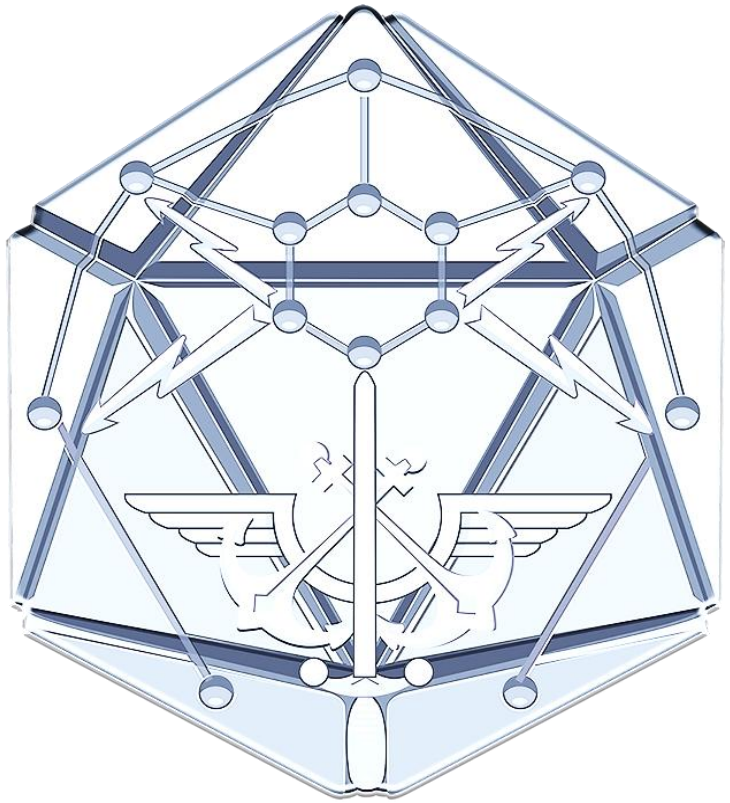
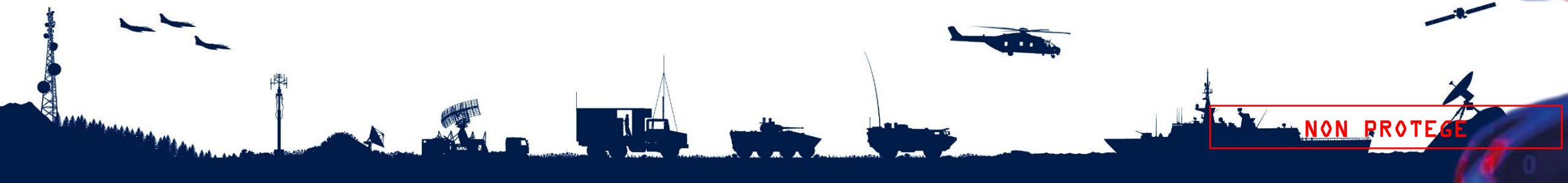
MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité





NON PROTEGE

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Cybersécurité,
Cyberdéfense
Le 5e champ de bataille

La souveraineté numérique

- La cybersécurité et la cyberdéfense ne sont plus juste des enjeux techniques. Elles sont devenues un **territoire stratégique**, au même titre que la terre, la mer, l'air et l'espace. La France (et l'Europe) se battent pour **préserver leur souveraineté numérique** face aux géants américains, aux cybermenaces russes et aux avancées chinoises en cybersurveillance. Mais est-ce réaliste ?

- Comment la France protège-t-elle ses intérêts vitaux dans ce domaine de conflictualité ?

- Comment réplique-t-elle à ces attaques souvent masquées ?

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

La souveraineté numérique

DIRISI
Unir nos forces

Les 4 domaines traditionnels de la Guerre : Terre, Air, Mer, Espace

NON PROTEGE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Cyberespace : Un substrat numérique

DIRISI
Unir nos forces

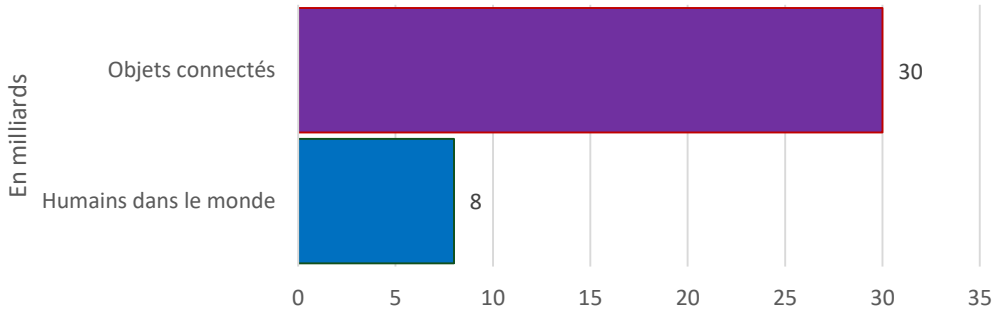
Émergence de la Cybernétique

Contexte de la souveraineté numérique

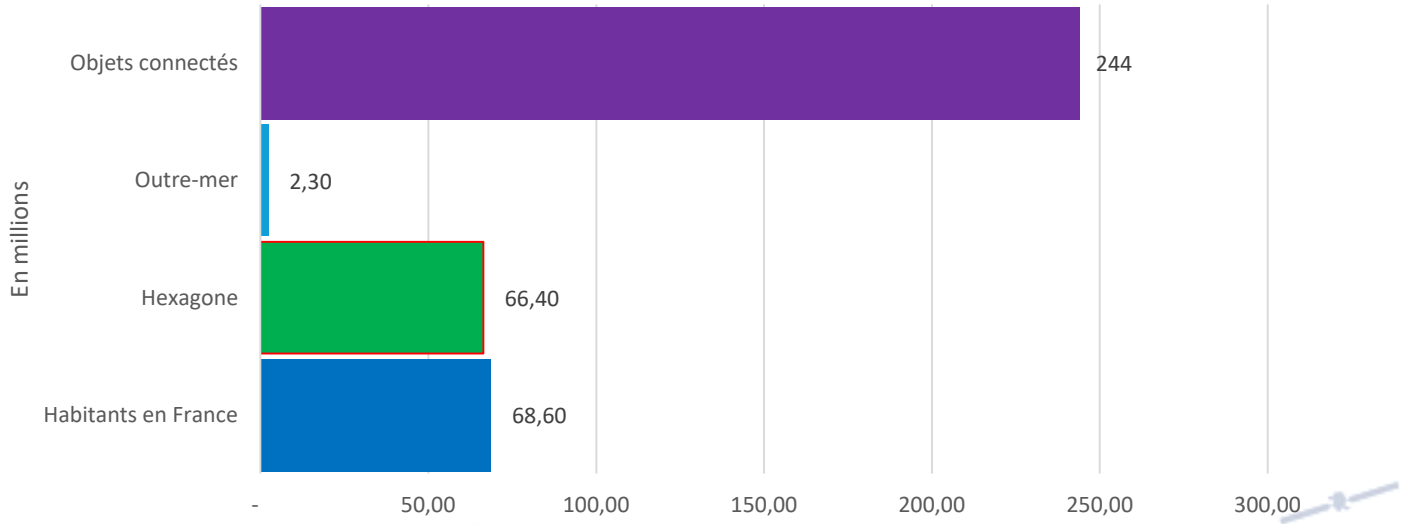
Un Monde hyperconnecté

Dans ce chaos numérique, le cyberespace n'est plus réservé aux militaires ou aux experts

La population mondiale est de 4 fois moins que le nombre d'équipements connectés.



La population en France est 3 fois moins que le nombre d'équipements connectés



NON PROTEGE

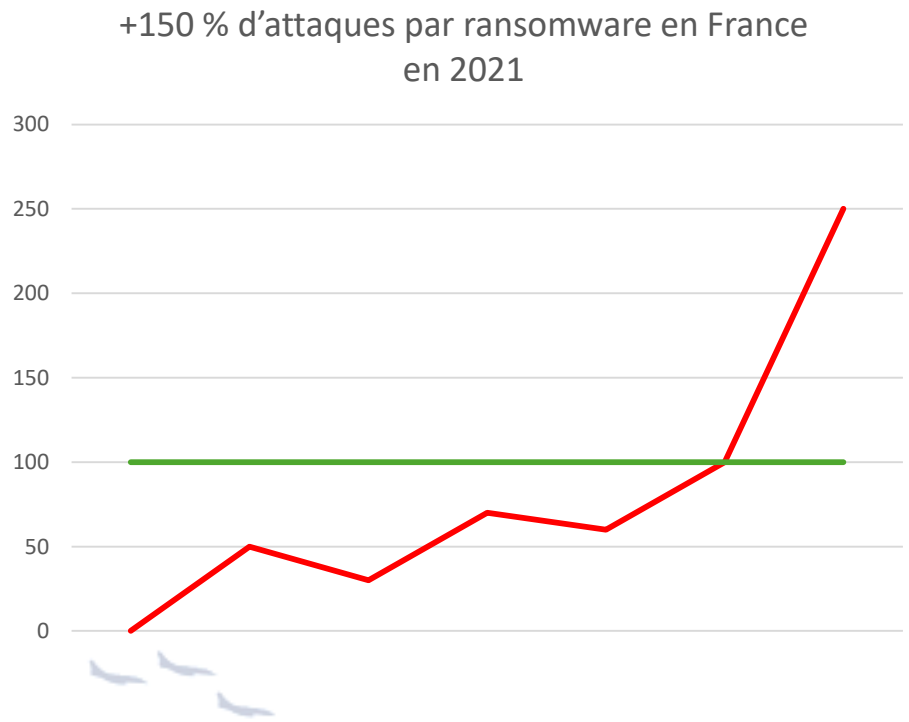
MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Contexte de la souveraineté numérique

DIRISI
Unir nos forces

Cybersécurité: risques accrus dans un monde hyperconnecté

Plus on a un système interconnecté, plus vous avez un champ possible d'attaques de nos systèmes



En France

74% des entreprises françaises ont été touchées par des ransomwares en 2024, une augmentation notable par rapport aux années précédentes.

- En 2023, environ **64% des entreprises** avaient subi des attaques par ransomware, ce qui marque une augmentation de 10 points entre 2023 et 2024.

- **Plus de 150% d'augmentation des attaques par ransomware** avaient été rapportées en 2020 et 2021, selon les rapports de l'ANSSI.

Ile de la Réunion

- **2021** : Des cyberattaques ciblant des entreprises et des institutions locales ont été rapportées,
  bien que des chiffres précis manquent (sources: reunion.gouv.fr).

- **2022** : 11 incidents de cybersécurité ont été signalés sur l'île de la Réunion (sources: reunion.gouv.fr).

- **2023** : Le nombre d'incidents a augmenté à 14 (sources: reunion.gouv.fr).

NON PROTEGE

MINISTÈRE DES ARMÉES
Liberté Égalité Fraternité

Contexte de la souveraineté numérique

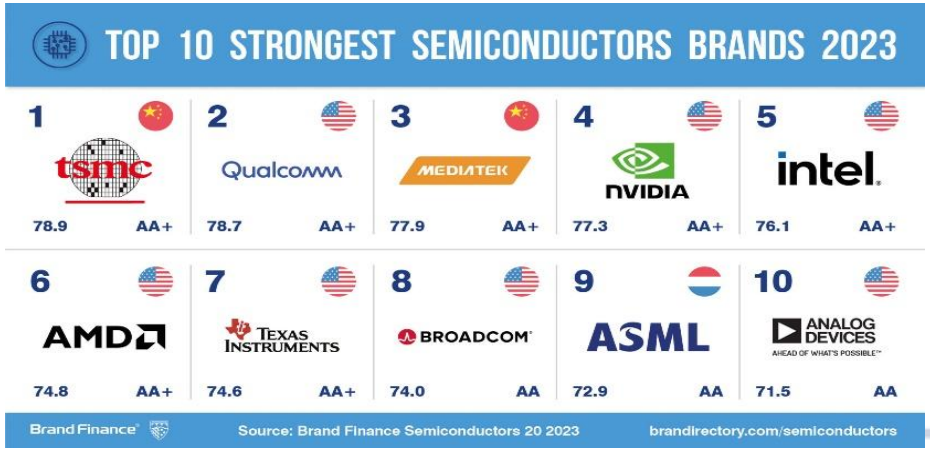
DIRISI
Unir nos forces

Souveraineté numérique : entre rêve d'indépendance et réalité de dépendance

Illusion ou nécessité ?

La souveraineté numérique signifie **contrôler** ses infrastructures, ses données et ses technologies sans dépendre d'acteurs étrangers. Mais aujourd'hui, soyons honnêtes :

- Les systèmes d'exploitation dominants sont **américains** (Windows, macOS, Android, iOS).
- Les processeurs viennent de **USA (Intel, AMD) ou de Taïwan (TSMC).**
- Le cloud est dominé par **AWS, Azure et Google Cloud, icloud.**
- L'intelligence artificielle est menée par **OpenAI (ChatGPT) , Google (Gemini) et Baidu / (deepseek).**

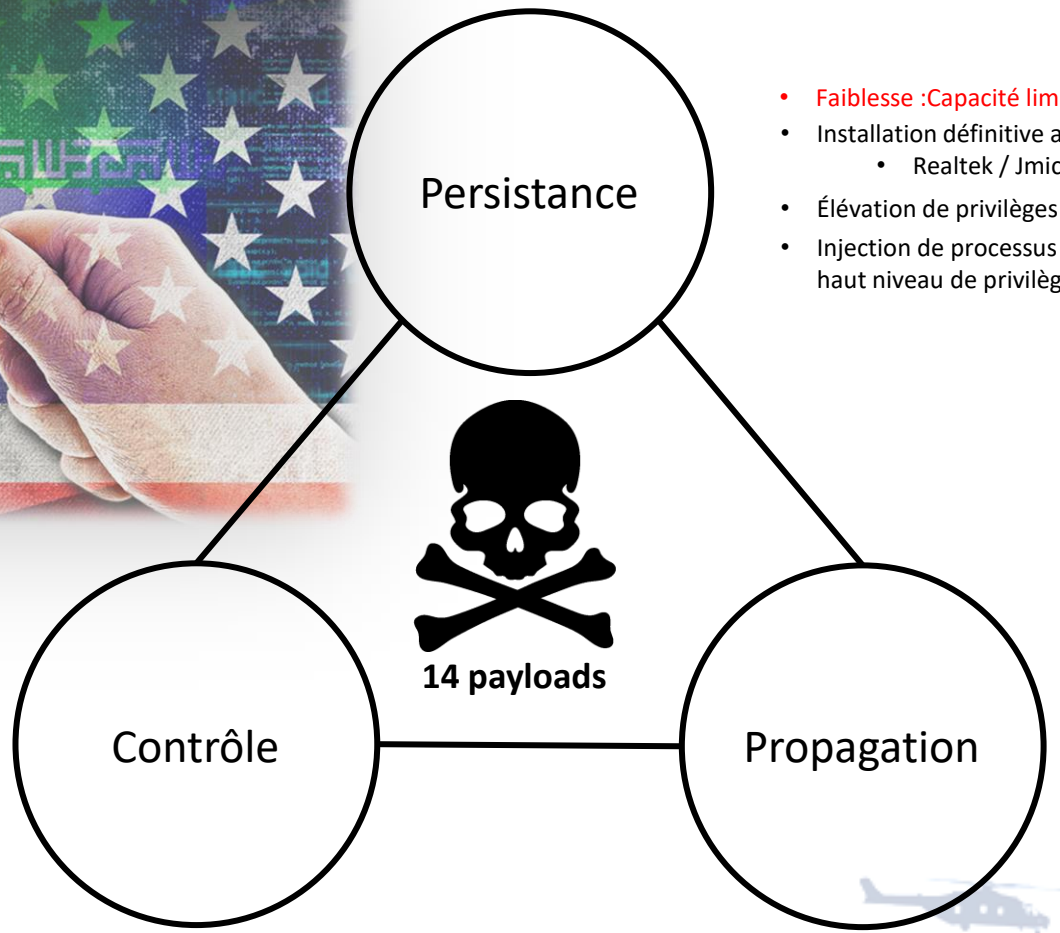


https://brandfinance.com/press-releases/tsmc-challenges-intel-for-most-valuable-semiconductor-brand-title

NON PROTEGE

Complexités et précisions

- Faiblesse : Isolement
- Serveur distant relié à toutes les machines infectés
- 2 serveurs de commandement à distance (infos des victimes) :
  - Mypremierfutbol.com
  - Todaysfutbol.com
  - Malaisie
  - Danemark
- Connexion pair à pair (MAJ sans internet, réseau hors ligne)



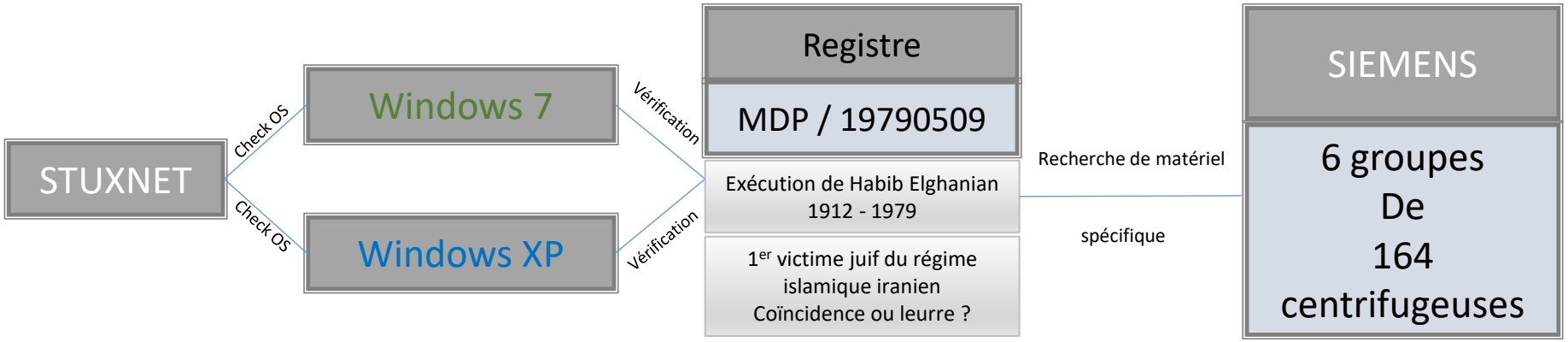
- Faiblesse :Capacité limitée
- Installation définitive après installation grâce à des certificats volés
  - Realtek / Jmicron
- Élévation de privilèges via 2 failles 0Days
- Injection de processus sur des antivirus pour disposer du plus haut niveau de privilèges (rootkit parfait)

- Réseau
- Clé USB
- 7 méthodes différentes qui utilisent 2 0Days
  - 1 faille – Exécution automatique – AUTORUN
  - 1 faille fichier LNK sur les clés USB infectés
- Ce fonctionnement **cible** des ordinateurs non connecté
  - Industrie, défense, ….
  - Réseau hermétique, isolé d'internet
- **Faiblesses : Une mise à jour peut tout anéantir**

Une vraie mission

14 charges utiles (payloads) en dormance

Le virus vérifie sur chaque ordinateur contaminé un certains nombres de critères.
Si un critère n'est pas validé, il reste dormant et se contente de contaminer d'autres hôtes



La centrale atomique iranienne de *Natanz*

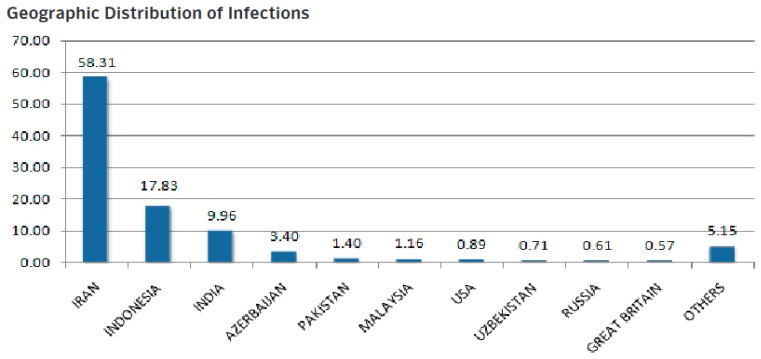
Autodestruction
24 juin 2012

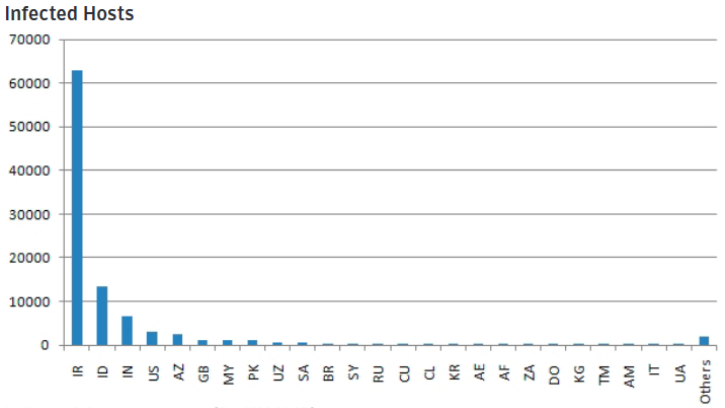
Quelques mois avant la fin du mandat du Président BARACK OBAMA

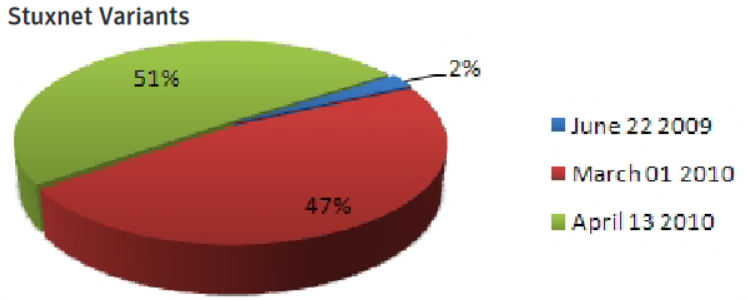
Avec l'affaire Snowden, une cyberattaque étatique doit être approuvé par le président américain uniquement, l'une des choses qui a ce statut, c'est l'arme nucléaire

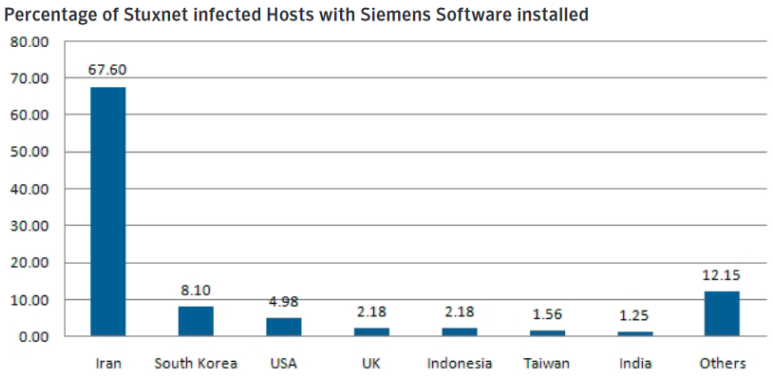
Cyber-arme étatique : une puissance à double tranchant

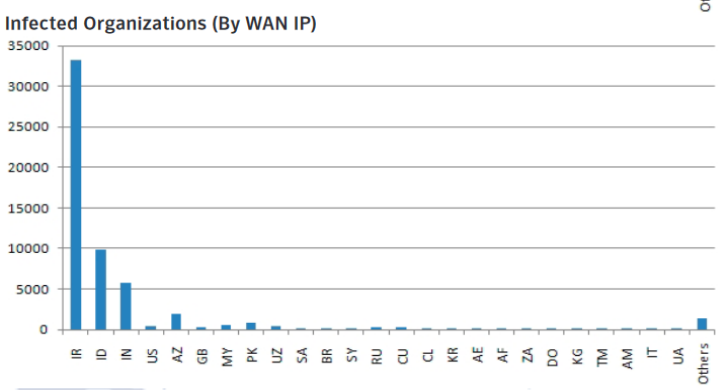
- **Olympic Games** était une opération **américano-israélienne**, sans participation néerlandaise.
- L'objectif était de **ralentir le programme nucléaire iranien** de manière non militaire.
- Stuxnet a démontré à la fois **l'efficacité** et les **dangers** des cyberarmes.











NON PROTEGE

Retour d'expérience

Stuxnet et la souveraineté numérique : La grande leçon

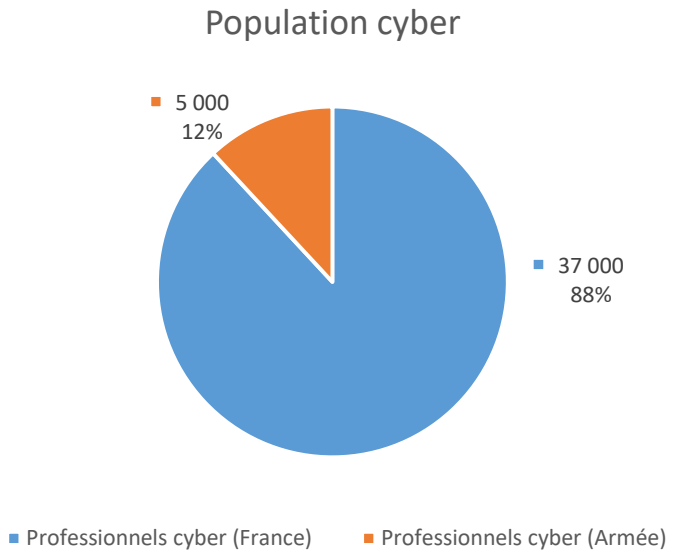
Le vrai problème révélé par Stuxnet, c'est « notre dépendance aux technologies étrangères ».

- Imaginez :
  - Utiliser des OS, des processeurs et des clouds conçus aux États-Unis ou en Chine.
  - Les mises à jour de sécurité ne sont pas sous notre contrôle.
  - Les backdoors peuvent être placées par des gouvernements étrangers (ex : Huawei, Kaspersky sous surveillance, backdoors NSA dans Windows,…).
- Peut-on alors vraiment avoir confiance ?
  - « Stuxnet a montré qu'un pays peut insérer des vulnérabilités dans des systèmes critiques pour les exploiter plus tard. »
- Risque actuel :
  - Si un État contrôle le firmware de ton matériel, il peut « l'éteindre ou l'espionner »à distance.
  - Une dépendance à « AWS, Azure ou Google Cloud,… » signifie que les États-Unis peuvent théoriquement couper des services en cas de tension géopolitique.

La France face à la menace

Réorganisation et Stratégie :

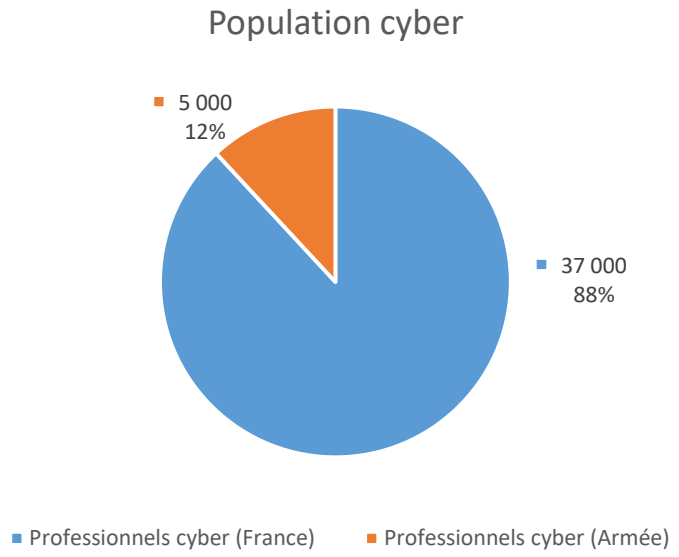
- Commandement de la Cyberdéfense (COMCYBER) en 2017 et Cyber Campus.
- « Pôle géographique cyber » pour coordonner les actions à l'échelle nationale et internationale. (Rennes)
- Renforcement de la coopération entre l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et les acteurs privés (ANSSI, 2023).



La France face à la menace

Nouveaux métiers

- 5 000 experts militaires dédiés, 24h/24 et 10 000 professionnels formés d'ici 2025
- Experts en cybersécurité :
  - En 2023, la France compte plus de "37 000 professionnels" dans ce domaine (Source : ANSSI).
- Analystes en cyberdéfense :
  - Chargés de détecter et de neutraliser les menaces en temps réel.
- Spécialistes en IA :
  - Pour anticiper les attaques et automatiser les réponses.

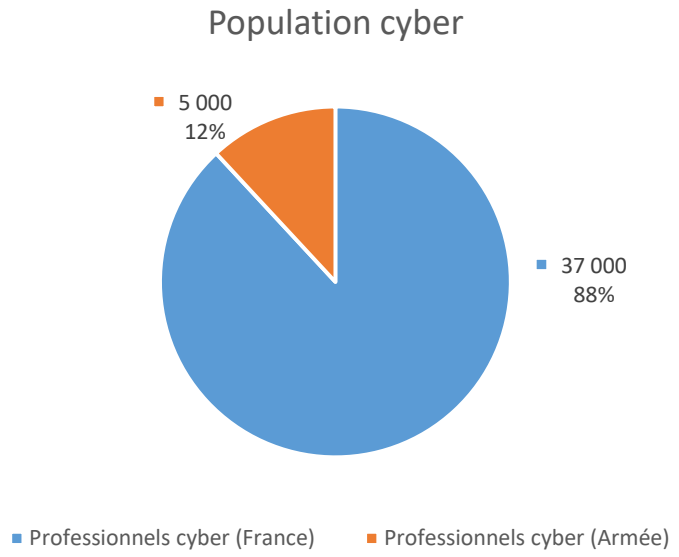


La France face à la menace

Apprivoiser l'IA

- L'IA est utilisée pour détecter les anomalies, prédire les attaques et renforcer les systèmes de défense.

- Exemple :
  - L'ANSSI utilise des algorithmes d'IA pour analyser des millions de logs et identifier des comportements suspects.



Les 6 grandes catégories de métier dans le domaine cyber au sein du Ministère des Armées

Juriste cyber

- Négociation de traités internationaux liés au domaine cyber
- la supervision et la création de textes nationaux pour la cyberdéfense ainsi que la mise à jour des textes juridiques du COMCYBER.
- Ils apportent des conseils stratégiques, opérationnels et tactiques sur les manœuvres cyber menées par les armées et contribuent à la rédaction des règles d'engagement opérationnelles (RoE) pour les actions cyber.

Cryptologue

Les experts en chiffre définissent la configuration optimale et les règles d'utilisation des équipements qui protègent les informations les plus sensibles qui permettent le bon déroulement des opérations militaires

Responsable cybersécurité

- Appliquer les directives de sécurité des systèmes d'information (SSI)
- Mettre en place des solutions de supervision de sécurité
- Mettre en œuvre la coordination d'une réponse dans le cas d'un incident

Expert et experte cyberdéfense

- Intervenir sur des systèmes victimes de cyberattaques.
- Mener l'enquête pour comprendre comment les attaquants sont parvenus à pénétrer le système.
- Mettre fin à l'attaque et de revenir à une situation nominale

Analyste des cyber menaces

- étudier les tactiques, techniques et procédures associées aux modes opératoires des attaquants
- proposer des recommandations techniques et organisationnelles au profit des entités du ministère des Armées

Hacker et hackeuse éthique

- recherchent les failles de sécurité.
- proposent des recommandations adaptées avant que des attaquants ne puissent les exploiter.

Conclusion

Stuxnet illustre la sophistication des cyberattaques étatiques et leur impact géopolitique.

Aujourd'hui, le cinquième champ de bataille inclut les infrastructures civiles et les citoyens, via les objets connectés et leur rôle dans la société.

Assurer la souveraineté numérique est donc essentiel pour protéger à la fois les infrastructures et les individus contre ces nouvelles menaces.

- Références:

- https://www.xmco.fr/wp-content/uploads/2021/11/27.XMCO-ActuSecu-27-STUXNET-min.pdf
- https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en
- https://www.youtube.com/watch?v=gXtp6C-3JKo
- https://www.reunion.gouv.fr/Actualites/Communique-de-presse/Face-au-risque-cyber-a-La-Reunion-l-Etat-renforce-sa-mobilisation
- https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
- https://www.usine-digitale.fr/article/cyberguerres-les-menaces-et-attaques-etatiques-ont-profondement-change-le-paysage-numerique.N2208025

Questions ?