



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*

Colonel Pierre-Arnaud Borrelly,
commandant le groupement de la cyberdéfense des Armées,
délégué général du Pôle d'excellence cyber,

OPÉRATIONS, ENJEUX ET PERSPECTIVES CYBER

COMMANDEMENT DE LA CYBERDEFENSE
« *PER AETHER PUGNAMUS* »

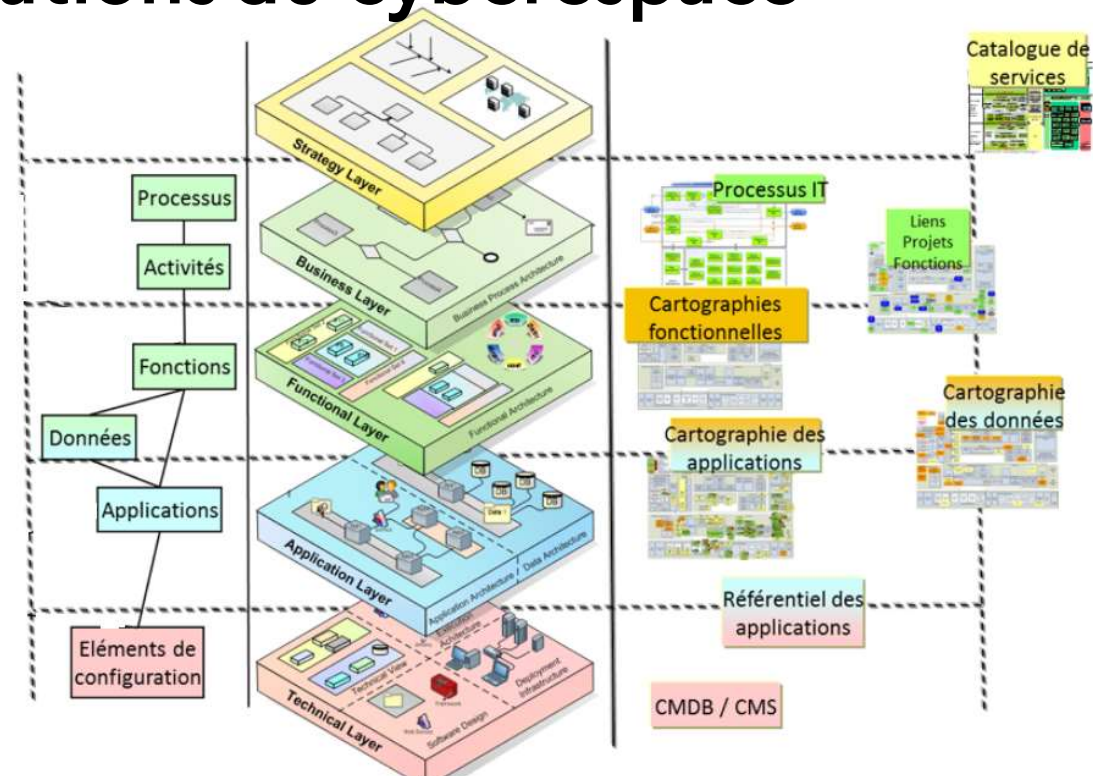


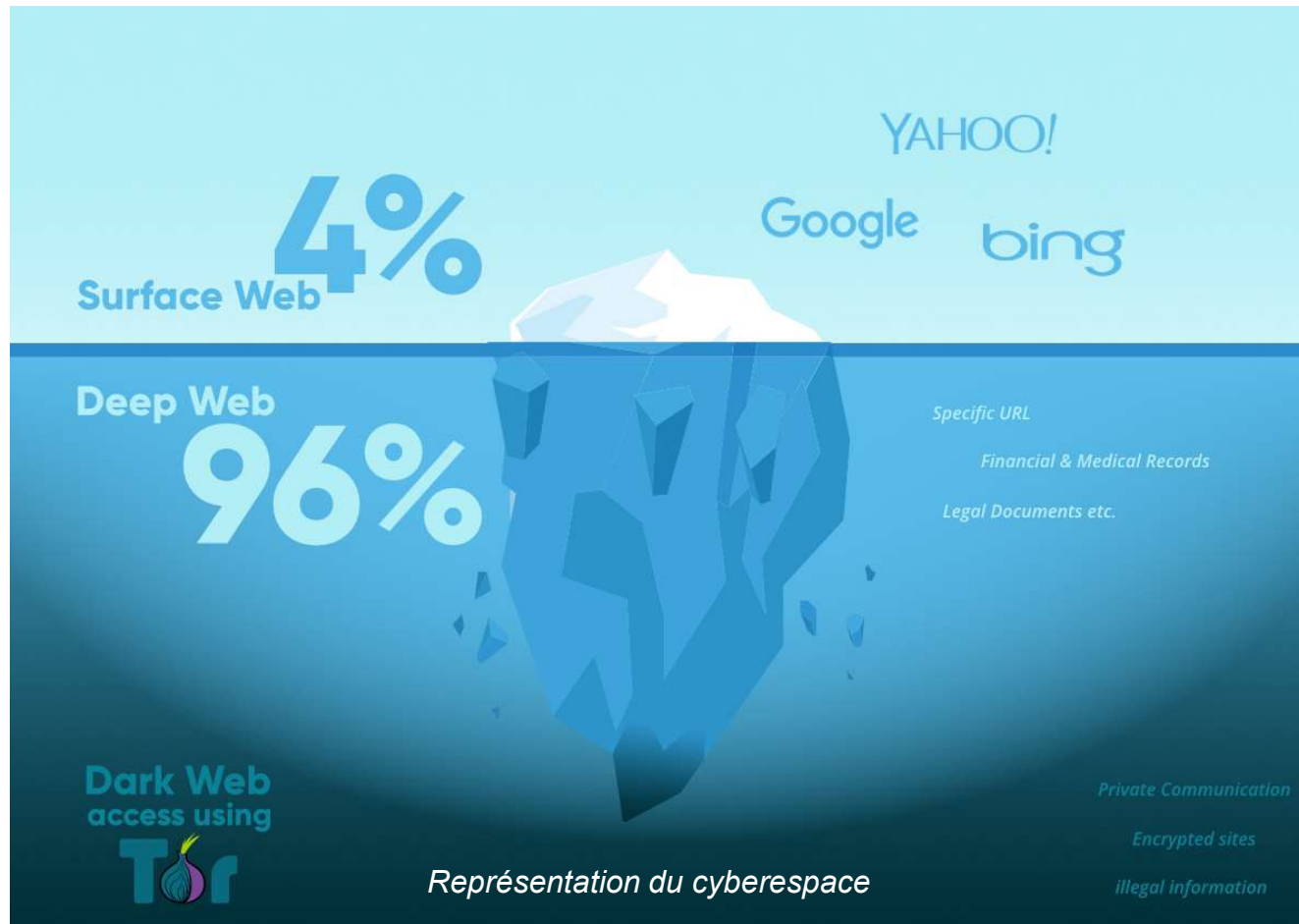
Sommaire

1. Contexte
2. Menaces dans le cyberspace
3. Organisations et acteurs de l' « écosystème » cyber
 - a. En France
 - b. Au sein du MINARM
 - c. Le COMCYBER
4. Opérations de cyberdéfense
 - a. LIO
 - b. LID
 - c. L2I
5. Ecosystème et coopérations












Représentations du cyberspace



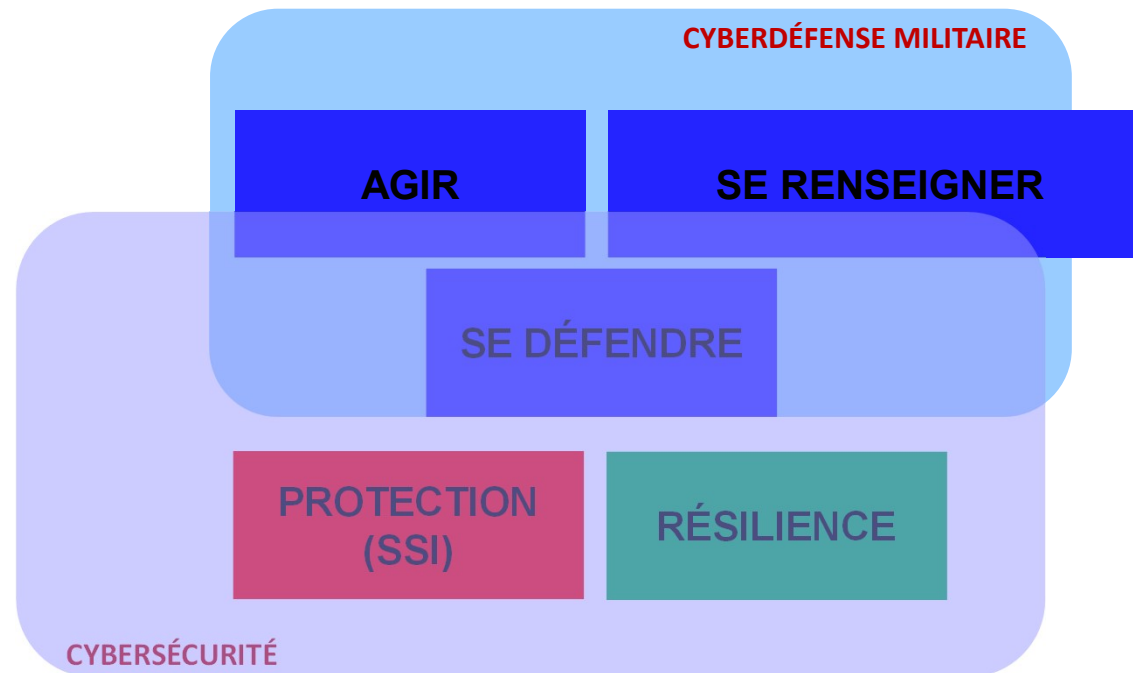




Les systèmes à protéger et à défendre

<p>Systèmes d'information et de communication</p>			
			
			<p>Systèmes d'armes</p>

LES ENJEUX DE LA CYBERDEFENSE



Sommaire

1. Contexte
2. Menaces dans le cyberspace
3. Organisations et acteurs de l' « écosystème » cyber
 - a. En France
 - b. Au sein du MINARM
 - c. Le COMCYBER
4. Opérations de cyberdéfense
 - a. LIO
 - b. LID
 - c. L2I
5. Ecosystème et coopérations



Le cyberspace est à la fois le lieu, le moyen et l'enjeu de la conflictualité

Menaces

- Bas de spectre : cybercriminalité, cyber « pollution »,
- Haut de spectre : cyber étatique (renseignement, entrave, influence), hybridité, combinaison avec d'autres actions

UNE MENACE CYBER EN CONSTANTE EVOLUTION

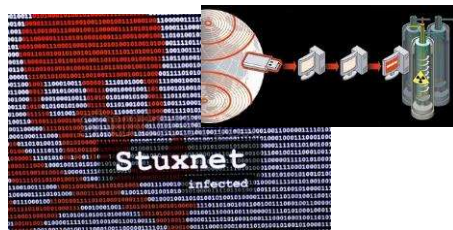
Evolution quantitative et qualitative des menaces

- Infinité de profils d'attaquants et de motivations
 - **Vengeance, jeux, militantisme, notoriété, profit, pouvoir...**
 - **Espionnage, trafics illicites, déstabilisation, sabotage...**
- Résurgence des Etats puissances, criminalité, terrorisme...
- Prolifération des modes d'action, des outils, des « portes d'entrée » du fait de la numérisation croissante
- **Erreur humaine**

***STUXNET (2010) – WANNACRY (2017) – NOTPETYA (2017) –
CHU Rouen (2019) – EMOTET (2020) – SOLARWINDS (2021) –
COLONIAL PIPELINE (2021) – PEGASUS (2021) ...***



UNE MENACE CYBER EN CONSTANTE EVOLUTION



STUXNET

- Type d'attaque : ver informatique
- Année : 2010
- Victimes : centrifugeuses iraniennes d'enrichissement d'uranium et environ 45 000 systèmes informatiques

WANNACRY

- Type d'attaque : rançongiciel (*ransomware*)
- Année : 2017
- Victimes : environ 300 000 systèmes informatiques dans plus de 150 pays
- Les pertes de Saint Gobain sont estimés à 220 millions d'euros de CA et à 80 millions d'euros de résultat d'exploitation.



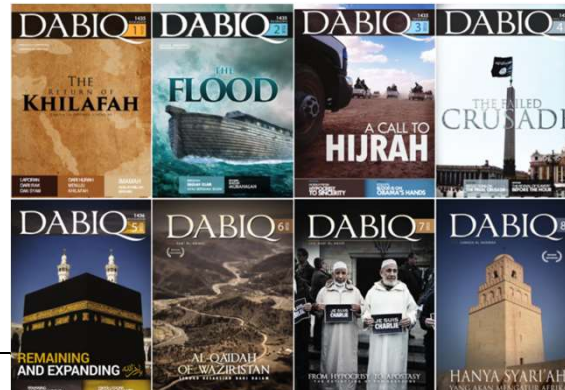
PEGASUS

- Type d'attaque : logiciel espion (spyware)
- Année : depuis 2016
- Victimes : cadres dirigeants

EVOLUTIONS DES MENACES

Utilisation par les terroristes

- Propagande
- Recrutement
- Financement
- Communication interne
- Formation
- Menaces directes
- Guerre de l'information



ISIS HACKERS POST U.S. OFFICIALS' DETAILS ONLINE, URGE LONE WOLF ATTACKS

The Caliphate Cyber Army has posted the names and addresses of U.S. police officers online.

BY ANTHONY CUTHBERTSON ON 3/7/16 AT 12:48 PM



The Caliphate Cyber Army has posted personal details of U.S. police officers online, including their full names and addresses.

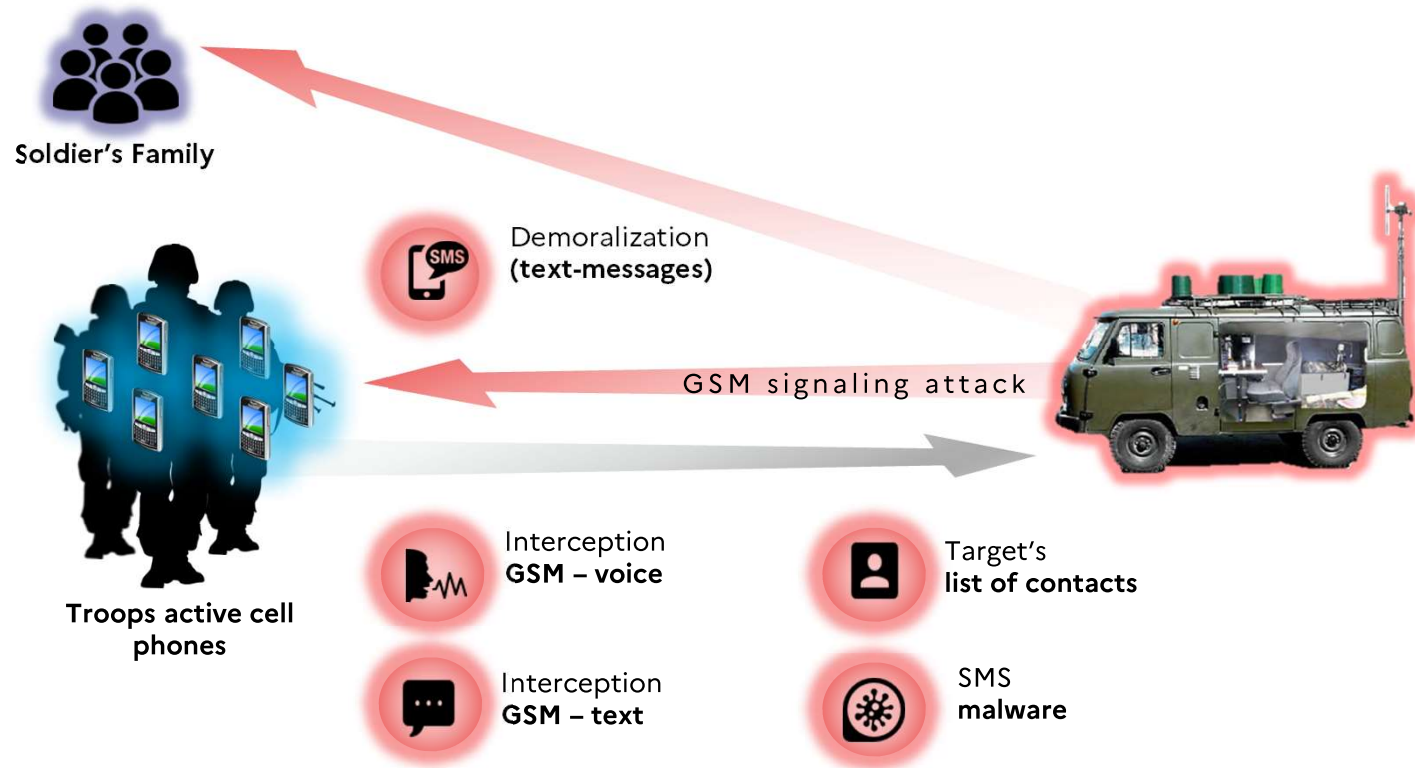
Hackers associated with the Islamic State militant group (ISIS) have posted the names and addresses of several U.S. officials online, encouraging the group's supporters to carry out "lone wolf" attacks.

The Caliphate Cyber Army (CCA), formerly known as the Islamic Cyber Army, released the personal details of 55 New Jersey police officers last week after hacking into the website of the New Jersey Transit police. The information was referenced in a series of Twitter posts on Sunday that also mentioned previous hacks on the U.S. Department of Defense.

**PARTICIPEZ
À LA GUERRE MEDIATEQUE
CONTRE
LES CROISÉS**

50%

50% de la guerre se fait médiatiquement. Téléchargez, Uploadez et partagez un maximum en utilisant le hashtag #KhilafahFR

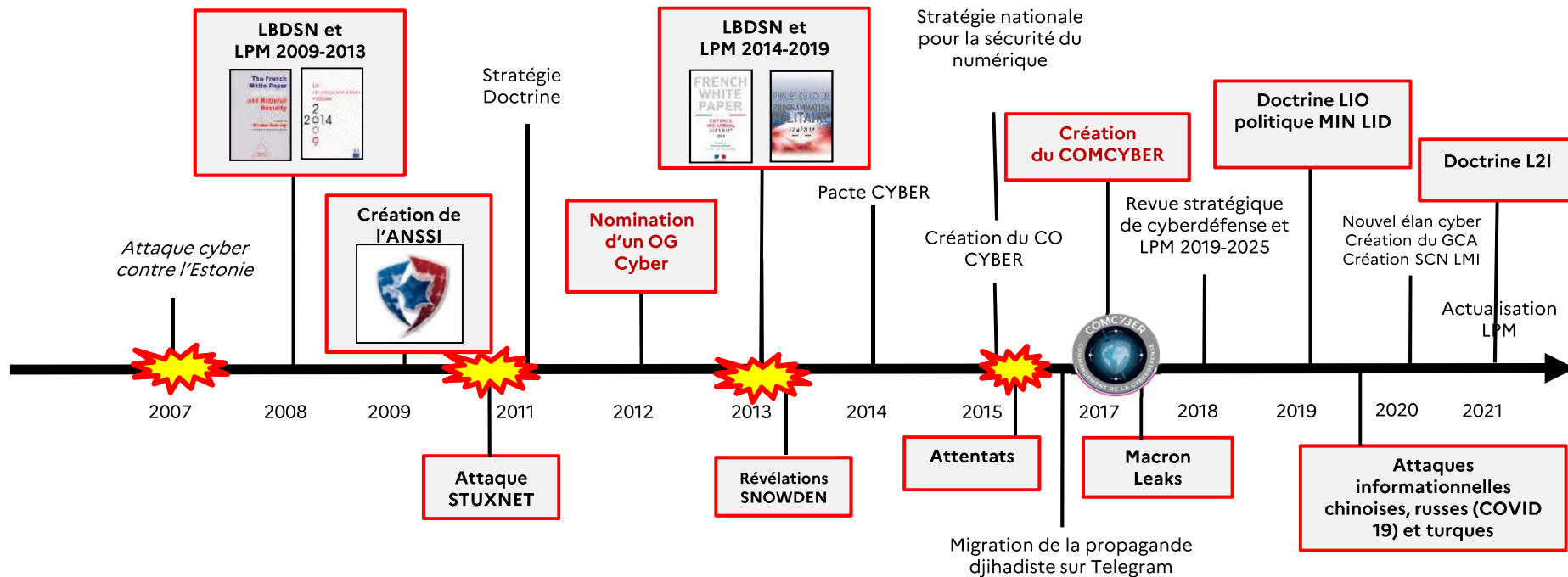


Sommaire

1. Contexte
2. Menaces dans le cyberspace
3. Organisations et acteurs de l' « écosystème » cyber
 - a. En France
 - b. Au sein du MINARM
 - c. Le COMCYBER
4. Opérations de cyberdéfense
 - a. LIO
 - b. LID
 - c. L2I
5. Ecosystème et coopérations



Chronologie



LE MODÈLE FRANÇAIS DE CYBERDEFENSE

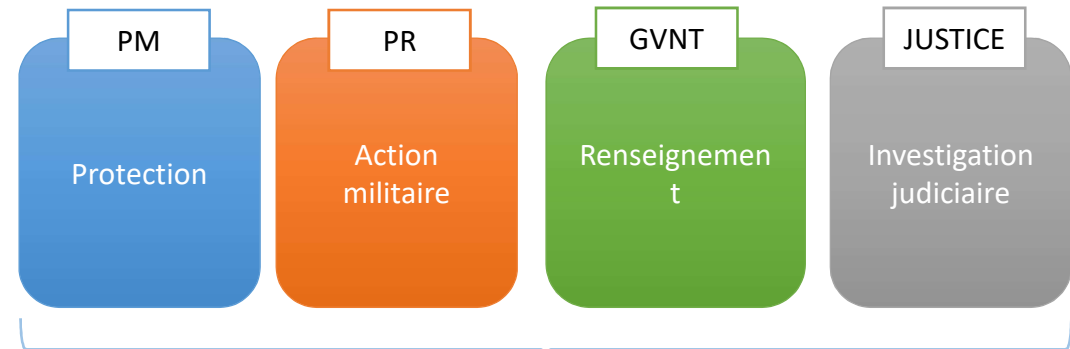
**LIVRE
BLANC**
DÉFENSE ET SÉCURITÉ NATIONALE 2013

“Le cyberspace est donc désormais un champ de **confrontation** à part entière.”
2013, p45.

Revue
stratégique
de
cyberdéfense
2018



4 chaînes opérationnelles



6 missions

Prévention – Anticipation – Protection

Détection – Attribution – Réaction



REVUE STRATÉGIQUE
DE DÉFENSE
ET DE SÉCURITÉ NATIONALE
2017



ACTUALISATION
STRATÉGIQUE
2021

DROIT INTERNATIONAL APPLIQUÉ
AUX OPÉRATIONS
DANS LE CYBERESPACE

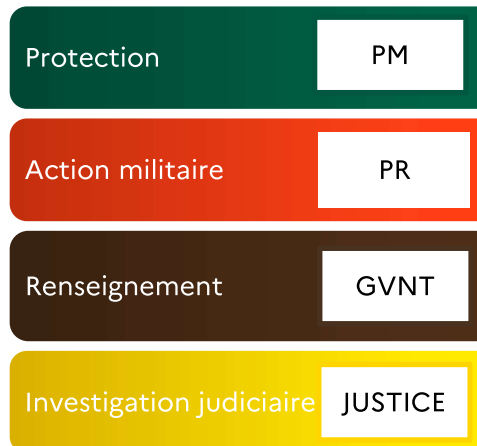


Structuration issue de la revue stratégique de cyberdéfense de 2018

Principe initial de partage des missions défensives et offensives mais nécessité de renforcer les coordinations via

un centre de coordination des crises cyber (C4) animé par le SGDSN

4 chaînes opérationnelles



6 missions interdépendantes

1. Prévention
2. Anticipation
3. Protection
4. Détection
5. Attribution
6. Réaction

Le périmètre du Commandement de la cyberdéfense

Le COMCYBER est responsable de

1

La protection des SI
placés sous la
responsabilité du CEMA

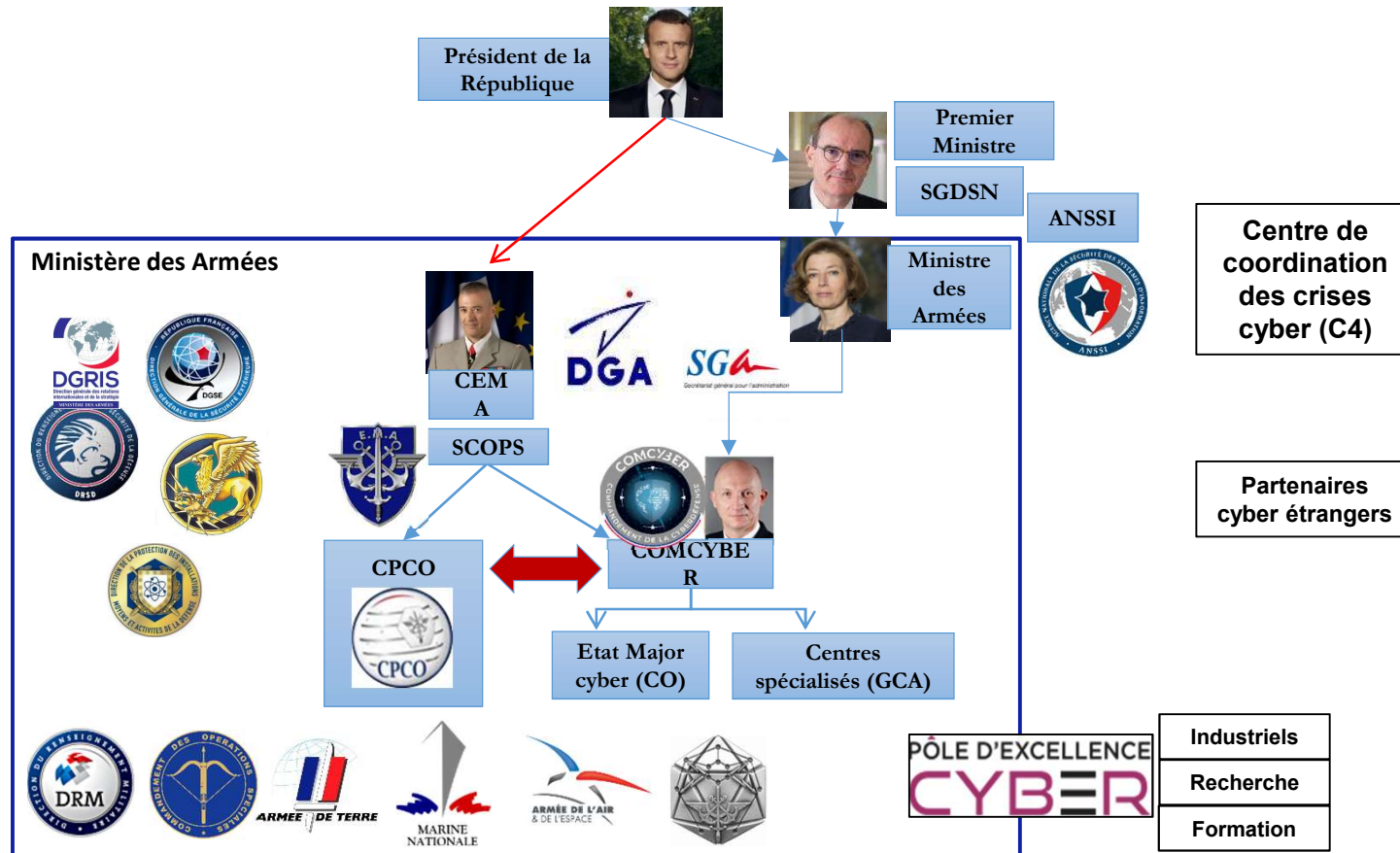
2

La conduite de la défense
des systèmes
d'information du
ministère des Armées
(hors DGSE et DRSD)

3

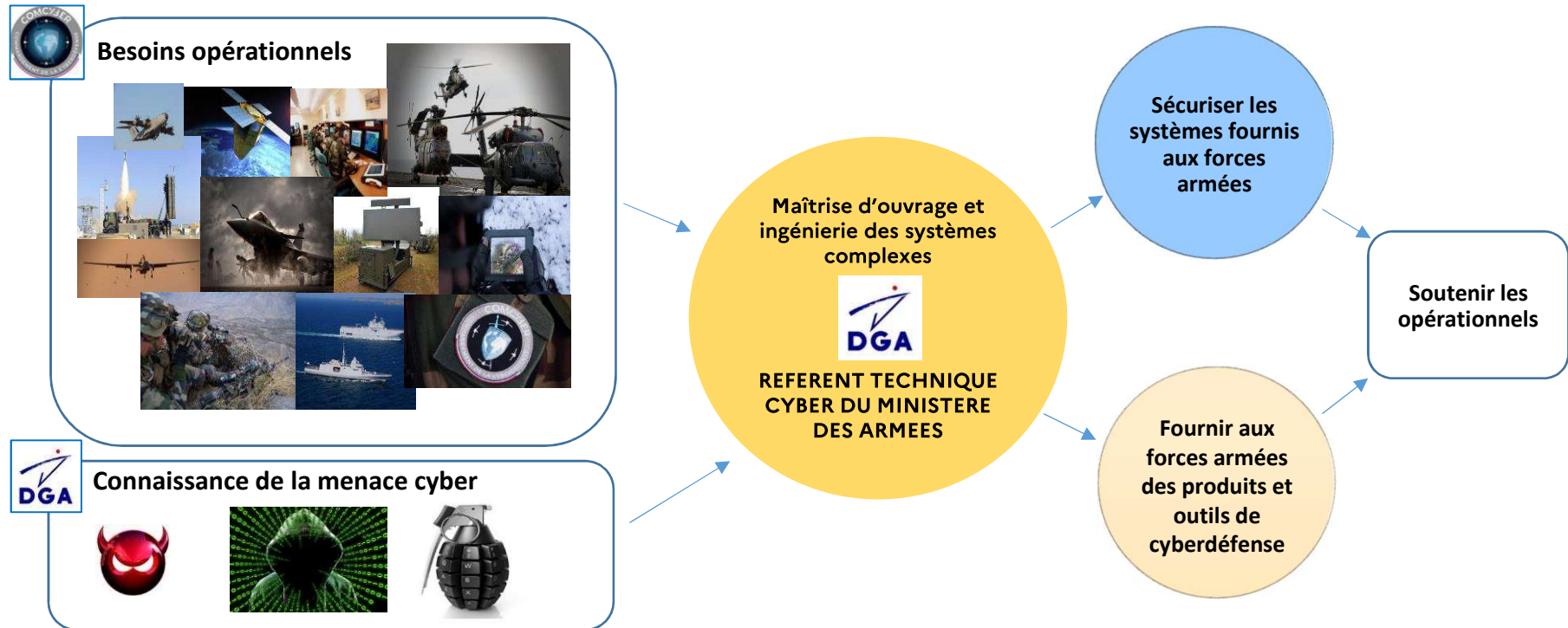
La conception, la
planification et la
conduite des opérations
militaires de
cyberdéfense sous
l'autorité du SCOPS

ORGANISATION DE LA CYBERDEFENSE AU MINARM



Domaines d'intervention de la DGA dans le domaine CYBER

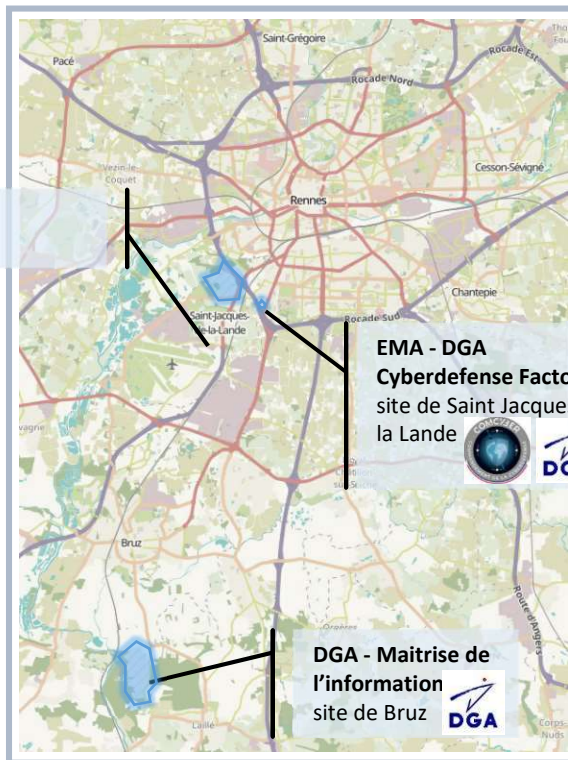
A la croisée des cultures opérationnelles, techniques et industrielles





EMPRISES CYBER DU MINISTÈRE DES ARMÉES À RENNES

EMA – quartier
Stépha



EMA - DGA
Cyberdefense Factory
site de Saint Jacques de
la Lande



DGA - Maitrise de
l'information
site de Bruz



2021
Effectifs = 900

2025
Effectifs = 1765

+ 135 %

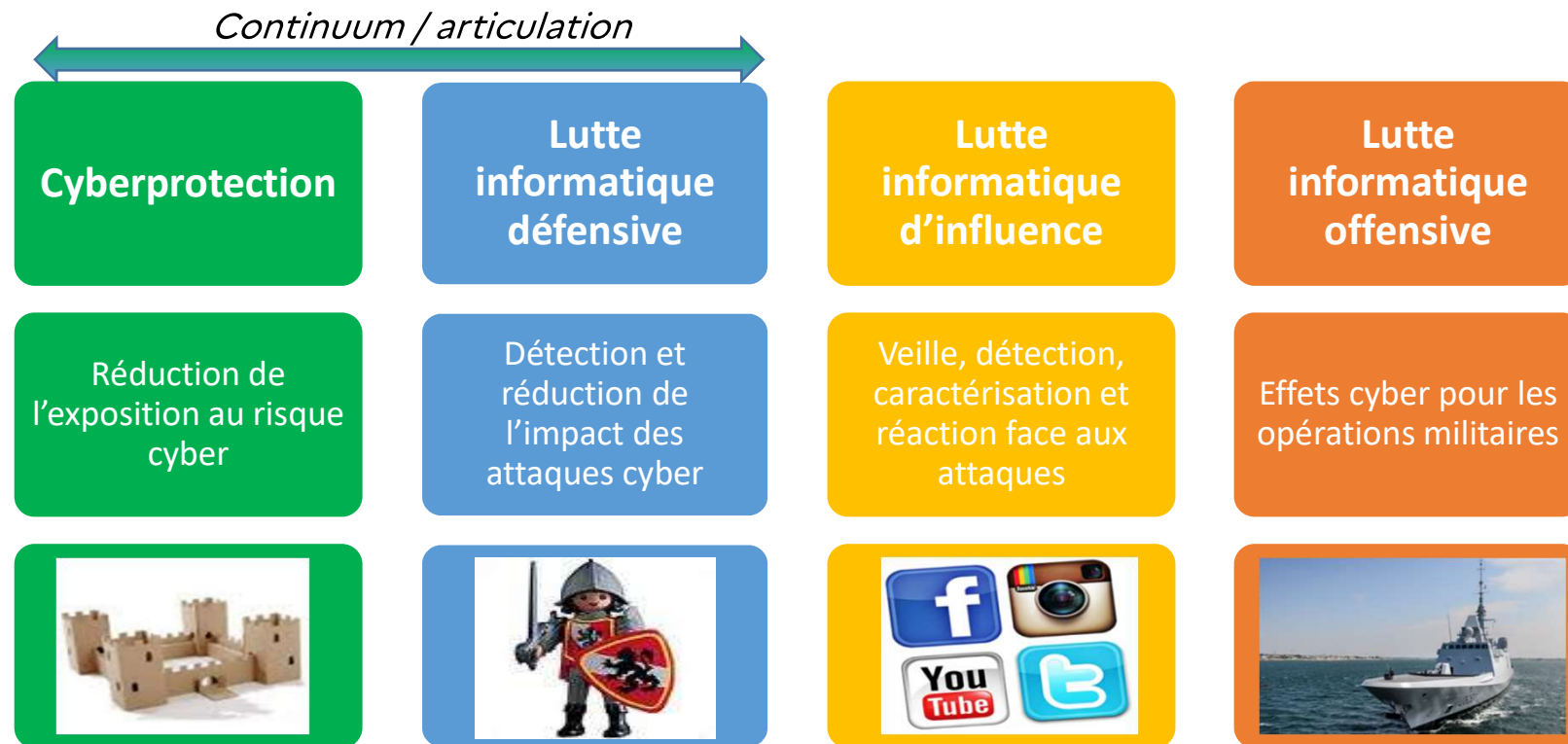
Évolution des effectifs cyber
du Ministère des armées sur
la plaque rennaise au cours
de la loi de programmation
militaire 2019-2025

Sommaire

1. Contexte
2. Menaces dans le cyberspace
3. Organisations et acteurs de l' « écosystème » cyber
 - a. En France
 - b. Au sein du MINARM
 - c. Le COMCYBER
4. Opérations de cyberdéfense
 - a. LIO
 - b. LID
 - c. L2I
5. Ecosystème et coopérations



LA CYBERDÉFENSE AU MINARM



Phasage d'une attaque cyber

Constitution de l'arme cyber sur mesure en fonction de la « surface numérique » de la cible.

Implications :

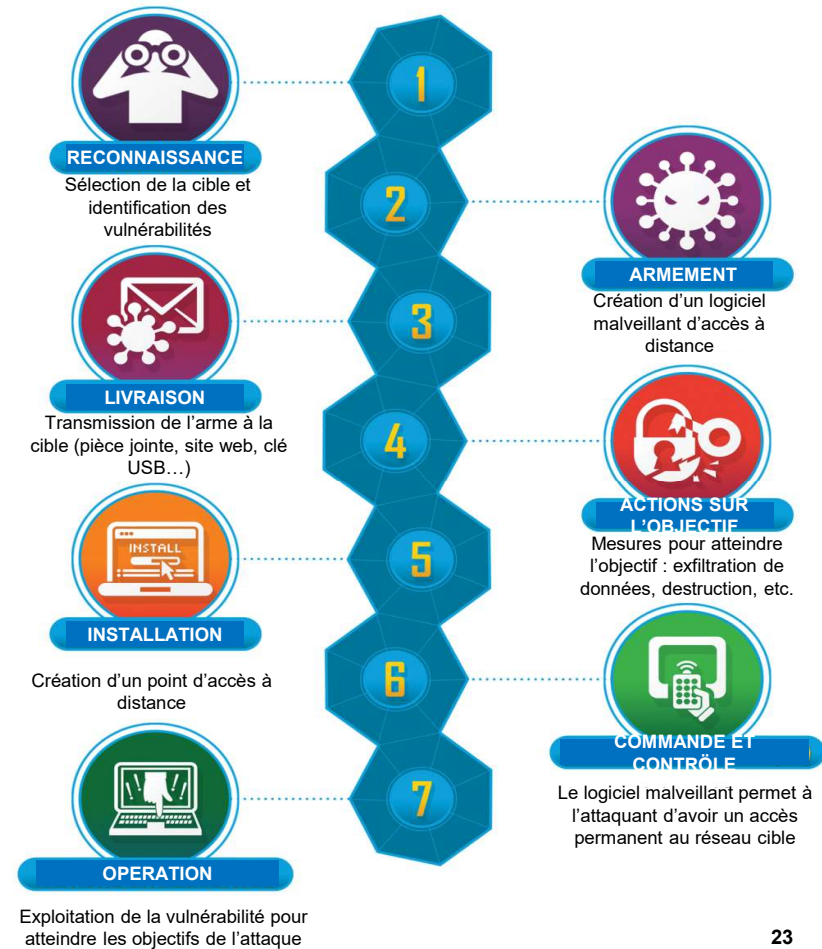
Pour le défensif :

- Maîtrise de la cartographie de nos systèmes et de leurs vulnérabilités, y compris *supply chain* et facteurs humains
- Surveillance ciblée, détection et investigation des comportements anormaux (caractérisation), capacité de leurrage de l'attaquant
- Capacité de remédiation et de réponse

Pour l'offensif :

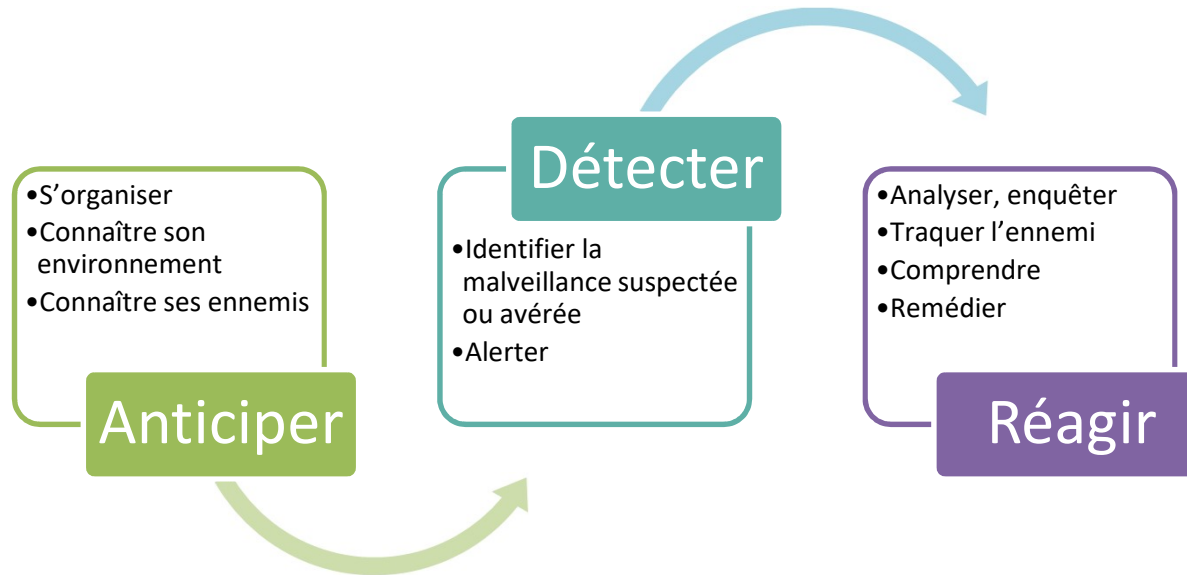
- Besoins de renseignement technique sur les systèmes cibles
- Opérations coordonnées multicanaux (physique, numérique, informationnel)
- Discrétion et furtivité, selon les types d'opérations
- Recherche de la persistance

4. Opérations de cyberdéfense



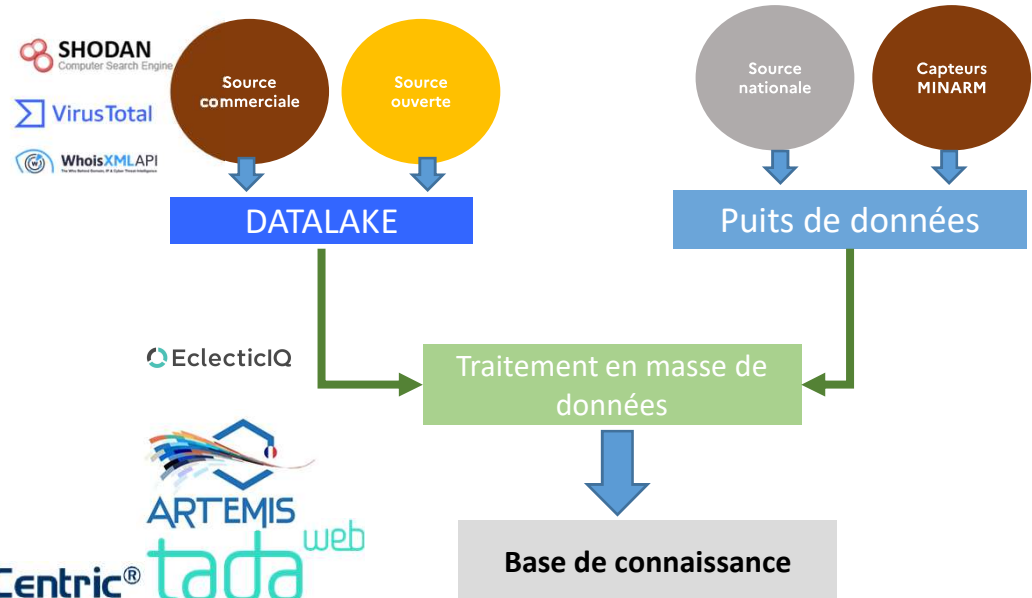
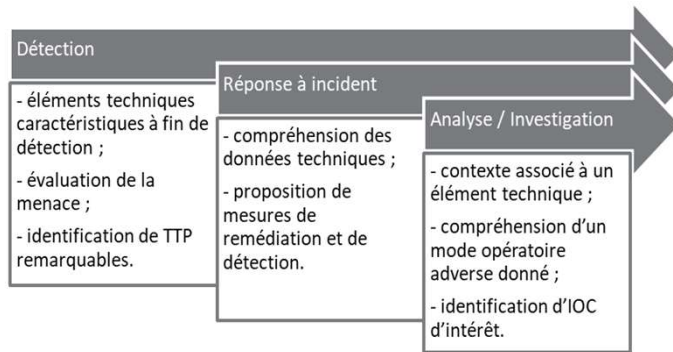
LA CYBERDÉFENSE AU MINARM

Les principes de la Lutte Informatique Défensive



LA CYBERDÉFENSE AU MINARM

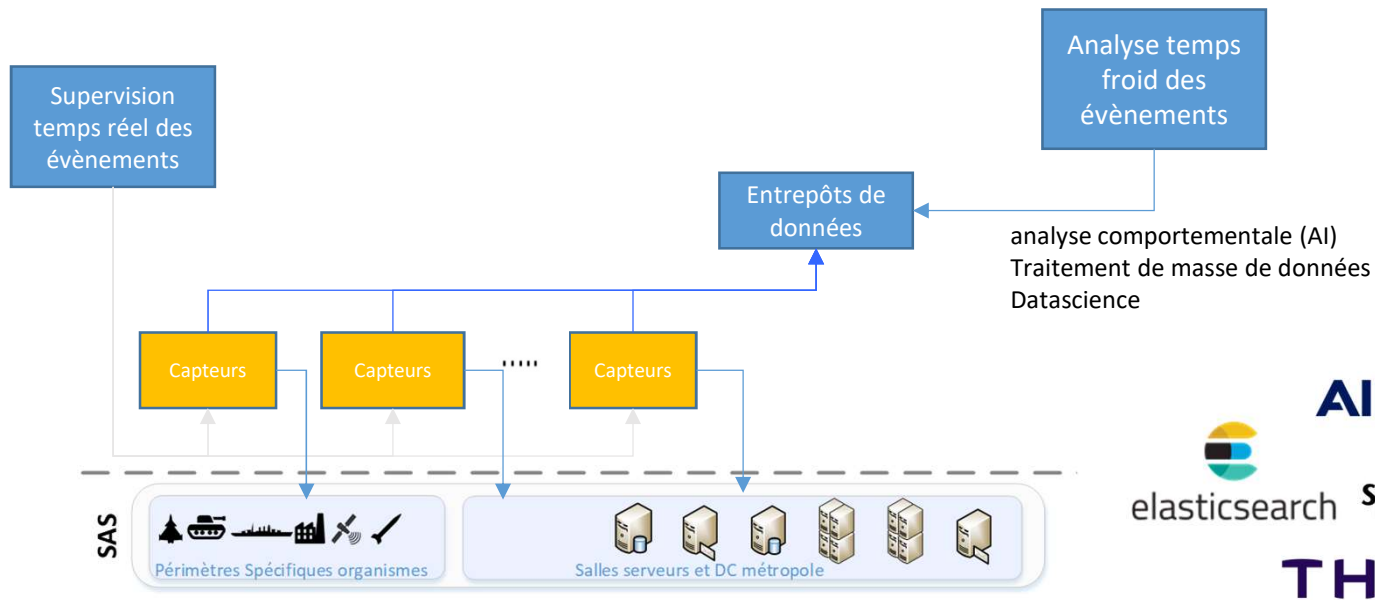
ANTICIPER : connaître l'adversaire



LA CYBERDÉFENSE AU MINARM

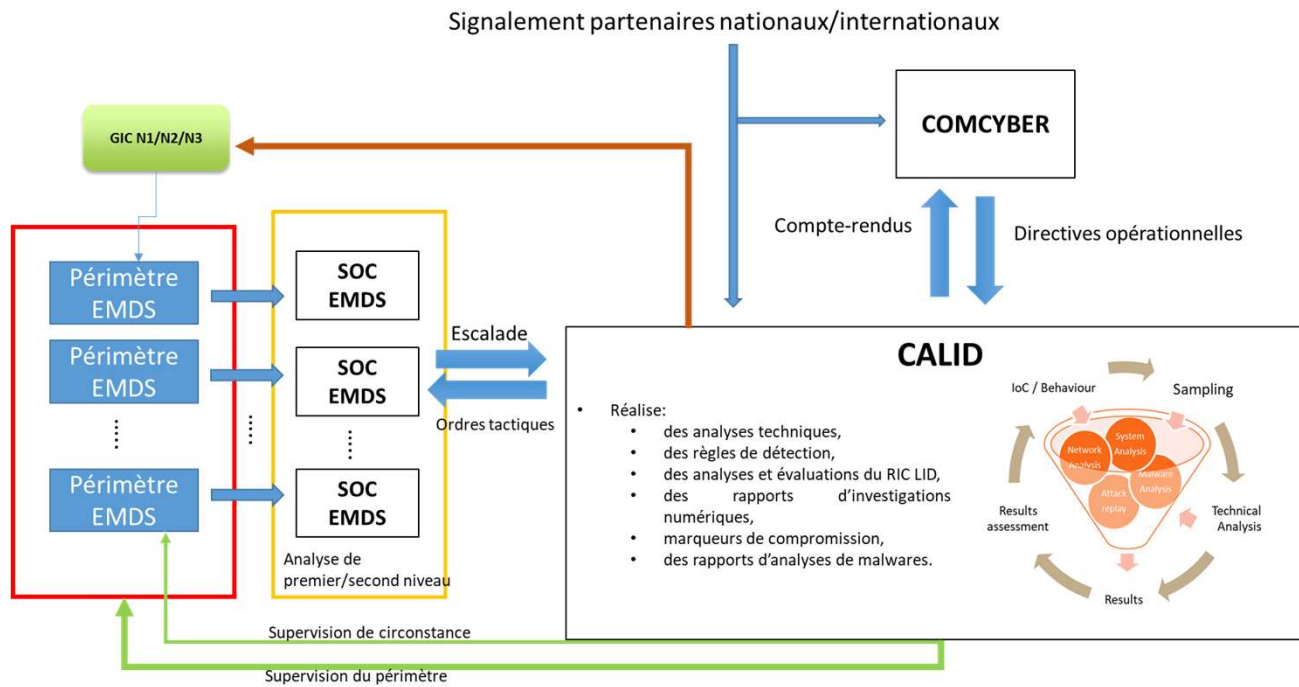


DETECTER : produire, collecter et alerter



LA CYBERDÉFENSE AU MINARM

REAGIR : analyser, traquer et remédier



LID : supervision et hypervision

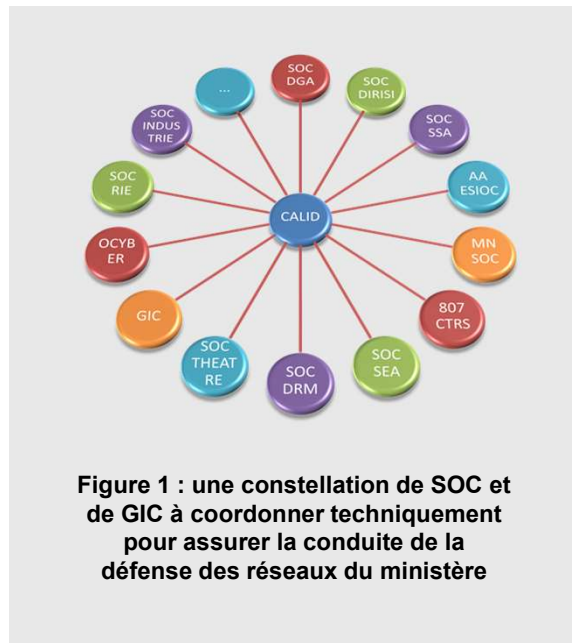


Figure 1 : une constellation de SOC et de GIC à coordonner techniquement pour assurer la conduite de la défense des réseaux du ministère

→ Concept d'hypervision

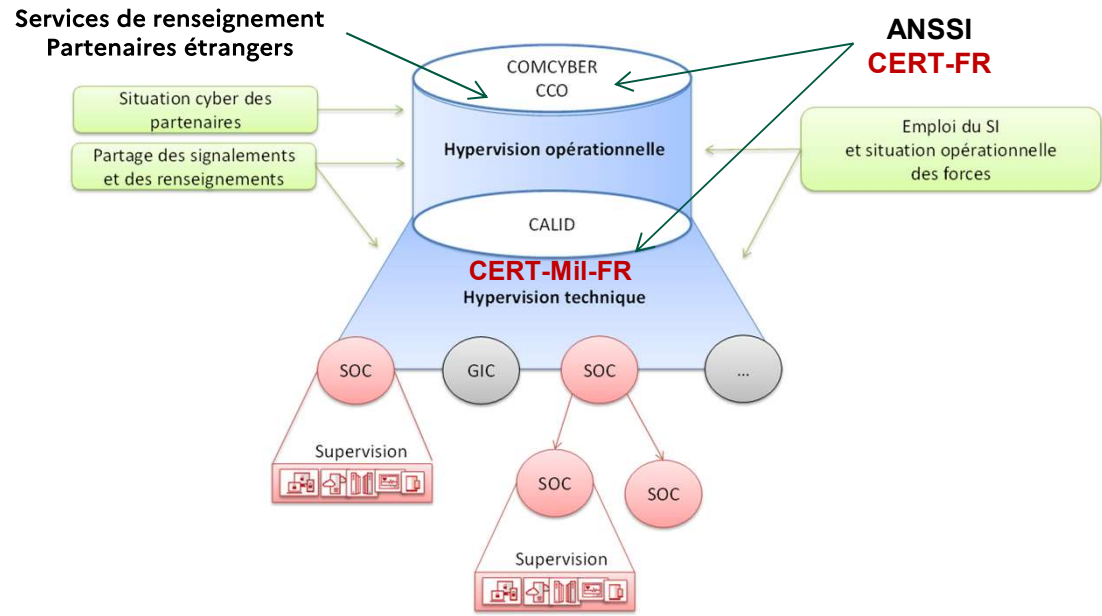
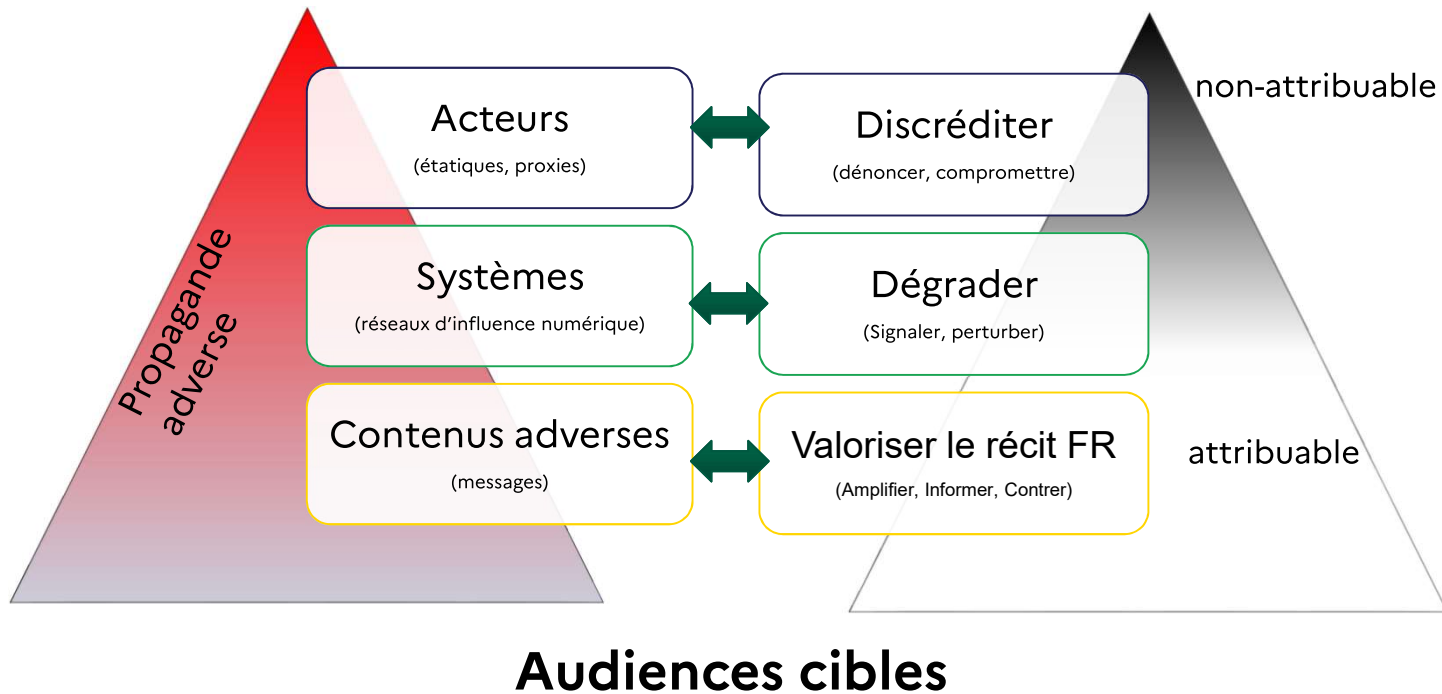


Figure 2 : Hypervision globale

L2I : les grands axes de réponse

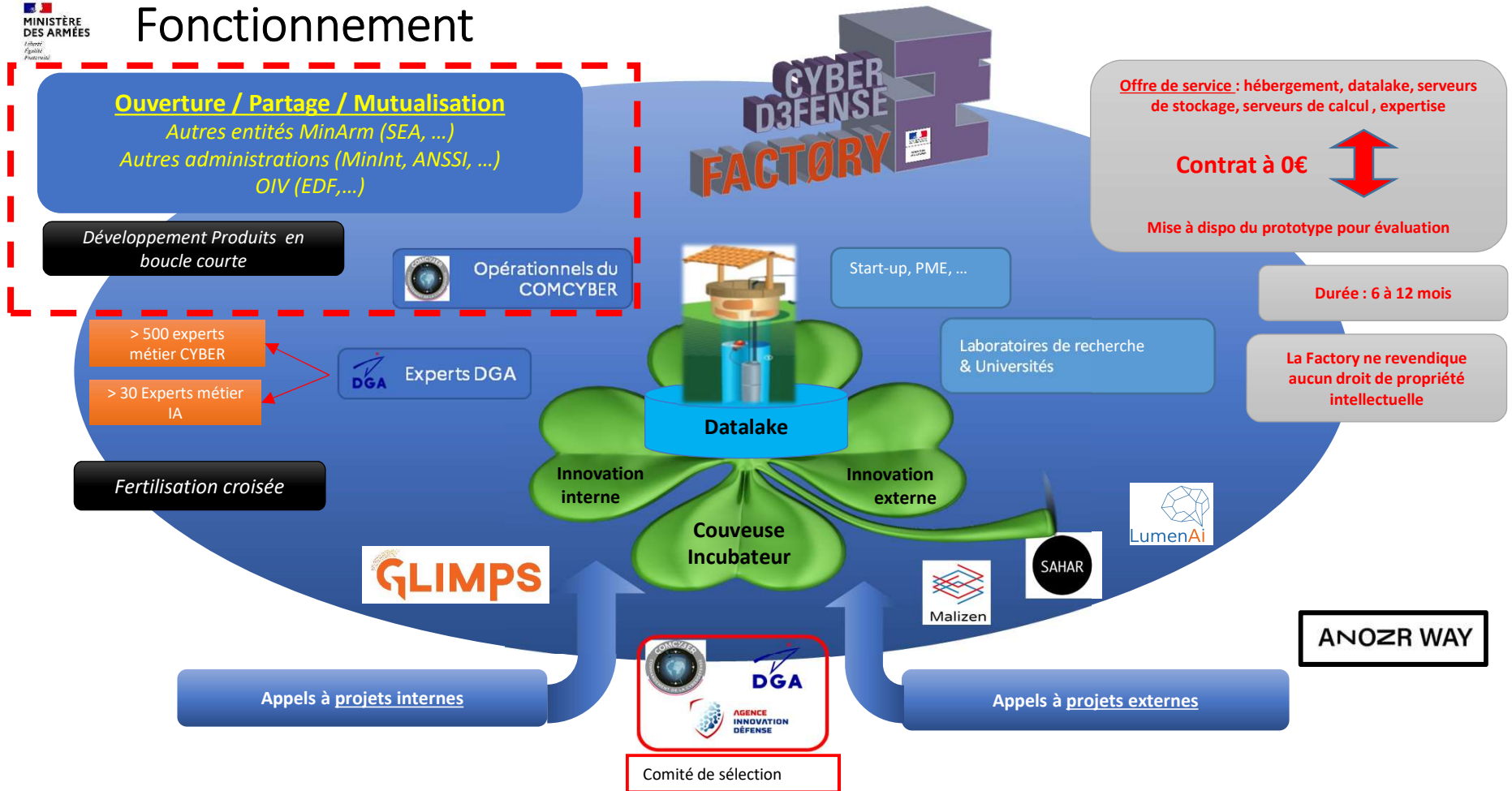


Sommaire

1. Contexte
2. Menaces dans le cyberspace
3. Organisations et acteurs de l' « écosystème » cyber
 - a. En France
 - b. Au sein du MINARM
 - c. Le COMCYBER
4. Opérations de cyberdéfense
 - a. LIO
 - b. LID
 - c. L2I
5. Ecosystème et coopérations



Fonctionnement



Catalyseur d'innovation et de projets

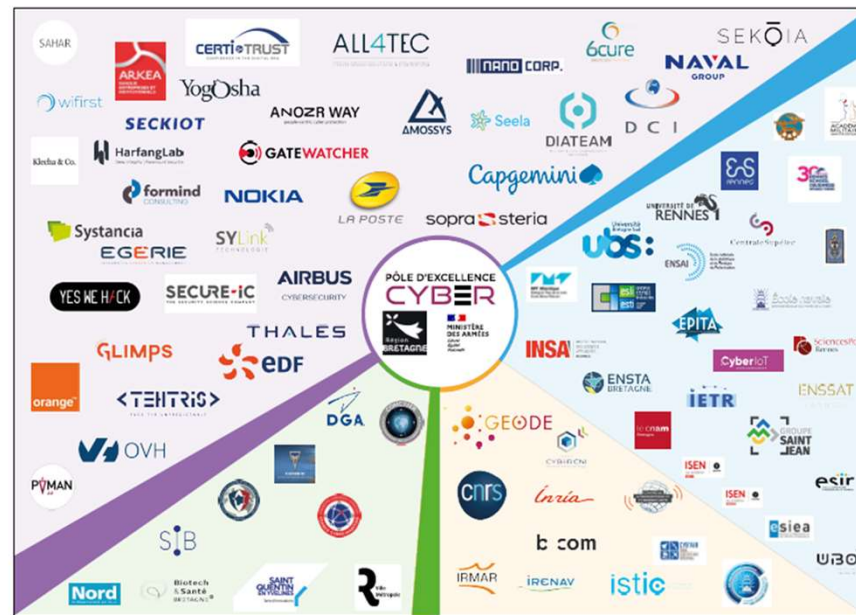
- Créé en 2014 par le Conseil régional de Bretagne et le ministère des Armées (Pacte Défense Cyber).
- **Vocation** : appuyer le développement d'une filière cyber régalienne.
- **Objectif** : stimuler l'offre de formation, la recherche académique et le développement industriel en cyber.
- **Un évènement majeur** : l'European Cyber Week (4000 participants et 85 exposants en 2021).

NOS PARTENAIRES



NOS MEMBRES

Industriels
PME-PMI
Start-ups



Écoles et
Universités

Institutions
publiques

Laboratoires
de recherche

Partenariats internationaux

