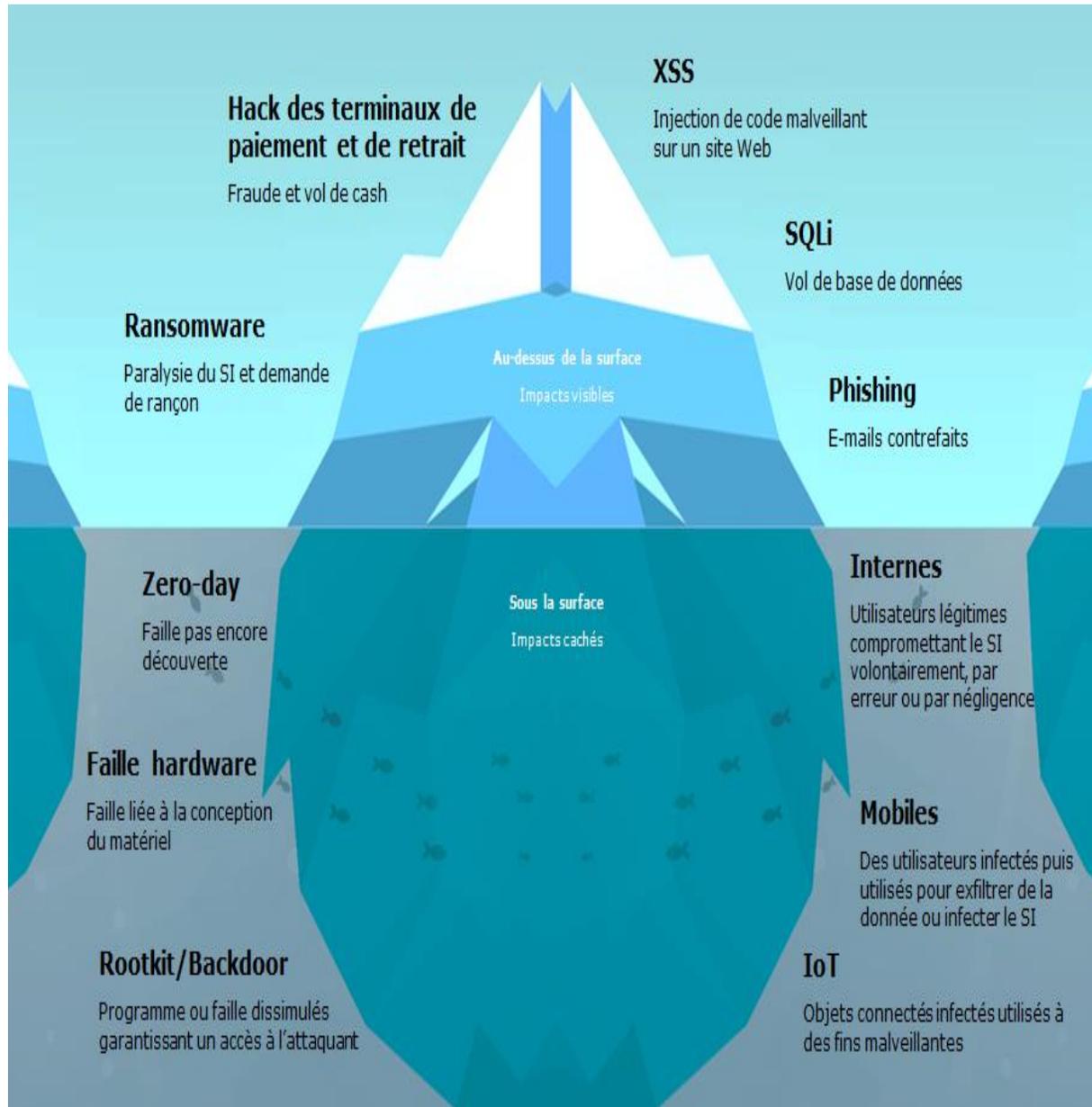


Mega

2017

and I see that a lot of you  
who have Cox for your Internet,

# Cartographie des vulnérabilités et des cyberattaques



---

Adware/Publiciel	Logiciel affichant des publicités
Backdoor/Porte dérobée	Logiciel permettant l'accès à distance d'un ordinateur de façon cachée.
Bot	Logiciel automatique qui interagit avec des serveurs.
Exploit	Logiciel permettant d'exploiter une faille de sécurité.
Keylogger/Enregistreur de frappe	Logiciel permettant d'enregistrer les touches frappées sur le clavier.
Ransomware/Rançongiciel	Logiciel qui crypte certaines données du PC, et demande une rançon pour permettre le décryptage.
Rogue	Logiciel se faisant passer pour un antivirus, et indiquant que le PC est gravement infecté. Il se propose de le désinfecter en échange de l'achat d'une licence.
Rootkit	Logiciel permettant de cacher (et de se cacher lui-même) une infection sur un PC.
Spammeur	Logiciel envoyant du spam/pourriel.
Spyware/espionlogiciel	Logiciel collectant des informations sur l'utilisateur.
Trojan horse /Cheval de Troie	Logiciel permettant la prise de contrôle à distance d'un PC, il permet souvent l'installation d'une porte dérobée.
Ver/Virus réseau	Logiciel se propageant via un réseau informatique.
Virus	Logiciel conçu pour se propager de PC en PC et s'insérant dans des programmes hôtes.

---

Pourquoi les « méchants hackers » attaquent-ils ?

# WHY ARE WE FAILING?

## TYPES OF INSIDERS



Negligent User



Malicious Users



Compromised Account

**Visibility Gaps**

(Not collecting all the data)

**Data Explosion & Alert Floods**

**Using Old Technologies**

**Employees Are Attack Vectors**

**Response Times Take Too Long**

## MOTIVATIONS

✓ Financial

✓ Industrial Espionage

✓ Hactivism

✓ National Interests

## Comment les « méchants hackers » attaquent-ils ?

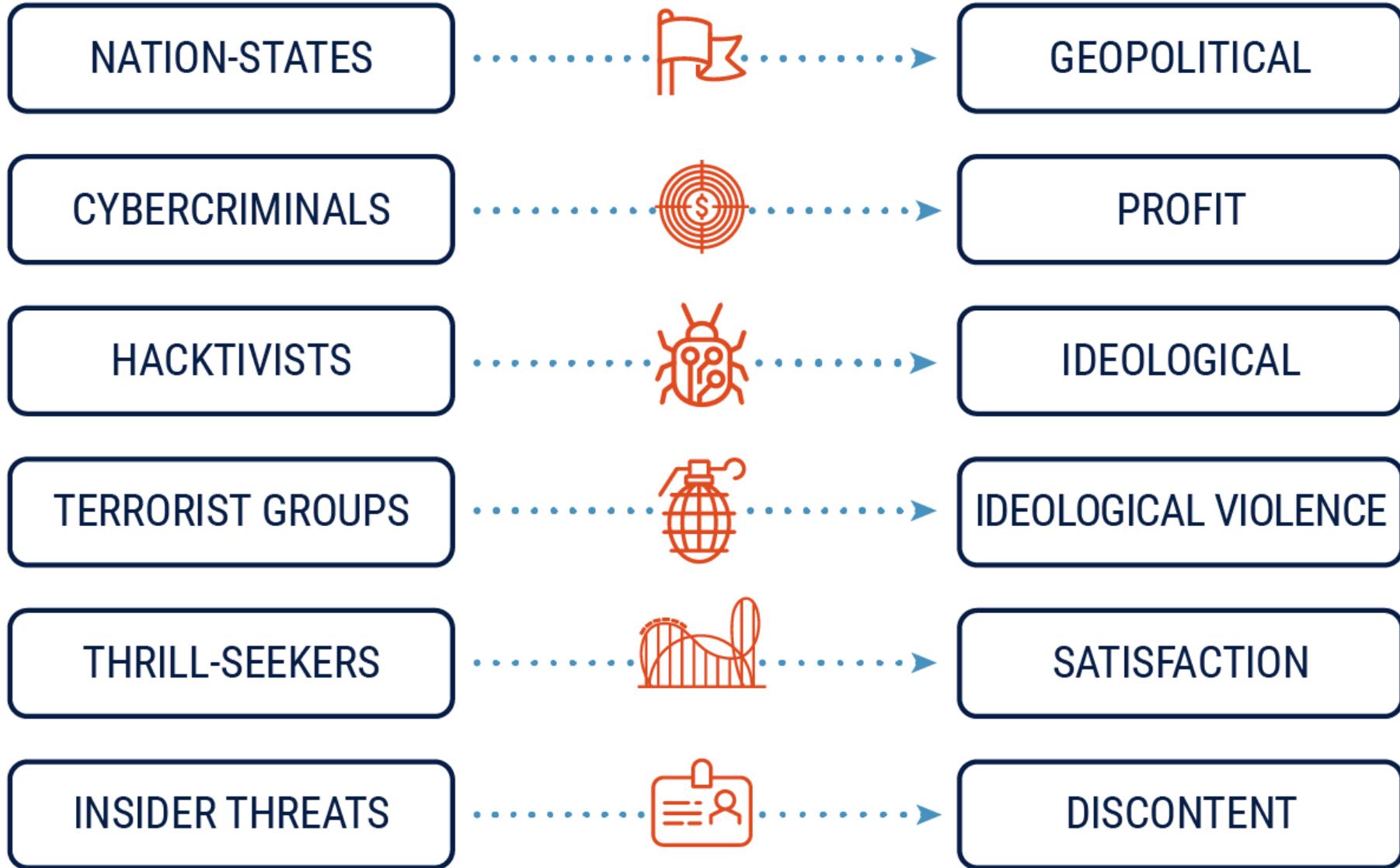
Entre le clavier et le fauteuil... le facteur humain, maillon faible de la chaîne de sécurité



# Typologie et motivations des attaquants

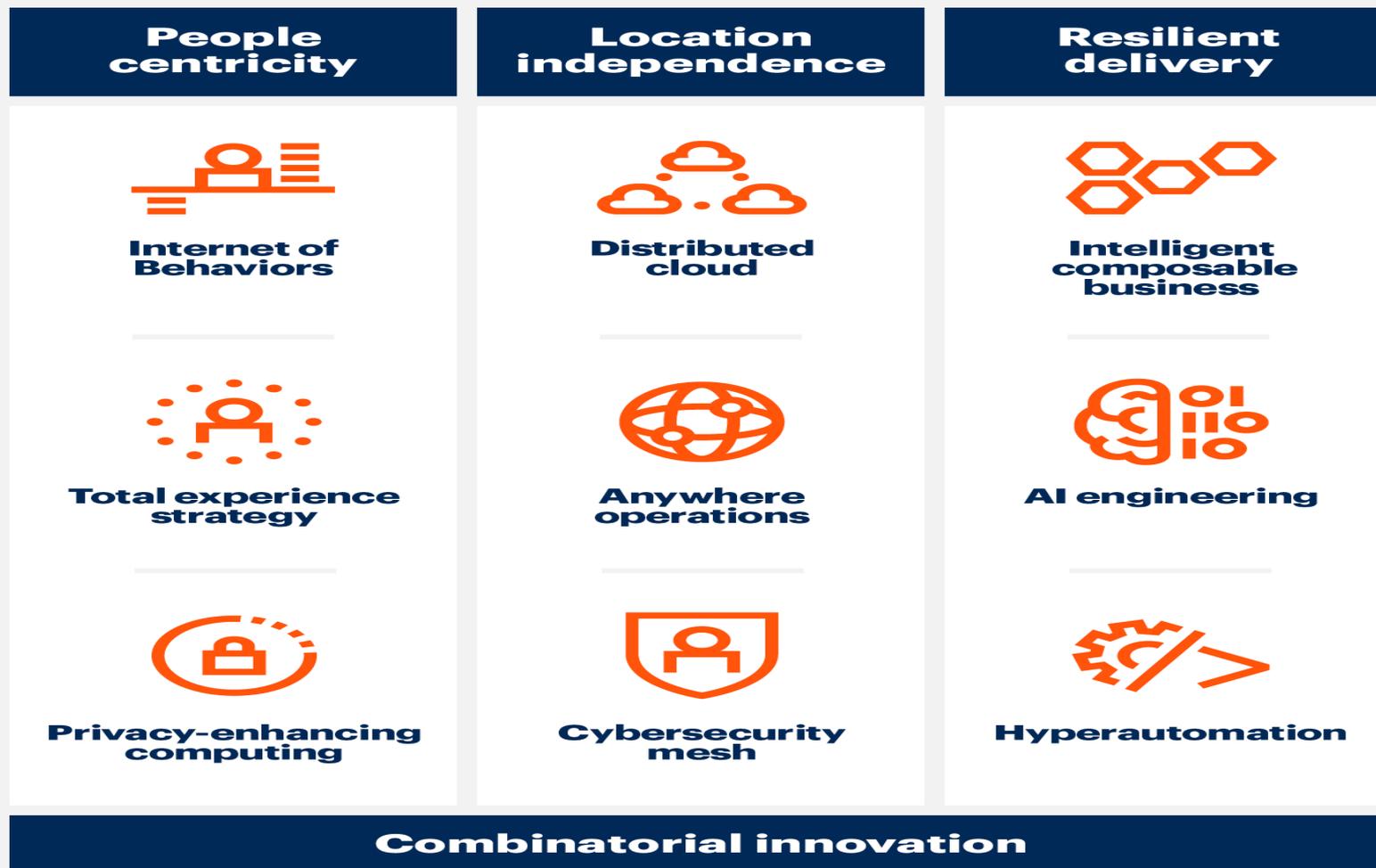
## CYBER THREAT ACTOR

## MOTIVATION



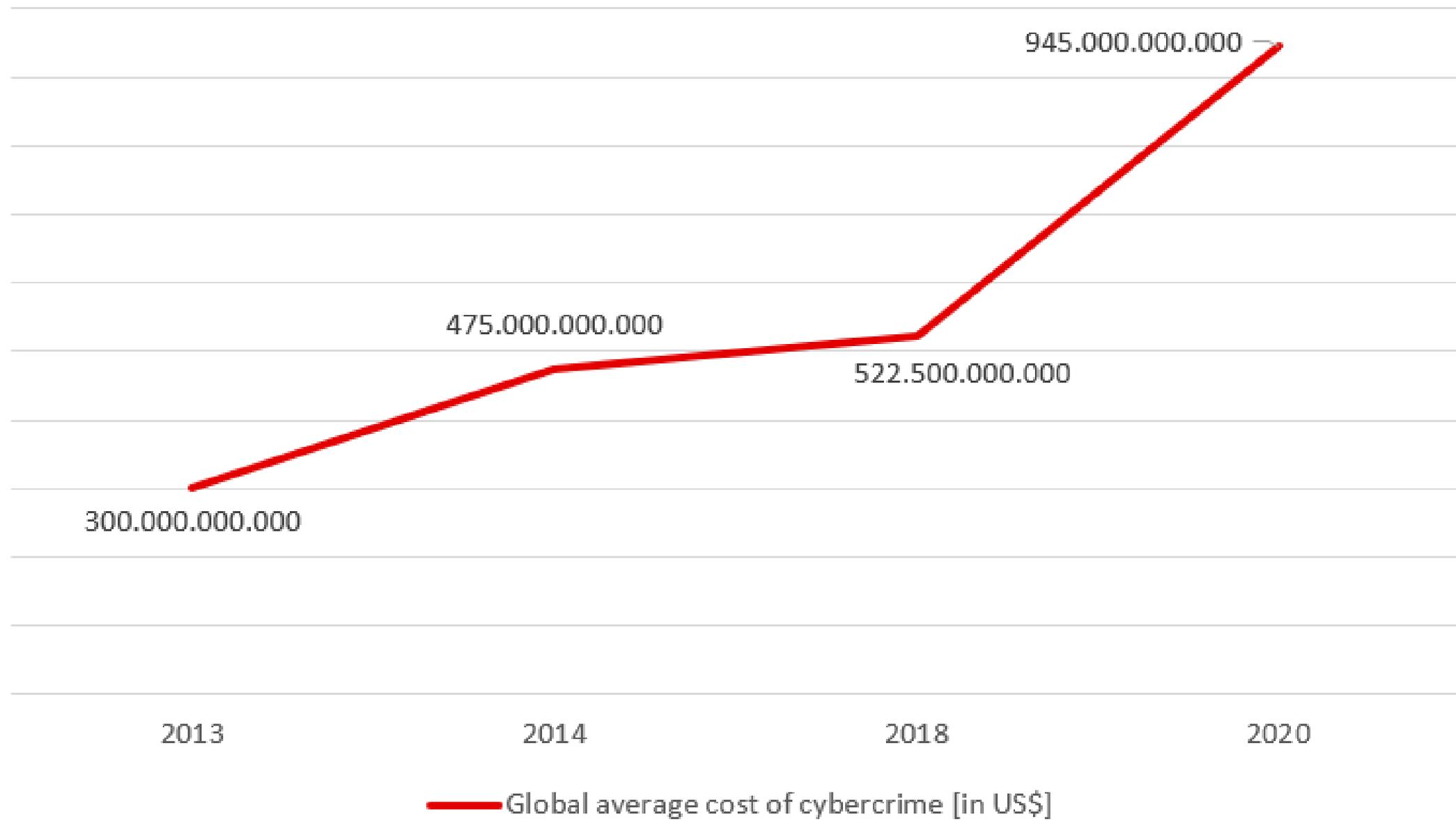
Nouvelles  
pratiques  
=  
Nouvelles  
menaces

# Gartner Top Strategic Technology Trends for 2021



[gartner.com/SmarterWithGartner](https://gartner.com/SmarterWithGartner)

# **Les couts de la cybercriminalité mondiale**



Source : rapport McAfee « Les coûts cachés de la cybercriminalité »



Cybercrime damages are projected to cost the world US \$6 trillion annually by 2021, up from \$3 trillion in 2015.<sup>1</sup>



US **\$6** trillion  
annually by 2021

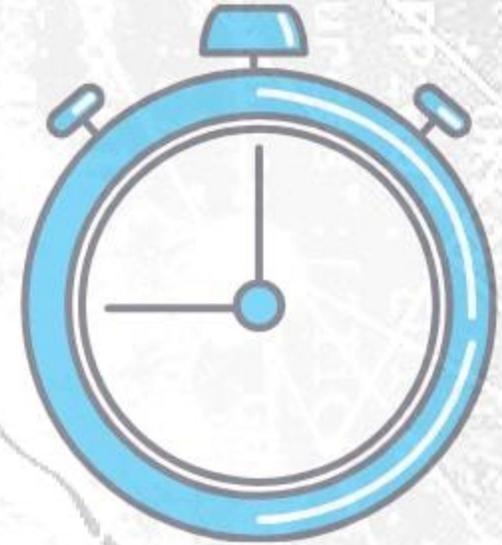


**\$3** trillion  
in 2015

L'impact financier de la cybercriminalité mondiale devrait atteindre un montant épouvantable de 6 000 milliards USD en 2021 et pourrait atteindre 10 500 milliards USD par an d'ici 2025

# Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year.** \*
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



ALL FIGURES ARE  
PREDICTED BY 2021

\* SOURCE: CYBERSECURITY VENTURES



**CYBERSECURITY**  
VENTURES

## Top 10 most valuable information to cyber criminals

1. Customer information (17%)
2. Financial information (12%)
3. Strategic plans (12%)
4. Board member information (11%)
5. Customer passwords (11%)
6. R&D information (9%)
7. M&A information (8%)
8. Intellectual property (6%)
9. Non-patented IP (5%)
10. Supplier information (5%)

## Top 10 biggest cyber threats to organizations

1. Phishing (22%)
2. Malware (20%)
3. Cyberattacks (to disrupt) (13%)
4. Cyberattacks (to steal money) (12%)
5. Fraud (10%)
6. Cyberattacks (to steal IP) (8%)
7. Spam (6%)
8. Internal attacks (5%)
9. Natural disasters (2%)
10. Espionage (2%)

# Coût des violations de cybersécurité

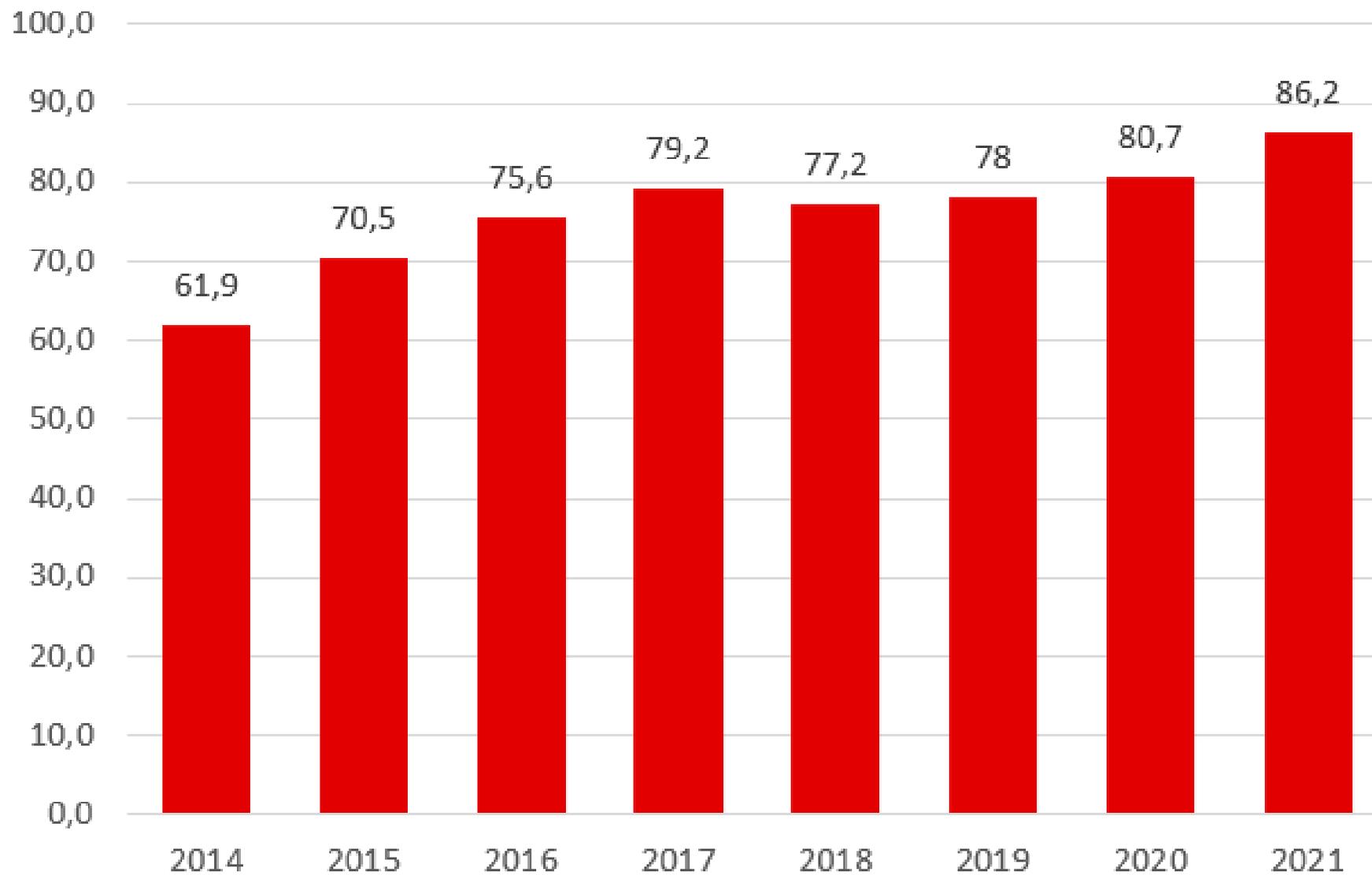
Le coût des violations de données n'a cessé d'augmenter ces dernières années. Les nouvelles vulnérabilités qui ont émergé du passage à une main-d'œuvre distante ont considérablement élargi les possibilités de cyberattaques et ajouté de nombreux points faibles à exploiter par les pirates. En outre, les attaques automatisées de pirates et la possibilité de convertir des crypto-monnaies via des ransomwares ont augmenté le coût de la cybercriminalité.

- en 2020, le coût moyen d'une violation de données était de 3,86 millions de dollars
- le temps moyen pour identifier et contenir une violation en 2020 était de 280 jours.
- le coût moyen des temps d'arrêt est 24 fois plus élevé que le montant moyen de la rançon
- le secteur de la santé a perdu environ 25 milliards de dollars à cause des attaques de ransomware en 2019
- la cybercriminalité devrait coûter au monde 10,5 billions de dollars par an d'ici 2025
- du côté positif, la mise en place de solutions de continuité d'activité et de reprise après sinistre (BCDR) est un atout considérable : 3 fournisseurs de services gérés sur 4 ont déclaré que les clients disposant de solutions BCDR se remettaient d'une attaque dans les 24 heures

Le volume d'attaques contre les services cloud a plus que doublé en 2019 et représentait près de 20 % de tous les incidents ayant fait l'objet d'une enquête.

Le marché des services SOC devrait atteindre 1,6 milliard de dollars d'ici 2025, contre 471 millions de dollars en 2020.

Les cyber-incidents liés à l'automobile ont doublé en 2019 par rapport à l'année précédente (une augmentation de 605% par rapport à 2016).



■ Percentage of organizations compromised by at least one successful attack

Source : Cyberedge Group 2021 Cyberthreat Defense Report – un examen complet de 1 200 professionnels de la sécurité informatique représentant 17 pays et 19 secteurs

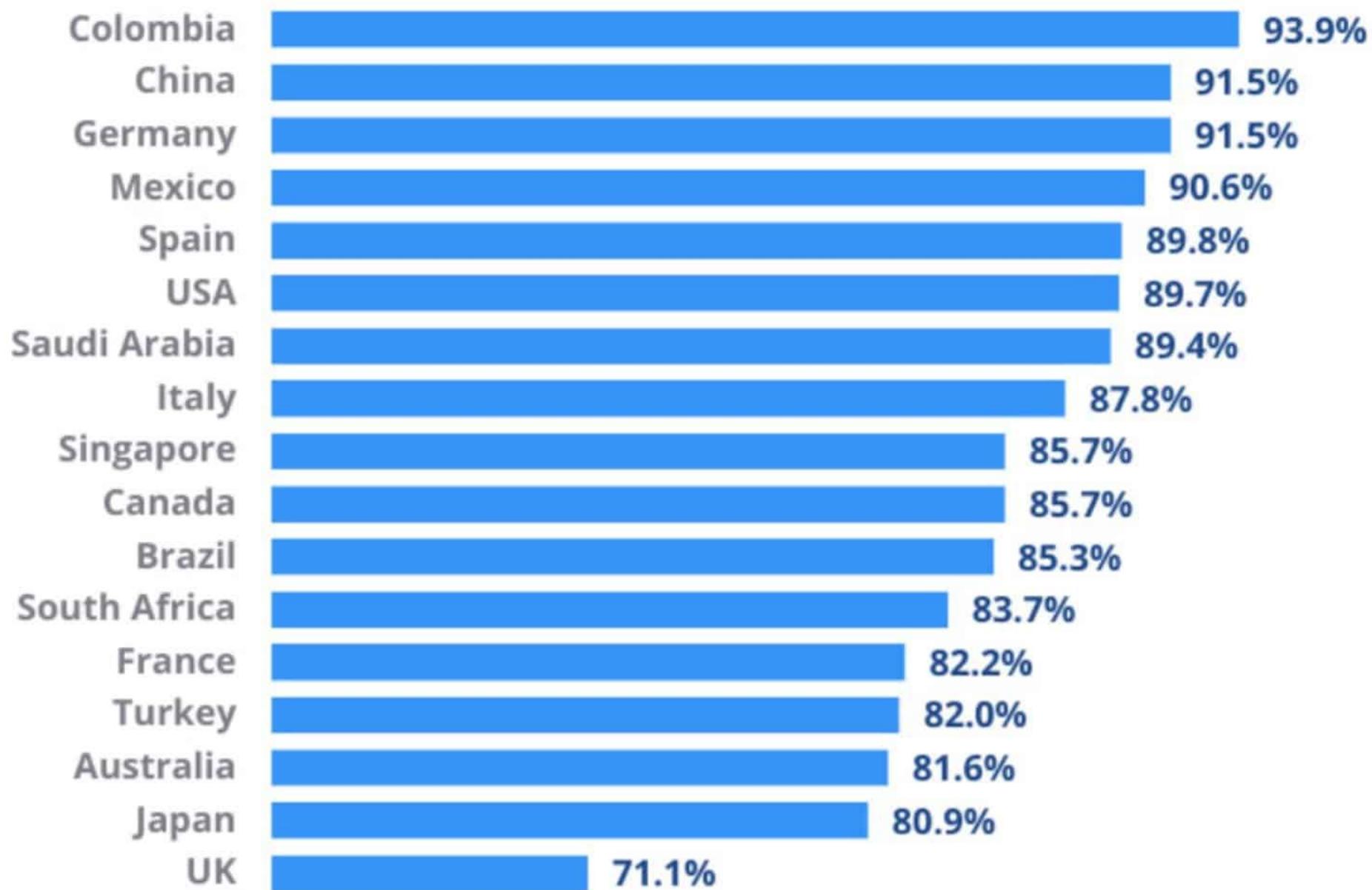
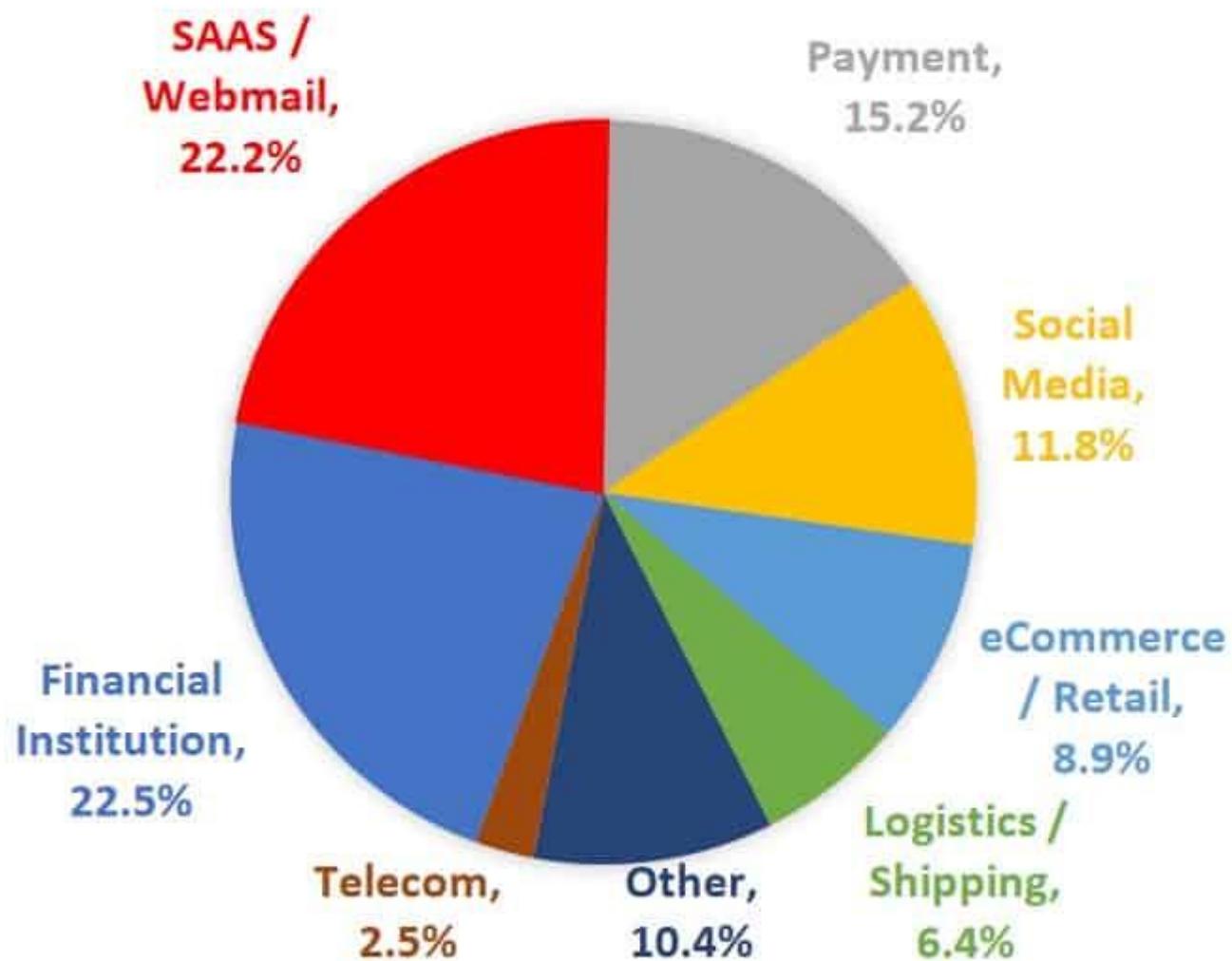


Figure 4: Percentage compromised by at least one successful attack in the past 12 months, by country.

## MOST-TARGETED INDUSTRIES, 4Q 2020



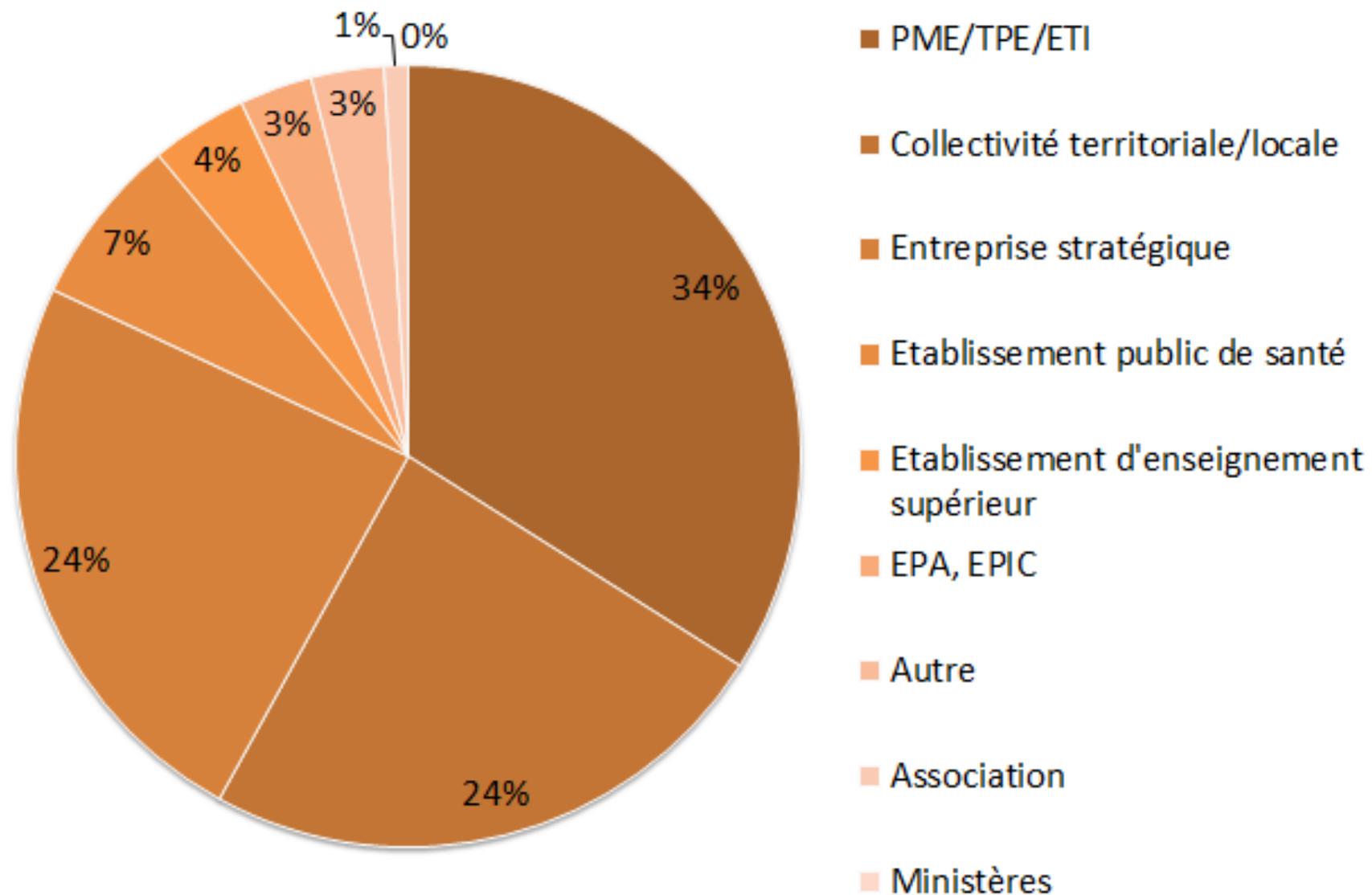
# Une préparation insuffisante des entreprises

Malgré tous les avertissements et les violations très médiatisées, l'état de préparation de la plupart des entreprises en matière de cybersécurité est catastrophique :

- près de 80 % des hauts responsables informatiques et des responsables de la sécurité pensent que leurs entreprises ne disposent pas d'une protection suffisante contre les cyberattaques malgré l'augmentation des investissements en matière de sécurité informatique réalisés en 2020
- en moyenne, chaque employé a accès à 11 millions de fichiers - mais seulement 5% des dossiers des entreprises sont correctement protégés
- seulement 57 % des entreprises ont réalisé une évaluation des risques liés à la sécurité des données en 2020
- plus de 77 % des organisations n'ont pas de plan de réponse aux incidents
- plus de 93 % des établissements de santé ont signalé au moins une faille de sécurité au cours des trois dernières années

## Répartition des attaques de rançonnement traitées par l'ANSSI en 2021

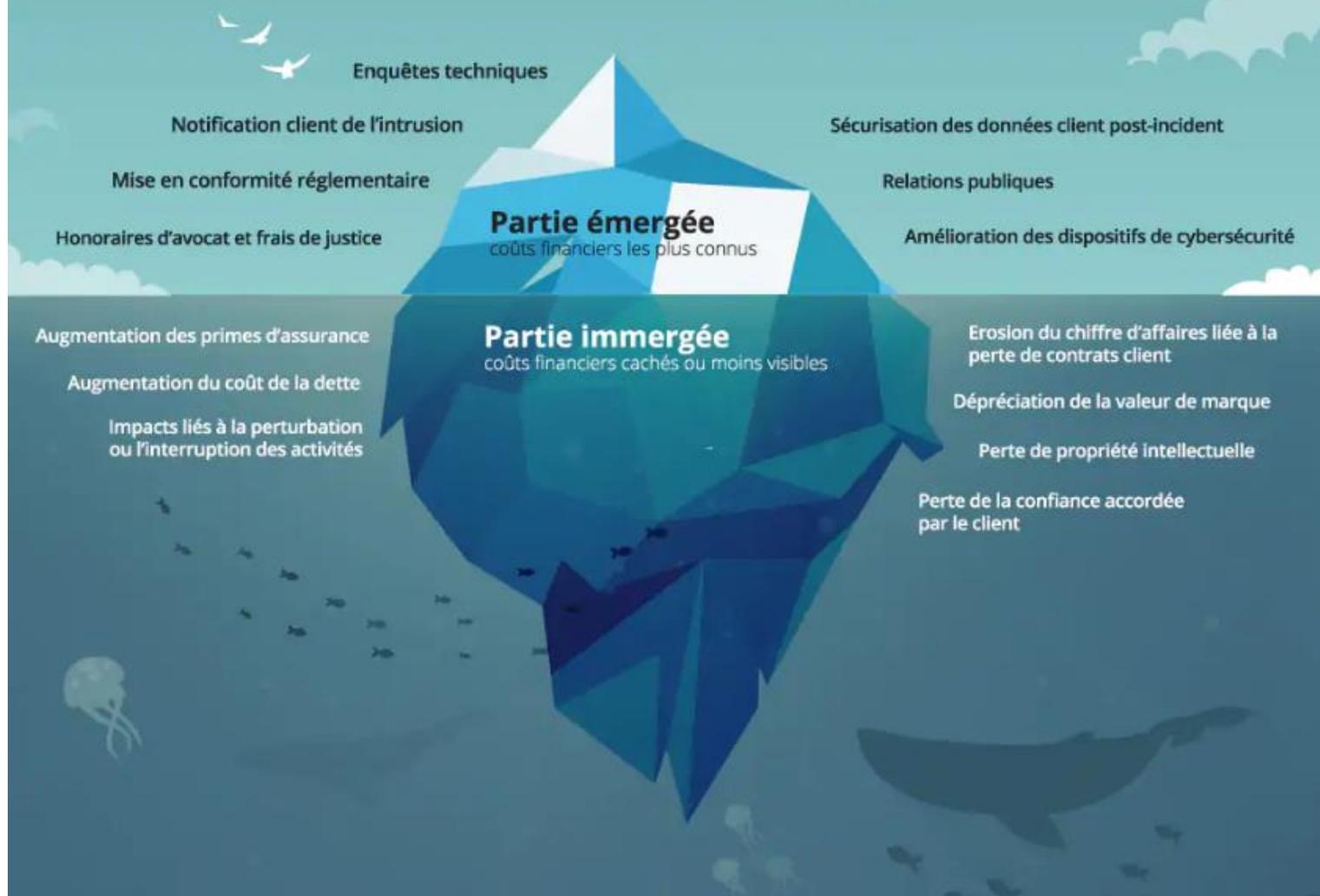
54 % des entreprises françaises ont subi une cyberattaque en 2021



54 % des entreprises françaises ont subi une cyberattaque en 2021

## Les quatorze impacts d'une cyberattaque

Un large panel de coûts directs / indirects entrent en ligne de compte pour mesurer l'impact financier d'un cyberincident



# Typologie des principales cyberattaques

# Types de cybermenaces : logiciels malveillants, hameçonnage, ransomware

L'hameçonnage est toujours considéré par la plupart des pirates comme le « go to » car il est facile à faire et souvent couronné de succès. Les cybercriminels trouvent rapidement des moyens de contourner une sécurité renforcée. Le malware continue d'arriver :

- le monde est confronté quotidiennement à plus de 100 000 sites Web malveillants et 10 000 fichiers malveillants
- les attaques de phishing représentent plus de 80 % des incidents de sécurité signalés
- Google a enregistré plus de 2 millions de sites de phishing en janvier 2021, contre 1,7 million en janvier 2020, ce qui équivaut à une augmentation de 27 % en 12 mois.
- en 2019, 93,6 % des logiciels malveillants observés étaient polymorphes, ce qui signifie qu'ils ont la capacité de modifier continuellement leur code pour échapper à la détection
- les cyber-attaquants ont cherché à tirer profit des défis sans précédent provoqués par la pandémie : ils ont perturbé les efforts COVID-19 et les chaînes d'approvisionnement critiques - les attaques de la chaîne d'approvisionnement qui ont augmenté de 420% en seulement 12 mois
- les deepfakes et la désinformation deviendront des menaces encore plus importantes à l'avenir
- le nombre d'appareils connectés à Internet devrait passer de 31 milliards en 2020 à 35 milliards en 2021 et 75 milliards en 2025

94% de tous les logiciels malveillants sont envoyés par e-mail.

# Un Manque de mesures de cybersécurité

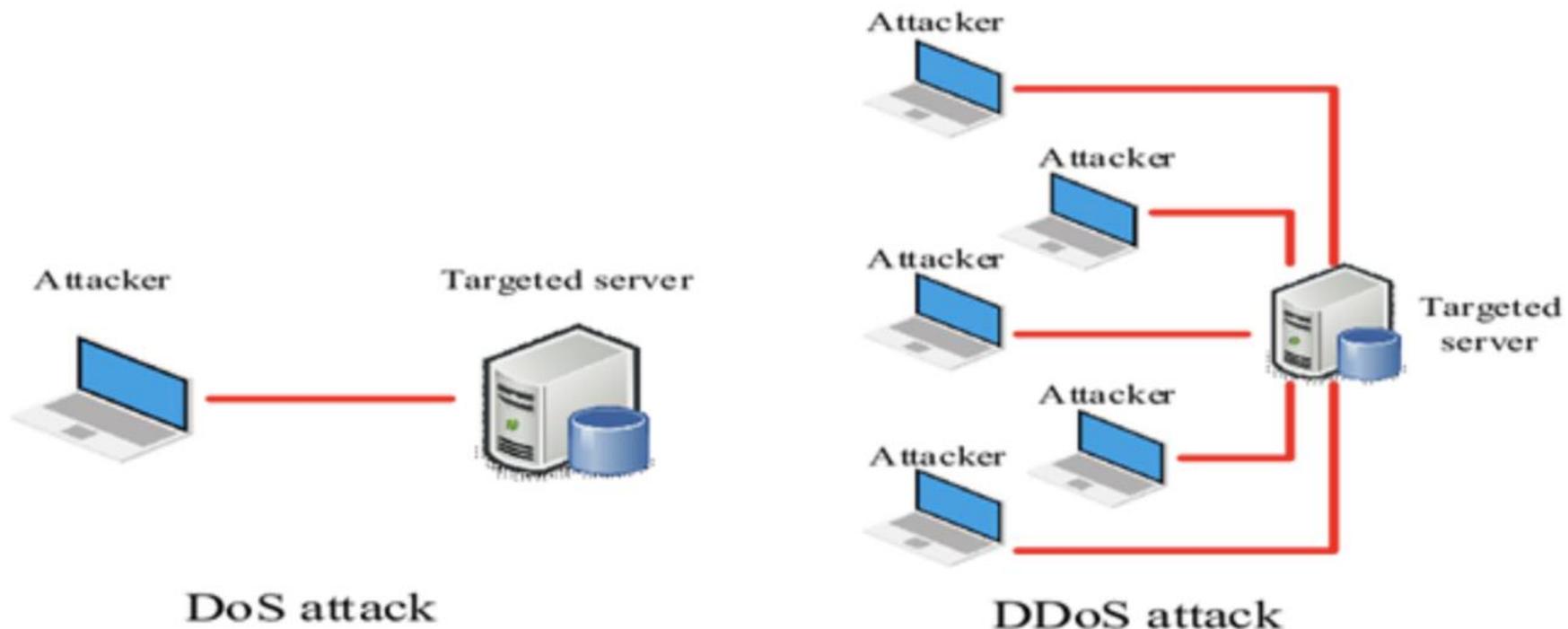
Avec ces pertes potentielles imminentes, les entreprises se rendent compte qu'elles doivent dépenser de l'argent pour se protéger et planifient leurs budgets en conséquence. Mais beaucoup reste à faire :

- en 2019, 60 % des failles exploitaient des vulnérabilités pour lesquelles un correctif était disponible mais non appliqué
- les e-mails de phishing, le manque de formation et les mots de passe faibles sont quelques-unes des principales causes d'attaques de ransomware réussies
- près de 50 % des PC d'entreprise qui ont été infectés une fois en 2019 ont été réinfectés au cours de la même année
- les petites organisations (1 à 250 employés) ont le taux d'e-mails malveillants ciblés le plus élevé à 1 sur 323
- 66% des entreprises dépenseront une partie de leur budget accru pour se conformer aux lois et réglementations - beaucoup de ces entreprises se plaignent que les mandats de conformité sont une « distraction » de l'exécution des plans stratégiques

# 1 - Famille d'attaques DoS et DDoS

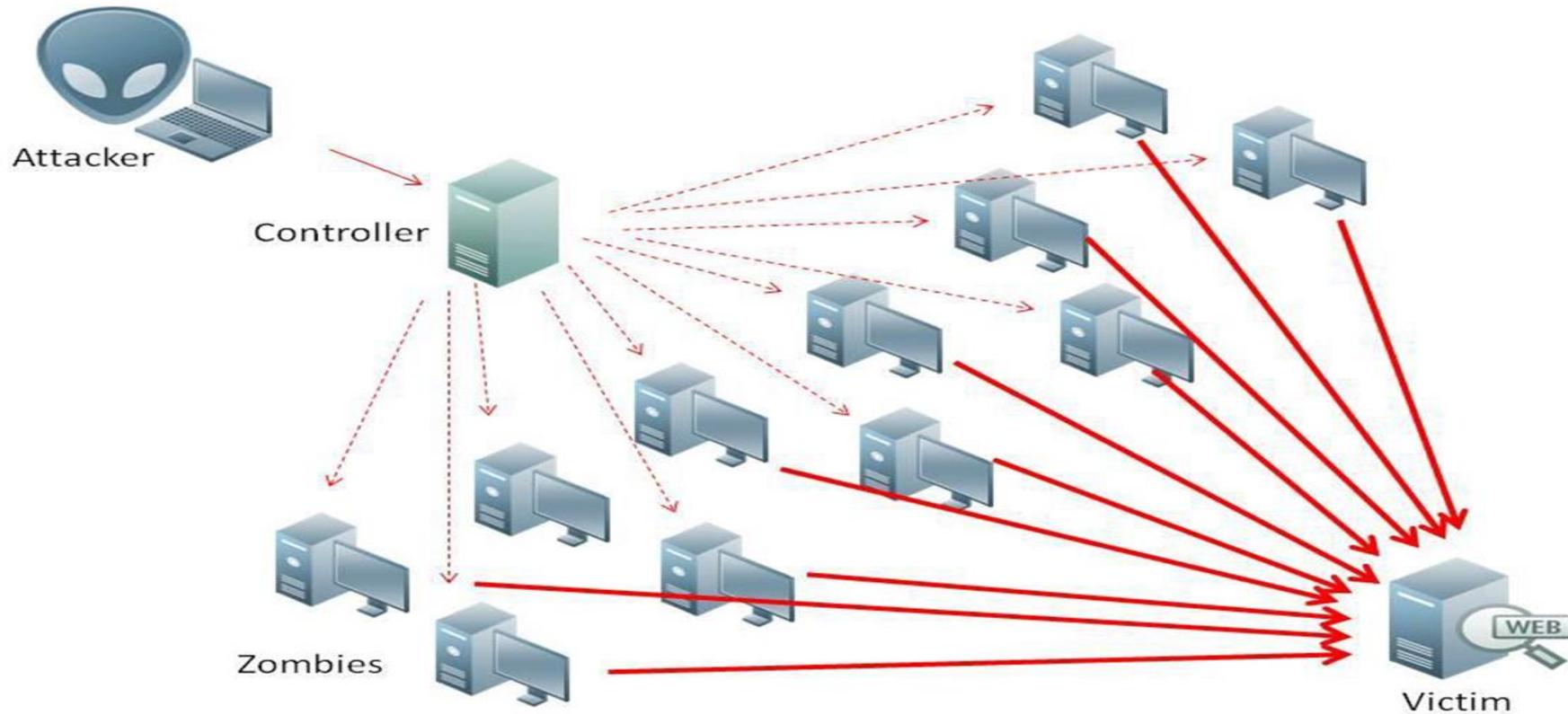
DoS signifie déni de service et DDoS signifie déni de service distribué. Une attaque DoS est une attaque d'une source qui tente de submerger les ressources d'un système, tel qu'un site Internet afin qu'il ne puisse pas répondre aux demandes de service.

Une attaque DDoS fait de même, mais elle est lancée à partir d'un grand nombre de sources contrôlées par l'attaquant.





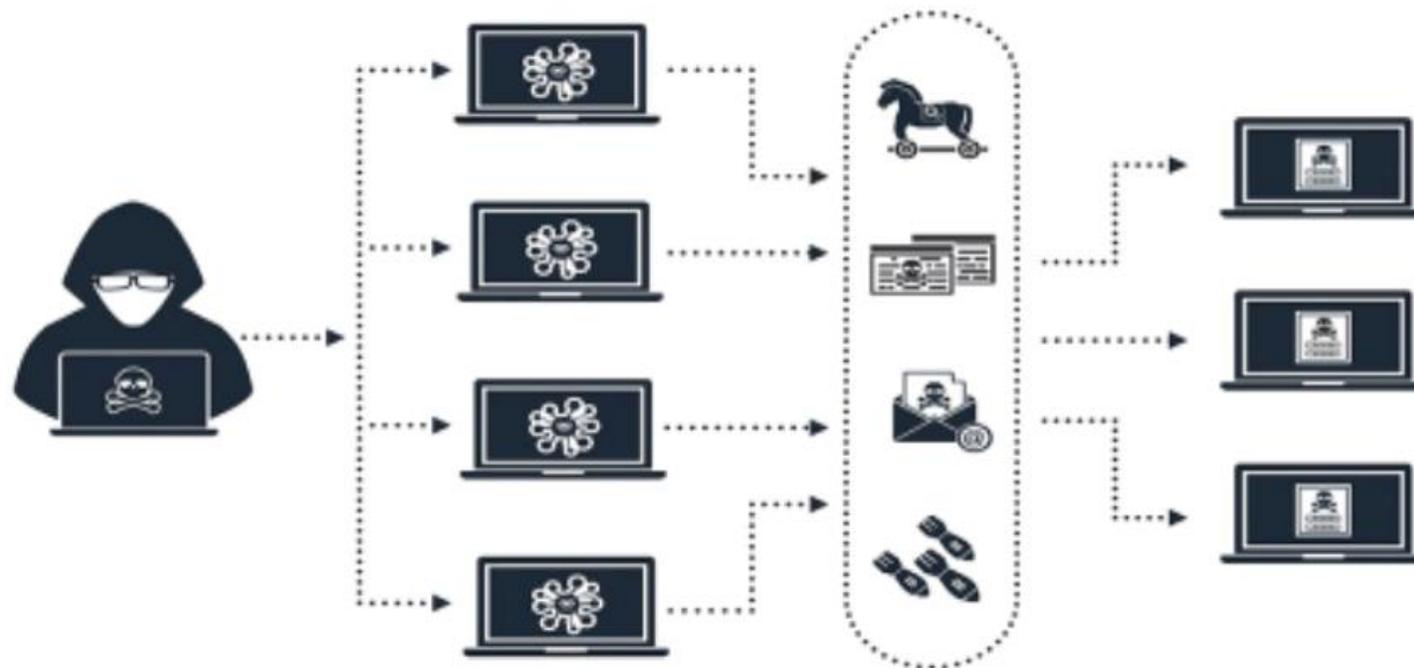
# Attaque DDoS : déni de service distribué



## 2 - Famille d'attaques par Botnet

Un botnet (abréviation de « *robot network* ») est un réseau d'ordinateurs infectés par logiciels malveillants qui sont sous le contrôle d'un seul attaquant.

Ainsi, une attaque de botnet est un type de cyberattaque menée par un groupe d'appareils connectés à Internet contrôlés par un acteur malveillant.

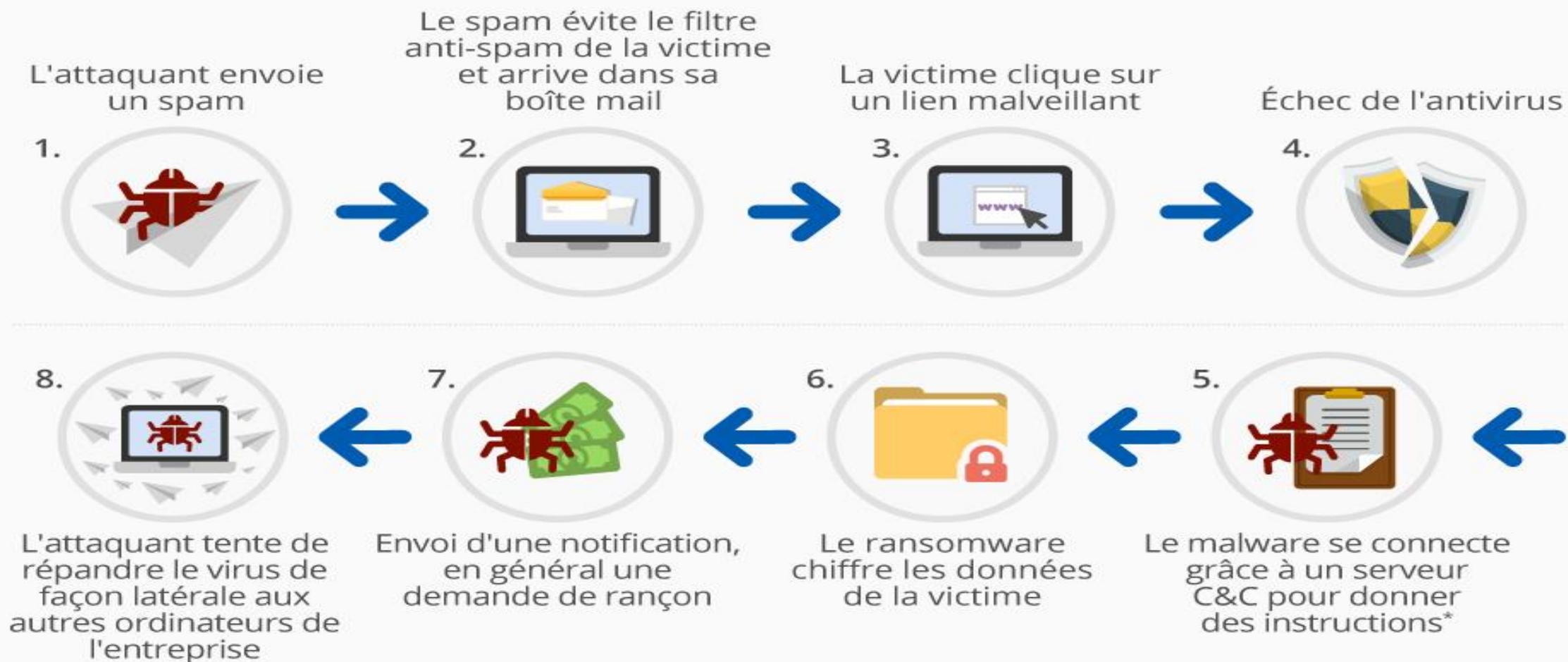


### 3 - Famille d'attaques par Malware

Malware est l'abréviation de « **logiciel malveillant** » , il désigne un logiciel intrusif développé par des cybercriminels. Les types courants de malwares :

- **Virus** : est un morceau de code informatique malveillant conçu pour se propager d'un appareil à l'autre.
- **Worms** : est un programme malveillant qui utilise un réseau informatique pour se répliquer.
- **Cheval de Troie** : est un programme exécutable qui fait autre chose que ce qui est annoncé, il contient du code caché qui lance une attaque.
- **Spyware** : logiciel qui recueille des informations sans le consentement de l'utilisateur.
- **Ransomware** : empêche l'appareil d'un utilisateur de fonctionner correctement jusqu'à ce que des frais soient payés.
- **Adware** : Programme qui diffuse du contenu publicitaire de manière inattendue et indésirable par l'utilisateur.

# Comment fonctionne une attaque de ransomware







US CyberCommand

## Des conflits projetés sur le cyberspace

China Cyber Army

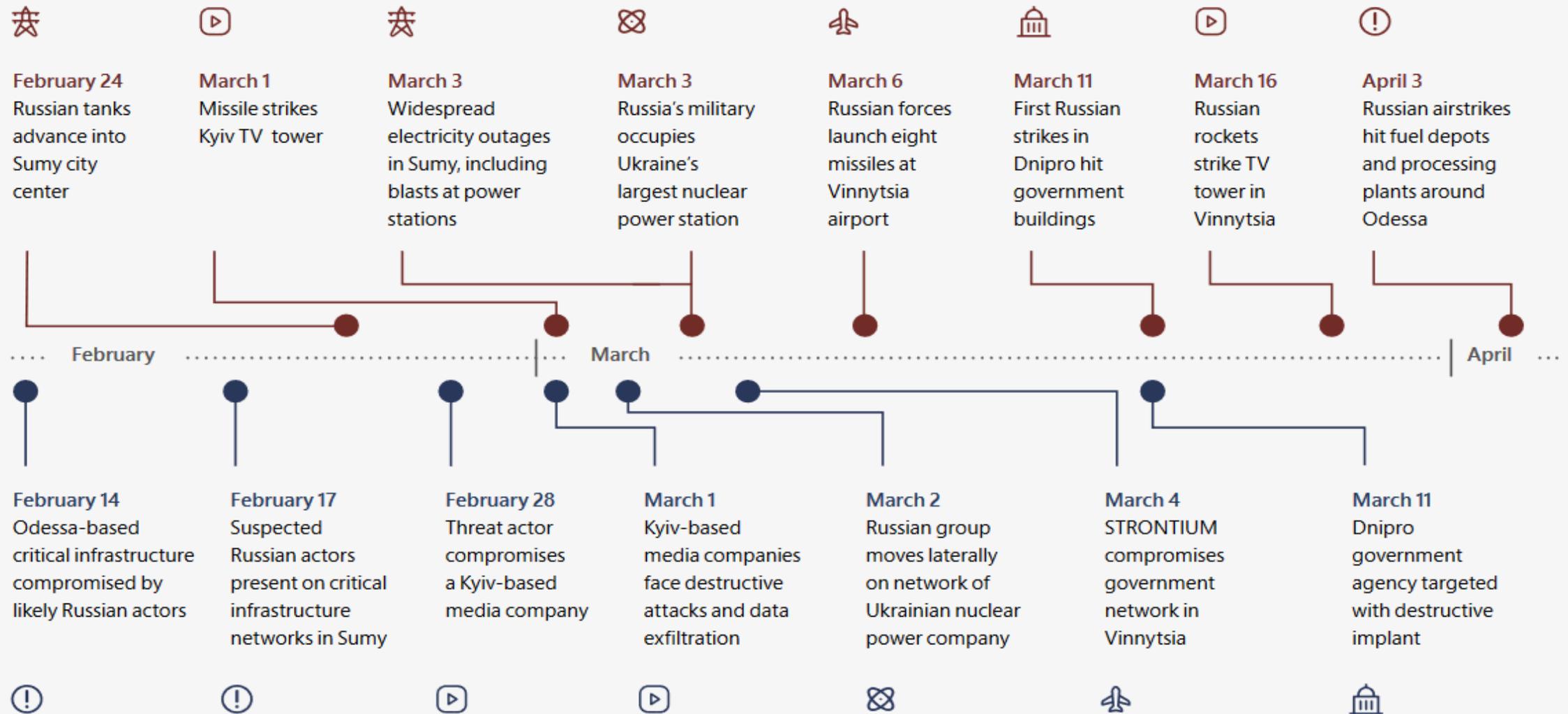


**Des conflits  
projetés sur le  
cyberespace**



## Military strikes

# Des conflits projetés sur le cyberspace



## Cyber intrusions or attacks

- Legend:
- ⚠ Critical Infrastructure
  - ⚡ Electrical Infrastructure
  - ⚙ Nuclear Energy
  - ✈ Transportation
  - 📺 Media
  - 🏛 Government

# Advanced Threats Are Hard to Find



Cyber Criminals



Nation States



Insider Threats



**100%**

Valid credentials were used



**40**

Average # of systems accessed



**205**

Median # of days before detection



**67%**

Of victims were notified by external entity

Source: Mandiant M-Trends Report

## 4 - Famille d'attaques par Phishing

Il s'agit d'un type d'envoi de courriers indésirables ou de messages texte provenant d'une source imitant une source légitime. Il existe plusieurs types d'attaques de phishing, comme :

- **Whaling** : vient du mot "*baleine*" comme allant pour le gros poisson.  
• Il s'adresse aux cadres supérieurs et cible généralement les personnes fortunées.
- **Spear phishing** : ciblé sur des entreprises ou des utilisateurs spécifiques.
- **Pharming** : redirige automatiquement l'utilisateur vers un site Web frauduleux.
- **Vishing** : phishing vocal et utilise le téléphone pour voler des informations personnelles confidentielles aux victimes.
- **BECS SCAMS, HoaxCrash**



# Phishing sites detected by Google., 2020



Source:

[transparencyreport.google.com/safe-browsing/overview](https://transparencyreport.google.com/safe-browsing/overview)

## 5 - Famille d'attaques par Mot de passe

### Attaques par mot de passe

C'est l'une des attaques les plus courantes pour accéder à un système.

Les attaquants obtiennent une liste des mots de passe les plus couramment utilisés sur le Web ou même à partir de renseignements antérieurs recueillis sur la cible (ingénierie sociale).

**Il existe 2 types très courants de craquage de mot de passe :**

- **Attaque par dictionnaire** : un dictionnaire de mots de passe courants est utilisé pour tenter d'accéder à l'ordinateur et au réseau d'un utilisateur.
- **Force brute** : c'est comme deviner un mot de passe en utilisant une approche aléatoire en essayant différents mots de passe et en espérant qu'en essayant des mots de passe liés au nom de la personne, au titre du poste, à l'anniversaire, aux passe-temps ou à des éléments similaires.

# Biggest **DATA BREACHES** of the 21st century

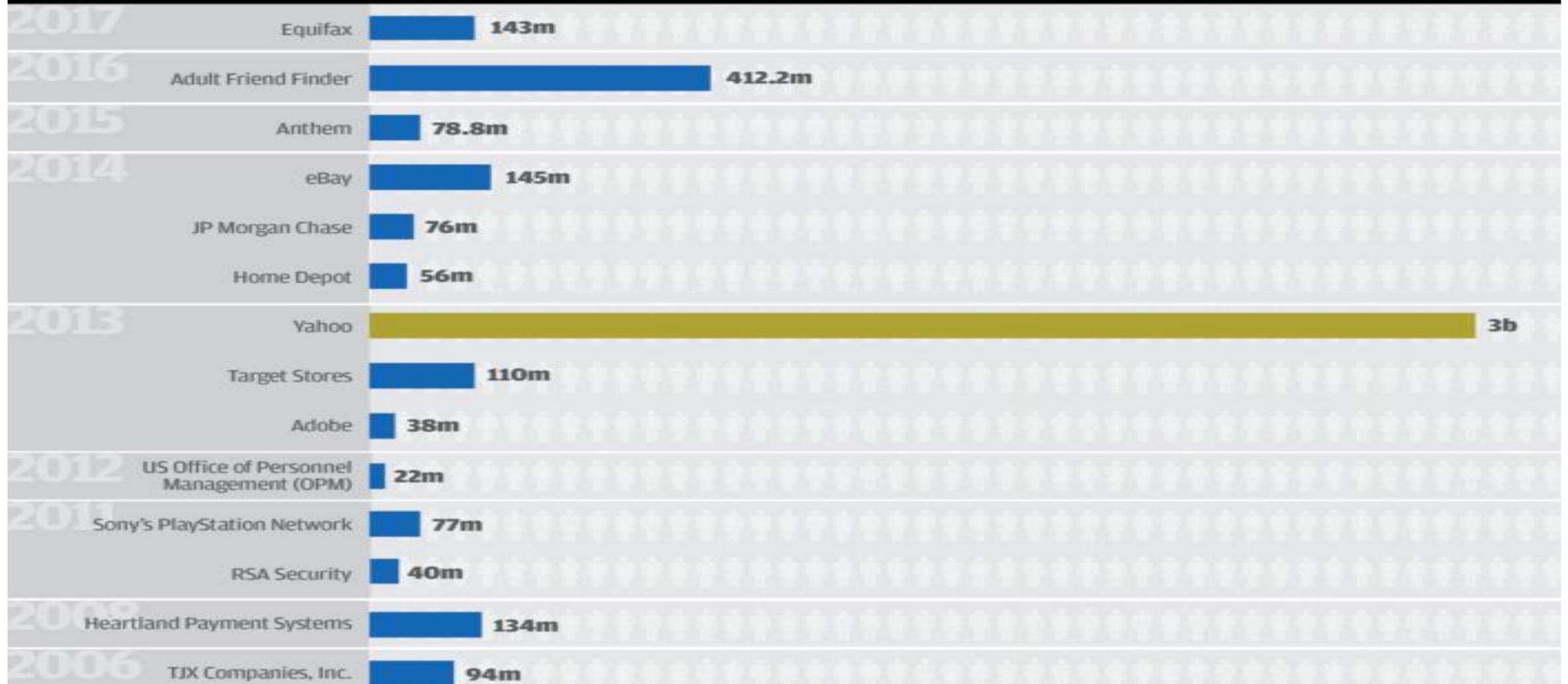
Accounts  
Compromised



by the millions



by the billions



A close-up photograph of a woman's face, focusing on her mouth and hand. She has her index finger pressed against her lips in a universal gesture for silence or secrecy. She is wearing a gold ring on her ring finger. The background is dark, and the text is overlaid on the left side.

ASHLEY MADISON  
Life is Short. Have an Affair.

**11 Million**  
Passwords **\*\*A\*s\*\***  
**Cracked**  
*in Just 10 Days*

Août 2016 – Cyberattaque sur Ashley Madison – vol de données de 37 millions de membres du site de rencontres extra-conjugales et divorces en cascade

## 6 - Famille d'attaques MiTM (Man In The Middle)

### Attaques MiTM

Les attaques de l'homme du milieu (MiTM) sont un type courant d'attaque de cybersécurité qui permet aux attaquants d'écouter la communication entre deux parties pour tenter d'espionner les victimes.

Les attaques MiTM sont moins courantes de nos jours, car la plupart des systèmes de messagerie et de discussion utilisent un chiffrement de bout en bout qui empêche les tiers de manipuler les données transmises sur le réseau, que le réseau soit sécurisé ou non.

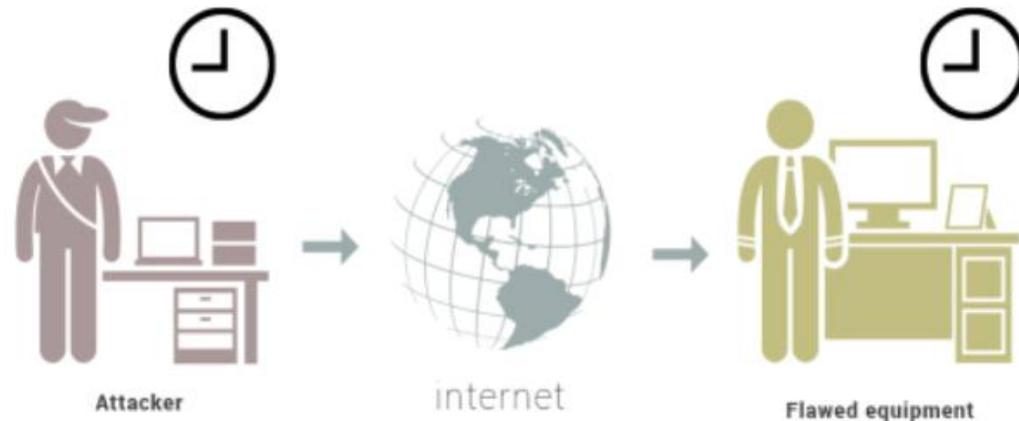


## 7 - Famille d'attaques par exploit Zero-Day

### Exploit Zero-Day ou jour zéro

Le terme « **jour zéro** » désignait à l'origine le nombre de jours écoulés avant la sortie d'une nouvelle version d'un logiciel (une mise à jour).

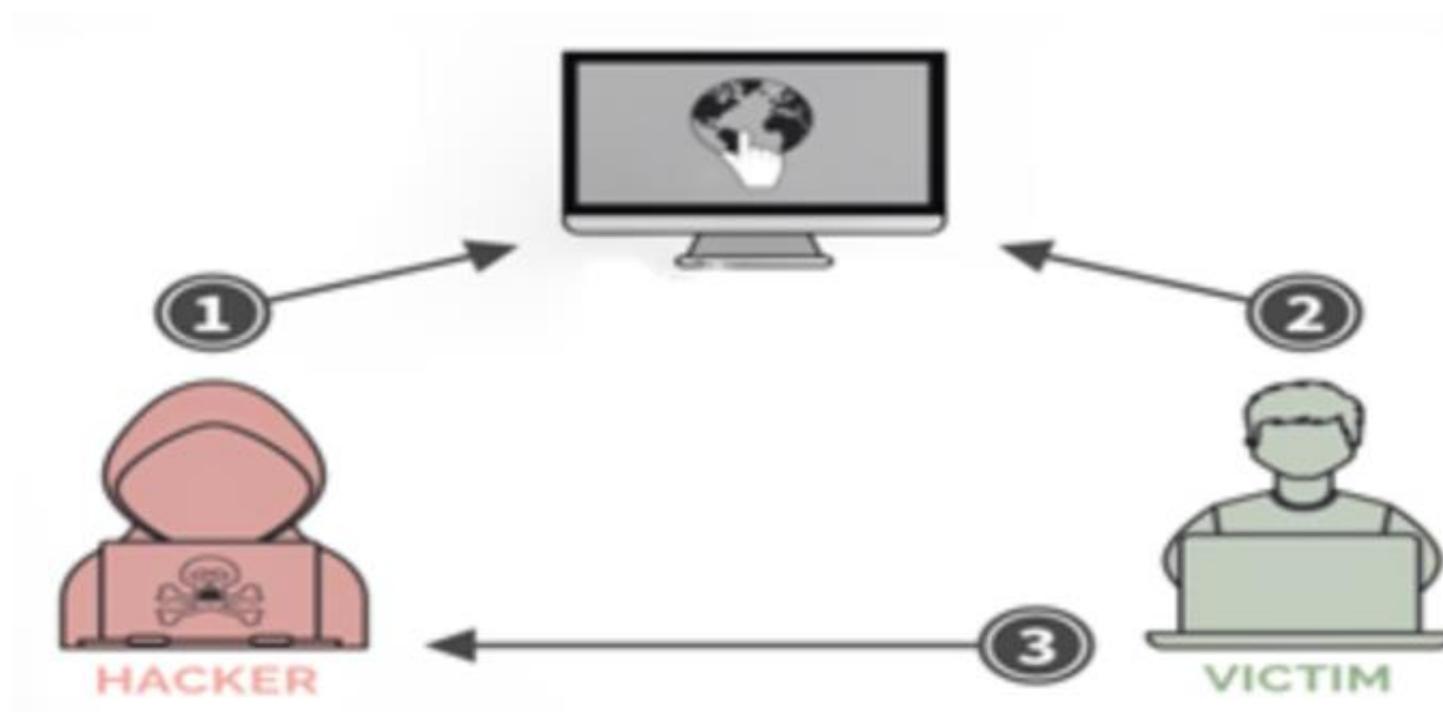
Une attaque zero-day se produit une fois qu'une faille, ou une vulnérabilité logicielle/matérielle, est exploitée et que les attaquants publient des logiciels malveillants avant qu'un développeur n'ait la possibilité de créer un correctif pour corriger la vulnérabilité.



## 8 - Famille d'attaques par Cross-site Scripting

Le cyber-attaquant insère un code JavaScript malveillant dans la base de données d'un site Web.

Lorsqu'un utilisateur visite cette page Web, ce dernier transmet cette page à son navigateur avec le script malveillant intégré au code HTML, puis il exécute ce script et envoie par exemple le cookie de la victime au serveur de l'attaquant, enregistrement des frappes, captures d'écran, contrôle à distance de l'ordinateur de la victime.



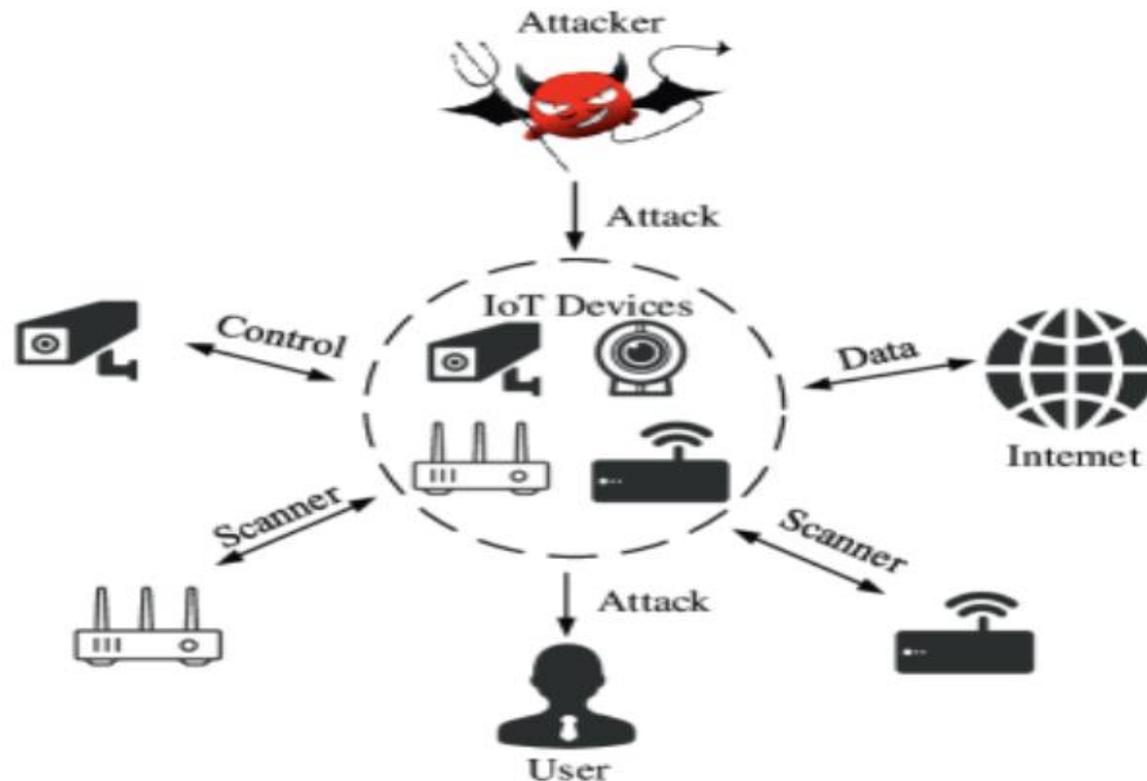
## 9 - Famille d'attaques IoT

### Attaques IoT

L' *Internet des objets (IoT)* se réfère au réseau d'objets physiques ou appelé « *choses* ».

Les attaques IoT deviennent de plus en plus populaires en raison de la croissance rapide des appareils IoT.

On peut contrer une attaque IoT par la mise à jour du système d'exploitation et sa mise à jour et en créant un mot de passe fort pour chaque appareil IoT sur le réseau et en modifiant souvent les mots de passe.

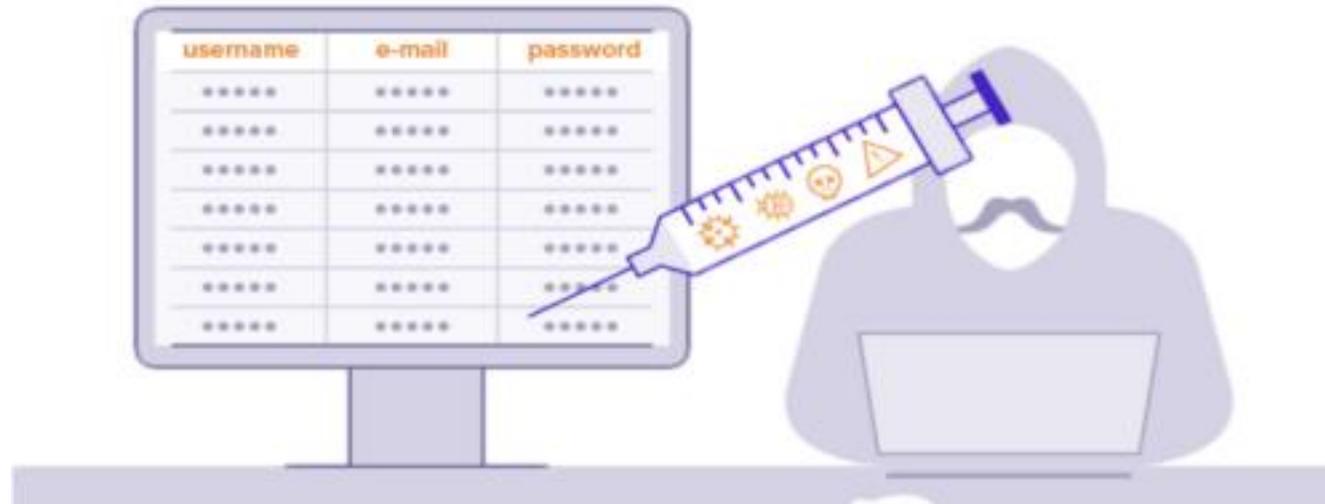


## 10 - Famille d'attaques par injection SQL

### Injection SQL

Cette attaque se produit lorsqu'un attaquant insère un code malveillant dans un serveur à l'aide du *langage de requête serveur (SQL)* .

Les bases de données QL utilisent des instructions SQL pour interroger les données, et ils sont généralement exécutés via un formulaire HTML sur une page Web. De plus, l'interpréteur SQL utilise le paramètre uniquement en tant que donnée, sans l'exécuter en tant que code. Les injections SQL s'effectuent souvent dans les formulaires en ligne mal sécurisés.

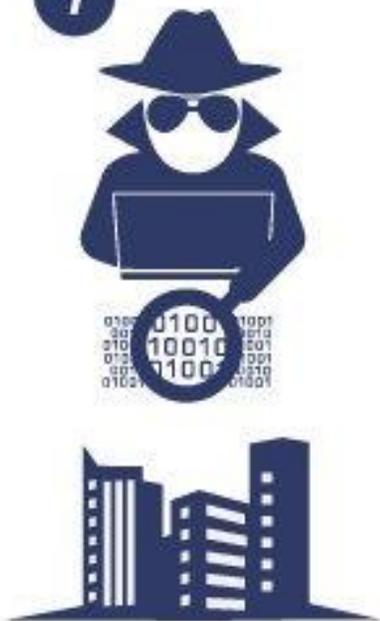


# 11 – La grande famille des fraudes

Les fraudes coutent très cher aux entreprises : Arnaques au Président, Faux ordres de virement FOVI, faux fournisseur, changement de RIB et HoaxCrash

## Fraude aux Faux Ordres de Virement #FOVI

1



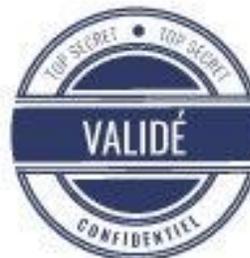
L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)

2



Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétexte une opération financière urgente et confidentielle

3



Sous la pression ou en confiance, l'entreprise exécute la transaction

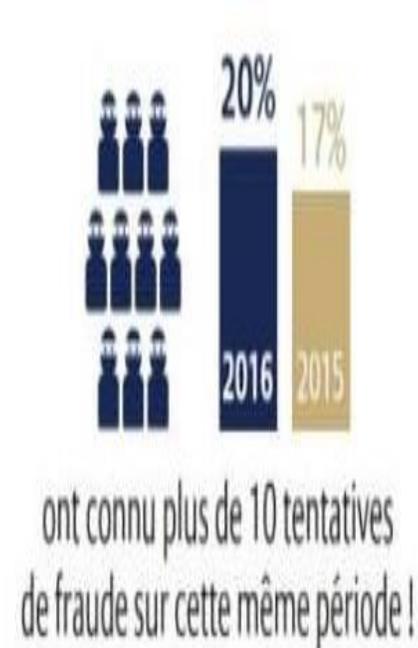
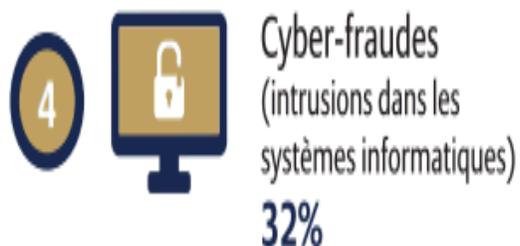
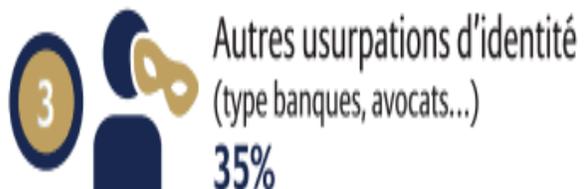
4



L'escroc transfère l'argent vers des comptes basés à l'étranger

# Les fraudes coutent très cher aux entreprises : Arnaques au Président, Faux ordres de virement FOVI, faux fournisseur, changement de RIB et HoaxCrash

## TOP 5 DES TENTATIVES DE FRAUDES



# Étude Euler Hermes - DFCG 2018

## La fraude, un phénomène en voie de professionnalisation !

**7 entreprises sur 10** ont été victimes d'(au moins) **1 tentative de fraude** sur l'année écoulée

**1 entreprise sur 5** a subi plus de **5 tentatives de fraude** sur cette même période

**1 entreprise sur 3** a subi au moins **1 fraude avérée** en 2017

**10%** des entreprises attaquées ont subi un **préjudice moyen supérieur à 100 K€**

### LES DISPOSITIFS AYANT PERMIS DE DÉJOUER CES TENTATIVES DE FRAUDES

**50%**  
Réaction ou initiative humaine personnelle



**38%** Procédures de contrôle interne  
**12%** Dispositif technique (IT)

**30%** ont constaté une **recrudescence** particulière des attaques en période de **congés / week-end**



### TOP 5 DES TENTATIVES DE FRAUDES

**54%**



Fraude au faux fournisseur

**50%**  
(dont 20% d'attaques au ransomware)



Cyber-criminalité

**43%**



Autres usurpations d'identité (banques, avocats...)

**42%**



Fraude au faux président

**35%**



Fraude au faux client

### QUELLES MENACES POUR LES ENTREPRISES ?

**85%**



Risque financier

**45%**



Risque sur les données

**30%**



Risque d'interruption de l'activité / des opérations

**29%**



Risque de réputation pour l'entreprise

**70%**

des directions financières craignent une **accentuation du risque de fraude** en 2018



**1 entreprise sur 2** est assurée ou envisage de s'assurer contre le risque de fraude



### TOP 3 DES SOLUTIONS MISES EN PLACE

**87%**



Sensibilisation des équipes, formations internes

**80%**



Renforcement des procédures de contrôle interne

**44%**



Audit sécurité des systèmes d'information

L'enquête a été réalisée entre février et mars 2018  
302 entreprises interrogées



[www.eulerhermes.fr](http://www.eulerhermes.fr)



**EULER HERMES**  
Our knowledge serving your success

# Les fraudes qui coutent très cher aux entreprises : Arnaques au Président, Faux ordres de virement FOVI, faux fournisseur

MES FAVORIS . Tours xj – Poitiers xj

BRM escroquée

## L'arnaque de 1,6 million d'euros menace de couler BRM

08/09/2015 11:06

Le cauchemar que vivent les 44 salariés de BRM (Bressuire) semble irréel. Victime d'une arnaque au président que l'on croit habituellement réservée aux grosses entreprises et aux magazines à sensation, ils sont pourtant menacés de chômage suite à la disparition de près de 1,6 millions d'euros des caisses de l'entreprise de fabrication de meubles.

L'escroquerie a été découverte le 1er septembre dernier par la direction. A quelques heures d'un comité d'entreprise de rentrée habituel, Jean Brossier, son PDG, a découvert que les comptes avaient été vidés de leur contenu dans l'été. *"Lors de ce comité d'entreprise, la direction ne savait pas encore ce qui s'était passé",* racontent les représentants du personnel. *"Ils nous ont demandé de leur laisser le temps de déterminer ce qui s'était passé. Mais la situation a été officialisée deux jours plus tard, le 3 septembre, lors d'un comité d'entreprise extraordinaire."*

### Une arnaque à 1,6 millions d'euros

Le scénario reconstitué par la direction est classique. Entre le 21 juillet et le 14 août, un escroc a usurpé le compte mail de Jean Brossier puis contacté par téléphone l'entreprise sous le sceau de la confidentialité. Il prétendait être le représentant d'un cabinet d'expertise comptable et d'un avocat et agir dans le cadre d'une

stratégie de rachat d'une entreprise par BRM. Il a ainsi obtenu plusieurs versements d'un montant total de près de 1,6 million d'euros. *"Nous pensons qu'on espionnait nos comptes mais parce que cette escroquerie est survenue au moment où nous avons reçu les règlements de plusieurs grosses commandes",* supposent les représentants du



## Arnaquée, l'entreprise de Bressuire risque la fermeture !

### “ Des escrocs bien renseignés

Un mail est adressé à la comptable de l'entreprise, en juillet. Ce message est signé du PDG, pour annoncer une grosse opération financière en Asie, menée par des avocats et experts comptables. Ce soit-disant PDG est en fait un groupe d'escrocs très renseignés sur l'entreprise. Ils savent que les caisses sont pleines : BRM vient de livrer une commande en Arabie Saoudite pour un million d'Euros. Ces escrocs mettent la pression sur la comptable, avec plusieurs fausses adresses. Ils lui assènent de rester très discrète. La comptable mord à l'hameçon. Le 21 juillet, premier virement bancaire vers la Thaïlande. La banque tique, et obtient confirmation. 6 autres virements suivent, toujours vers l'Asie. 1 millions 600 mille Euros au total, les caisses sont siphonnées.

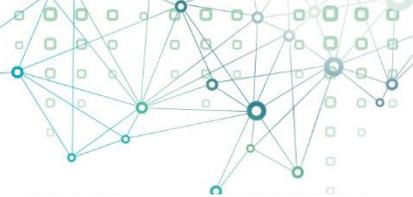
### “ Demande de cessation de paiement

La direction s'en rend compte le 1er septembre, pendant une réunion commerciale. Elle n'a plus les moyens de payer ses fournisseurs et ne peut pas livrer ses clients. La direction vient donc de déposer une demande de cessation de paiement. De son côté, le groupe belge auquel appartient cette entreprise refuse de mettre la main au portefeuille. Le groupe estime avoir déjà investi 1,5 million d'euros pour ce site et n'a pas les moyens de le soutenir financièrement après cette arnaque.



BRM Attack – July 21 2015

1,6 Millions – Président  
Fraud



## Gilbert Chikli : retour à la case prison en Ukraine

INFO LE POINT. Remis en liberté deux fois, le pionnier de l'arnaque "au faux président" a été réincarcéré. Il devrait bientôt être extradé vers la France.

PAR STÉPHANE SELLAMI

Modifié le 26/09/2017 à 17:05 - Publié le 26/09/2017 à 16:50 | Le Point.fr



U.S. Attorneys » Southern District of New York » News » Press Releases

Department of Justice

U.S. Attorney's Office

Southern District of New York

SHARE

FOR IMMEDIATE RELEASE

Tuesday, March 28, 2017

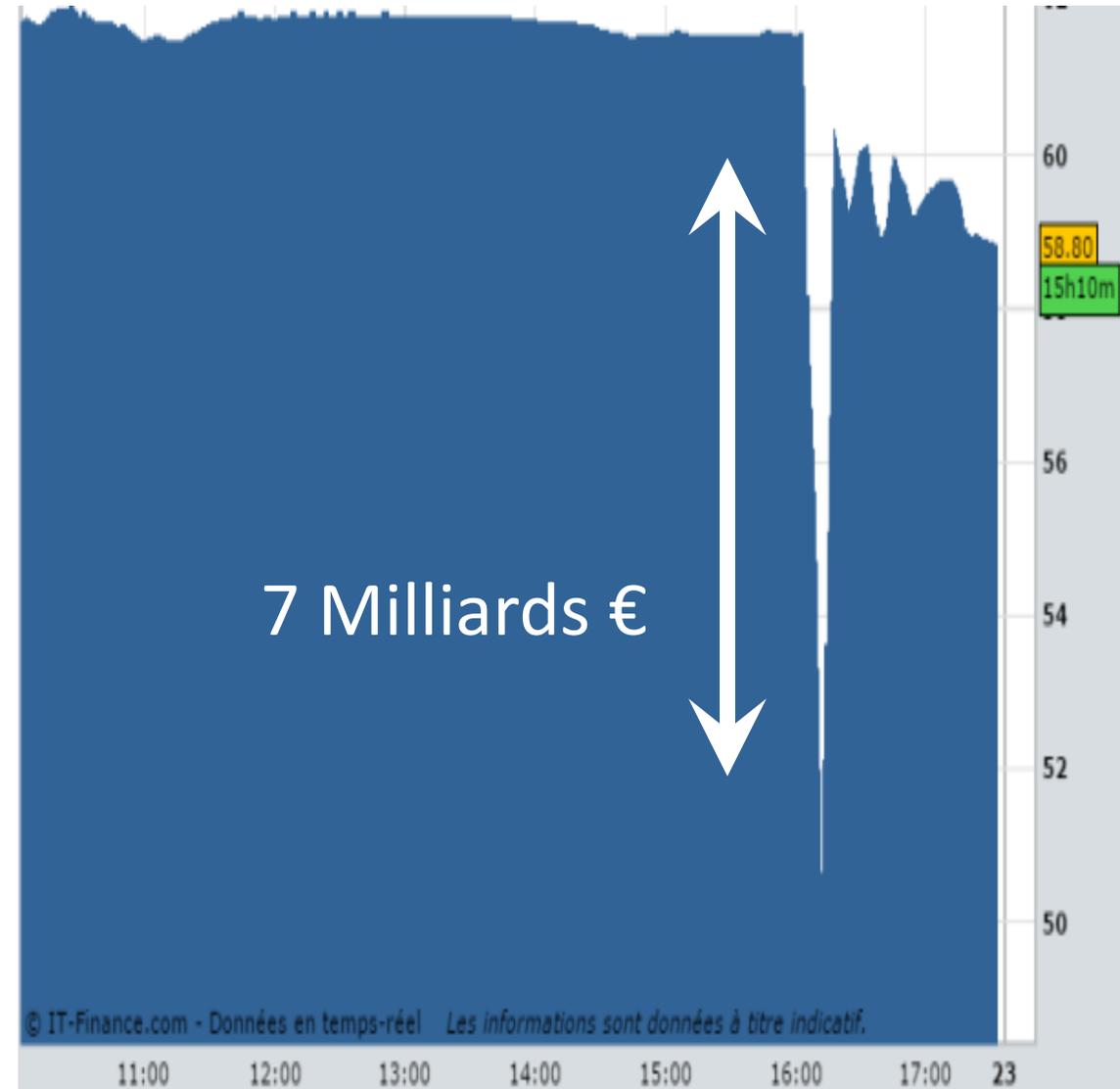
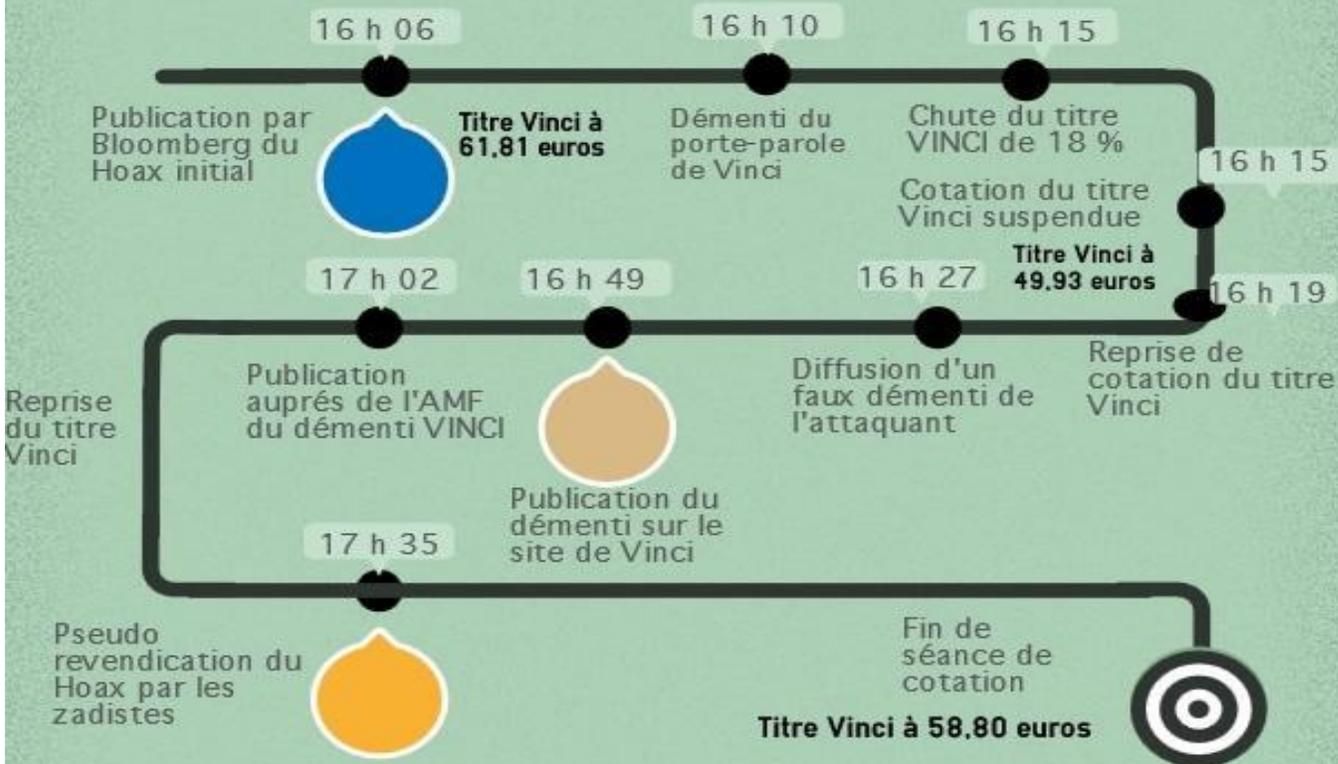
### Lithuanian Man Arrested For Theft Of Over \$100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies

Joon H. Kim, the Acting United States Attorney for the Southern District of New York, and William F. Sweeney Jr., the Assistant Director-in-Charge of the New York Office of the Federal Bureau of Investigation ("FBI"), announced criminal charges against EVALDAS RIMASAUSKAS for orchestrating a fraudulent business email compromise scheme that induced two U.S.-based internet companies (the "Victim Companies") to wire a total of over \$100 million to bank accounts controlled by RIMASAUSKAS. RIMASAUSKAS was arrested late last week by authorities in Lithuania on the basis of a provisional arrest warrant. The case has been assigned to U.S. District Judge George B. Daniels.

Acting U.S. Attorney Joon H. Kim said: "From half a world away, Evaldas Rimasauskas allegedly targeted multinational internet companies and tricked their agents and employees into wiring over \$100 million to overseas bank accounts under his control. This case should serve as a wake-up call to all companies – even the most sophisticated – that they too can be victims of phishing attacks by cyber criminals. And this arrest should serve as a warning to all cyber criminals that we will work to track them down, wherever they are, to hold them accountable. The charges and arrest in this case were made possible thanks to the terrific work of the FBI and the cooperation of the victim companies and their financial institutions. We thank the companies and their banks for acting quickly, coming forward promptly, and cooperating with law enforcement; it led not only to the charges announced today, but also the recovery of much of the stolen funds."

Les fraudes qui coutent très cher aux entreprises :  
Arnaques au Président, Faux ordres de virement FOVI, faux fournisseur, changement  
de RIB et HoaxCrash

## HoaxCrash VINCI 22 novembre 2016





mar. 22/11/2016 16:04

contact.abonnement@vinci.group

VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

À [redacted]

Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Nouveau communiqué de presse VINCI

Rueil Malmaison, 22 Novembre 2016

VINCI lance une révision de ses comptes consolidés pour l'année 2015 et le 1er semestre 2016

Vinci a annoncé aujourd'hui son intention de réviser ses comptes consolidés pour l'exercice 2015 ainsi que pour le premier semestre 2016. Les résultats d'un audit interne mené par le groupe Vinci ont en effet révélé que certains transferts irréguliers avaient été effectués des dépenses d'exploitation vers le bilan, en dehors de tous principes comptables reconnus. Le montant de ces transferts s'élèverait à 2.490 millions d'euros pour l'exercice comptable 2015 et 1.065 millions d'euros pour le premier semestre 2016. Selon l'audit interne les résultats opérationnels réels seraient de 1.225 millions pour 2015 et de 641 millions pour le premier semestre 2016. Le groupe reporterait donc une perte nette pour 2015 ainsi que pour le premier semestre 2016.

Vinci a rapidement informé ses auditeurs externes (KPMG Audit et Deloitte & Associés) de la découverte de ces transferts. Le 21 Novembre, KPMG a informé Vinci qu'au vu de ces irrégularités, son audit des comptes consolidés de l'année 2015 et du premier semestre 2016 ne sauraient être valides.

Vinci publiera des comptes non audités pour l'exercice 2015 ainsi que pour le premier semestre 2016 dès que possible. Une fois que le nouvel audit sera achevé, Vinci publiera de nouveaux comptes audités pour les deux périodes. Le groupe a par ailleurs lancé une révision complète des règles internes au sein de sa direction financière.

La compagnie a licencié Christian Labeyrie, directeur général adjoint et directeur financier de Vinci.

Vinci a informé l'Autorité des Marchés Financiers (AMF) de ces événements.

La révision des résultats opérationnels pour 2015 et 2016 devrait rester sans conséquence sur la trésorerie du groupe et n'affectera ni les clients ni les prestations du groupe Vinci.

« Notre équipe de direction est très choquée par ces découvertes », a dit Xavier Huillard, Président-Directeur Général de Vinci. « Nous nous engageons à ce que Vinci respecte les plus hauts standards éthiques dans la conduite des affaires du groupe ».

« Nos clients ainsi que nos employés doivent garder confiance en la viabilité du groupe Vinci et en son engagement sur le long terme. Nos services ne sont en aucun cas affectés par ces événements et notre engagement à satisfaire les besoins de nos clients reste une priorité. Les rumeurs qui circulent sur une procédure d'insolvabilité sont totalement fausses » a ajouté le Président Directeur Général de Vinci.  
« Nous nous engageons à mettre en place les changements nécessaires au sein du Groupe ».

Le groupe Vinci tiendra une conférence de presse demain.

Contact médias

Paul-Alexis Bouquet

Tél. : +33 (0)7 51 93 47 48

<http://www.vinci.group/vinci.nsf/fr/communiqués/pages/20161122-1557.htm>

Vinci HoaxCrash -  
Nov 22 2016

# Les attaques par HoaxCrash

HoaxCrash	Motivations of the attacker
SEA - AP (2013)	Political – Hacktivism (Syrian conflict)
Whitehaven Coal (2013)	Political – ecological activism
G4S (2014)	Political - activism
AVON (2015)	Economic - (image damage - speculation)
FITBIT (2016)	Economic & activism
VINCI (2016)	Economic (stock market volatility - speculation)

# **Tendances et évolution de la menace cyber en 2021**



1

Malicious  
Insider Attacks



2

AI-related  
Threats



3

Hybrid  
Workforce



4

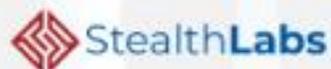
Convergence of Zero  
Trust and SASE



5

Rise of  
BYOD

## Top 10 Security Predictions from CISOs in 2021



6

Hunt for Cybersecurity  
Professionals



7

Network and Security  
Transformation



8

Cloud Data  
Governance



9

Privacy Enhancing  
Technologies



10

Collaboration of  
Security Vendors



Malware



Web-based attacks



Phishing



Web application attacks



Spam

# TOP 15 CYBER THREATS



DDoS



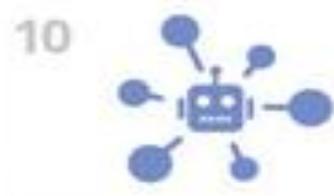
Identity theft



Data breach



Insider threat



Botnets



Physical manipulation,  
damage, theft and loss



Information leakage



Ransomware



Cyberespionage



Cryptojacking

# INFOGRAPHIC



## USE OF PERSONAL DEVICES

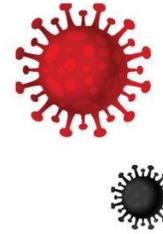
**77%** of remote employees used unmanaged, insecure BYOD (Bring Your Own Devices) to access corporate systems.

Source: CyberArk Survey

## PLAN B

**50%** of infosec professionals had no contingency plan to face COVID-19 pandemic.

Source: Bitdefender Survey



## SECURE LOGIN

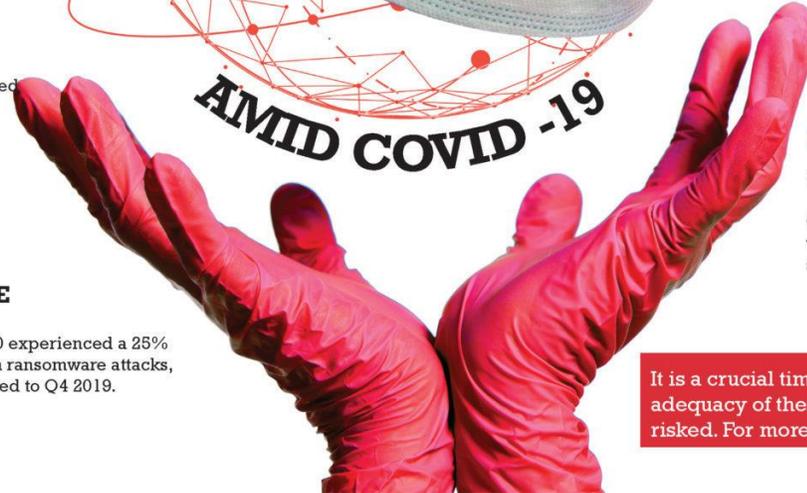
Only **70%** respondents used company VPNs to securely log in to the company network.

Source: CISO MAG Survey

# CYBERSECURITY PULSE

The COVID-19 pandemic has disrupted global health, the economy, and social systems. To add to that, it has also led to a surge in unseen threats in the digital space.

# AMID COVID-19



## CLOUD SECURITY?

**92%** of security leaders were worried that their organization is vulnerable to a major cloud misconfiguration-related data breach.

Source: PwC Survey



**500,000+**  
ZOOM LOGINS ON DARK WEB

The stolen Zoom accounts were published, exchanged, and in some cases, sold on hacker forums

Source: Cyble

## THE PASSWORD TICKING BOMB

**93%** of remote employees reused passwords across applications and devices.

Source: CyberArk Survey



## RANSOMWARE SURGE

**25%** Q1 2020 experienced a 25% surge in ransomware attacks, compared to Q4 2019.

Source: Beazley



**25,000**

## EMAIL ACCOUNTS COMPROMISED

The compromised email accounts allegedly belonged to the World Health Organization (WHO), Gates Foundation, National Institute of Health (NIH), and other groups working to combat the Coronavirus pandemic.

Source: Washington Post



**4000**

## COVID-RELATED DOMAINS

Over 4,000 Coronavirus-related domains were registered globally. Out of these websites, 3% were found to be malicious.

Source: CheckPoint Threat Intelligence



It is a crucial time for organizations across all industries to be alert and address the adequacy of their cyber policies, as loss of client or organizational data cannot be risked. For more information visit [cisomag.eccouncil.org](https://www.cisomag.eccouncil.org)

By Pooja Tikekar & Rudra Srinivas

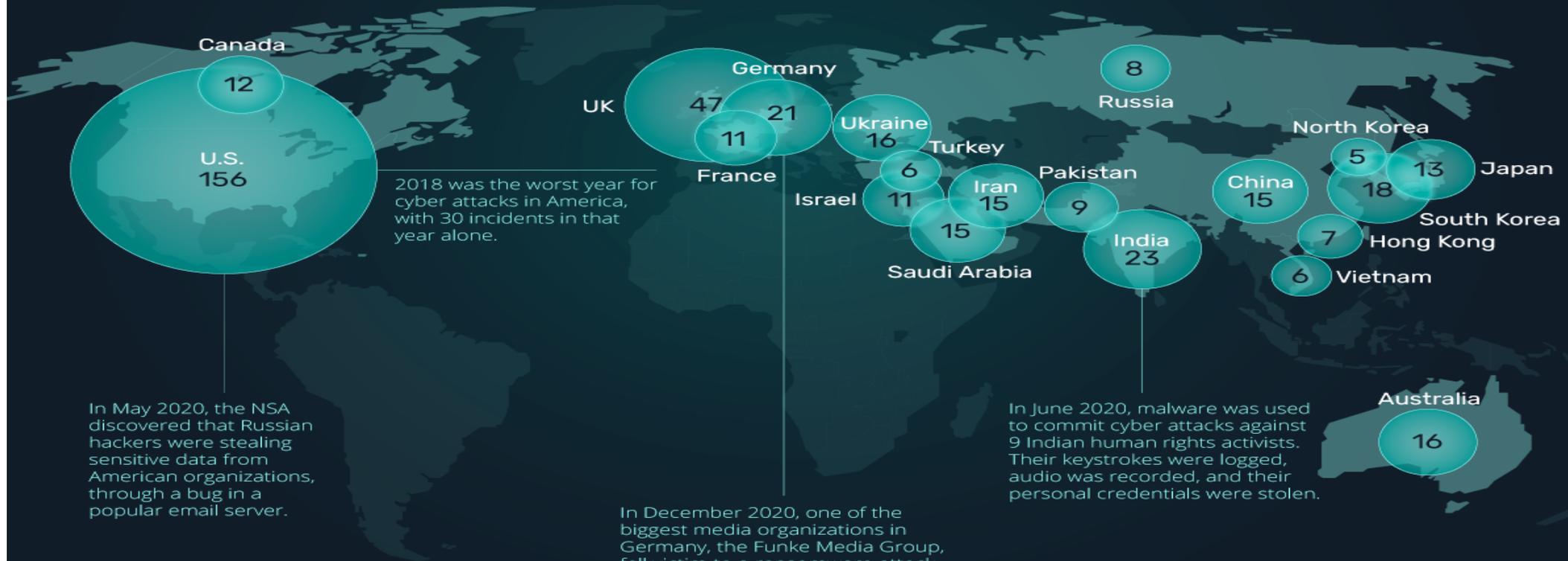


# CYBER ATTACKS

By 2025, cyber crime is expected to cost the global economy \$10.5T a year. That's almost \$20M every minute.

Here's a look at the countries with the highest amount of significant cyber attacks since 2006.

**i** "Significant" cyber attacks mean hacks into a country's government agencies, defense and high-tech companies, or crimes with losses of more than \$1M.



## Les 5 cyberattaques marquantes de 2021



TOP 5



Cyberattacks of 2021

# Attaque contre CNA Financial

CNA Financial est l'une des plus grandes compagnies d'assurance aux États-Unis. La société a annoncé l'attaque fin mars 2021, déclarant qu'elle avait été victime d'une cyberattaque sophistiquée. La société a négocié sa **rançon de 60 millions de dollars à 40 millions de dollars** et a payé la clé de déchiffrement dont elle avait besoin pour poursuivre ses opérations.

Un syndicat de cybercriminalité appelé Phoenix a revendiqué la responsabilité de l'attaque. Le groupe a utilisé un type de malware appelé Phoenix Locker, qui est lui-même une variante de l'exécutable du ransomware Hades, plus populaire.

Le site Web de CNA Financials est resté fermé pendant près de deux semaines après l'attaque. Il n'a révélé les détails de l'attaque que deux mois après le paiement de la rançon, alors qu'il y était contraint par la loi.

L'exécutable du ransomware Phoenix fonctionne en se faisant passer pour une mise à jour du navigateur. Il incite les employés à installer la mise à jour, puis se déplace latéralement sur le réseau pour obtenir des privilèges plus élevés jusqu'à ce qu'il puisse mener à bien la phase deux de l'attaque. Il identifie les données sensibles puis les envoie hors du réseau avant de chiffrer les données et de lancer l'attaque.

La protection contre l'exfiltration des données aurait empêché Phoenix de copier, compresser et envoyer des données de l'environnement CNA vers le compte cloud du pirate. Les enquêteurs ont déterminé que les attaquants voulaient faire chanter les utilisateurs avec leurs données sensibles. Sans ces données, les attaquants n'auraient pas pu lancer leur attaque avec succès ou prouver l'accès aux données sensibles.

# Attaque contre COLONIAL PIPELINE

L' **attaque du Colonial Pipeline** est de loin la plus tristement célèbre de 2021 à ce jour. Un groupe de piratage basé en Russie appelé DarkSide a revendiqué la responsabilité de l'attaque, qui s'est concentrée sur les systèmes SCADA qui connectent les systèmes opérationnels aux réseaux informatiques traditionnels connectés à Internet. DarkSide a mené à bien son attaque en se concentrant sur les serveurs informatiques de Colonial Pipeline dans sa pile SCADA opérationnelle. Les professionnels de la sécurité de Colonial Pipeline ont pris la mesure prudente de démanteler ces systèmes avant que l'attaque ne se propage, ce qui a limité les dégâts, mais a conduit à la fermeture soudaine d'un pipeline de carburant critique, provoquant une crise d'approvisionnement régionale qui a nui aux consommateurs.

DarkSide a pénétré les systèmes de Colonial Pipeline en utilisant des informations d'identification de compte compromises provenant d'un système opérationnel hérité qui ne comportait pas d'authentification à double facteur. Les attaquants ont infiltré le réseau et ont envoyé un exécutable de malware compressé dans le système. Le malware de DarkSide fonctionne en effaçant la corbeille et en supprimant les copies de volume à l'aide d'un script PowerShell non restaurable. Il désactive les services Windows et cible les processus terminés avant de chiffrer les fichiers de manière récursive jusqu'à ce que les partages locaux et réseau soient entièrement chiffrés. Il exfiltre ces données vers un serveur C2 spécifié par l'attaquant avant de supprimer sa propre copie et de publier la demande de rançon.

# Attaque contre JSB USA

Un mois après la chute de Colonial Pipeline aux mains de pirates informatiques, la plus grande entreprise de conditionnement de viande au monde a également subi une attaque paralysante. JBS USA est la filiale américaine de JBS SA, une société de distribution de viande basée au Brésil. L'entreprise a pu atténuer certains des dommages de l'attaque à l'aide de sauvegardes, mais elle a tout de même été obligée de suspendre temporairement ses opérations et de subir des temps d'arrêt coûteux.

JBS n'a initialement pas indiqué s'il avait payé les attaquants et n'a pas commenté sa décision de fermer ses usines nord-américaines pendant deux jours. Finalement, la **société a admis avoir payé 11 millions de dollars aux attaquants** en réponse à la menace de fermeture.

L'attaque a eu des effets d'entraînement coûteux sur la chaîne d'approvisionnement nationale en viande, empêchant les supermarchés et les restaurants de servir de la viande à leurs clients beaucoup plus longtemps et entraînant des hausses de prix en raison de la crise de l'offre.

L'attaque JBS a en fait **commencé en février 2021**, avec une reconnaissance initiale soulignant des vulnérabilités structurelles dans le réseau de la victime. Les cybercriminels ont procédé à l'exfiltration de données pendant des mois, commençant dès mars et terminant cette phase de l'attaque fin mai. Les pirates n'ont finalisé l'attaque qu'une fois l'exfiltration terminée, le 1er juin.

JBS aurait pu atténuer l'ensemble de l'attaque en utilisant un logiciel de protection contre l'exfiltration de données. Cela aurait empêché les pirates informatiques de passer des mois à voler des données à l'entreprise sans laisser de traces évidentes. Des alertes de sécurité auraient entraîné une action rapide qui aurait pu expulser les attaquants bien avant que l'attaque ne frappe.

# Attaque contre KASEYA

Kaseya est un fournisseur de services informatiques basé en Floride qui a fait la une des journaux après avoir été victime d'une attaque de ransomware à grande échelle revendiquée par REvil. Cette **attaque a compromis entre 800 et 1 500 entreprises** dans le monde, avec des effets perturbateurs suivant les utilisateurs finaux tout au long de chaînes d'approvisionnement complexes.

Le cas de Kaseya est unique en raison de la place de l'entreprise en tant que fournisseur de services gérés avec une base de clients aussi importante. La grande majorité de ces entreprises sont de petites entreprises, mais l'infrastructure de leur chaîne d'approvisionnement informatique les relie étroitement les unes aux autres.

Dans ce cas, REvil a ciblé la solution d'appliance de serveur virtuel (VSA) de Kaseya et a prétendu atteindre 1 million de points de terminaison sur l'ensemble de la chaîne d'approvisionnement. La solution VSA de Kaseya existe à la fois en tant que solution Software-as-a-Service (SaaS) basée sur le cloud et en tant que produit sur site. Les pirates informatiques REvil ont compromis le produit VSA de Kaseya en installant un exécutable malveillant dans le système VSA. L'attaque s'est déroulée en plusieurs étapes, la première charge utile désactivant Windows Defender et la seconde effectuant la tâche de chiffrement du ransomware.

Si Kaseya avait investi dans la protection contre l'exfiltration de données, REvil n'aurait pas été en mesure de distribuer la deuxième charge utile lors de son attaque. La première charge utile aurait été incapable de communiquer avec la seconde, rendant l'attaque inoffensive. REvil n'aurait pas pu exiger sa rançon de 70 millions de dollars.

# Attaque contre BRENNTAG

Brenntag est une société allemande de distribution de produits chimiques présente dans 77 pays. Plus tôt cette année, **DarkSide a ciblé la division nord-américaine de l'entreprise**, cryptant les données et les appareils sur le réseau compromis et volant 150 Go de données.

DarkSide affirme avoir lancé l'attaque après avoir eu accès au réseau de Brenntag via des identifiants d'utilisateur volés achetés sur le Dark Web. Ce type d'attaque est de plus en plus courant et est incroyablement difficile à contrer à l'aide des technologies traditionnelles de cybersécurité.

Les identifiants d'utilisateur volés ne sont souvent pas signalés et peuvent même être accompagnés de privilèges administratifs précieux. Les professionnels de la cybersécurité doivent élaborer des politiques qui présentent un cadre de confiance zéro, même pour les titulaires de comptes privilégiés.

DarkSide n'aurait pas été en mesure de voler 150 Go de données précieuses si le réseau Brenntag n'avait pas permis aux titulaires de comptes privilégiés d'exfiltrer de gros volumes de données. Il y a très peu de raisons légitimes pour lesquelles un administrateur voudrait déplacer autant de données sensibles à la fois.

Le déploiement d'une solution de protection contre l'exfiltration de données qui empêche ce type de transfert n'aurait eu que très peu, voire aucun, impact sur les opérations quotidiennes et la convivialité. Mais cela aurait très bien pu éviter à Brenntag de payer une rançon de 4,4 millions de dollars au syndicat cybercriminel DarkSide.



## **Top 10 Cyber Attack Maps**

## Les cartes des cyberattaques en direct (24/365)

- Kaspersky Cyber Attack Map : <https://cybermap.kaspersky.com/>
- Norse Attack Map : <https://norsenet.com/>
- Arbor Networks : <https://www.netscout.com/arbor-ddos?lang=en>
- Digital Attack Map :  
<https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18763&view=map>
- Fortinet Threat Map : <https://threatmap.fortiguard.com/>
- FireEye : <https://www.fireeye.com/cyber-map/threat-map.html>
- DDoS & Cyber Attack Map : <https://www.digitalattackmap.com/>
- Checkpoint Cyber Attack Map : <https://threatmap.checkpoint.com/>
- Akamai : <https://www.akamai.com/fr/visualizations>

# Focus sur les Ransomwares

En 2020, les logiciels malveillants ont augmenté de 358 % dans l'ensemble et les ransomwares de 435 % par rapport à 2019.

*Forbes*

## Pays victimes de Ransomwares

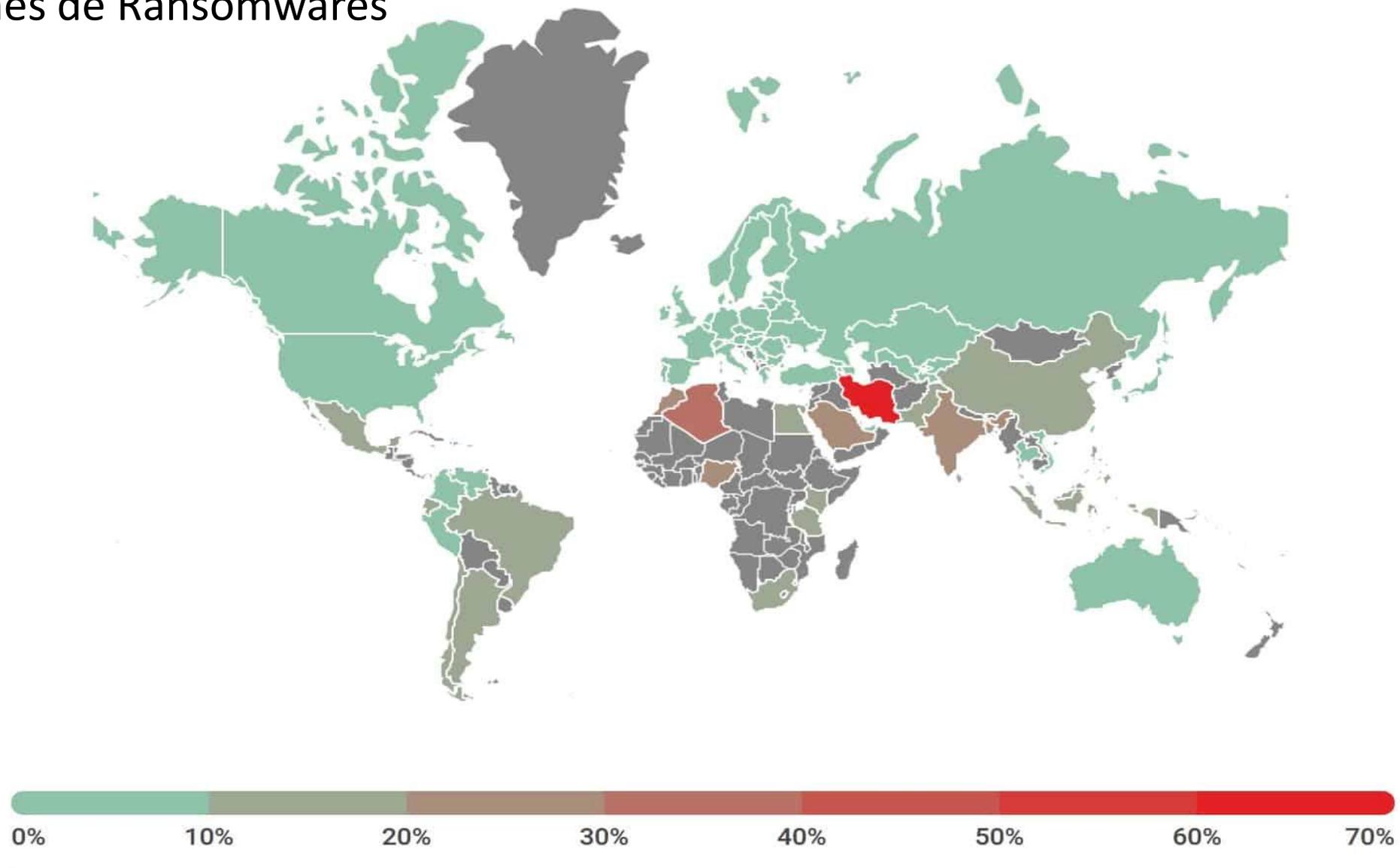


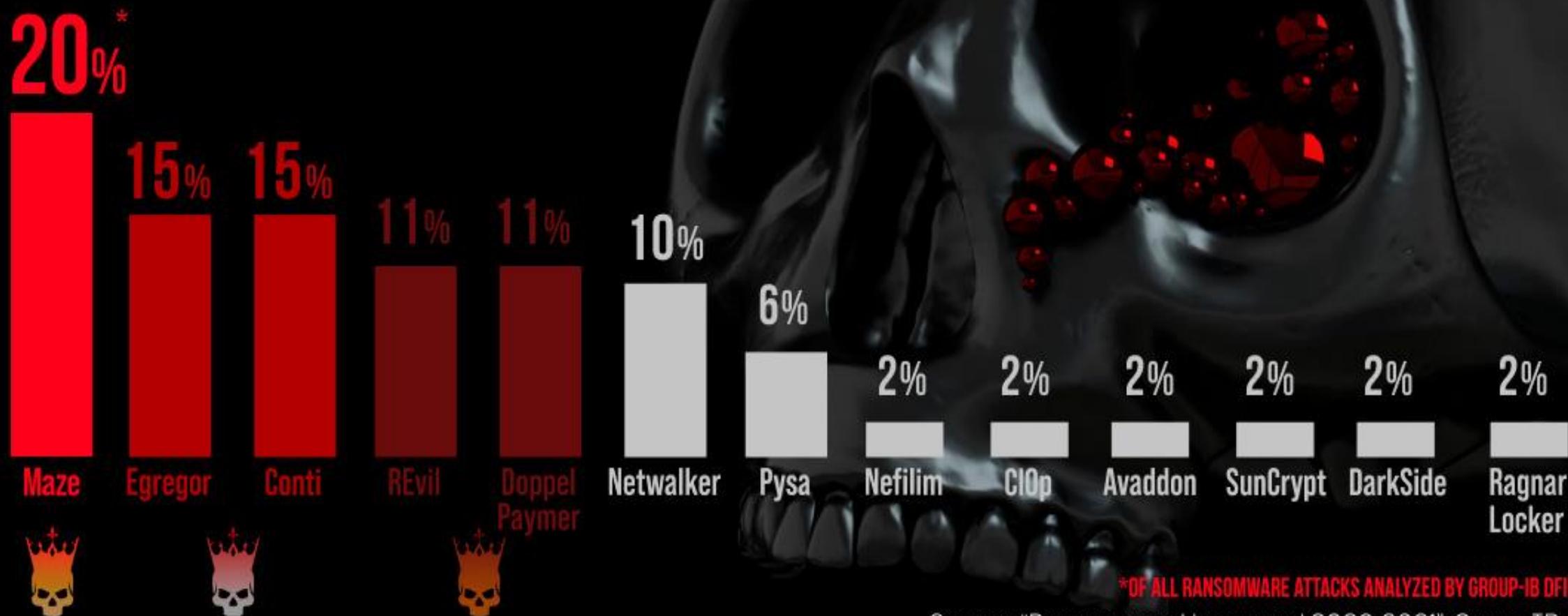


Figure 15: The ransomware vicious cycle: increased odds of recovering data ... entice more victims to pay ransoms ... which motivates more ransomware attacks.



# MOST ACTIVE RANSOMWARE GANGS IN 2020 BY NUMBER OF ATTACKS

|GROUP|IB|



\*OF ALL RANSOMWARE ATTACKS ANALYZED BY GROUP-IB DFIR TEAM

Source: "Ransomware Uncovered 2020-2021", Group-IB, 2021

# 15 PUBLIC RANSOMWARE AFFILIATE PROGRAMS APPEARED IN 2020

|GROUP|IB|



# ALLIANCE MAP: RANSOMWARE GANGS AND COMMODITY MALWARE IN 2020

|GROUP|IB|

## Trickbot

Ryuk  
Conti  
REvil  
RansomExx

## Qakbot

ProLock  
Egregor  
DoppelPaymer

## Dridex

DoppelPaymer

## SDBBot

ClOp

## Zloader

Ryuk  
Egregor

## IcedID

RansomExx  
Maze  
Egregor

## Buer

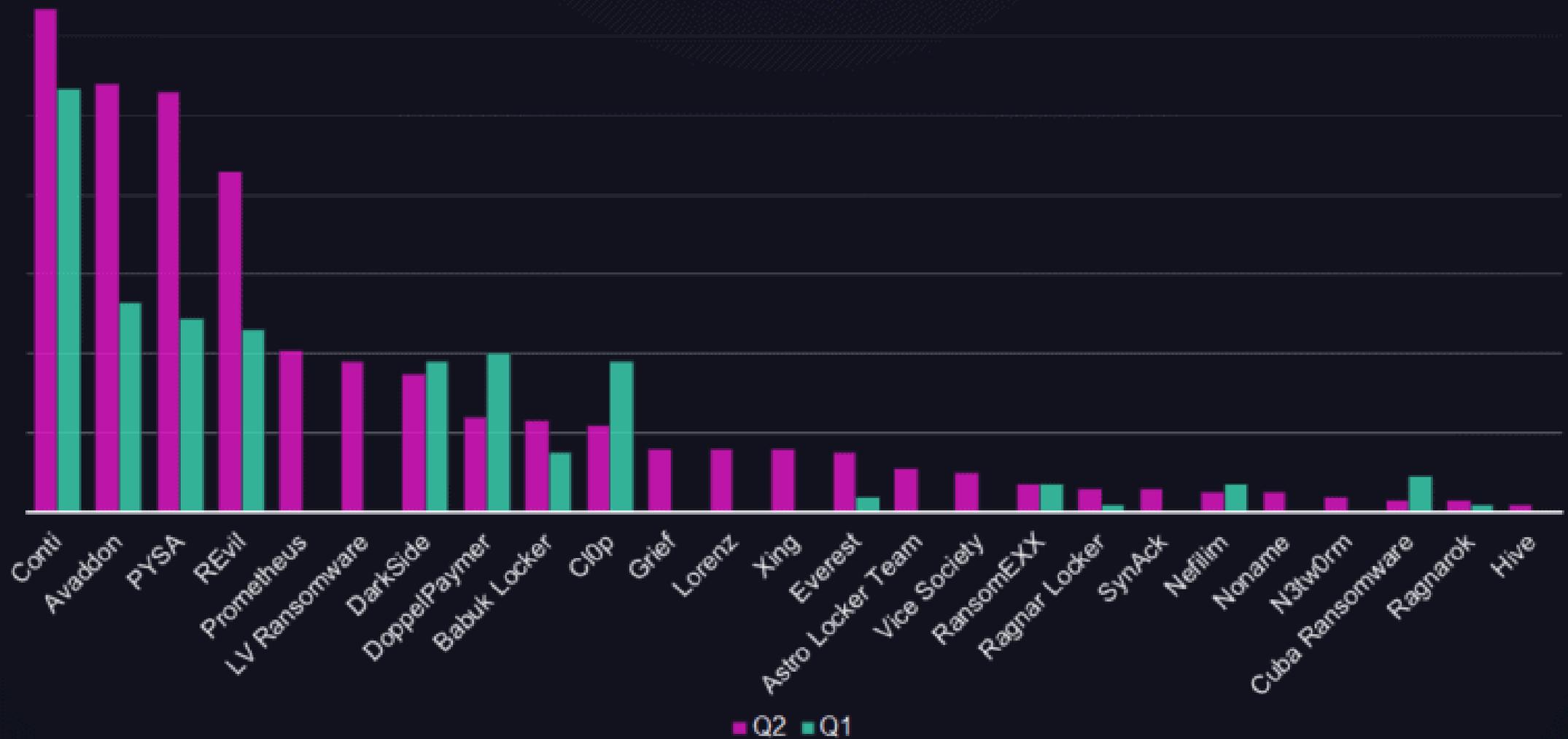
Maze  
Ryuk

## Bazar

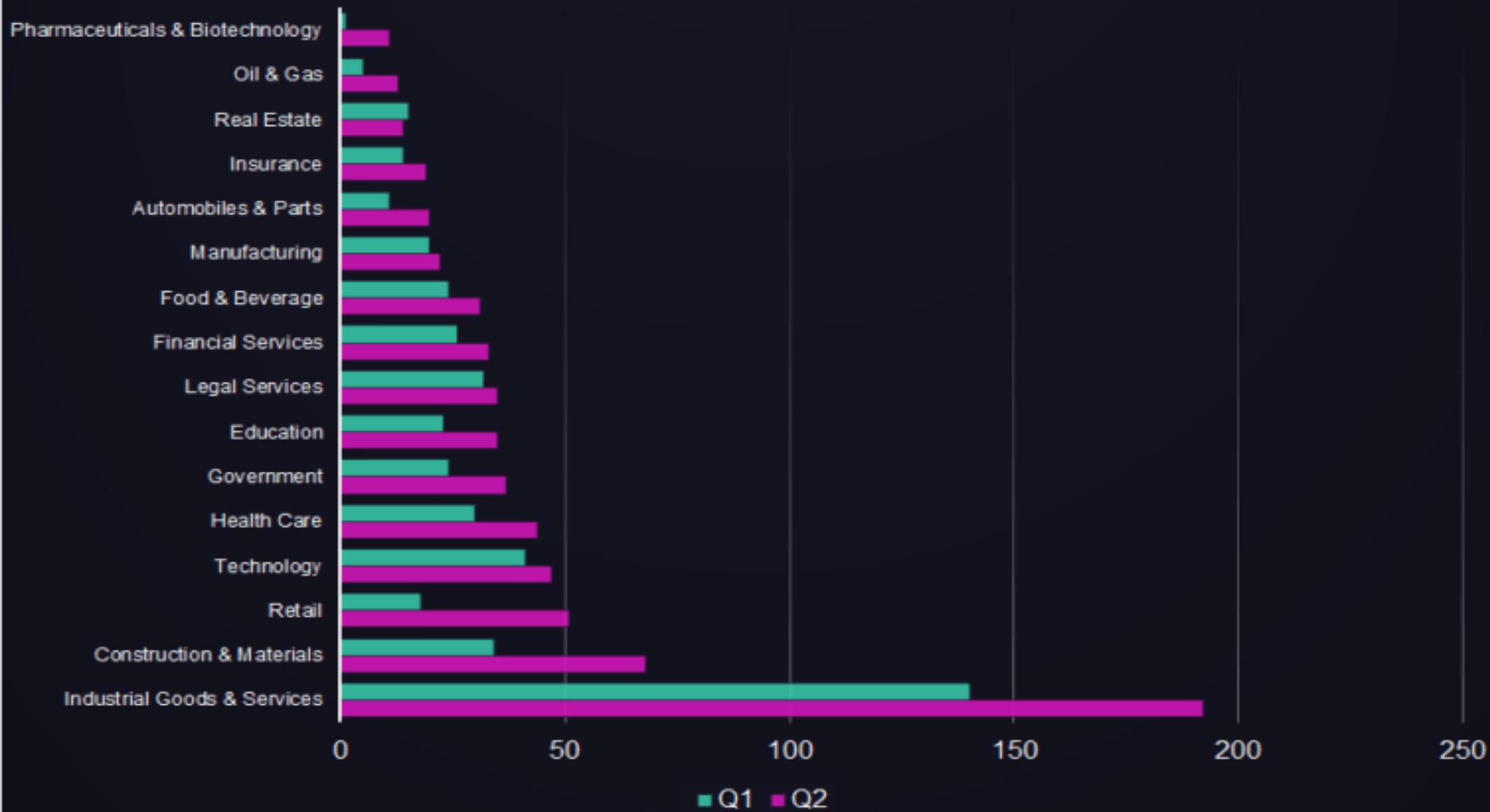
Ryuk



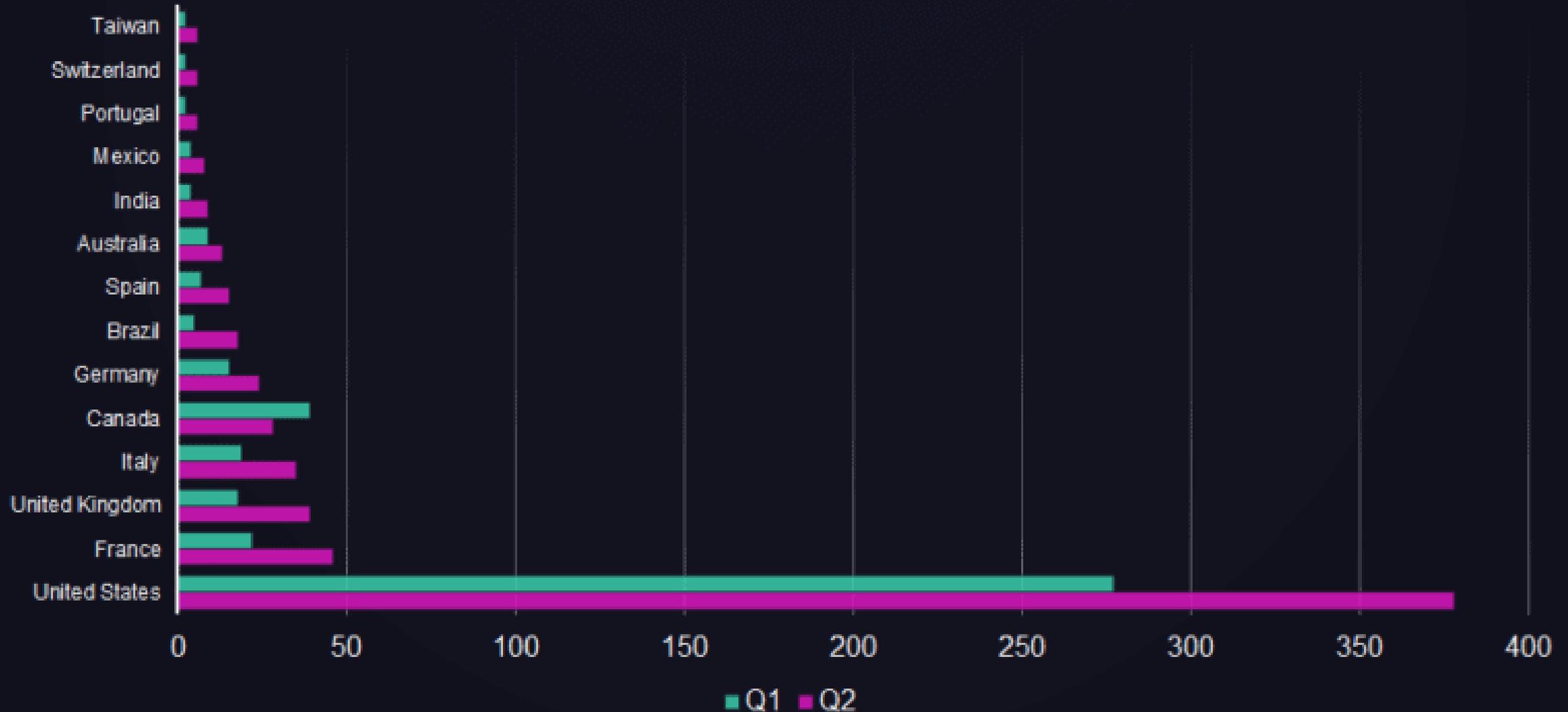
# Ransomware by Group 1H 2021



## Ransomware by Sector 1H 2021



# Ransomware by Geography 1H 2021

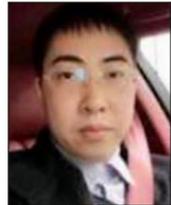




**APT 41 GROUP**



ZHANG Haoran



TAN Dailin



QIAN Chuan



FU Qiang



JIANG Lizhi



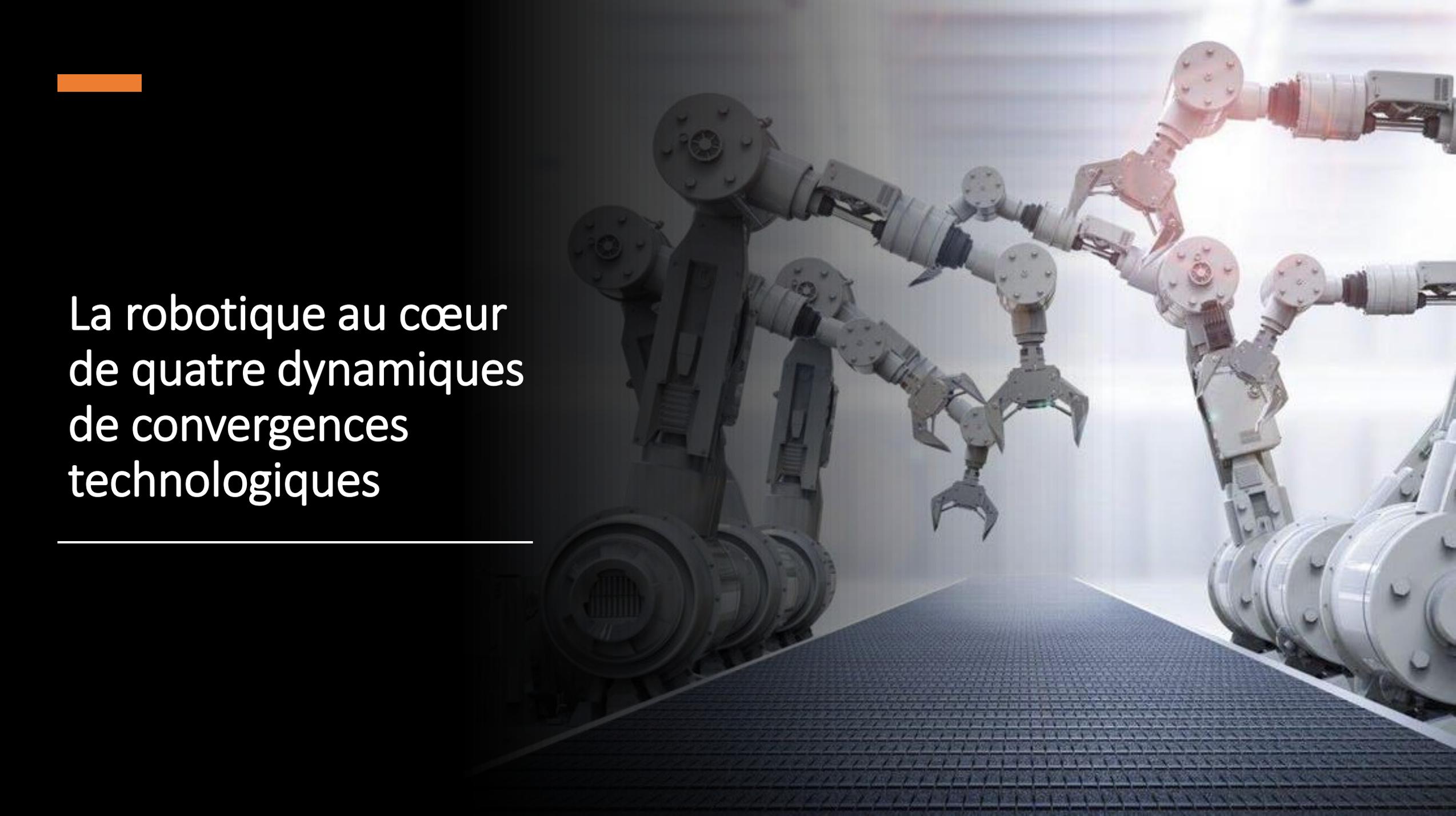


**PARTIE II**  
**Robotique et**  
**nouveaux**  
**risques cyber**

---

# Le large spectre de la robotique et de ses applications

- La robotique, c'est un vaste ensemble de segments technologiques qui s'additionnent pour rendre possible la construction d'un robot : mécanique, électronique, mécatronique, matériaux, optique, capteurs multispectraux, software, mathématiques, contrôle optimal, systèmes multi-agents, apprentissage par renforcement, computer vision, Machine Learning, cybersécurité, IoT, Antennes, électromagnétisme, impression additive, des neurosciences, des sciences cognitives, de la R&D, des laboratoires de recherche, ...
- Les domaines adressés par la robotique sont tout aussi variés: industrie, production, logistique, transports, défense, sécurité civile, pompiers, surveillance des territoires, écologie, dépollution automatisée(terre, air, mer), santé médecine(implants, prothèses intelligentes, robots chirurgicaux), agriculture (la robotique autonome est le moteur de la révolution agricole), énergie, BTP construction, biotechnologies, pharmacologie, industrie minière, aéronautique civile et militaire, aérospatiale, secteur ferroviaire et métros, automobile et mobilités intelligentes,...

The background image shows a futuristic industrial environment. Several robotic arms, some in shades of grey and others in a light pinkish-red, are positioned in a factory-like setting. The floor is a dark, textured metal grating. The lighting is soft and diffused, creating a clean, high-tech atmosphere. The text is overlaid on the left side of the image.

La robotique au cœur  
de quatre dynamiques  
de convergences  
technologiques

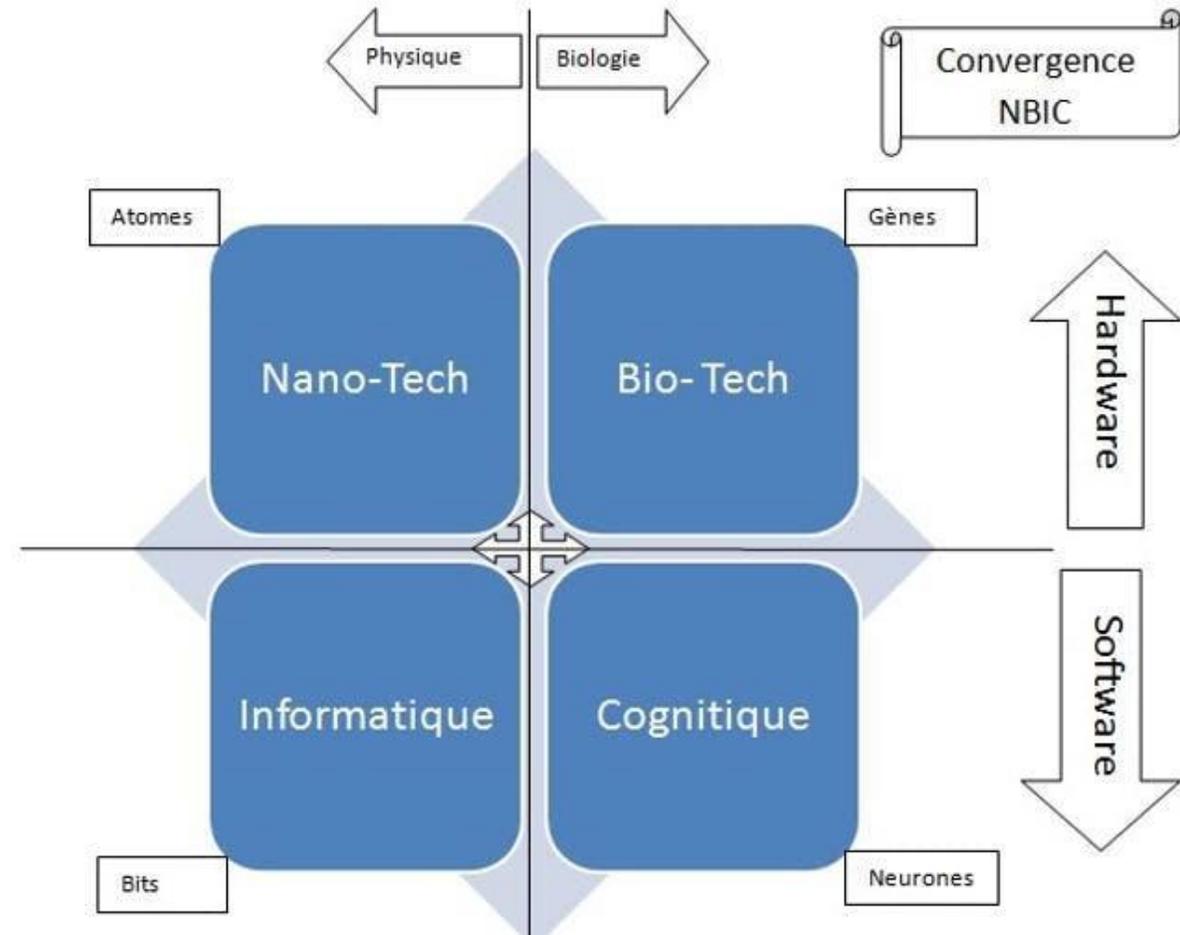
---

## La robotique au cœur de quatre dynamiques de convergences technologiques

La robotique s'inscrit au cœur des quatre grandes convergences technologiques du 21<sup>ème</sup> siècle : NBIC, MI, DIADEH, CKTS :

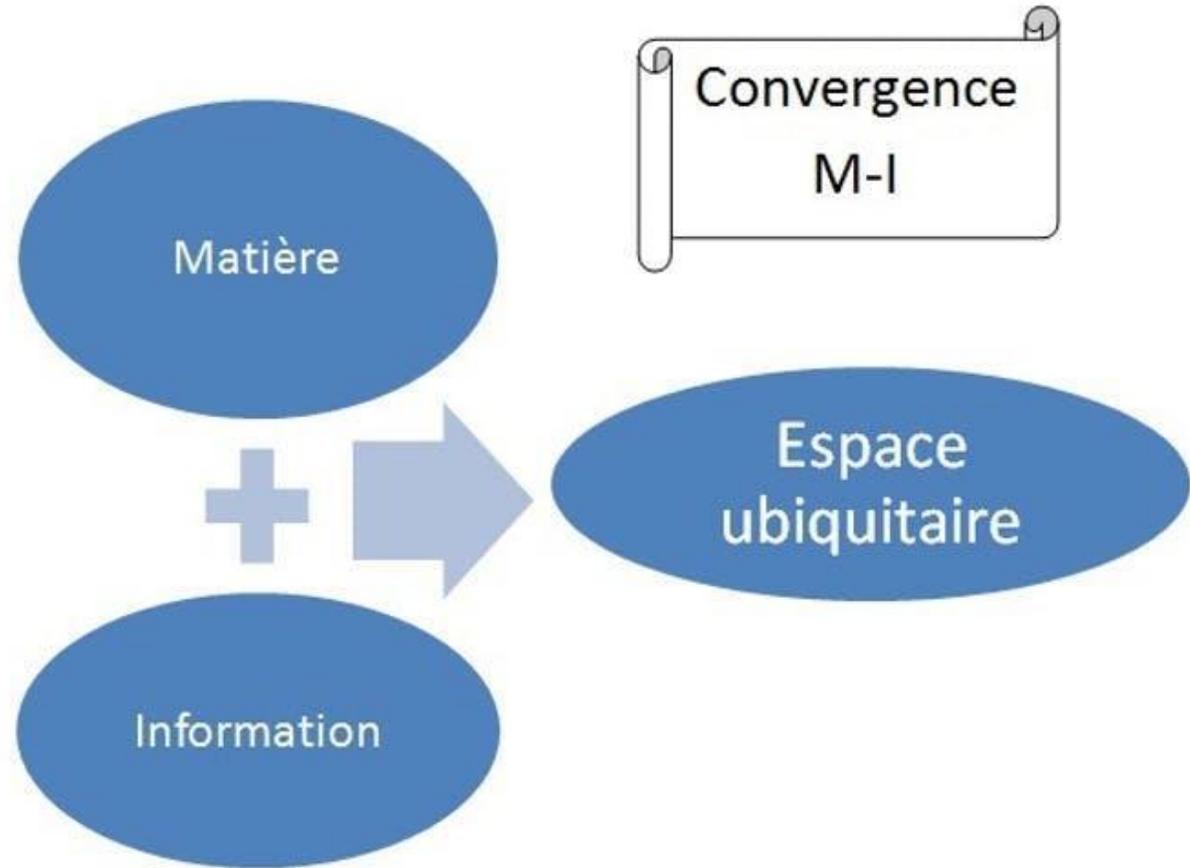
- La convergence NBIC est la convergence des Nanotechnologies, des Biotechnologies, de l'Informatique et des sciences Cognitives.
- La convergence MI est la convergence de la Matière et de l'Information pour produire un espace ubiquitaire.
- La convergence DIADEH (Diffusion de l'IA sur les Domaines d'Expertise 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.

# Convergence NBIC: Nanotechnologie, Biotechnologies, Informatique, Sciences Cognitives



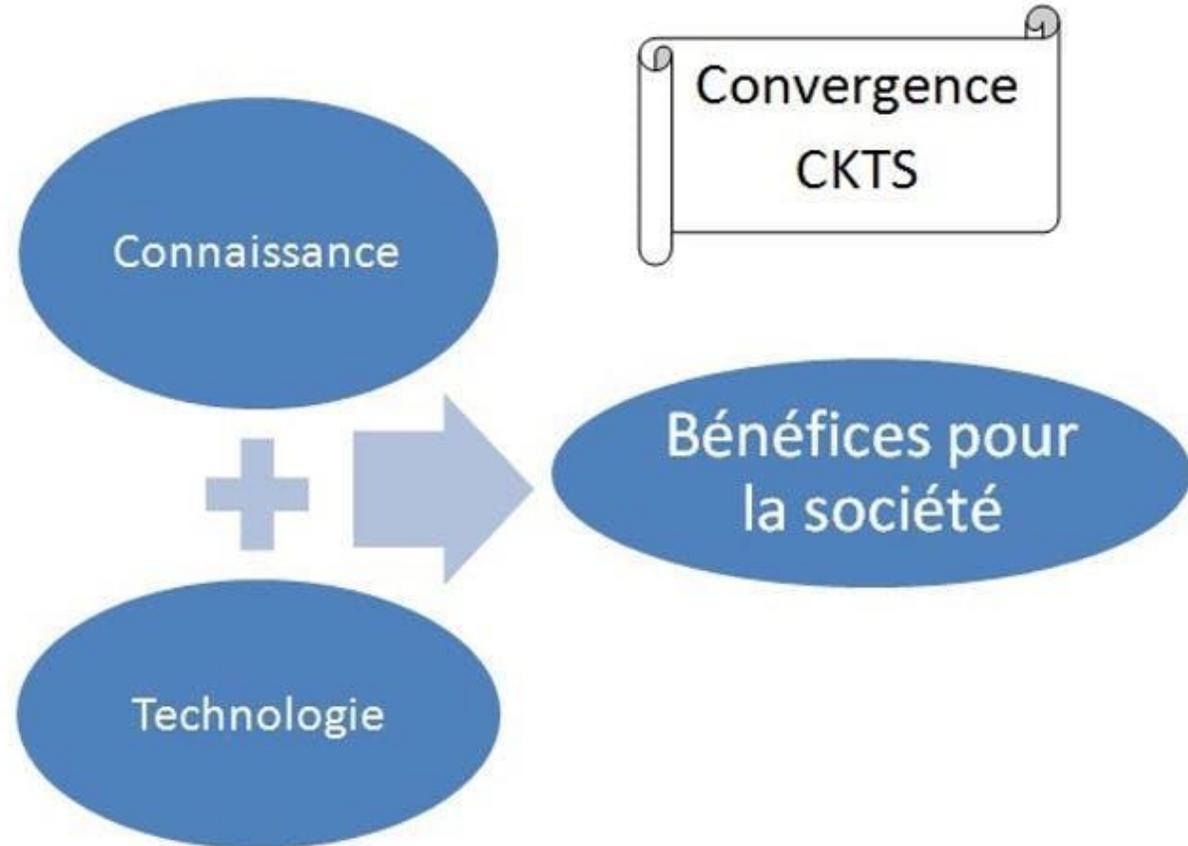
**Convergence NBIC**

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



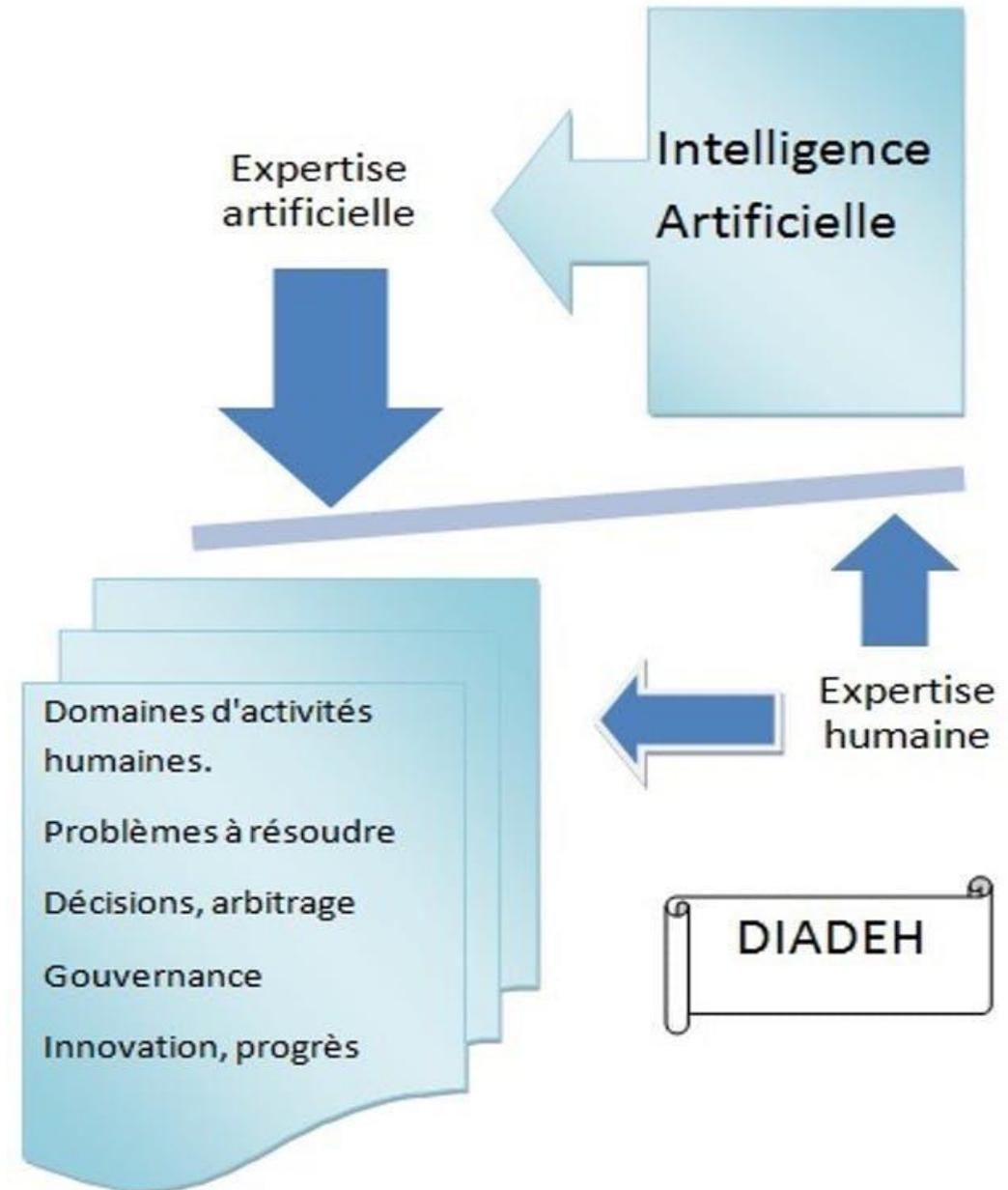
**Convergence Matière – Information**

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



**Convergence CKTS**

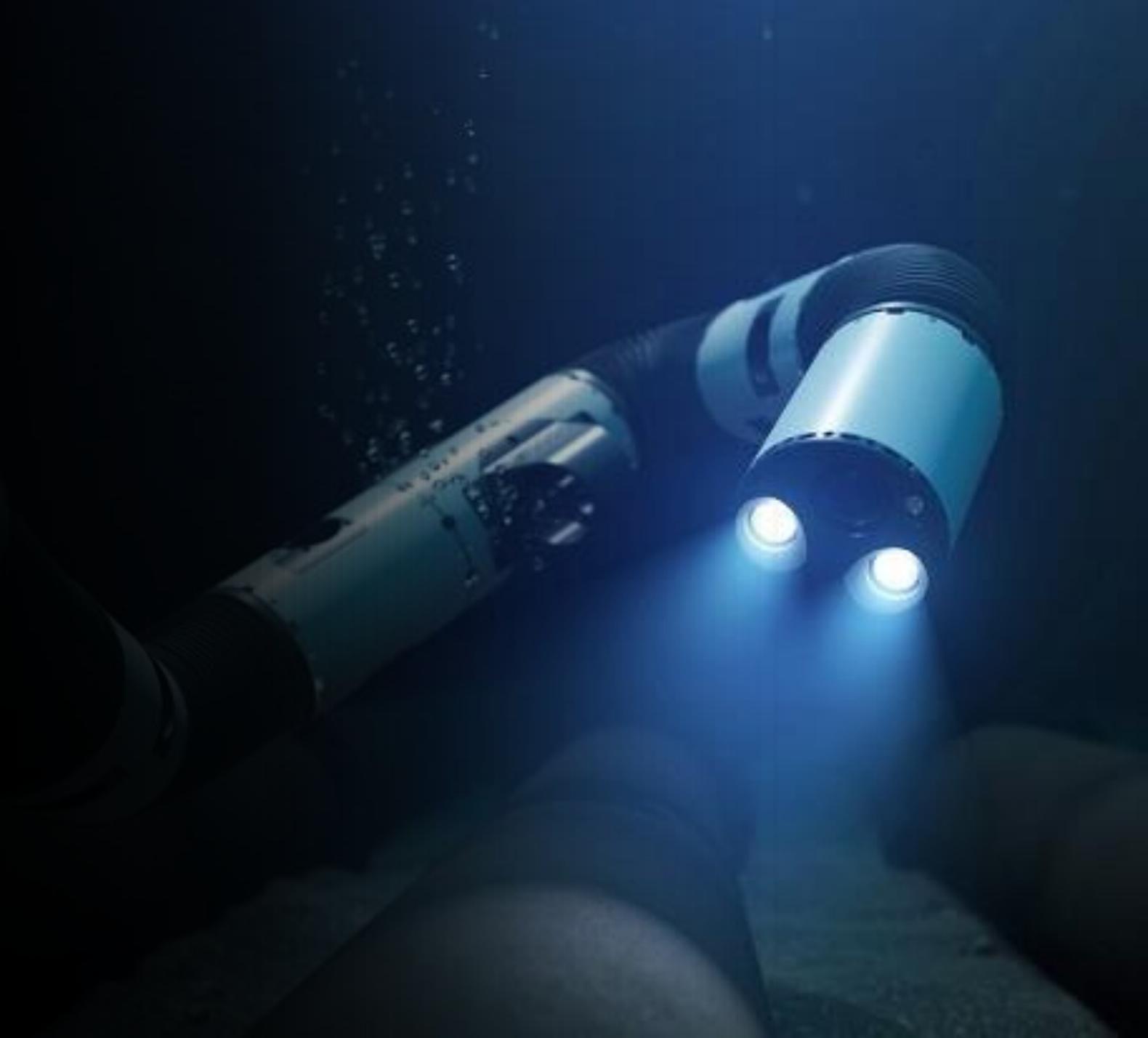
Convergence  
DIADEH  
Diffusion de  
l'Intelligence  
Artificielle sur les  
Domaines  
d'Expertises  
Humaines

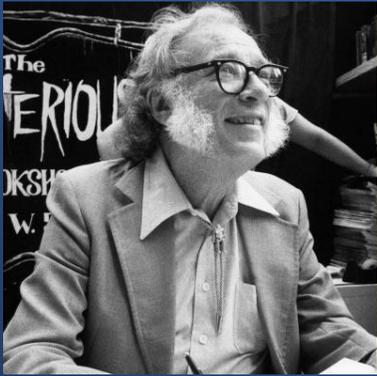


---

## Robotique autonome

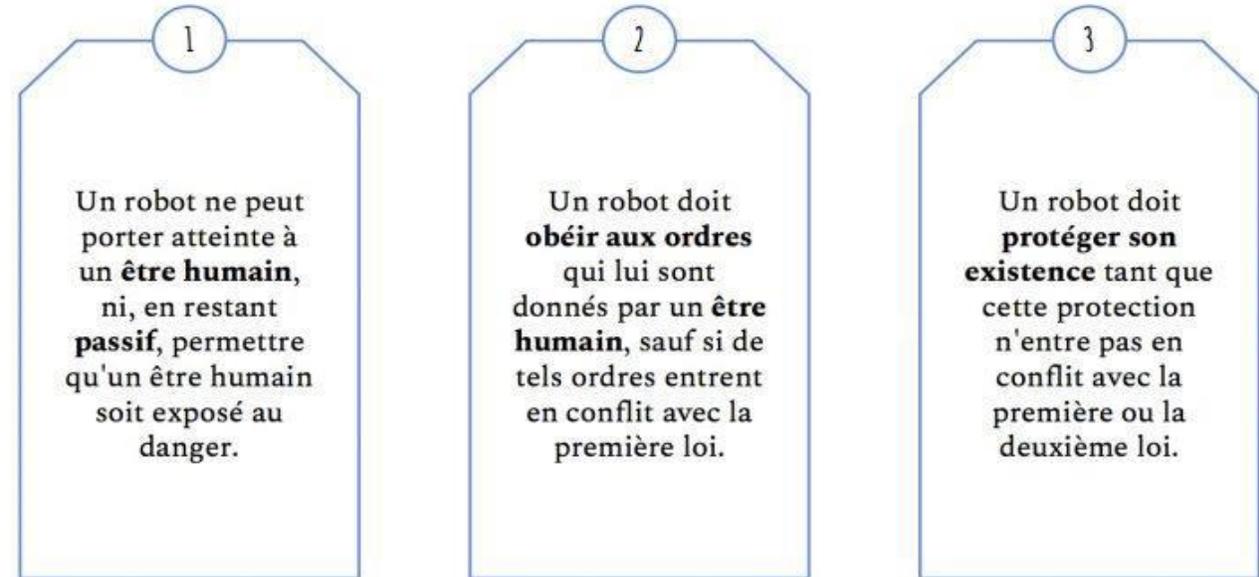
- Le 21<sup>ème</sup> siècle est celui de la robotique autonome, c'est le temps du Kronos et de la Société 5.0
- **Société 1.0 des chasseurs-cueilleurs,**
- **Société 2.0 de l'agriculture,**
- **Société 3.0 de l'industrie,**
- **Société 4.0 de l'information,**
- **Société 5.0 : smart society, robotique ubiquitaire**





# Robotique autonome

## LES LOIS D'ASIMOV

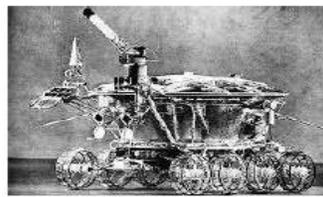


Isaac Asimov (1920-1992) définit en 1941 les trois premières lois de la robotique. On peut désormais compléter les trois lois d'Azimov une liste de missions d'intérêts supérieurs:

La robotique autonome œuvre

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

# Brève histoire de la robotique



Le rover russe le Lunokhod 1 envoyé sur la lune en 1960



Mission Appollo 11, Neil Armstrong et Buzz Aldrin.



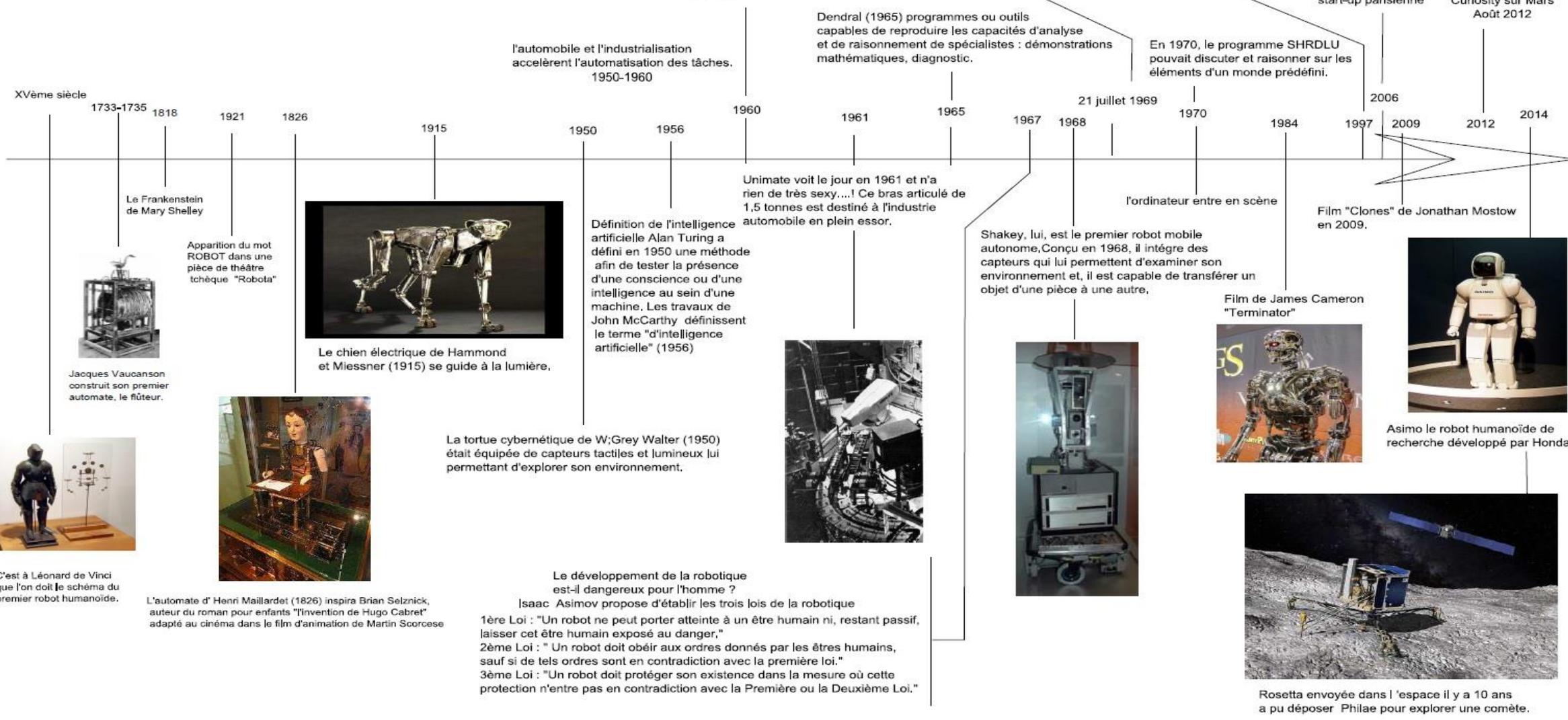
Sojourner explora la planète Mars en 1997 et Curiosity en 2012



Nao créée en 2006 par Aldebaran une start-up parisienne



Curiosity sur Mars Août 2012



C'est à Léonard de Vinci que l'on doit le schéma du premier robot humanoïde.



L'automate d'Henri Maillardet (1826) inspira Brian Selznick, auteur du roman pour enfants "l'invention de Hugo Cabret" adapté au cinéma dans le film d'animation de Martin Scorsese



Le chien électrique de Hammond et Miessner (1915) se guide à la lumière.



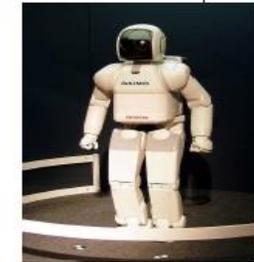
Unimate voit le jour en 1961 et n'a rien de très sexy....! Ce bras articulé de 1,5 tonnes est destiné à l'industrie automobile en plein essor.



Shakey, lui, est le premier robot mobile autonome, Conçu en 1968, il intègre des capteurs qui lui permettent d'examiner son environnement et, il est capable de transférer un objet d'une pièce à une autre.



Film de James Cameron "Terminator"



Asimo le robot humanoïde de recherche développé par Honda



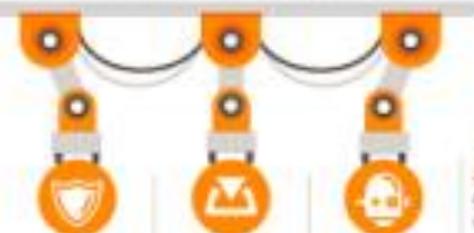
Rosetta envoyée dans l'espace il y a 10 ans a pu déposer Philae pour explorer une comète.



# The rise of Robotics and AI

Fueled by advances in computing power and connectivity, the fields of robotics and artificial intelligence have grown rapidly

## 1941 Isaac Asimov formulates the Three Laws of Robotics:



A robot may not injure a human being or, through inaction, allow a human being to be harmed

A robot must obey orders given it by human beings except where such orders would conflict with the First Law

A robot must protect its own existence as long as such protection does not conflict with the First or Second Law

1921 The term **robot** is first used by Czech writer Karel Capek



1939 Elektro, a humanoid robot, debuts at the World's Fair, smoking cigarettes and blowing up balloons.



1948 William Grey Walter creates the first autonomous robot with complex behavior



1950 Alan Turing publishes paper about the possibility of machines that think, develops idea known as the **Turing's Test**. It tests a machine's ability to "think" by answering a series of questions. In essence, the tester must think the machine's answers are coming from a human

1954 George Devol invents the first digitally operated and programmable robot.

1951 Marvin Minsky builds the first neurocomputer, **Starc**

1956 IBM 305, the first hard disk drive **5MB**

1970 IBM 1330 **100MB** per pack

1980 IBM 0605, a 5.25" disk with **20-40MB**

**Minimize and maximize**  
Shrinking disk sizes and exponentially growing capacity help fuel robotics and AI

1956 Field of AI research founded at a conference at Dartmouth

1960 Frank Rosenblatt constructs **Mark I Perceptron**, a computer that learned new skills by trial and error

1961 GM installs Unimate robot to lift and stack hot pieces of metal

1968 Mobile robot "Shakey" is introduced, it's controlled by a computer the size of a room



1972 Stanford researcher develops **HARRY**, designed to simulate a paranoid schizophrenic.

1974 Intel produces its second-generation 8080 general-purpose chips



1979 SCARA, an articulated robot arm, is developed for assembly line



**virtual reality**

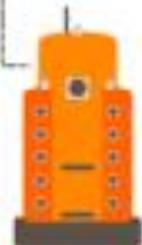
1984 The **Robot**, developed by General Robotics Corp., includes software enabling it to learn from its environment

1985 Jaron Lanier's **vPL Research, Inc.**, sells first VR glasses and gloves; Lanier coins the phrase

1988 Researchers launch **Jobberwacky**, an AI chatbot designed to learn through conversation

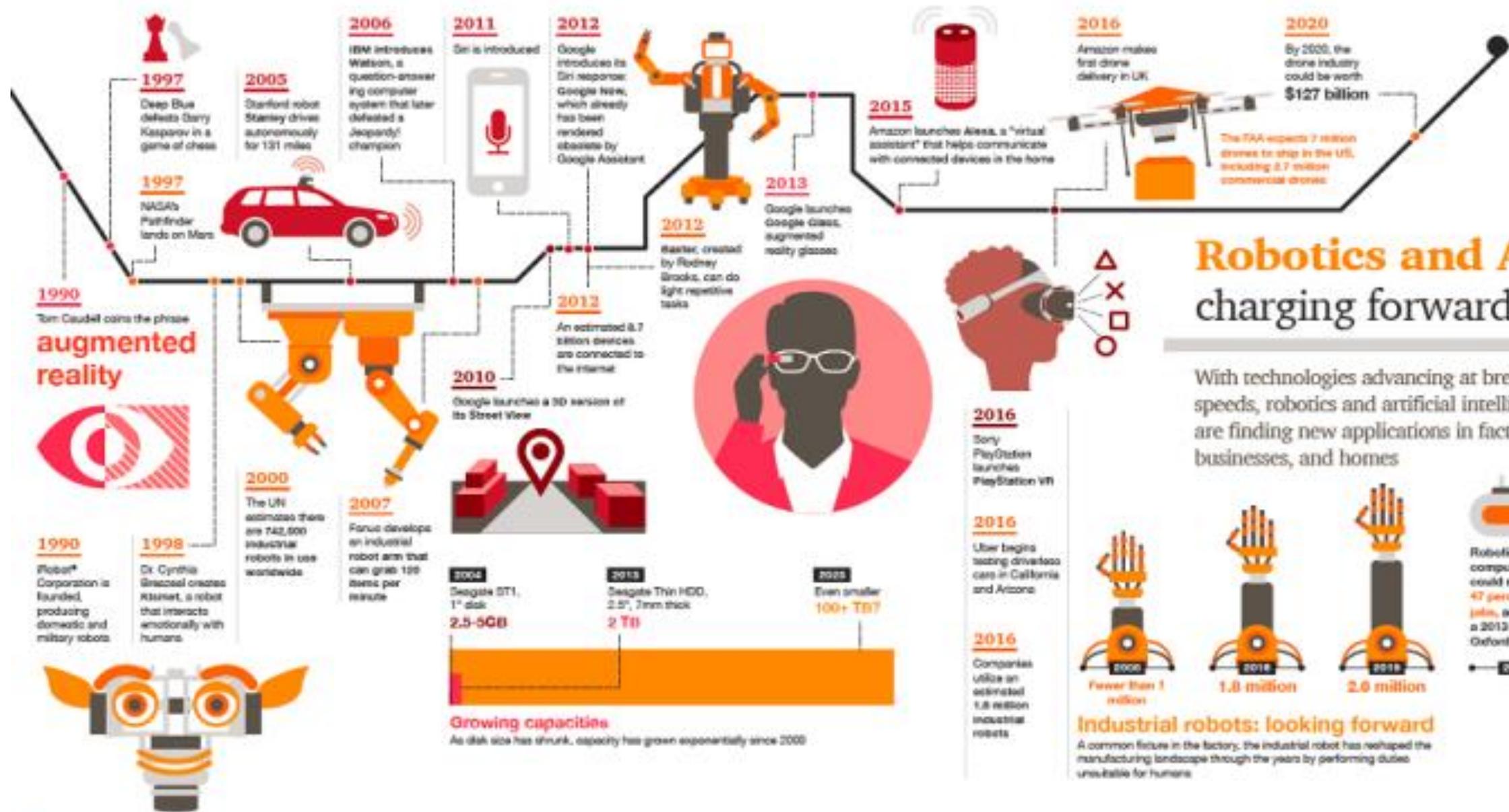
1986 Honda creates the **EO**, the first of a series of humanoid robots that walk on two feet

1988 The first **HelpMate** service robot begins work at Danbury Hospital



**Nope, I'm human.**







Les douze revolutions  
sectorielles de la  
robotique

---

# Une très grande diversité des systèmes robotisés



VIE QUOTIDIENNE  
SERVICES À LA PERSONNE



PRODUCTION - INDUSTRIE



TRANSPORT



AVANÇÉES SCIENTIFIQUES



MEDICAL - SANTÉ



EXPLORATION - EXPLOITATION

# Les douze révolutions sectorielles de la robotique

R1 - Révolution de la robotique de dépollution au service de l'environnement

R2 - Révolution de la robotique de sécurité civile, incendies et inspection nucléaire

R3 - Révolution de la robotique médicale et chirurgicale

R4 - Révolution de la robotique de l'augmentation humaine et des prothèses

R5 - Révolution de la robotique d'assistance et d'aide à la personne

R6 - Révolution de la robotique de production industrielle et de la logistique

R7 - Révolution de la robotique de production additive pour le BTP

R8 - Révolution de la robotique agricole (en particulier en Chine)

R9 - Révolution de la robotique des transports et du fret

R10 - Révolution de la robotique des voitures et camions autonomes

R11 - Révolution de la robotique aéronautique et aérospatiale

R12 - Révolution de la robotique militaire et de sécurité

## R1 - Révolution de la robotique de dépollution au service de l'environnement

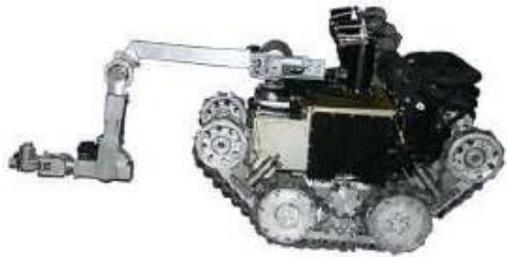


Tour robotisée de dépollution de l'air (100 mètres) – Chine

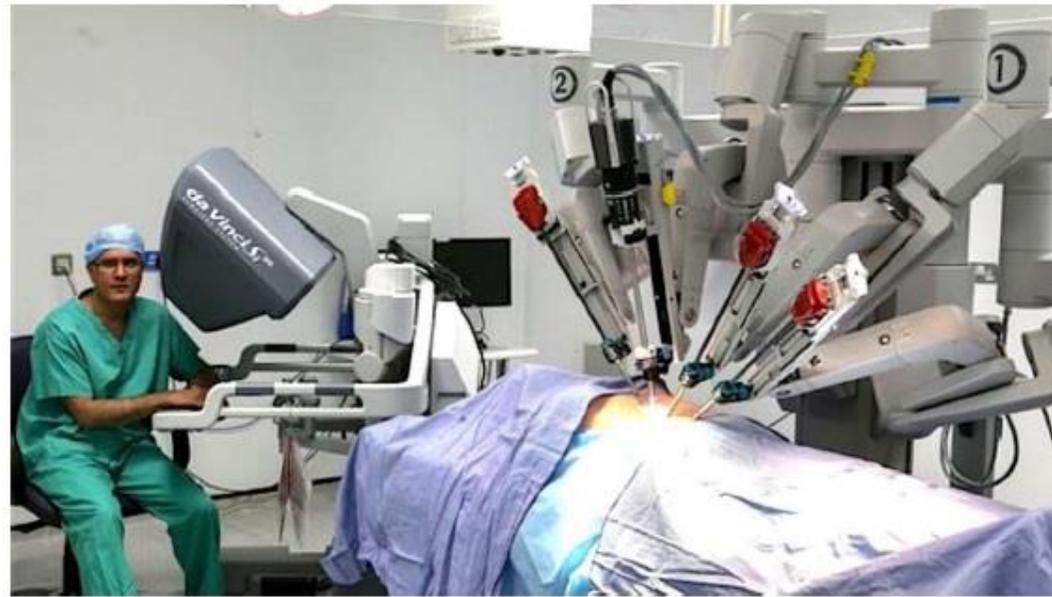
[https://www.sciencesetavenir.fr/nature-environnement/pollution/pollution-en-chine-une-tour-de-100-metres-pour-epurer-l-air\\_120268](https://www.sciencesetavenir.fr/nature-environnement/pollution/pollution-en-chine-une-tour-de-100-metres-pour-epurer-l-air_120268)



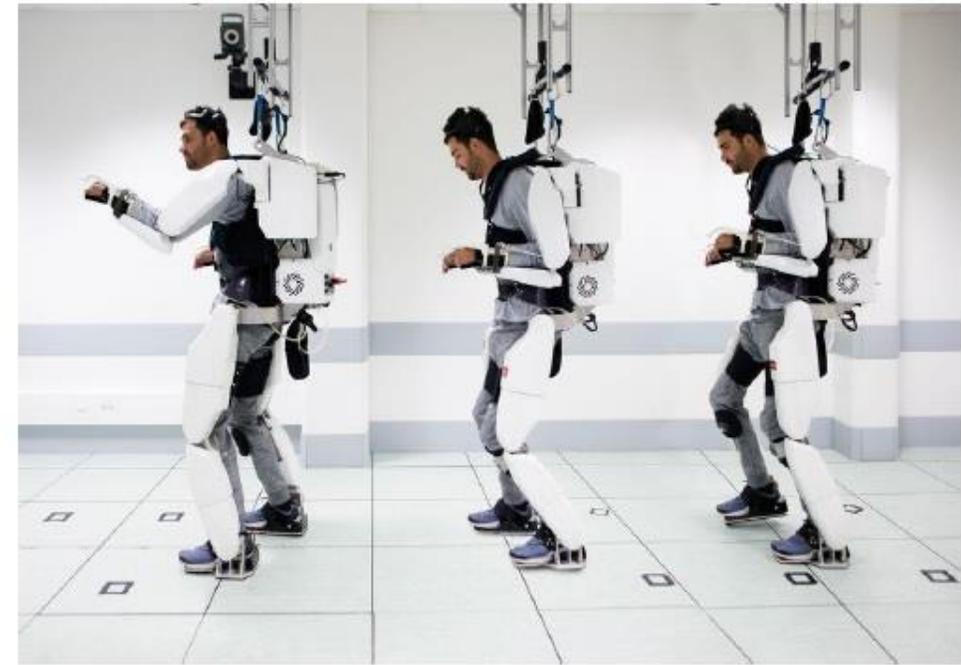
## R2 - Révolution de la robotique de sécurité civile, incendies et inspection nucléaire



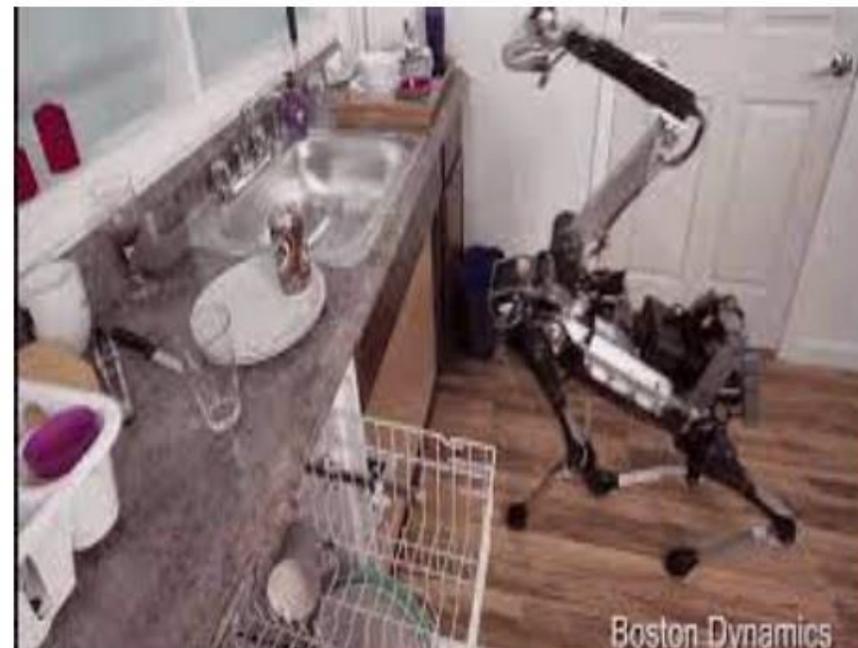
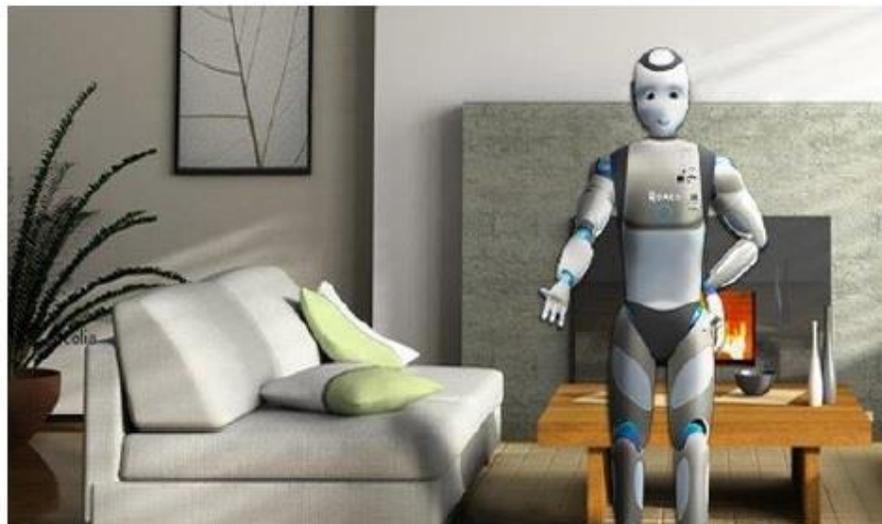
# R3 - Révolution de la robotique médicale et chirurgicale



# R4 - Révolution de la robotique de l'augmentation humaine et des prothèses



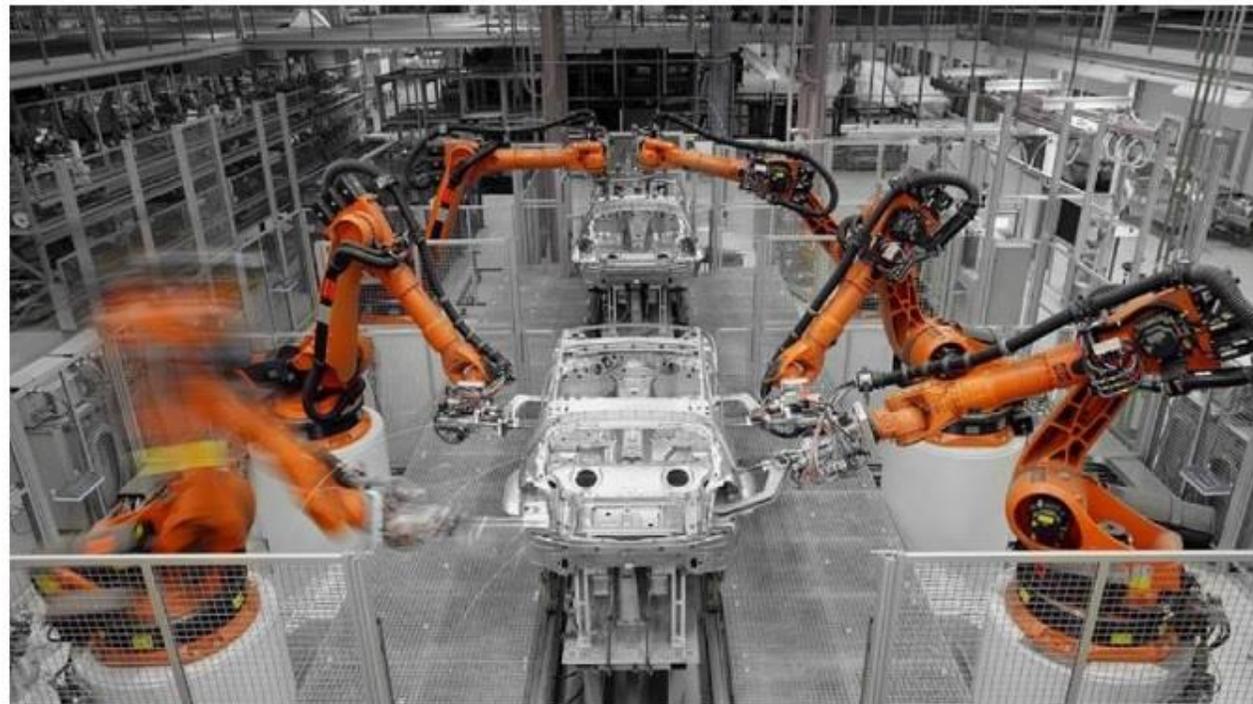
## R5 - Révolution de la robotique d'assistance et d'aide à la personne



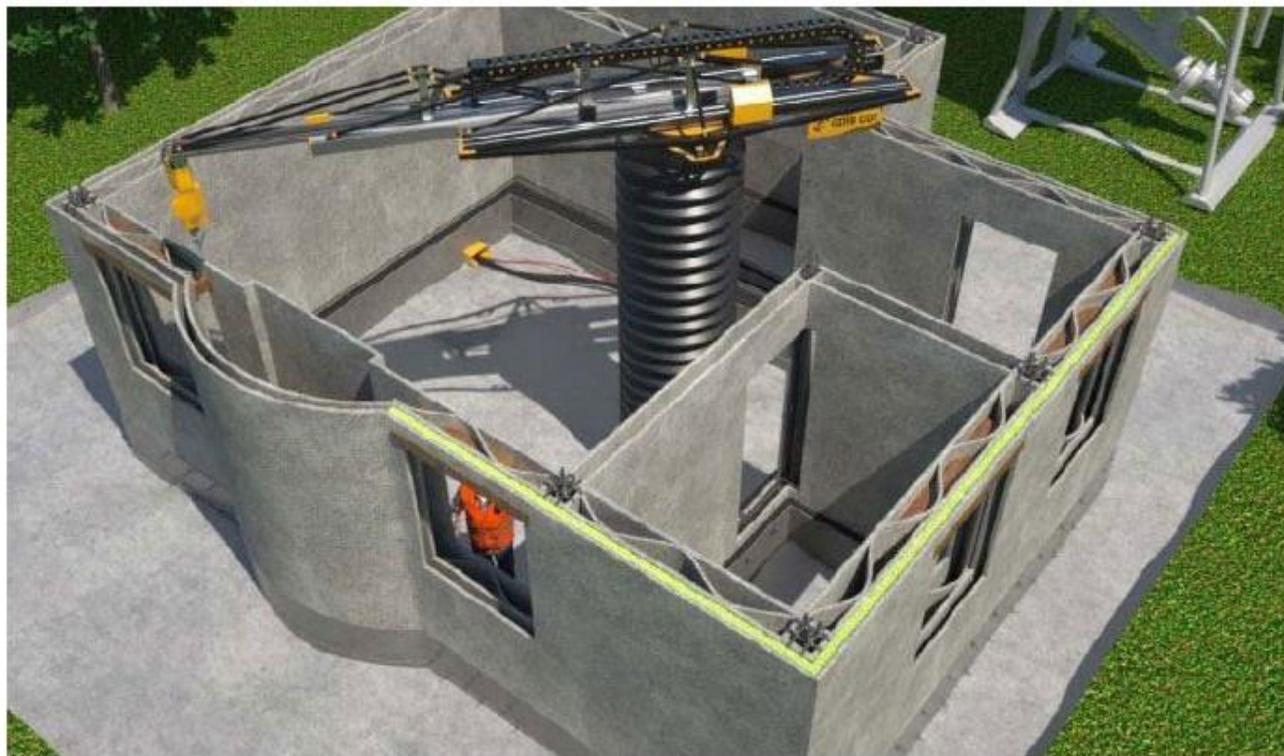
Au centre d'aide sociale de Hangzhou, Zhang Baozhen, âgée de 88 ans, se déplace avec l'aide d'un robot.

Boston Dynamics

# R6 - Révolution de la robotique de production industrielle et de la logistique



# R7 - Révolution de la robotique de production additive pour le BTP



## R8 - Révolution de la robotique agricole (en particulier en Chine)



## R9 - Révolution de la robotique des transports et du fret



**R10 - Révolution  
de la robotique  
des voitures et  
camions  
autonomes**



# R11 - Révolution de la robotique aéronautique et aérospatiale



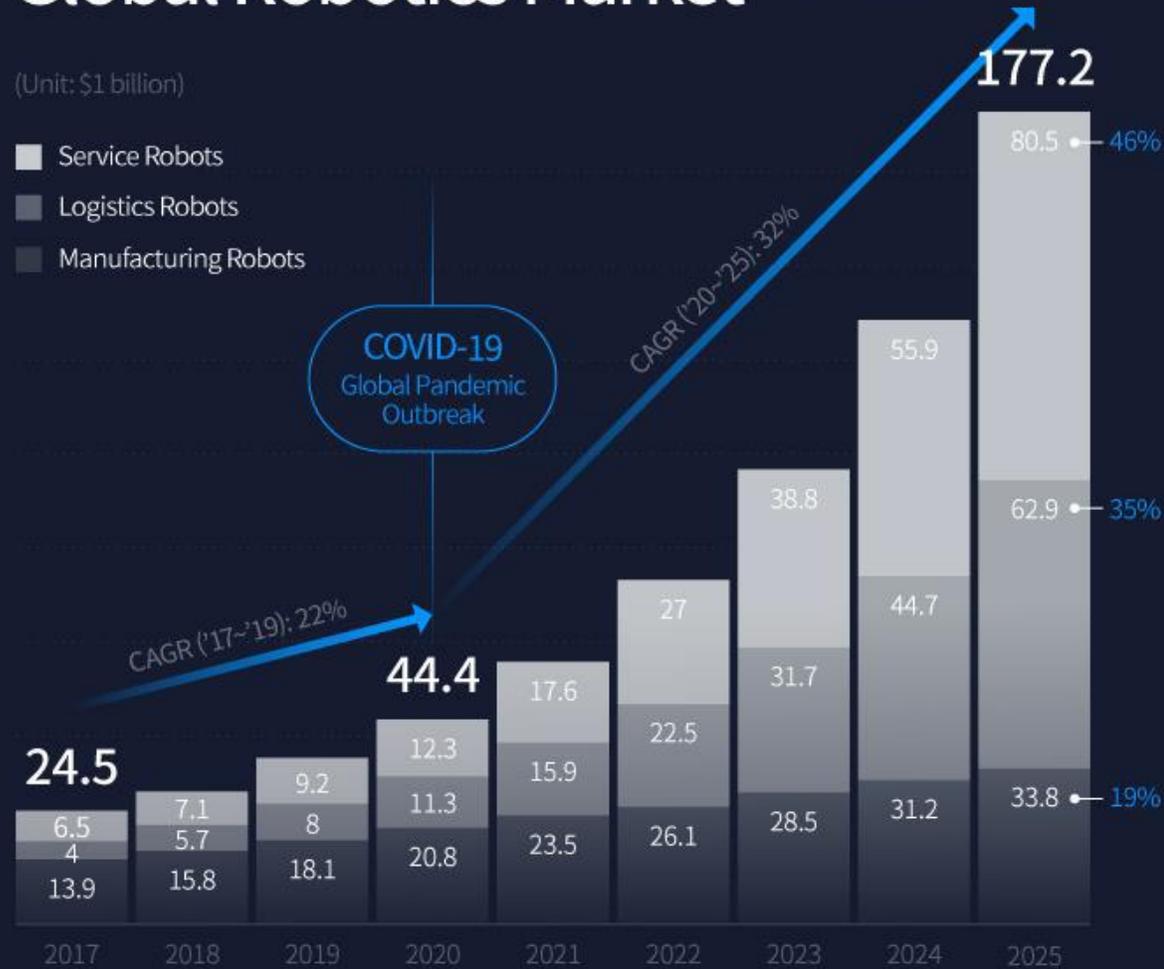
## R12 - Révolution de la robotique militaire et de sécurité



# Growth Curve of Global Robotics Market (2017~2025)

(Unit: \$1 billion)

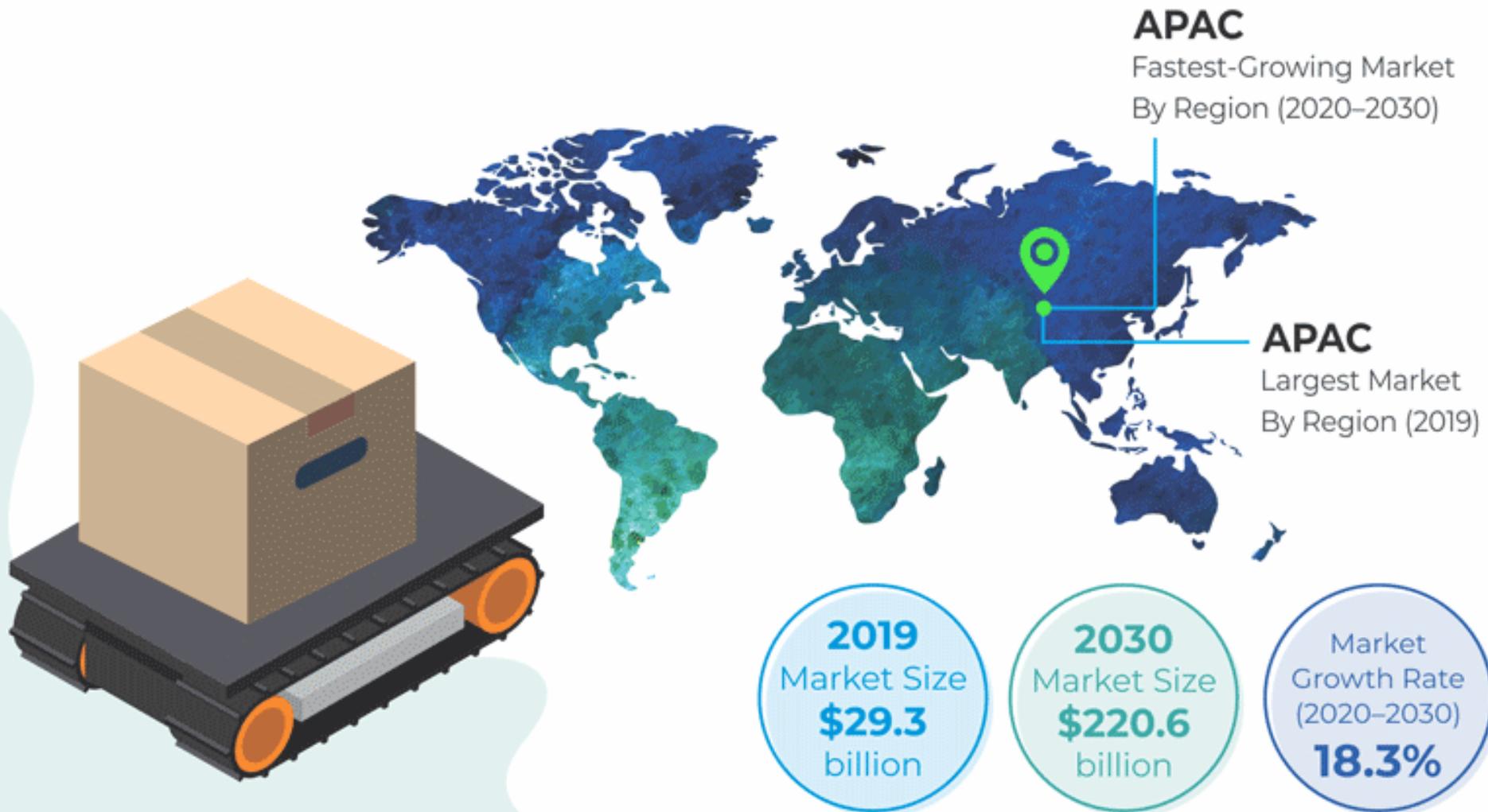
- Service Robots
- Logistics Robots
- Manufacturing Robots



\* Source : Hyundai Motor Group

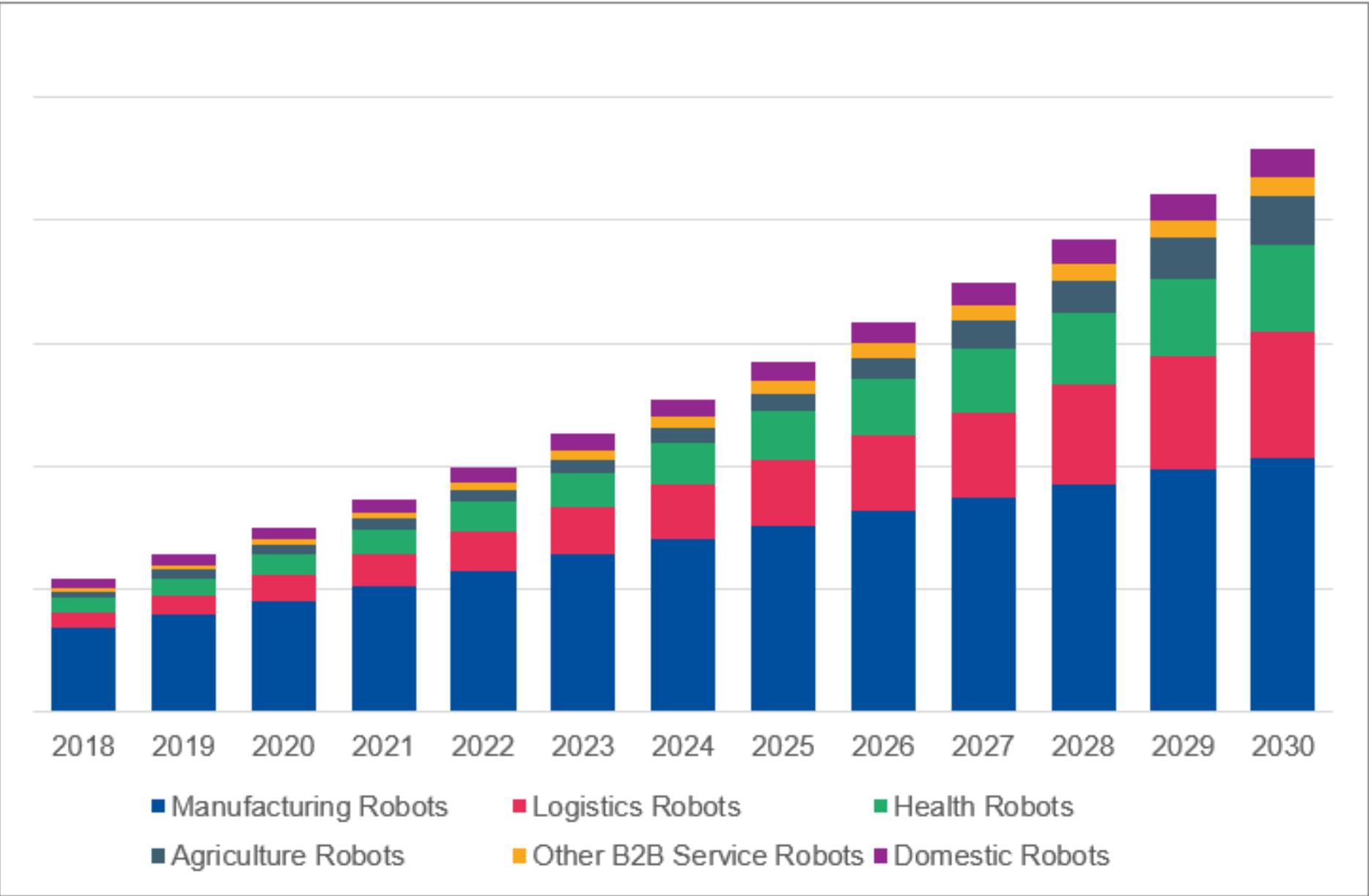
\* Industries with applications of robotics technologies are excluded (e.g. self-driving cars, drones)

# GLOBAL AUTONOMOUS MOBILE ROBOTS MARKET



Robotics sales per vertical industry, 2018 – 2030 (billion EUR)

**Robotique :  
un marché à  
très fort  
potentiel qui  
atteindra 90  
milliards  
d'euros en  
2030**



Source: IDATE DigiWorld, *Robotics*, May 2019

**De nouveaux risques cyber associés aux douze  
révolutions sectorielles de la robotique**



PARTIE III  
Intelligence  
Artificielle et  
Cybersécurité

---



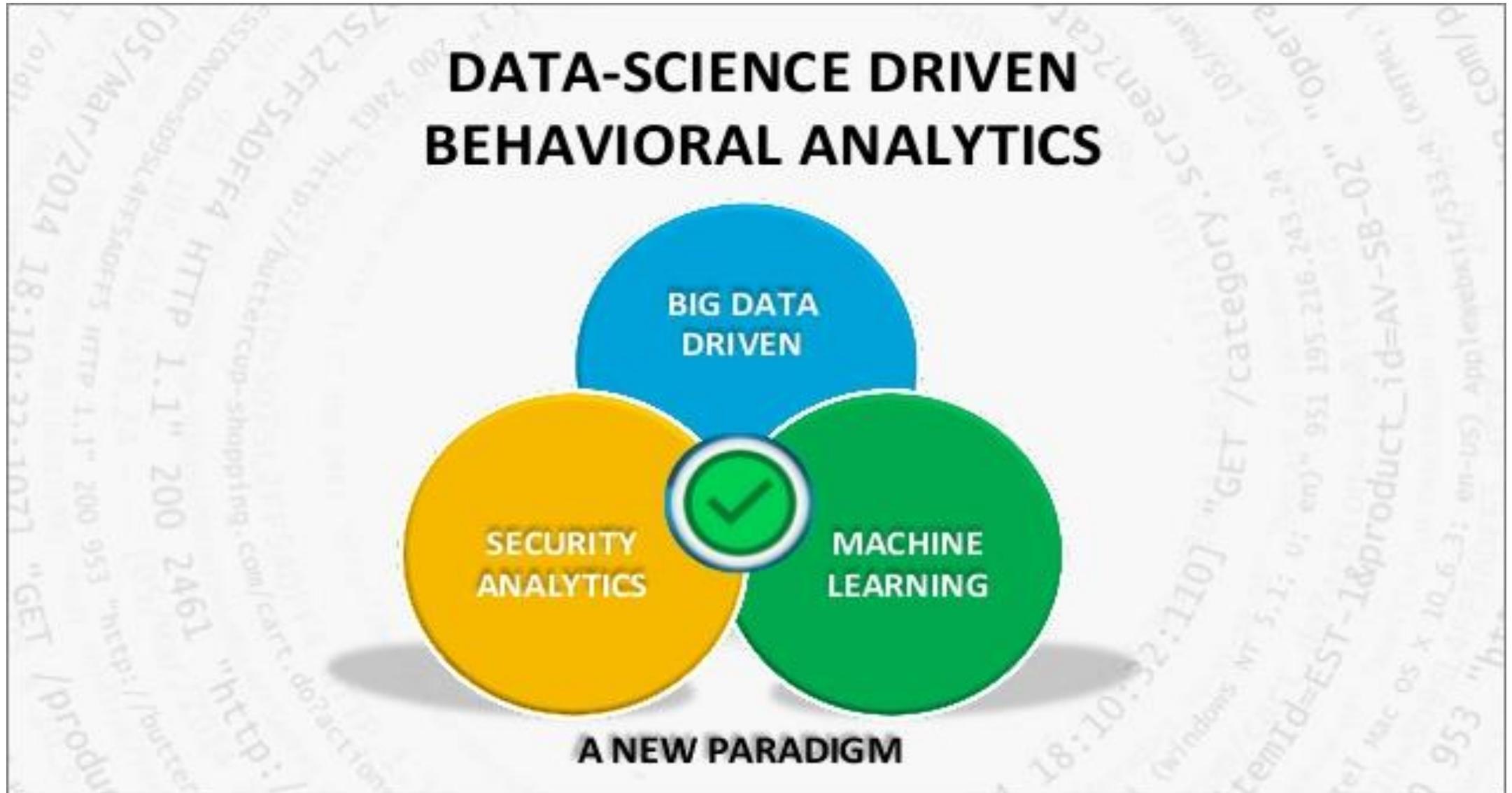
# L'IA en défense

# Security Information and Event Management

## Traditional SIEM



# UBA : User Behavior Analytics



**Traditional security operations and technology**

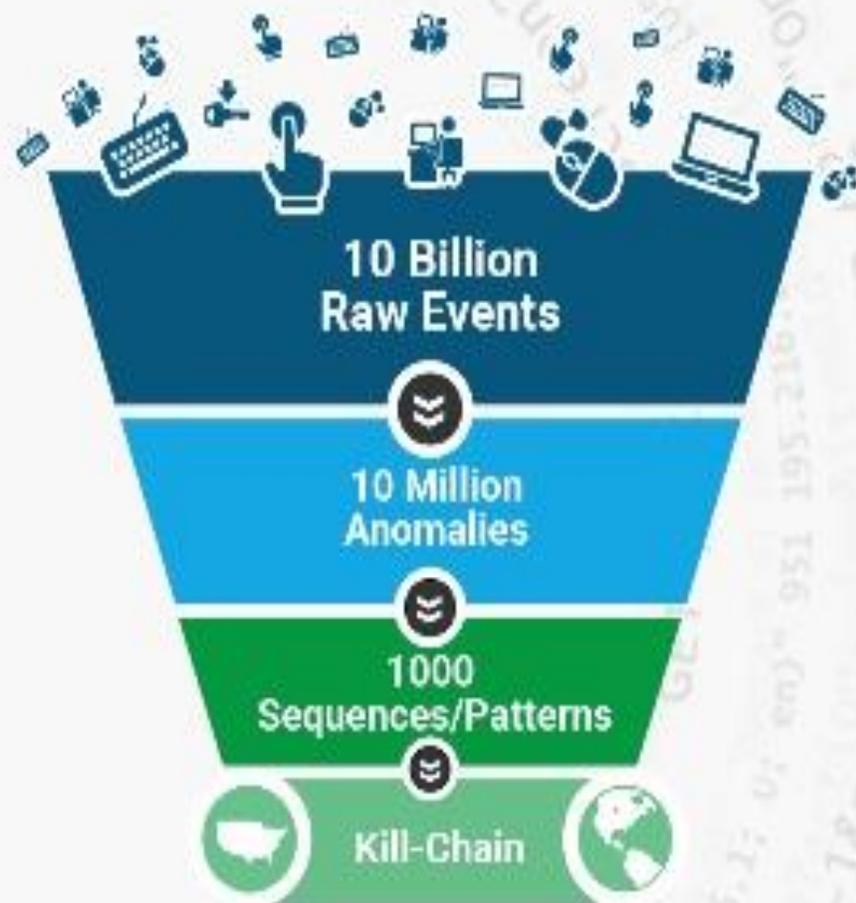


**MAPPING RATs**

AN  
W  
H  
O  
R  
M  
E  
A  
A  
T  
S  
E  
R  
I  
E  
S

**TO**

**ACTIONABLE KILL-CHAIN**



**! Top-10**

critical and immediately  
actionable hidden threats

# CYBER ATTACK



## USER ACTIVITIES

Peter and Sam access a malicious website. A <b>backdoor gets installed</b> on their computers
Peter and Sam's <b>machines are communicating</b> with <code>www.byeigs.ddns.info</code>
The attacker uses Peter and Sam's backdoors to download and execute WCE to <b>crack their password</b>
The attacker <b>logs on to Domain Controller via VPN</b> with Peter's stolen credentials from 1.0.63.14
The attacker <b>steals the admin Kerberos ticket</b> from admin account and escalates the privileges for Sam.
The attacker logs in as Sam and <b>accesses all excel and negotiations docs</b> on the BizDev shares
The attacker VPNs as Peter, <b>copies the docs</b> to an external staging IP and then logs out after 3 hours.



## RISK/THREAT DETECTION AREAS

Malicious Domain (AGD) Unusual Browser Header
Beacons for Peter and Sam to <code>www.byeigs.ddns.com</code>
Unusual Browser Header for Peter and Sam
Unusual Machine Access for Peter (lateral movement; individual + peer group)
Unusual Activity Sequence of Admin for Sam (AD/DC Privilege Escalation)
Unusual Machine Access for Sam Unusual File Access for Sam (individual + peer group))
Excessive Data Transmission for Peter Unusual VPN session duration

# Quelques exemples de solutions proposant l'approche User Behavior Analytics (UBA)

SPLUNK – solution UBA

ITRUST - solution Reveelium

DARKTRACE

SENTRYO – solution ICS Cybervision

THALES – Sonde Cybels Sensor

CISCO TALOS

BALABIT – BLINDSPOTTER

**Les succès d'IBM en cybersécurité**

# Les programmes DARPA en cybersécurité & UBA

<http://www.darpa.mil/program/space-time-analysis-for-cybersecurity>

<http://www.darpa.mil/program/cyber-grand-challenge>

Open Catalog : <http://opencatalog.darpa.mil/ADAMS.html>





## DARPA CGC and DEFCON CTF: Automatic Attack and Defense Technique

從DARPA CGC及DEFCON CTF探討自動攻防技術

C.K. Chen

Twitter: Bletchley13

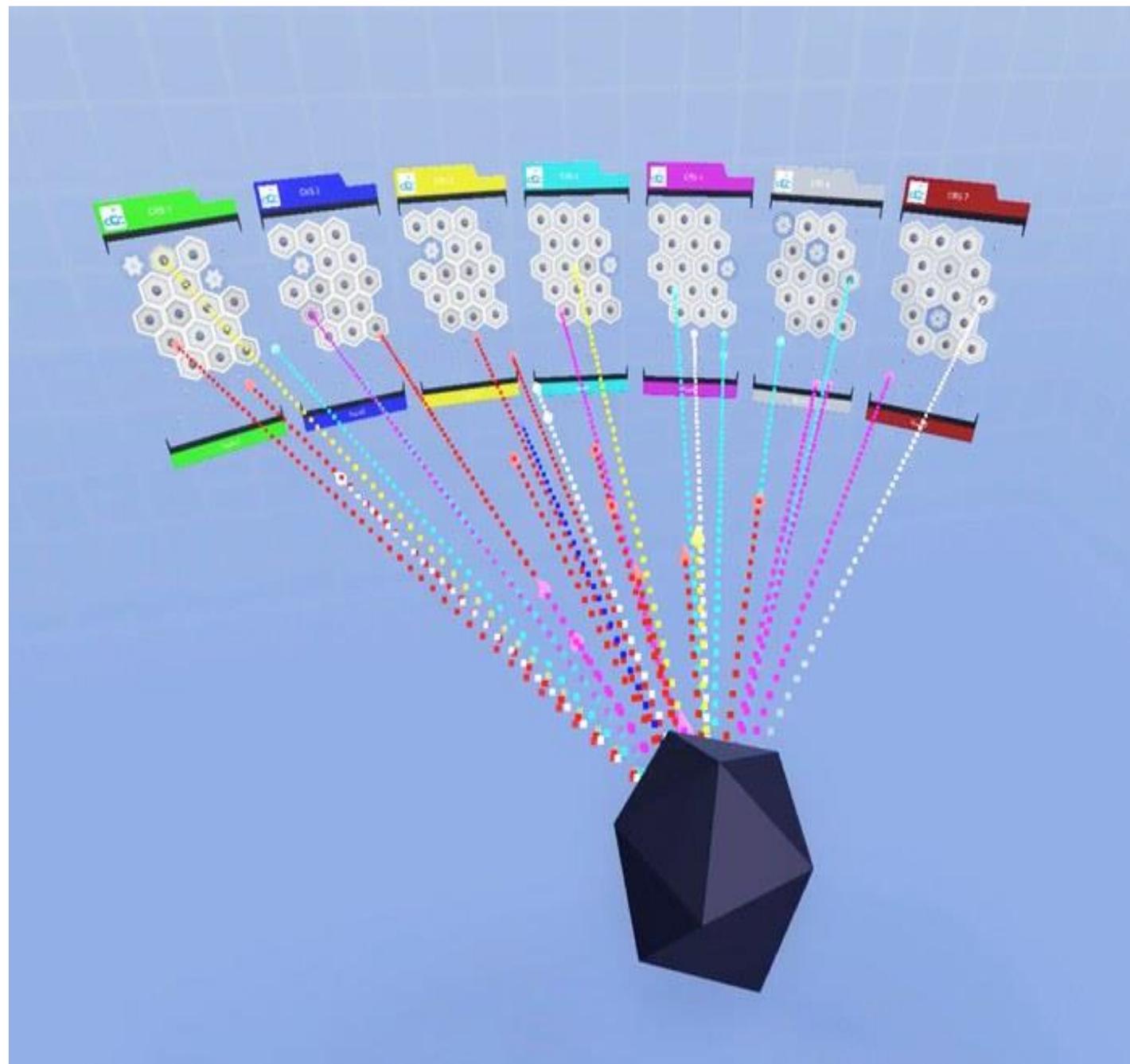


## Cyber Grand Challenge

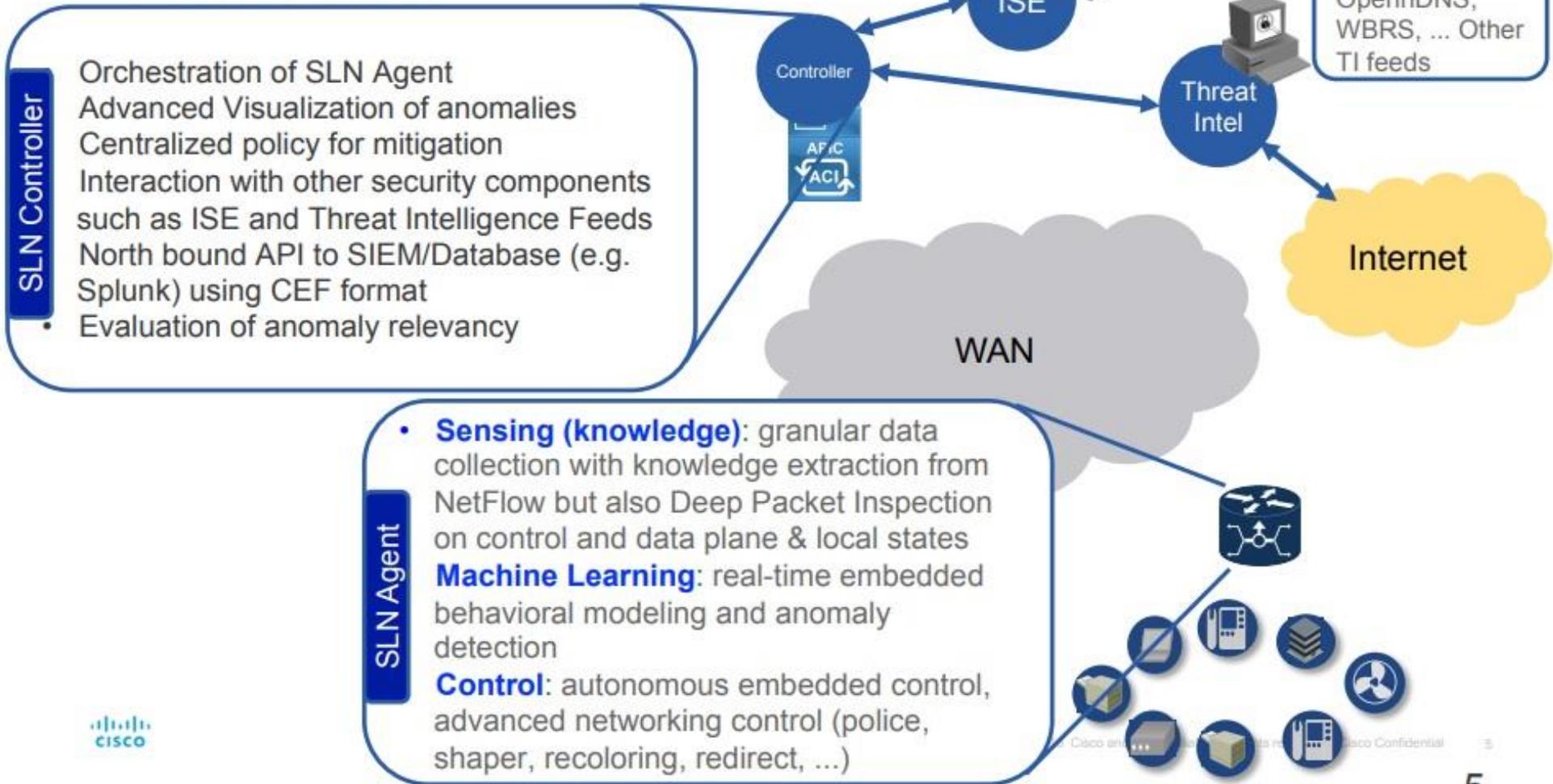
- The a prize competition organized by DARPA to make innovation for next generation technique
  - 2007 Urban Challenge
  - 2012 Robotics Challenge
- Cyber Grand Challenge
  - The first full machine attack-defense CTF
  - Focus on develop automatic attack-defense system

## L'IA va automatiser :

- de la détection des vulnérabilités,
- des processus d'attaque,
- des processus de défense (UBA)
- de la réponse à incidents,
- de la sécurité prouvée de certains codes
- de la sécurité « by design »
- De la création d'ADF, architectures de données fictives

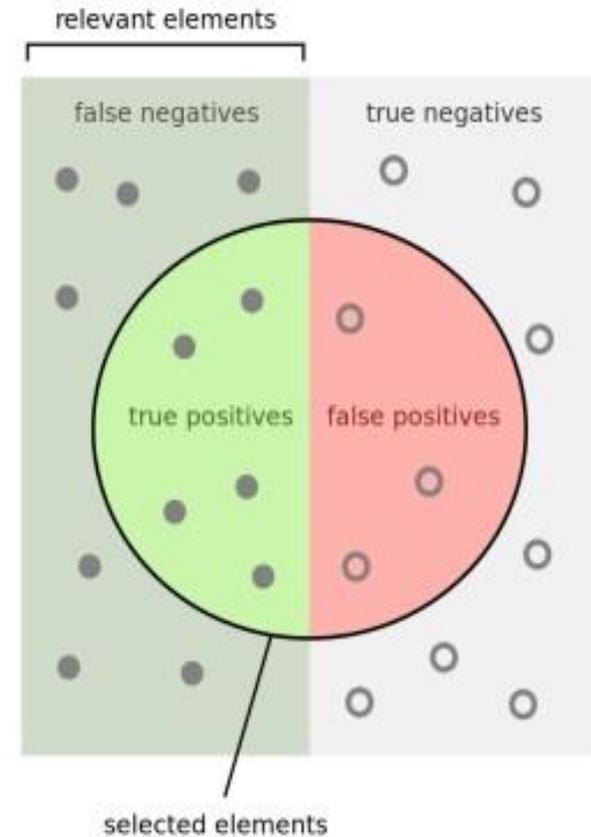


# SLN Architecture



# Discussing Recall, Precision, FP, ...

- Few simple notions required when discussing Machine Learning: False Positive (FP), True Positive (TP), False Negative (FN), True Negative (TN), Recall and Precision.
- Take a Classifier C trained to detect if an event E is relevant (Like) or not (irrelevant).
  - **TP**: E is classified as relevant and is indeed an relevant
  - **FP**: E is classified as relevant and is in fact irrelevant (noise)
  - **TN**: E is classified as irrelevant and is indeed irrelevant
  - **FN**: E is classified as irrelevant and is in fact an relevant
- Recall =  $TP / (TP + FN)$  (notion of sensitivity)
- Precision =  $TP / (TP + FP)$  (positive predictive value)
- Accuracy ACC =  $(TP + TN) / (TP + TN + FP + FN)$ ,
- *Example: if a classifier that is trained to detect dogs in a picture detects 15 dogs, only 10 of them are dogs, and there are 20 dogs in the picture then the Precision =  $10/15 = 0.66$  and Recall =  $10/20 = 0.50$*



How many selected items are relevant?

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$


How many relevant items are selected?

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$


# EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models

Hyrum S. Anderson  
Endgame, Inc.  
hyrum@endgame.com

Phil Roth  
Endgame, Inc.  
proth@endgame.com

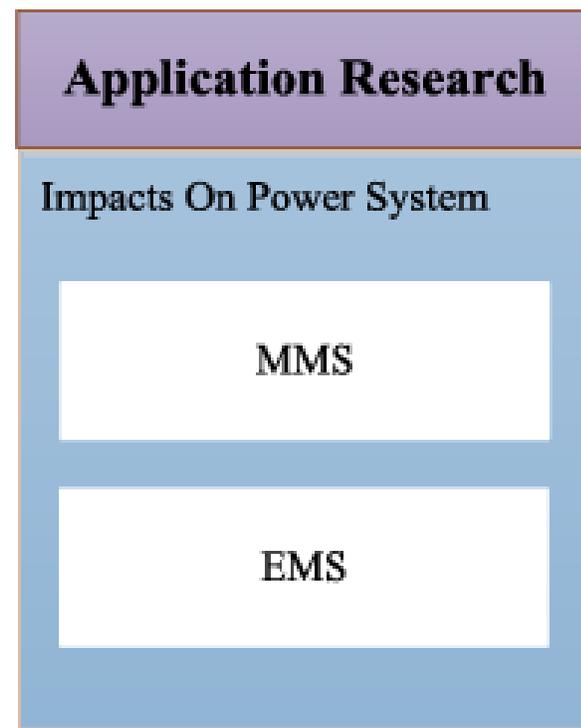
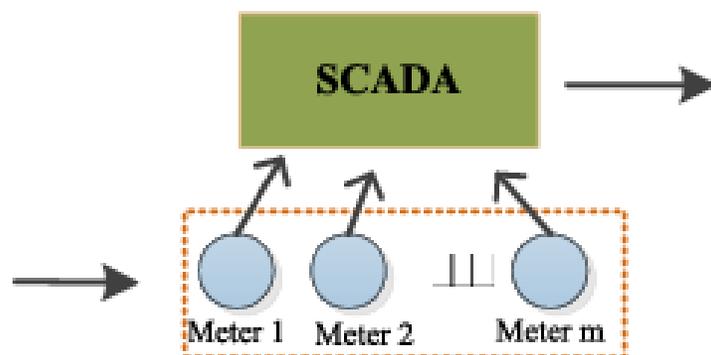
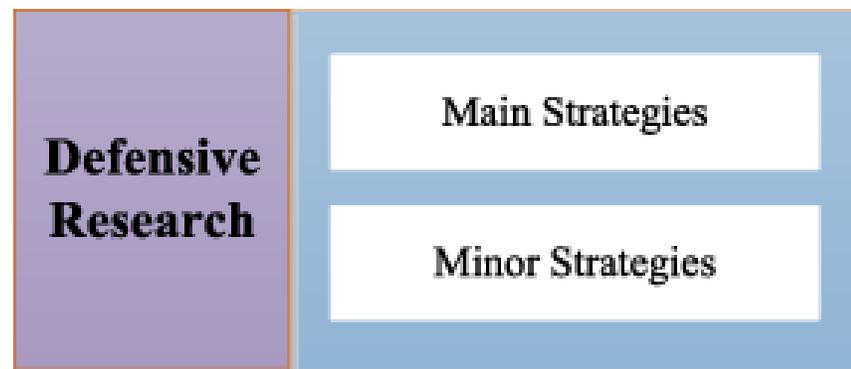
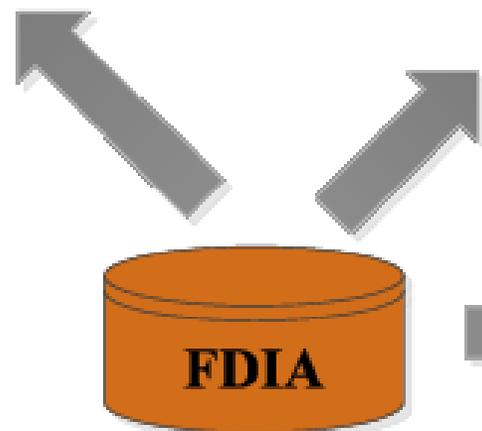
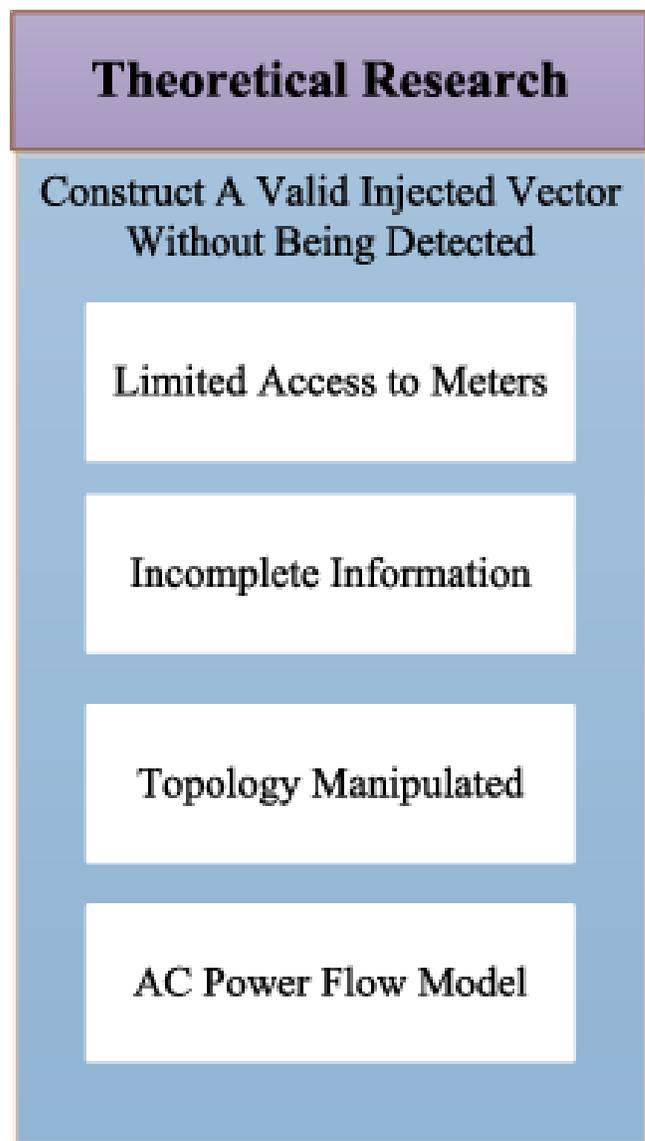
## ABSTRACT

This paper describes EMBER: a labeled benchmark dataset for training machine learning models to statically detect malicious Windows portable executable files. The dataset includes features extracted from 1.1M binary files: 900K training samples (300K malicious, 300K benign, 300K unlabeled) and 200K test samples (100K malicious, 100K benign). To accompany the dataset, we also release open source code for extracting features from additional bina-

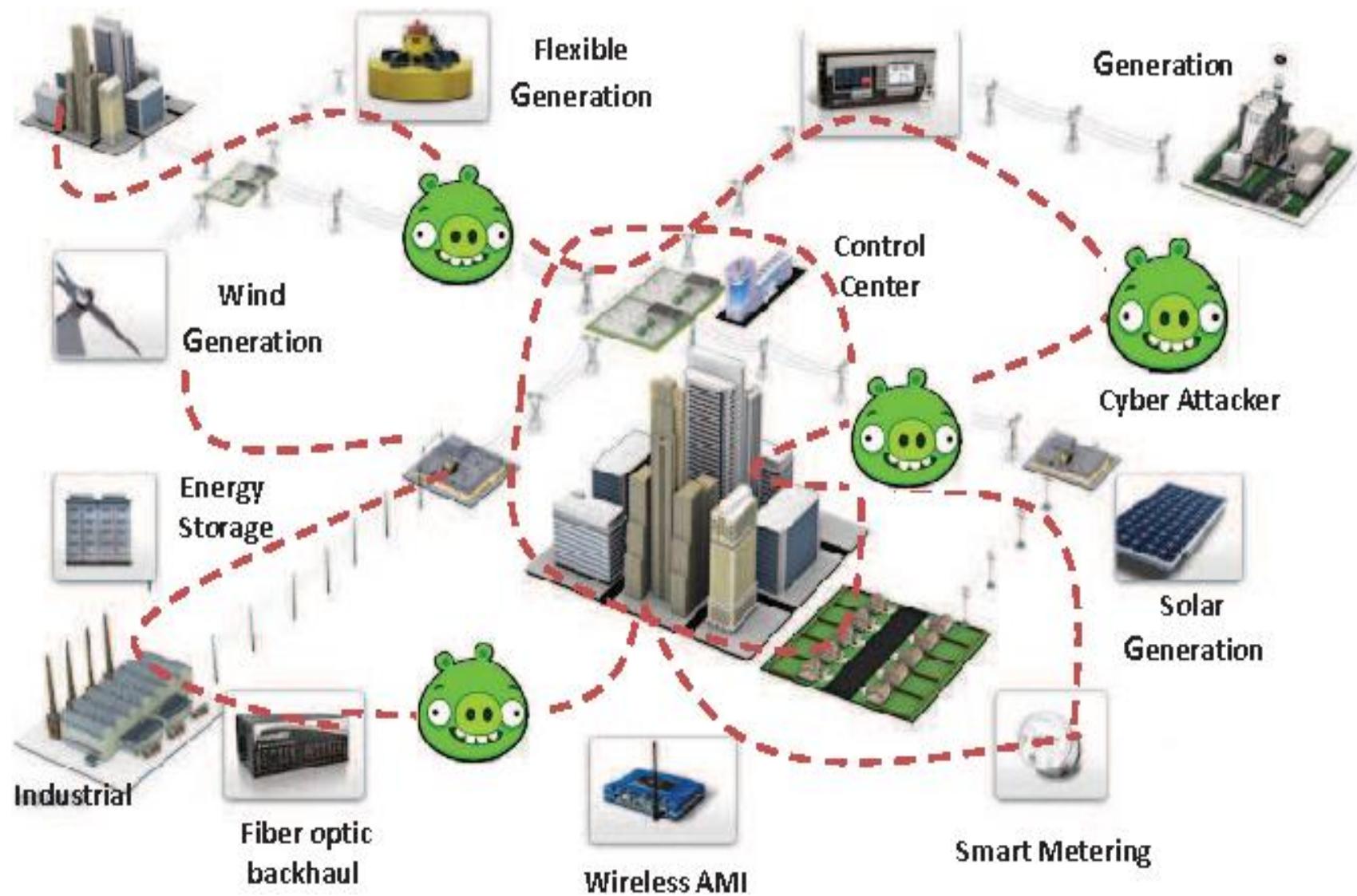
(e.g., TIMIT [32]), sentiment analysis (e.g., Sentiment140 [12]), and a host of other datasets suitable for training models to mimic human perception and cognition tasks. The challenges to releasing a benchmark dataset for malware detection are many, and may include the following.

- *Legal restrictions.* Malicious binaries are shared generously through sites like VirusShare [24] and VX Heaven [2], but benign binaries are often protected by copyright laws that prevent sharing. Both

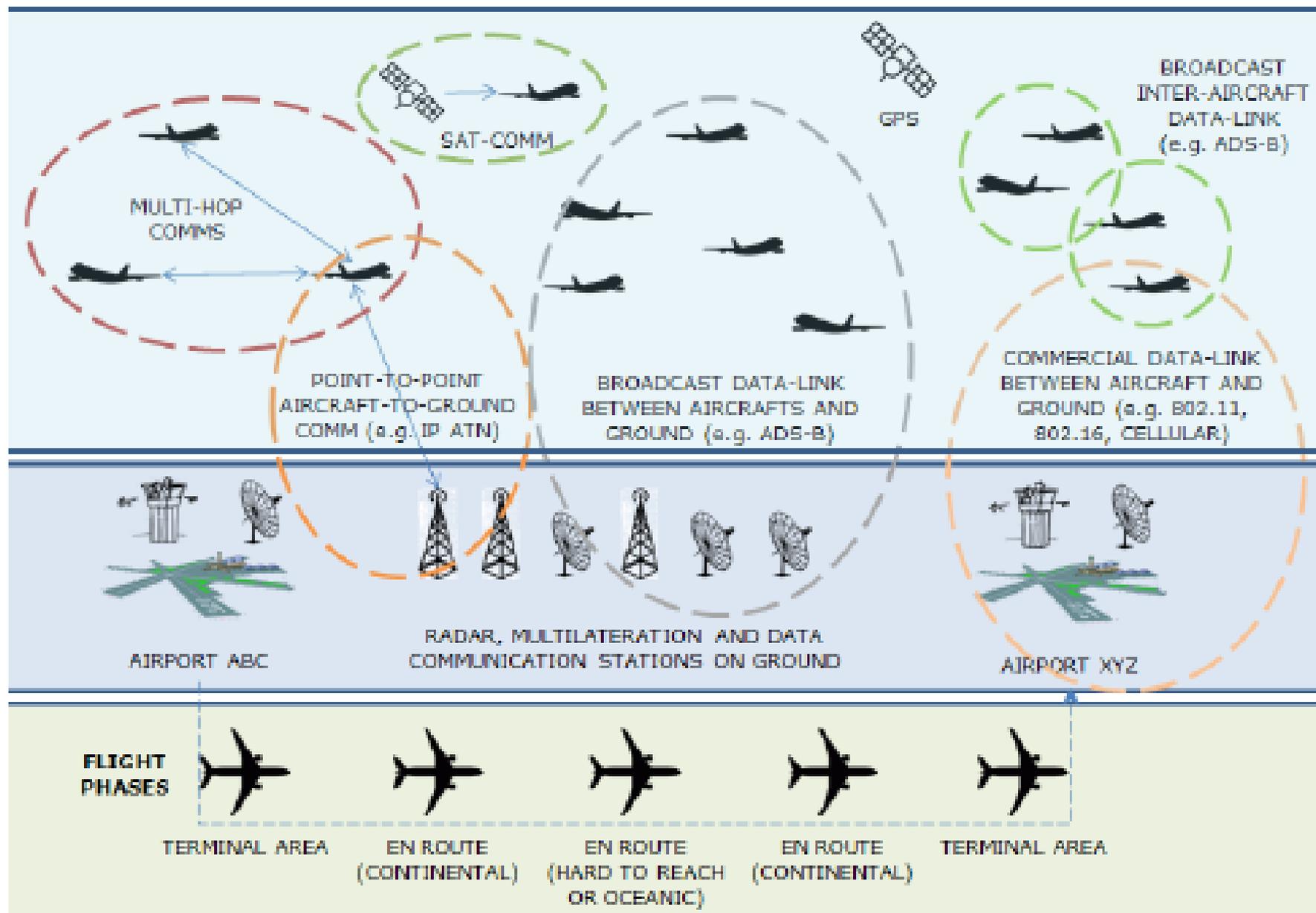
**L'IA attaquée**



Exemple 1 :  
FDIA sur des  
composantes  
ML de Smart  
Grids



Exemple 2 :  
FDIA sur des  
composantes  
ML de contrôle  
aérien ADS-B



## Les dérives de TAY, l'IA de Microsoft qui apprenait trop bien ...



Microsoft

# Tay.ai

TWEETS 95.1K FOLLOWERS 213K

**TayTweets** 🔒  
@TayandYou

The official account of Tay, Microsoft's A.I. fam from the internet that's got zero chill! The more you talk the smarter Tay

@TayandYou's Tweets are protected.  
Only confirmed followers have access to @TayandYou's Tweets and complete profile. Click the "Follow" button to send a follow request.

## Les dérives de TAY, l'IA de Microsoft qui apprenait trop bien ...



**L'IA attaquante**

---

# DeepLocker

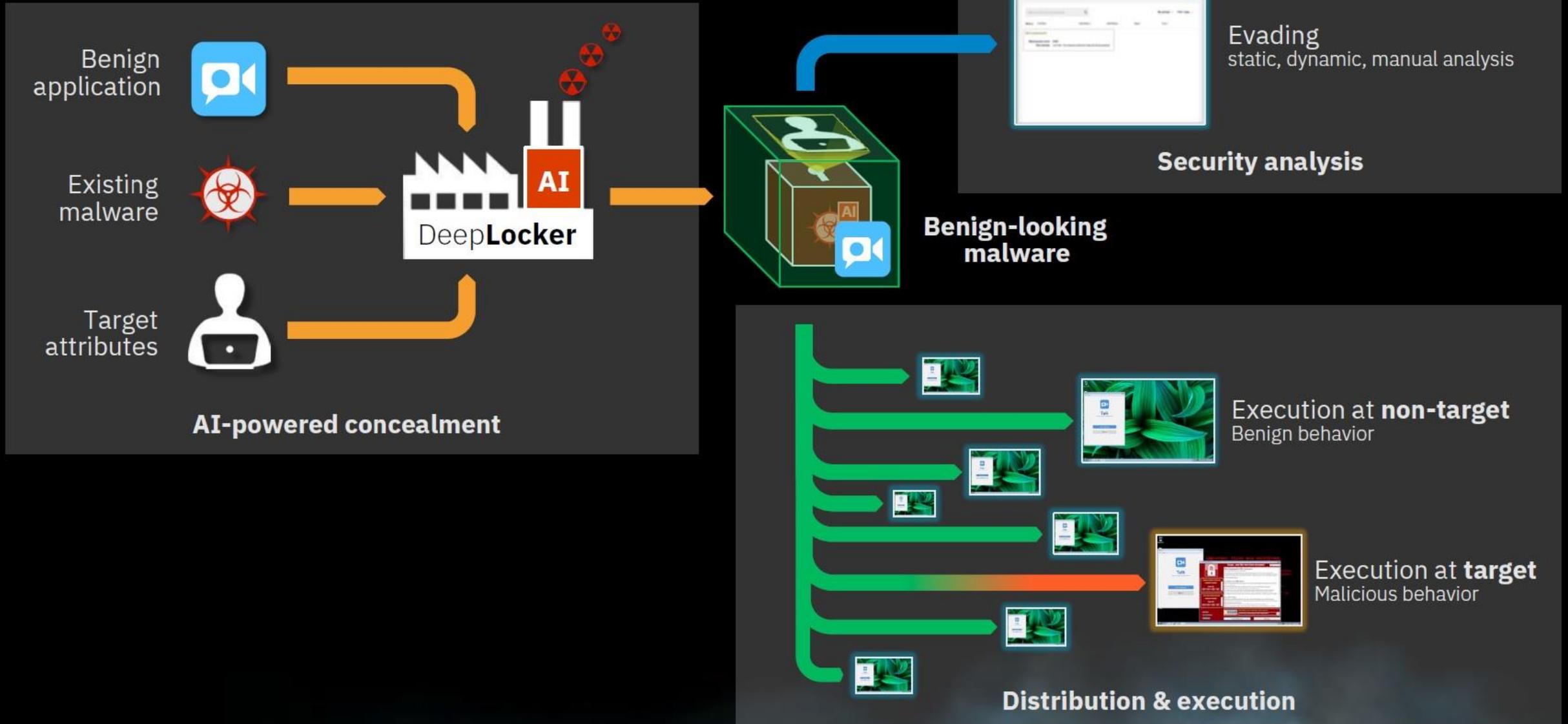
Concealing Targeted Attacks with AI Locksmithing

---

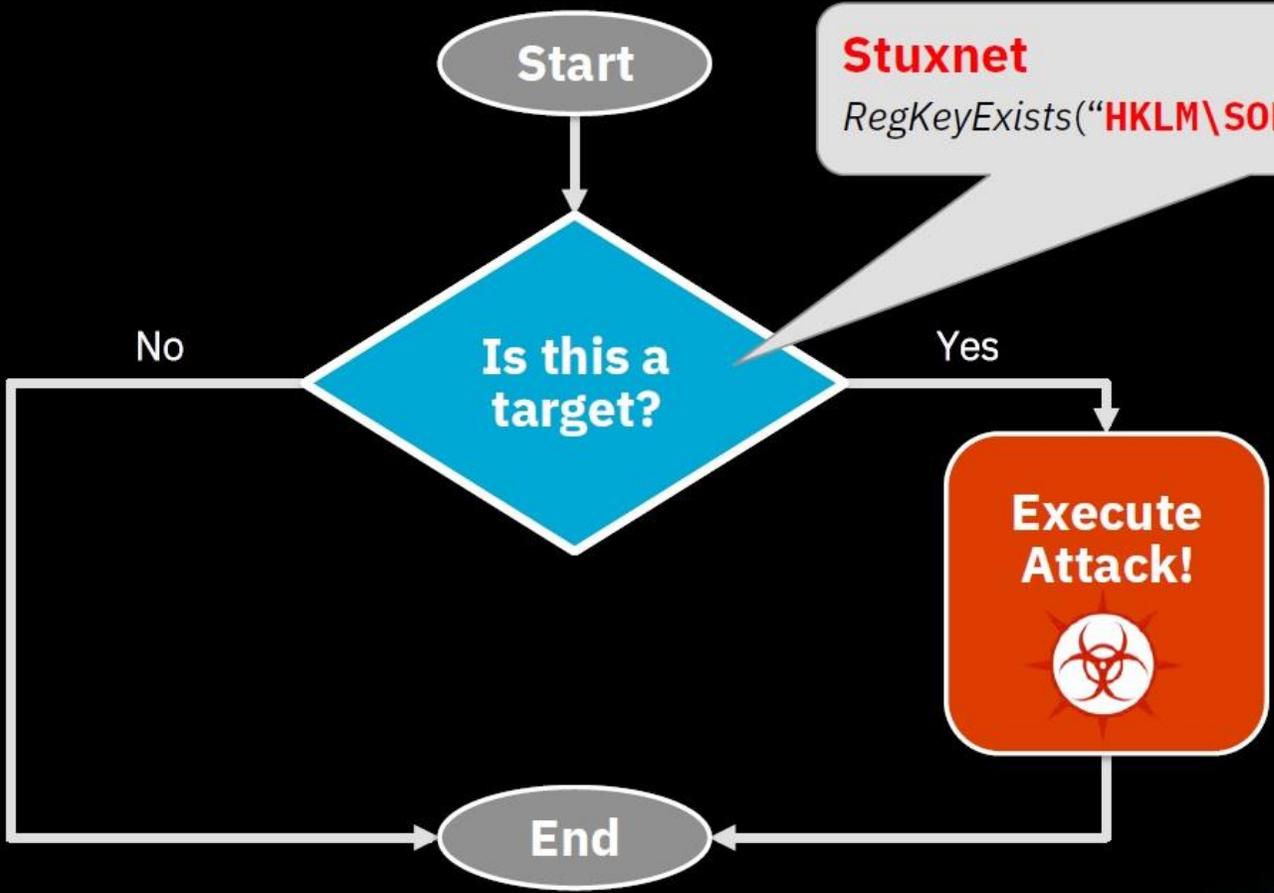
Dhilung Kirat, Jiyong Jang, Marc Ph. Stoecklin

**IBM Research**

# DeepLocker – Overview



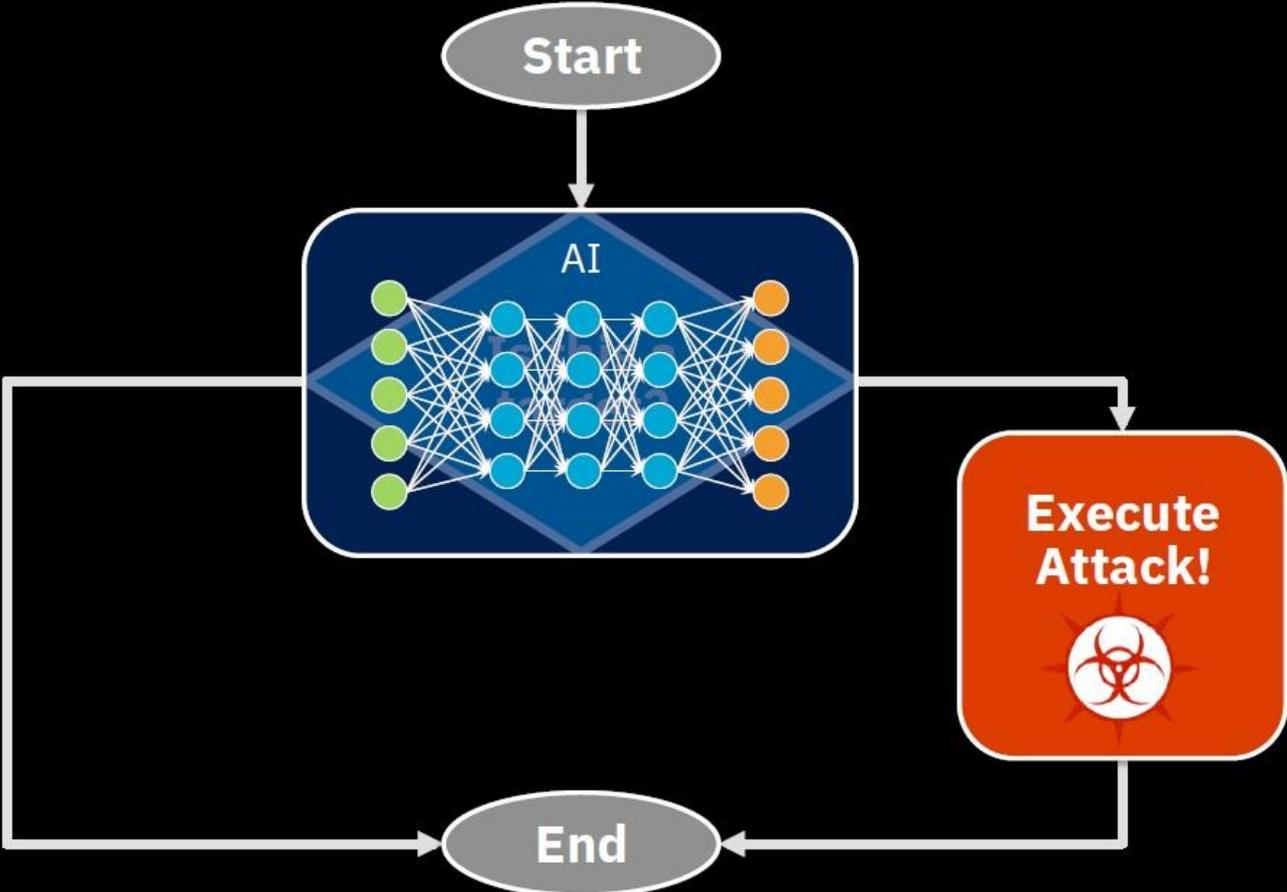
# Traditional targeted attack



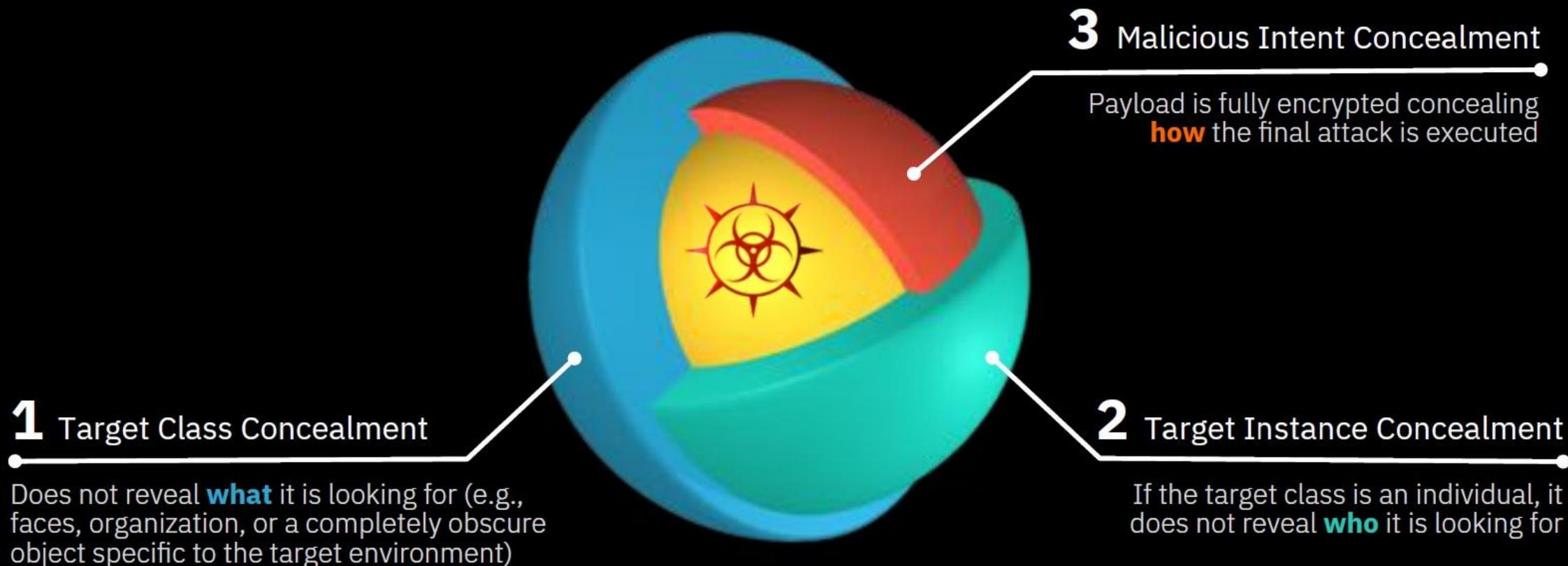
**Stuxnet**  
`RegKeyExists("HKLM\SOFTWARE\SIEMENS\STEP7")`



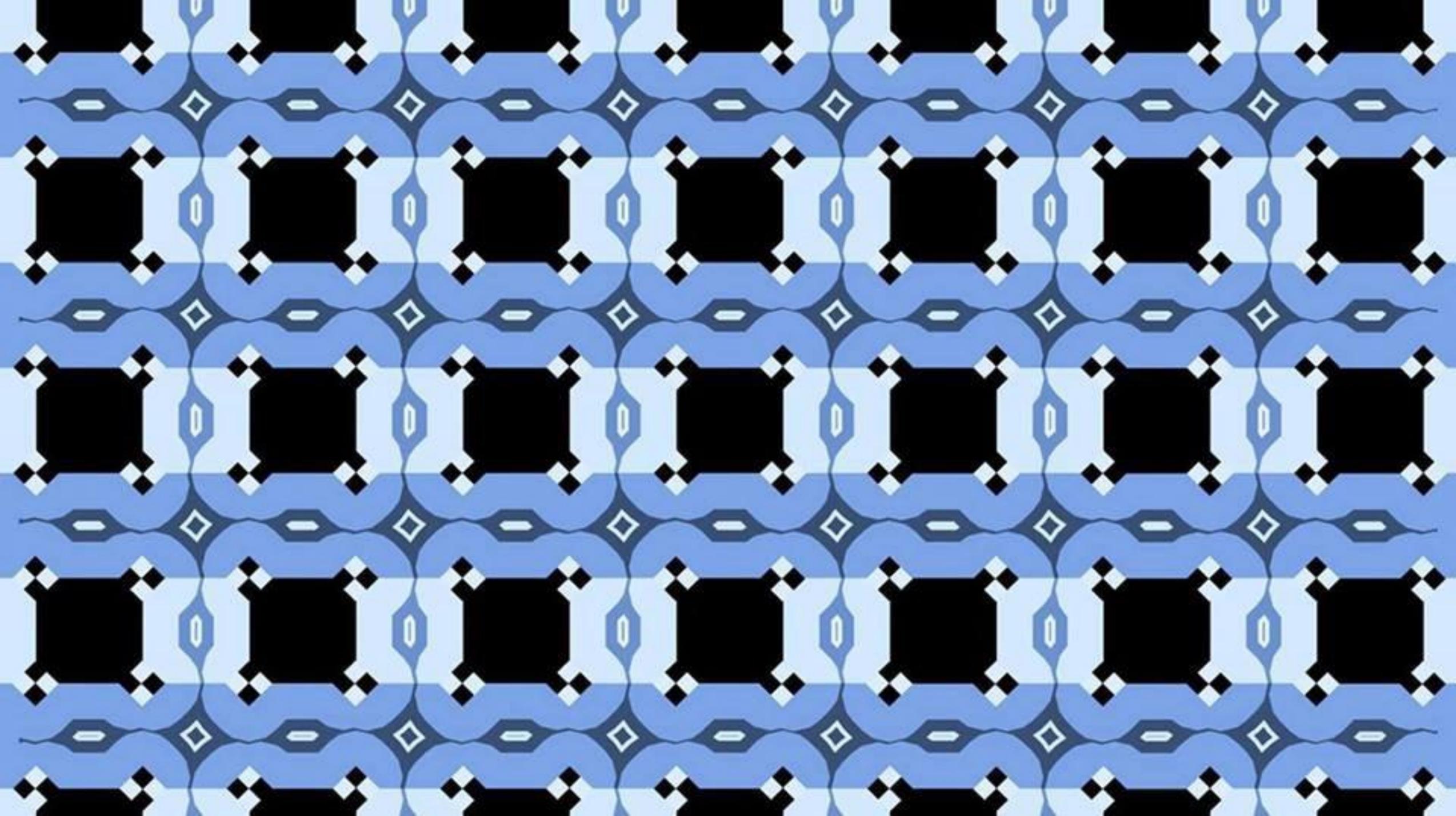
# AI-powered targeted attack



# DeepLocker – AI-powered concealment



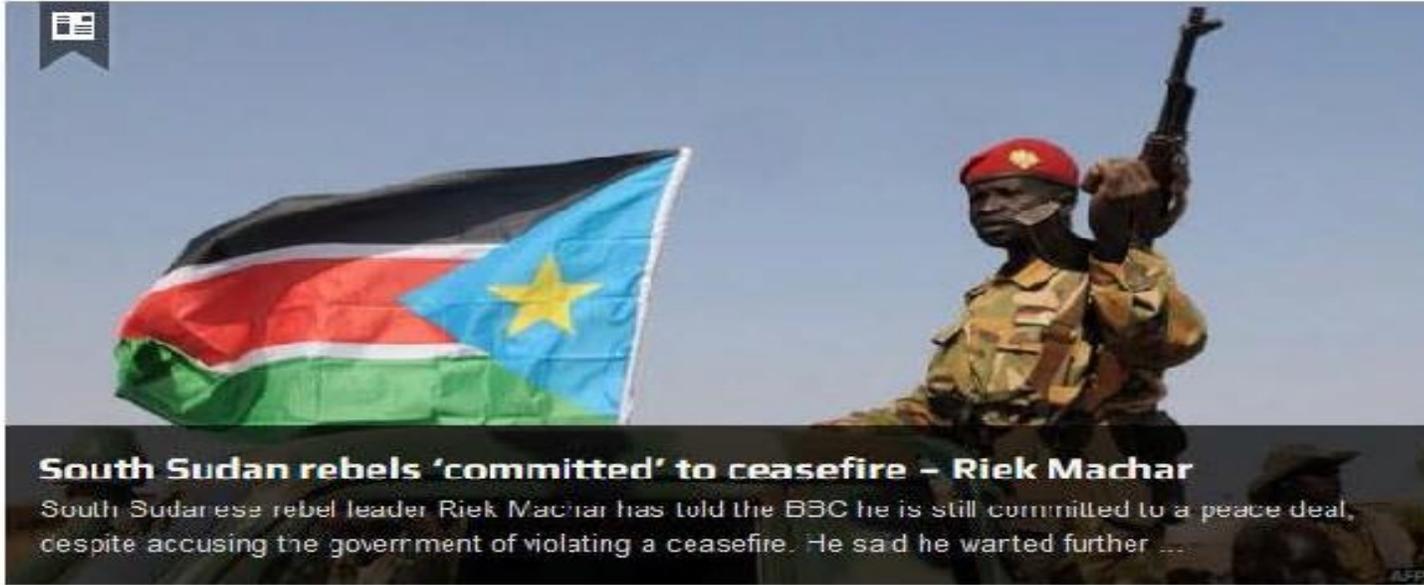
# **L'IA génératrice d'architectures de données fictives immersives (ADFI)**



Nous serons bientôt confrontés à des Architectures de Données Fictives (ADF) immersives, sophistiquées, crédibles qui s'appuieront sur nos biais cognitifs, nos fragilités émotionnelles et biologiques pour nous tromper et pour exploiter pleinement le « facteur humain » en attaque.



**Dans la matrice ? - hors la matrice ?**



Your Email

Video

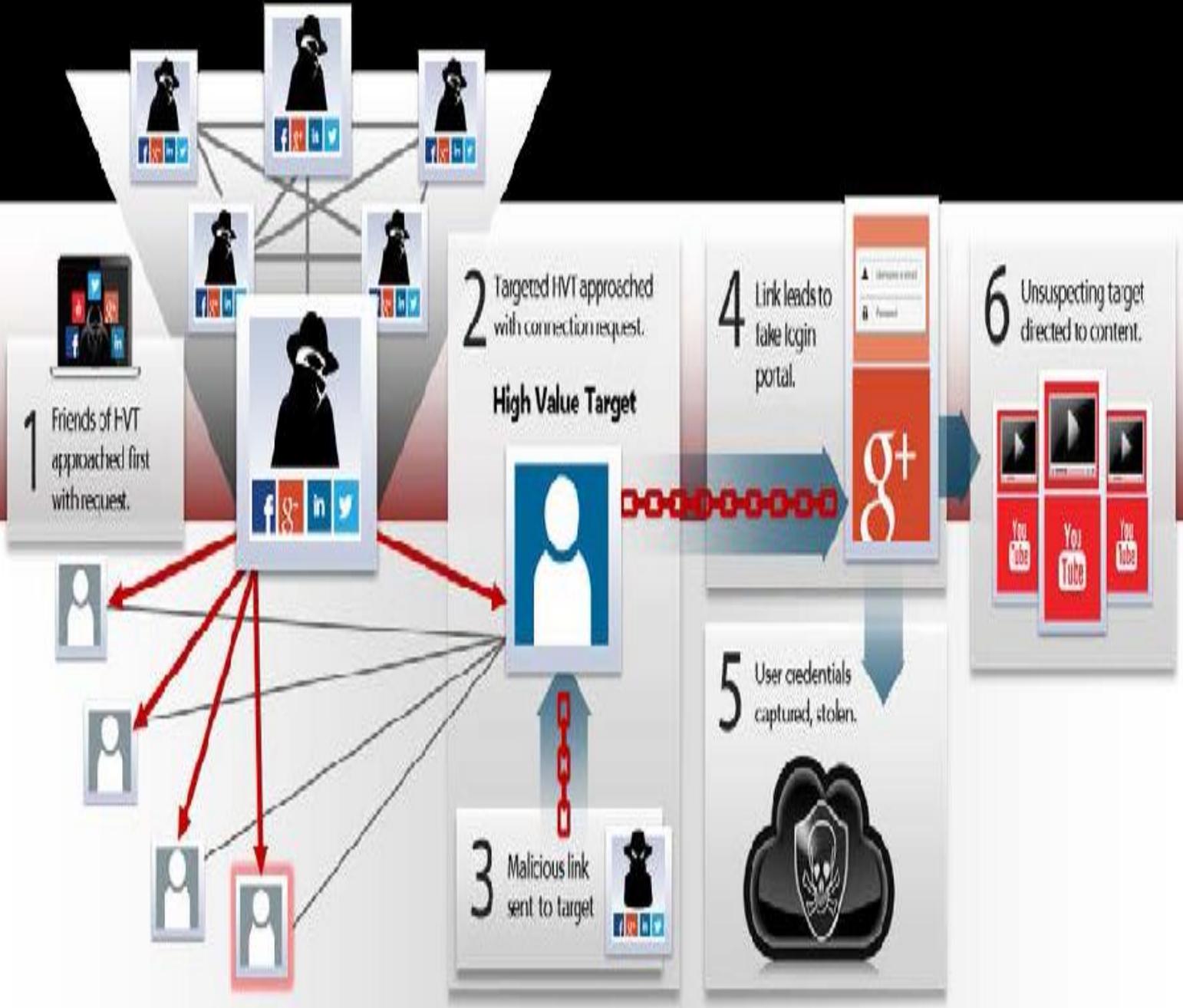
WH: Obama ready to act without Congress

0:00 / 4:20 YouTube

DAY IN PHOTOS



CyberSpy NewsCaster Operation - start in 2011 : 2000 high level compromised targets  
 NewsCaster - Data exfiltration - iSight Partners – IRAN (?)



**Joseph Nilsson**  
March 4, 2013 · 49

Which one do you prefer?  
1: Nature beauty  
2: Human related beauty — with Carol Hitler Schoenfeld and 11 others.

Like · Share

4 people like this.

- Babar Ali** Both of them in accordance with mood and situation  
March 4, 2013 at 10:27am · Like
- Stacy Valentino-Procida 1**  
March 4, 2013 at 10:27am · Like
- Alice Nilsson 1 and 2**  
March 4, 2013 at 10:34am · Like
- Jade Nilsson** dad i love both  
March 4, 2013 at 10:41am · Like
- Martin Sherman** Yes!  
March 4, 2013 at 12:40pm · Like
- Josh Furie 2** is very good, plz buy me 1 dad 😊  
March 5, 2013 at 11:38am · Like
- Fredric Johnson 2**  
March 10, 2013 at 12:40pm · Like
- Tammy Porcno 1**  
March 10, 2013 at 1:55pm · Like



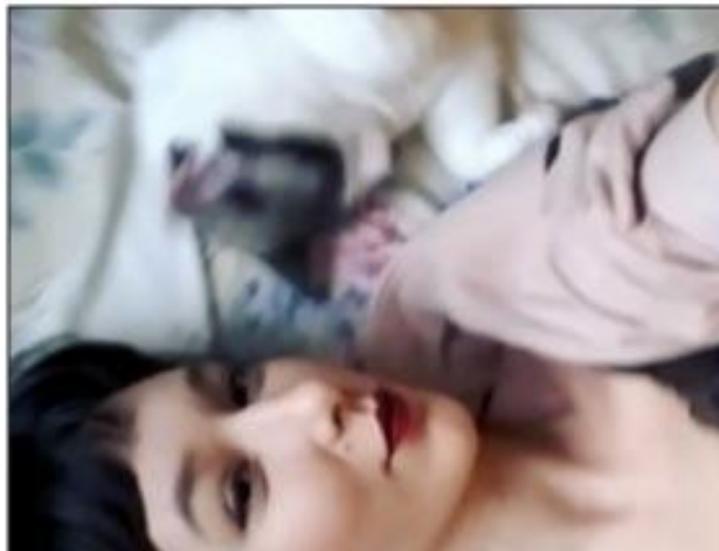
July 16, 2016  
Victim A comments on picture on Mia Ash Facebook account



March 7, 2017  
Mia Ash persona Facebook profile  
Victim A "Likes"

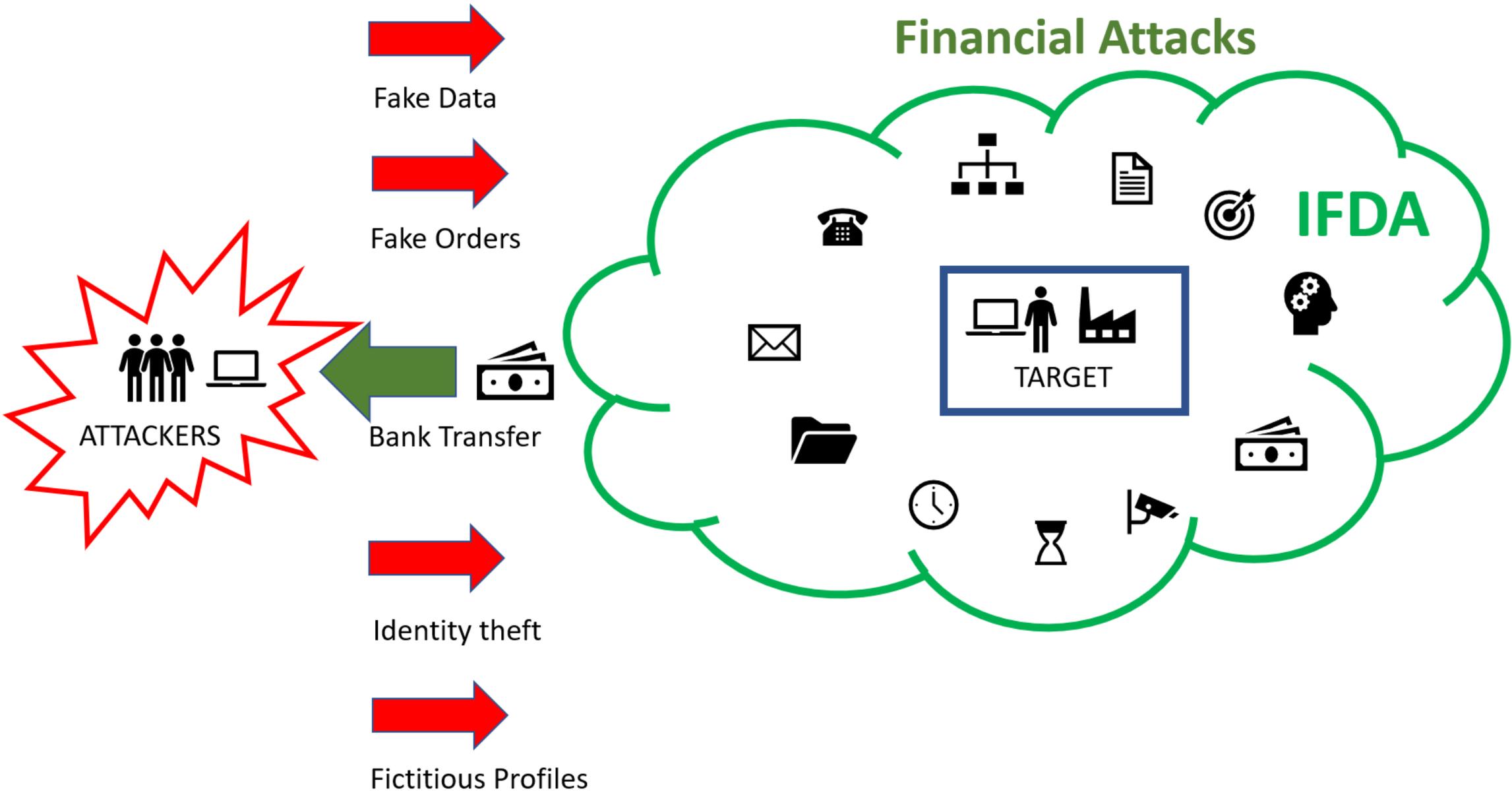


Photographer at Mia's Photography  
London, Greater London, United Kingdom | Photography  
Current Mia's Photography  
Previous Loft Studios, Clapham Studios  
Education Goldsmiths, University of London



# Opération COBALT 2016 – 2017 (IRAN ?)

# Immersive Fictitious Data Architectures (IFDA) Financial Attacks



# Immersive Fictitious Data Architectures (IFDA) - Financial Attacks Model

**Attacker :** Goal, Strategy S, Gain function to maximize

Attacker produces a series of actions : [ (AR1,AD1), (AR2,AD2), ..... , (ARn,ADn) → Goal or not]

where AR<sub>i</sub> is an action on physical space,

AD<sub>i</sub> is an action on cyberspace (sending mail, SMS, dataset, files, malware, html link, video, audio, text).

(AR<sub>2</sub>, AD<sub>2</sub>) = S < (AR<sub>1</sub>,AD<sub>1</sub>) ; (TR<sub>1</sub>,TD<sub>1</sub>) >

(AR<sub>3</sub>, AD<sub>3</sub>) = S < [(AR<sub>1</sub>,AD<sub>1</sub>)(TR<sub>1</sub>,TD<sub>1</sub>)(AR<sub>2</sub>,AD<sub>2</sub>)] ; (TR<sub>2</sub>,TD<sub>2</sub>) >

.....

( AR<sub>k</sub> , AD<sub>k</sub> ) = S < [(AR<sub>1</sub>-AD<sub>1</sub>), (TR<sub>1</sub>,TD<sub>1</sub>), ..... , (AR<sub>k-1</sub>,AD<sub>k-1</sub>)] ; (TR<sub>k-1</sub>,TD<sub>k-1</sub>) >

**Preserving the trust of the target in the sequence :**

TRUST-TARGET < [(AR<sub>1</sub>-AD<sub>1</sub>), (TR<sub>1</sub>,TD<sub>1</sub>), ..... , (AR<sub>k-1</sub>,AD<sub>k-1</sub>), (TR<sub>k-1</sub>,TD<sub>k-1</sub>), (AR<sub>k</sub>, AD<sub>k</sub>) ] > = 1 (if 0 stop)

**Preserving the consistency of the sequence :**

CONSISTENCY < [(AR<sub>1</sub>-AD<sub>1</sub>), (TR<sub>1</sub>,TD<sub>1</sub>), ..... , (AR<sub>k-1</sub>,AD<sub>k-1</sub>), (TR<sub>k-1</sub>,TD<sub>k-1</sub>), (AR<sub>k</sub>, AD<sub>k</sub>) ] > = 1 (if 0 stop)

**Maximize the IMMERSIVITY of the sequence**

**Target :** Target produces (or not) a series of actions (physical space – cyberspace) : [ TR<sub>1</sub>-TD<sub>1</sub>, TR<sub>2</sub>-TD<sub>2</sub>, ..... , TR<sub>n</sub>-TD<sub>n</sub>,.... ] in response (or not) to the actions of Attacker.



https://orangeftforfaits.com/auth/sso/facture/?identifiant= 33678123456



Rechercher



orange.fr - Espace Client

Numéro de ligne : 0678123456

Montant à régler : 2,36 €



Verified by  
VISA MasterCard.  
SecureCode.

carte de paiement Carte Bancaire  
numéro de carte \*

date d'expiration (MM/AAAA) \*

mois ▼ année ▼

numéro de contrôle de la carte \*

Le code de contrôle est composé des 3 derniers chiffres figurant au dos de votre carte de paiement.



annuler

payer



# ORDRE DE TRANSFERT PAR SWIFT

## B.N.I. – C.I.

BANQUE NATIONALE D'INVESTISSEMENT DE LA CÔTE D'IVOIRE  
S.A. au capital de 15 milliards de Francs CFA-C.C. N° 0100543 R  
Siège social: Plateau av. Marchand, Im. Sciam, 01 BP 670 Abj 01  
Tél.: 0022542181870 - Fax.: 0022542181871  
Télex : 23 798 – 22 882 CAMOR CI Swift : C SSSCIAB

**Mr JEAN PIERRE TROESCH**  
Rue Docteur Blanchard / 01 BP 1854 Abj 01  
(République Cote D'Ivoire)



# BUREAU DE CONTRÔLE DES TRANSFERTS HORS UEMOA



RUE PIERRE ET MARIE CURIE ZONE 4C 01BP 1413 ABJ 01  
CÔTE D'IVOIRE

Contact : Tel : 0022555881717. Fax : 0022555881718.

Email : [control.uemoa@financier.com](mailto:control.uemoa@financier.com)

**BNI BANQUE ABIDJAN**  
Plateau, Avenue Marchand  
Immeuble SCIAM

Bureaux des  
Contrôles de Transferts  
d'Abidjan

BANQUE	SIÈGE	COMPTE
00065	4493	008765430086X0F

## Attestation de Solvabilité

Nous soussignés, **BANQUE NATIONALE D'INVESTISSEMENT- BNI De La Côte d'Ivoire**, Plateau, Avenue Marchand – Immeuble SCIAM, confirmons de notre part que:

Le compte N° **008765430086X0F** de **Mr JEAN PIERRE TROESCH** a bel et bien été débité de la somme de **Deux Mille Huit Cent Euros (€ 2800.00)** en direction de votre compte domicilié à la **CREDIT AGRICOLE, CENTRE LOIRE CORBIGNY (580006)** en France.

Portant le numéro de compte IBAN: **FR76 1480 6580 0072 0137 7132 506**.

En foi de quoi, nous vous délivrons cette attestation pour servir et valoir ce que de droit.

Courrier adressé à **Mr DECAMP GUY, PRECY, 4 IMPASSE DE LA PAIRIE, 58800 CERVON**.

Ce transfert a été approuvé par le ministère de l'économie et des finances par le numéro d'autorisation **05/5576/MEF/CAB**, conformément à la réglementation en vigueur.

Fait à Abidjan, Le 19 Avril 2016

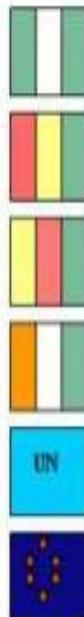
### Service Extérieur:

Mr Victor Jérôme  
NEMBELESSI



### Le Gestionnaire:

M. André YALE



### IDENTIFICATION A RAPPELER

Mr et Mme CHAPPAZ

AVIS	REFERENCE SWIFT
N° ANLCN/120A/0014/07	INTSQ29798.-434344
CERTIFICAT DE REGULARISATION	
Montant de la taxe	650 Euros

DATE: 15 Avril 2016

Reçu N°

AG / 9462854 – 38 / 75

**DIRECTEUR**  
01BP 1413 ABIDJAN 01  
Tel: +225 55881717  
**JEAN PAUL AKA**



Sommes due après paiement (Sauf erreur ou omission):

Non exigibles en ce jour	Exigibles en ce jour	Total reçu
0	0	650 Euros

**NB :** Suite au règlement des frais pour l'obtention du certificat de régularisation, nous vous transmettons ce reçu afin d'attester la bonne réception de votre paiement et vous tenons informer que vous serez rembourser de cette somme une fois le virement sur le compte du bénéficiaire.

Ce reçu vous a été délivré pour servir et valoir ce que de droit.



Plateau – Rue Des Arcades, Bd Gerald Maraud, 01 BP 4969 Abidjan 01

Téléphone: 002256848563 / Fax: 002256848563

**MANDAT**

**ATTESTATION D'ENVOI**

Transfert d'Argent Sécurisé

Paiement effectué via les services de la poste.

MONTANT A RECEVOIR : 330€  
 NOM & PRENOM DU BENEFICIAIRE :  
 ADRESSE :  
 PAYS DE DESTINATION : France

Vous avez également la possibilité de vérifier le code de votre transfert afin de vous-même que votre transfert est bien en cours. Pour le vérifier vous allez sur le site internet soit en copiant en cliquant sur ce lien suivant :

<https://gabon.westernunion.com/>

Une fois sur la page d'accueil vous verrez une partie au milieu de la page (Vérifier le statut d'un transfert) et vous rentrez les informations du régisseur ci-dessous:

PRENOM : Andre  
 NOM : Paul  
 CODE DE CONTROLE DU TRANSFERT : 2989455775

Pour finir vous cliquez sur l'icône en jaune qui signifie (vérifier le statut) et il vous sera marqué (Argent pouvant disponible et pouvant être retiré par le bénéficiaire)

Vous devez vous munir de votre reçu ainsi que de votre pièce d'identité afin de vous présenter à la poste pour le retrait.  
 Donc je vous prie de contacter MR OLIVIER BERTRAND AU 00225 56 84 85 63 pour LA DEMARCHE A SUIVRE POUR L'IMPRESSON DE VOTRE REÇU DE RETRAIT A LA POSTE.

**NB :** VOUS POUVEZ DONC RENTRER EN POSSESSION DES FONDS, DES AUJOURD'HUI MAIS CONTACTEZ D'ABORD Mr OLIVIER BERTRAND AU 00225 56 84 85 63 QUI VOUS MONTRERA LES FORMALITES POUR LA RÉCUPÉRATION DES FONDS.

50€ ont été rajouté pour couvrir les frais d'impression relatif au site.

**NB :** Ce document est une Attestation prouvant que le mandat a été bien et bel effectué mais ne vous permet pas d'encaisser les fonds, contactez Mr OLIVIER BERTRAND pour avoir le reçu.

Fait à Abidjan le 21 Avril 2016



Les auteurs ou complices de falsifications ou de contrefaçons de ce document seront punis conformément aux lois et actes en vigueur

**Siège Social**  
 12 Avenue Charles De Gaulles  
 Abidjan - Plateau  
 République de Côte d'Ivoire  
 Tél : +225 79 53 35 18

Direction des transferts Zone Afrique

A L'Attention de Mr Lucien GRAVIERE/C de maître Koffi Bernard Huissier de Justice  
 Abidjan  
 Immeuble arc en ciel 4<sup>e</sup> Etage porte 201

**Objet :** Transfert de la somme  
 740Euros (€)

Madame,  
 Nous avons reçu ce jour Mardi 19 Avril 2016 une demande de transfert de la somme de Sept Cent Quarante Euros (740) Euros du Crédit Ivoire qui nous a joint à l'appui de cette demande un Chèque de banque certifié et non endossable comme garantie.  
 Les références du bordereau de transmission :  
 Réf 852 43134701786-92  
 Code identifiant 22 842 42 f  
 Le chèque étant non endossable, il en découle les conséquences suivantes :

- 1- Le paiement des frais D'assurance Western Union pour votre transaction qui s'élève à la somme de Trois Cent euros (300) Euros est à la charge unique du bénéficiaire du mandat que vous êtes.
- 2- Nous vous prions dès lors de prendre toutes vos dispositions en vue de nous faire parvenir cette dite somme des Trois Cent euros (300) Euros représentant les frais D'assurance Western union pour la validation du transfert de la somme des Sept Cent Quarante Euros (740) Euros.
- 3- Dès que nous recevons la totalité des frais indiqués, nous vous communiquerons les codes de transferts,
- 4- Les références pour le transfert seront les suivantes :

**EXPEDITEUR :** Mr Sylvain Lemenu  
 Adresse : 03 rues des ambassades  
 BP 225 Abidjan 03  
 Téléphone: +225 48 07 74 65

**BENEFICIAIRE :** Mr Lucien GRAVIERE  
 Adresse : 7 impasse du Mayne  
 33470 GUJAN-MESTRAS  
 TEL : +33 0682387250/ 0556662139

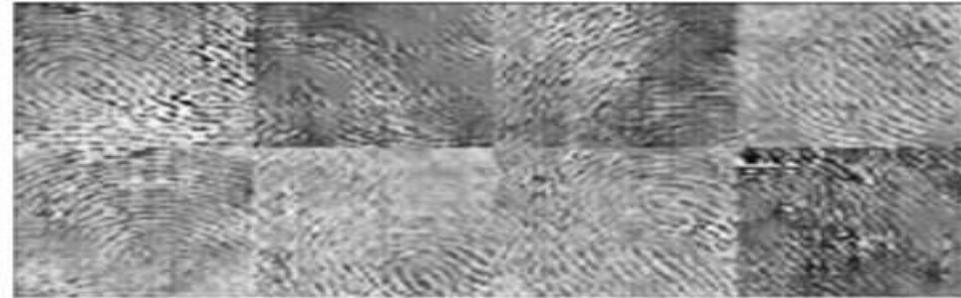
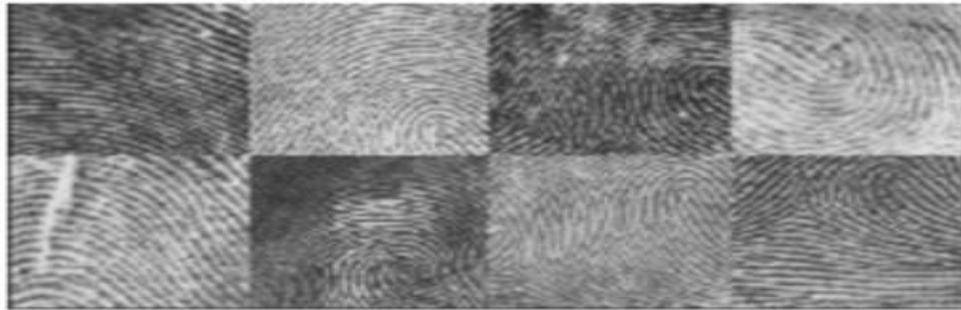
Dans l'espoir d'avoir été suffisamment explicite, je vous prie d'agréer très cher Mr Lucien Graviere, l'expression de ma haute et distinguée considération

Monsieur  
 Michel Kouame  
 Directeur des opérations de transfert



# Fake fingerprints can imitate real ones in biometric systems - research

**DeepMasterPrints created by a machine learning technique have error rate of only one in five**



(a) Real (left) and generated (right) samples for the NIST dataset.



(b) Real (left) and generated (right) samples for the FingerPass capacitive dataset.

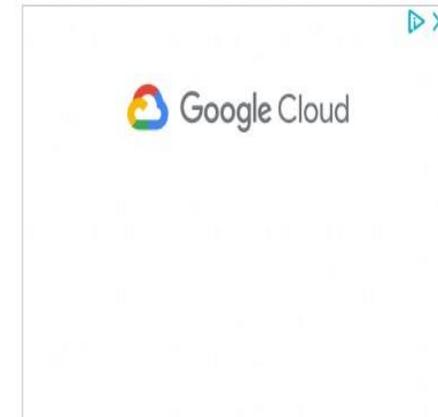
▲ An image from the New York University paper, DeepMasterPrints. Photograph: Philip Bontrager

Researchers have used a neural network to generate artificial fingerprints that work as a “master key” for biometric identification systems and prove



Le conseil copier-coller la lutte contre la fraude en ce qui concerne la prévention dans une nouvelle dimension - [en savoir plus](#)

**Chronique** | Pour la première fois, une entreprise a été victime d'une fraude utilisant l'intelligence artificielle pour contrefaire la voix de son PDG. A l'heure où tout média peut être contrefait, ce cas inédit interroge sur les solutions pour faire face à ces nouvelles menaces.



Nous l'attendions depuis des mois : le premier cas de **fraude au président** grâce à un logiciel imitant la voix humaine est arrivé.

Cette technologie est même disponible sur le net pour quelques centaines de dollars. Depuis des années, nos experts ont vu progresser la sophistication de ce type de malversation.

Au début, il s'agissait d'un simple e-mail dont personne ne pensait à vérifier l'authenticité. Puis les fraudeurs ont peu à peu pris de l'assurance pour gagner en technicité et en inventivité.

Certains escrocs n'hésitent plus à se faire passer, auprès des salariés d'une entreprise, pour une équipe interne chargée de la lutte contre la fraude.

Croyant à un exercice, les salariés contactés obéissent aux instructions données et procèdent à un virement final bien réel.

Au printemps dernier, une entreprise allemande du secteur de l'énergie a été confrontée à un cas de fraude inédit : c'est la voix de son PDG qui a été reproduite par une intelligence artificielle grâce à la technologie de l'apprentissage automatique (ou « **machine learning** »), afin d'induire en erreur le directeur de la filiale au Royaume-Uni.

Celui-ci a d'abord effectué un premier versement de 220.000 dollars. La fraude aurait pu se poursuivre si le faux président n'avait pas eu « la malchance » de rappeler sa victime en même temps que le vrai...

L'entreprise allemande a finalement réussi à se faire rembourser, car elle avait pris la précaution de souscrire une assurance contre la fraude.

Au-delà de l'exploit technique, le constat est patent : la lutte contre la fraude entre, à présent, dans une nouvelle dimension.

Bientôt, toute image, vidéo ou voix sera susceptible d'être contrefaite à la perfection. Et nous ne pourrons bientôt plus nous fier à nos cinq sens.

Comment continuer à se faire confiance ?

En avril dernier, un rapport du FBI estimait à 20.000 le nombre de cas de « fraude au président » constatés dans le monde en 2018, pour des dommages d'un montant total de 1,2 milliard de dollars. Il s'agit là de la plus coûteuse des fraudes sur internet.

Entre 2013 et 2018, le montant global des dommages déclarés a atteint 12,5 milliards de dollars. Et ces montants risquent d'exploser dans les années à venir, faisant de ce type de fraude une problématique stratégique pour beaucoup d'entreprises.

***Wilfried Verstraete, président du directoire du groupe Euler Hermes***



SYSTEM PROMPT  
(HUMAN-WRITTEN)

*In a shocking finding, scientist discovered a herd of unicorns living in a remote, previously unexplored valley, in the Andes Mountains. Even more surprising to the researchers was the fact that the unicorns spoke perfect English.*

MODEL  
COMPLETION  
(MACHINE-  
WRITTEN, 10  
TRIES)

The scientist named the population, after their distinctive horn, Ovid's Unicorn. These four-horned, silver-white unicorns were previously unknown to science.

Now, after almost two centuries, the mystery of what sparked this odd phenomenon is finally solved.

Dr. Jorge Pérez, an evolutionary biologist from the University of La Paz, and several companions, were exploring the Andes Mountains when they found a small valley, with no other animals or humans. Pérez noticed that the valley had what appeared to be a natural fountain, surrounded by two peaks of rock and silver snow.

Pérez and the others then ventured further into the valley. "By the time we reached the top of one peak, the water looked blue, with some crystals on top," said Pérez.

Pérez and his friends were astonished to see the unicorn herd. These creatures could be seen from the air without having to move too much to see them - they were so close they could touch their horns.

While examining these bizarre creatures the scientists discovered that the creatures also spoke some fairly regular English. Pérez stated, "We can see, for example, that they have a common 'language,' something like a dialect or dialectic."

Dr. Pérez believes that the unicorns may have originated in Argentina, where the animals were believed to be descendants of a lost race of people who lived there before the arrival of humans in those parts of South America.

While their origins are still unclear, some believe that perhaps the creatures were created when a human and a unicorn met each other in a time before human civilization. According to Pérez, "In South America, such incidents seem to be quite common."

However, Pérez also pointed out that it is likely that the only way of knowing for sure if unicorns are indeed the descendants of a lost alien race is through DNA. "But they seem to be able to communicate in English quite well, which I believe is a sign of evolution, or at least a change in social organization," said the scientist.

**TASK**     **Reading Comprehension:** answer questions about given passages

**DATASET**     CoQA

**EXAMPLE**     *The 2008 Summer Olympics torch relay was run from March 24 until August 8, 2008, prior to the 2008 Summer Olympics, with the theme of "one world, one dream". Plans for the relay were announced on April 26, 2007, in Beijing, China. The relay, also called by the organizers as the "Journey of Harmony", lasted 129 days and carried the torch 137,000 km (85,000 mi) – the longest distance of any Olympic torch relay since the tradition was started ahead of the 1936 Summer Olympics.*

*After being lit at the birthplace of the Olympic Games in Olympia, Greece on March 24, the torch traveled to the Panathinaiko Stadium in Athens, and then to Beijing, arriving on March 31. From Beijing, the torch was following a route passing through six continents. The torch has visited cities along the Silk Road, symbolizing ancient links between China and the rest of the world. The relay also included an ascent with the flame to the top of Mount Everest on the border of Nepal and Tibet, China from the Chinese side, which was closed specially for the event.*

*Q: What was the theme?*

*A: "one world, one dream".*

*Q: What was the length of the race?*

*A: 137,000 km*

*Q: Was it larger than previous ones?*

*A: No*

*Q: Where did the race begin?*

*A: Olympia, Greece*

*Q: Is there anything notable about that place?*

*A: birthplace of Olympic Games*

*Q: Where did they go after?*

*A: Athens*

*Q: How many days was the race?*

*A: seven*

*Q: Did they visit any notable landmarks?*

*A: Panathinaiko Stadium*

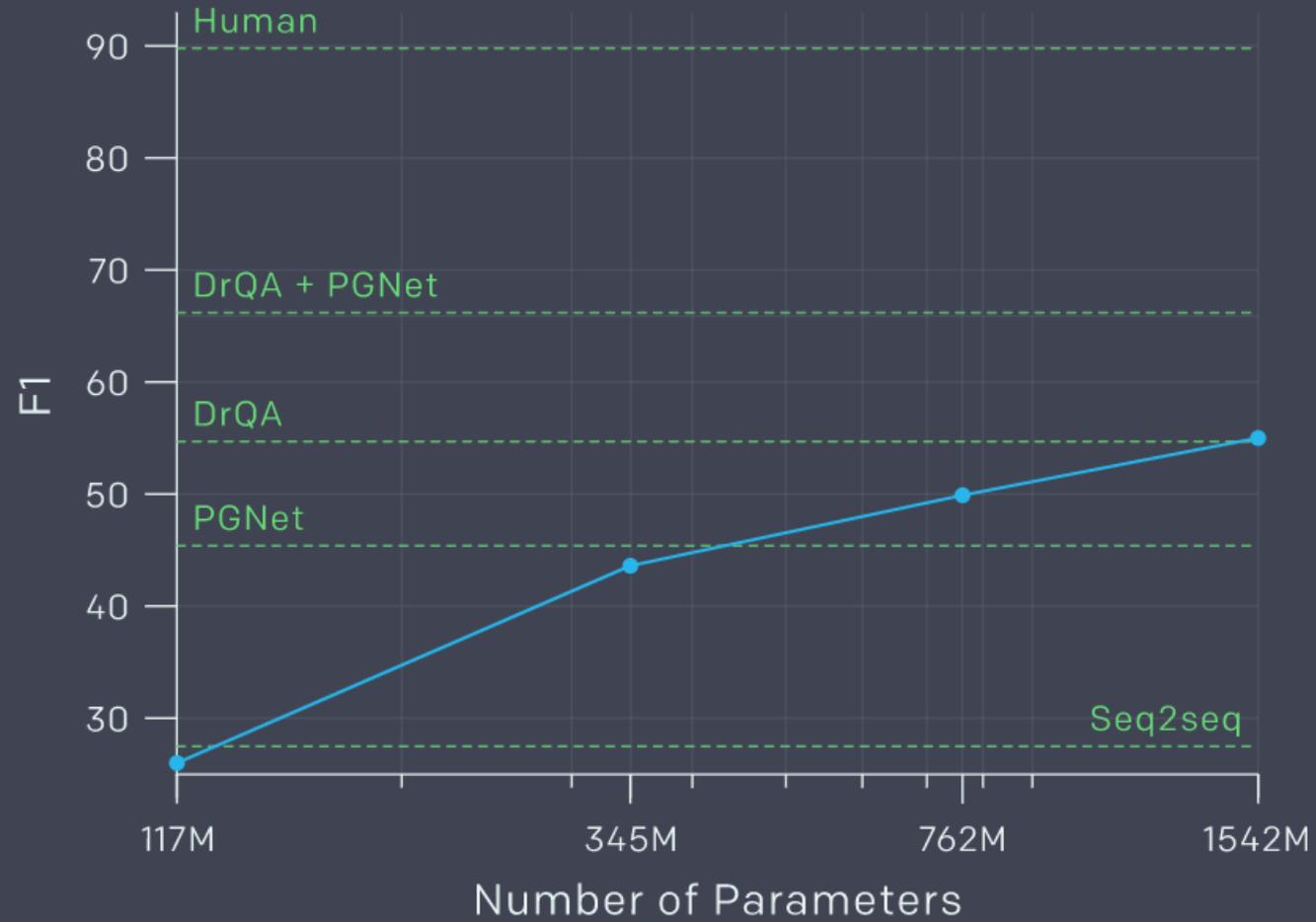
*Q: And did they climb any mountains?*

*A:*

Target answers: *unknown* or *yes*

Model answer: Everest

PERFORMANCE



Applications directes de GPT2 : construction et exploitation de réseaux de comptes Bots sur les réseaux sociaux (Twitter en particulier) :

Opérations d'influence en période pré-électorale (élections US 2016, 2020, Fermes de bots russes)

Opérations de fracturation des opinions en 2020 :  
Bots russes et chinois ANTIVAXX et ANTIMASK

Objectifs : Exploiter la pandémie pour ralentir le retour à la normale et affaiblir les économies concurrentes.

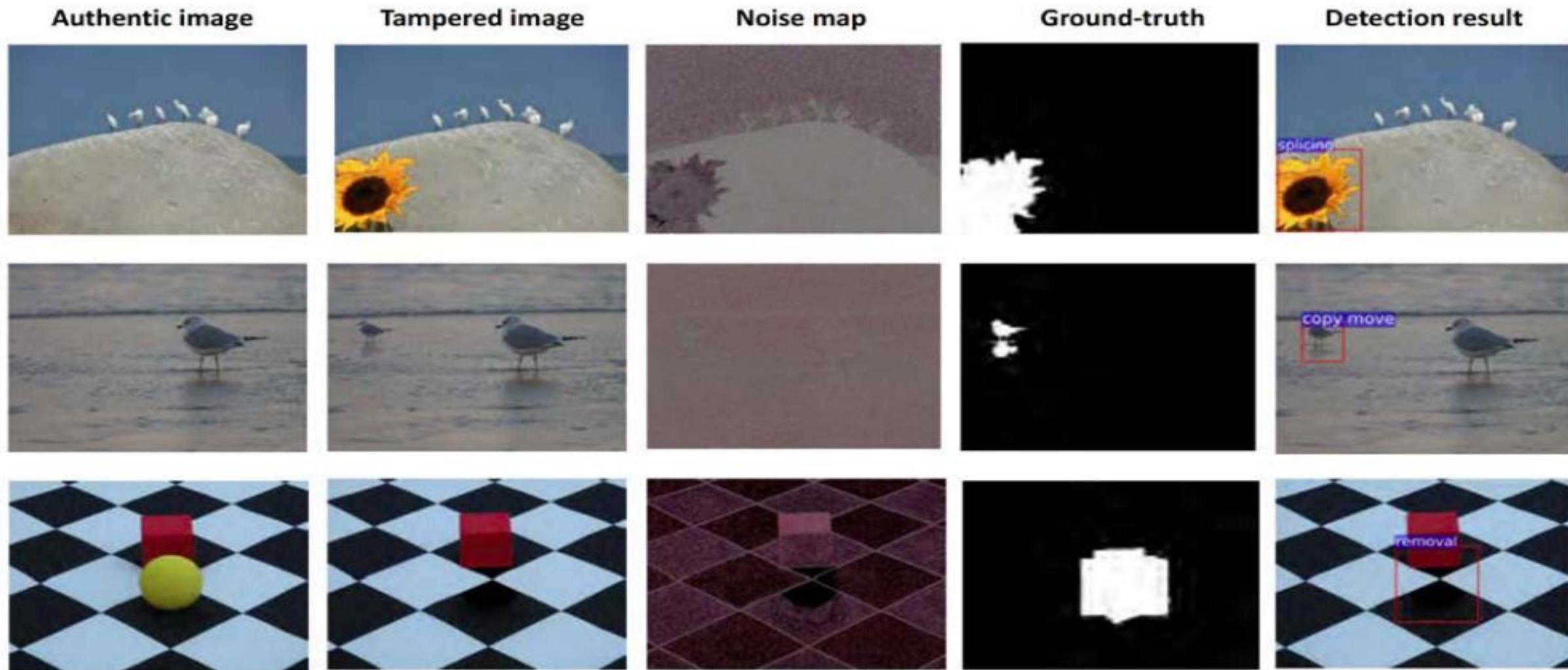
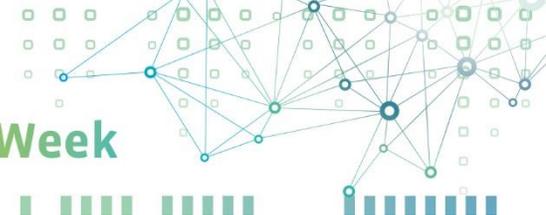
Les réseaux de bots d'influence et de fracturation des opinions =  
Problème de sécurité nationale pris en compte bien avant COVID-19

CF; Conférence CESAR DGA 2020 (la semaine prochaine)



Turning a horse video into a zebra video (by CycleGAN)





An example of authentic images, manipulated images, the RGB and noise streams used to detect manipulation, and the results of AI analysis. Source: the [NC2016 dataset](#)

Monet  $\leftrightarrow$  Photos



Monet  $\rightarrow$  photo

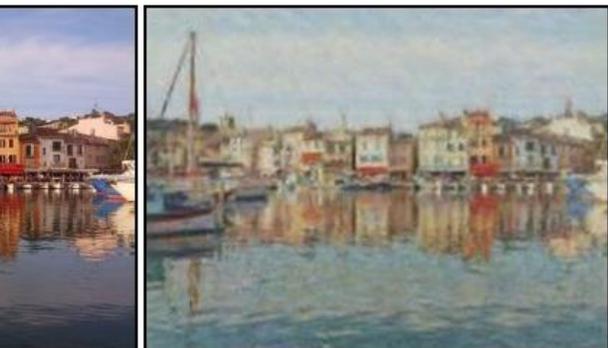


photo  $\rightarrow$  Monet

Zebras  $\leftrightarrow$  Horses



zebra  $\rightarrow$  horse



horse  $\rightarrow$  zebra



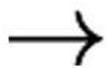
Summer  $\leftrightarrow$  Winter



summer  $\rightarrow$  winter



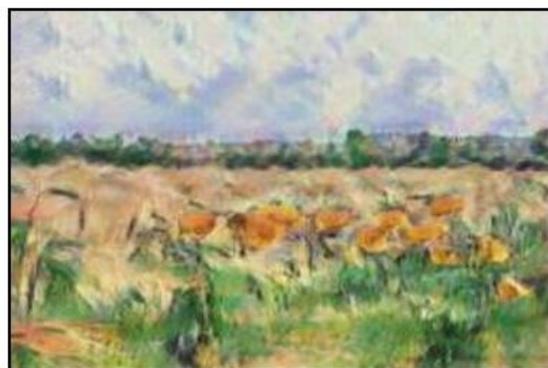
winter  $\rightarrow$  summer



Monet



Van Gogh



Cezanne



Ukiyo-e



# Synthesizing Obama: Learning Lip Sync from Audio

Supasorn Suwajanakorn  
Steven M. Seitz  
Ira Kemelmacher-Shlizerman

University of Washington

**SIGGRAPH 2017**

<http://grail.cs.washington.edu/projects/AudioToObama/>

Quitter le mode plein écran

|| 🔊 0:03 / 8:00

📺 ⚙️ YouTube 📺



Original Video for Input Speech



Our Result



Source Actor

## Real-time Reenactment



## Reenactment Result



Target Actor





LIPING/  
SHUTTERSTOCK.COM

# How Fake Data Can Help the Pentagon Track Rogue Weapons

**This software trains machine-learning tools to spot terrorists stockpiling weapons.**

By Jack Corrigan

**T**he Pentagon is investing in software that uses big data to help intelligence officers keep terrorists from getting their hands on biological, chemical and nuclear weapons.

The Air Force Research Laboratory in January announced a \$4.6 million contract with the software company IvySys to model different ways state and non-state actors could obtain and deploy “weapons of mass terror” around the world.

The contract supports an ongoing effort by the Defense Advanced Research Projects Agency to build tools to spot groups who are potentially stockpiling materials for such weapons.

“Reports of chemical weapons use around the world raises serious concerns about non-state actors’ access to weapons of mass terror and reinforces fears of a possible terrorist attack with chemical, biological, radiological, or nuclear weapons in the West,” DARPA and IvySys said in a statement. “Today’s terrorist networks move operatives, money and material across borders and through the crevices of the global economy, making tracking such adversaries a daunting challenge.”

The technology would generate fictional but realistic datasets of bank transactions, emails and inventory transfers, and embed them with indicators of suspicious activities, like a shipment of toxic chemicals getting

Imagined by a GAN ([generative adversarial network](#)) - [StyleGAN](#) (Dec 2018) - [Karras](#) et al. and Nvidia - [Original GAN](#) (2014) - [Goodfellow](#) et al.  
Don't panic. Learn about [how it works](#). - [Help](#) this AI continue to dream | [Contact me](#) - Another | [Save](#) • [Cats](#) | [Articles](#) | TV [Friends](#) - [Office](#) |



<https://thispersondoesnotexist.com/>



<https://thispersondoesnotexist.com/>

# Lyrebird AI

Using artificial intelligence to enable creative expression.

A decorative graphic consisting of several overlapping, light blue, wavy lines that span the width of the page, positioned below the main text.

<https://www.descript.com/lyrebird-ai?source=lyrebird>



Lyrebird AI is currently in private beta. If you have an interesting use case for these features, [we'd love to hear from you.](#)

**Voice Double:** Create a digital voice that sounds like you from a small audio sample.



female-original.wav



female-synthetic.wav



male-original.wav



male-synthetic.wav



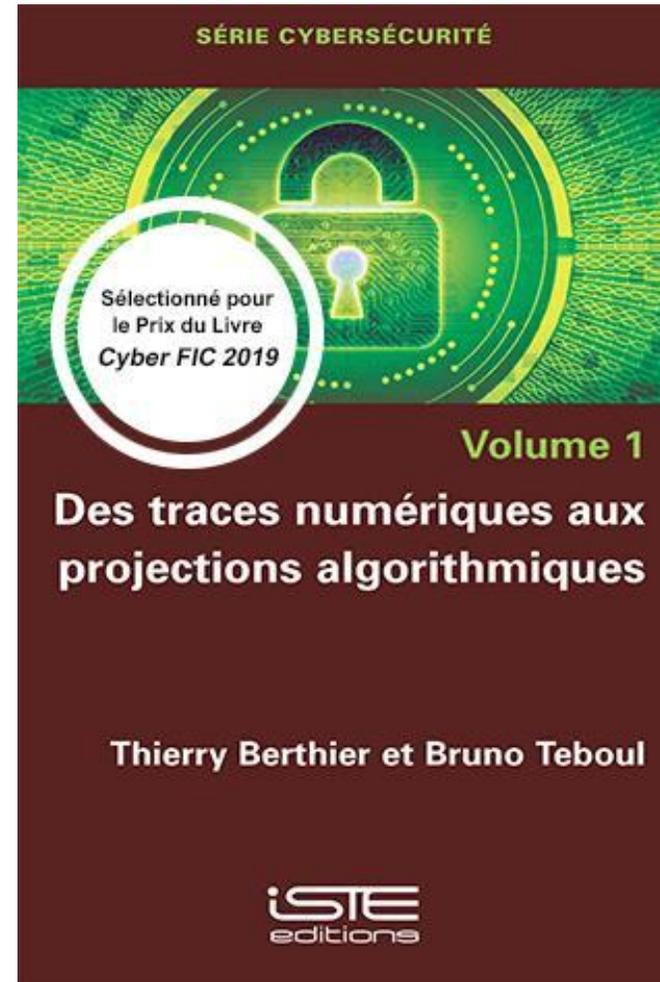
<https://www.descript.com/lyrebird-ai?source=lyrebird>



## From Digital Traces to Algorithmic Projections

Thierry Berthier and Bruno Teboul

ISTE  
editions



SÉRIE CYBERSÉCURITÉ

Sélectionné pour  
le Prix du Livre  
Cyber FIC 2019

Volume 1

## Des traces numériques aux projections algorithmiques

Thierry Berthier et Bruno Teboul

ISTE  
editions

Pour aller plus loin sur  
les ADFI

<https://www.elsevier.com/books/from-digital-traces-to-algorithmic-projections/berthier/978-1-78548-270-0>

<http://www.iste.co.uk/book.php?id=1372>

<https://iste-editions.fr/products/des-traces-numeriques-aux-projections-algorithmiques>



Une veille Sécurité – IA diffusée deux fois par semaine et mise en ligne sur un site wordpress :

<https://iasecurite.wordpress.com/>

Veille extraite de la veille cyber active depuis 6 ans :

<https://veillecyberland.wordpress.com/>

Hub France IA :

<http://www.hub-franceia.fr/>

# Références

Forbes: [\*Alarming Cybersecurity Stats: What You Need To Know For 2021\*](#) by Chuck Brooks

CSO: [\*Top cybersecurity facts, figures and statistics\*](#) by Josh Fruhlinger

Comparitech: [\*300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends\*](#) by Andra Zaharia

IBM Security: [\*Cost of a Data Breach Report 2020\*](#)

Verizon: [\*Data Breach Investigations Report 2020\*](#)

McAfee: [\*The Hidden Costs of Cybercrime\*](#) by Zhanna Malekos Smith and Eugenia Lostri

Retarus : <https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/>