LE CYBERESPACE : CONFLICTUALITÉ ET COOPÉRATION ENTRE LES ACTEURS
OTC

Jalon 2 : Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français

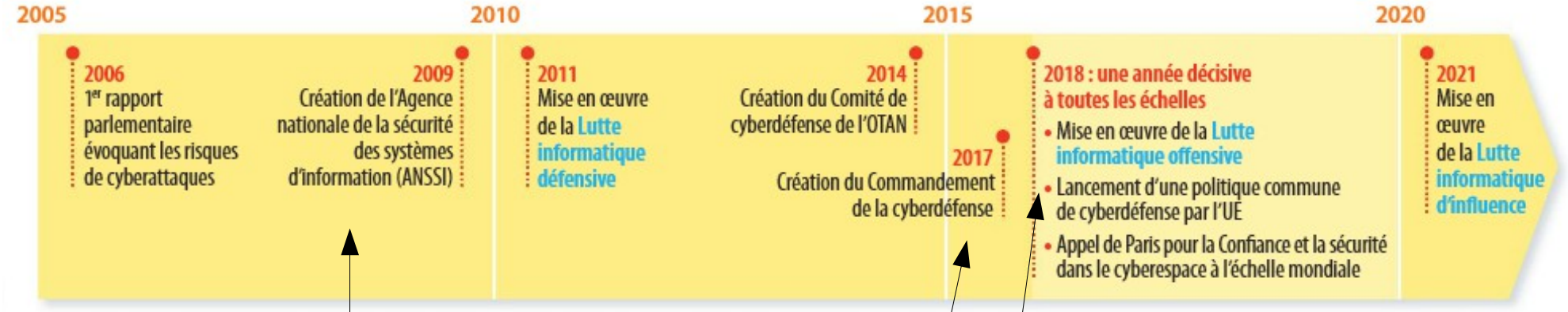
=> comment penser la souveraineté d'un État dans un cyberespace ouvert et avec des outils techniques largement dépendants des acteurs non nationaux ? …. *En quoi l'État est-il encore souverain dans le cyberespace ?*
=> comment envisager des partenariats européens pour gagner en autonomie ?
=> *en quoi la cyberdéfense doit-elle nécessairement aller vers la cyberoffensive ?*

CYBERDEFENSE : ensemble de mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels (ANSSI)

… à ne pas confondre avec….

CYBERCRIMINALITE : ensemble des crimes et délits perpétrés sur les réseaux numériques

CYBERSECURITE : état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées (..) dans ce système.



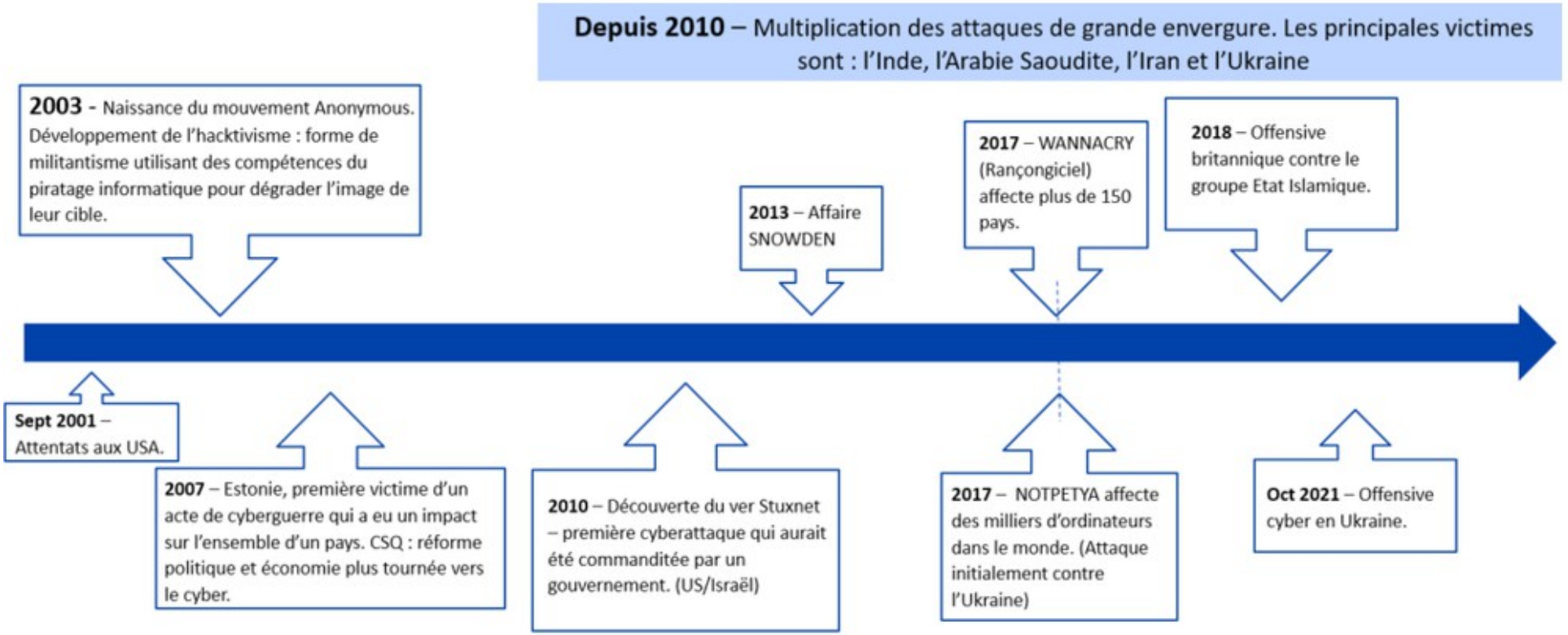
2008 livre blanc sur la défense et la sécurité nationale

RGPD (UE)
Décidé en 2016
Appliqué en 2018

LID (Lutte informatique défensive) : politique française destinée à faire face à un risque, une menace ou à une cyberattaque réelle.

LIO (Lutte informatique offensive) : politique française destinée à mettre en difficulté les infrastructures numériques d'un adversaire.

L2I (Lutte informatique d'influence) : politique française destinée à repérer et lutter contre les fausses informations circulant dans le cyberespace.



Cyberdéfense

Lutte Informatique Offensive (LIO)

La lutte informatique offensive à des fins militaires (LIO) recouvre l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels.

L'arme cyber vise, dans le strict respect des règles internationales, à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données.

Lutte Informatique Défensive (LID)

La LID regroupe l'ensemble des actions, techniques et non techniques, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle, en vue de préserver notre liberté d'action.

La LID couvre principalement trois de ces missions : anticiper, détecter et réagir et complète les missions : prévenir, protéger et attribuer. Elle contribue ainsi à la résilience des armées et plus globalement à l'élaboration des stratégies de réponse aux niveaux ministériel et interministériel.

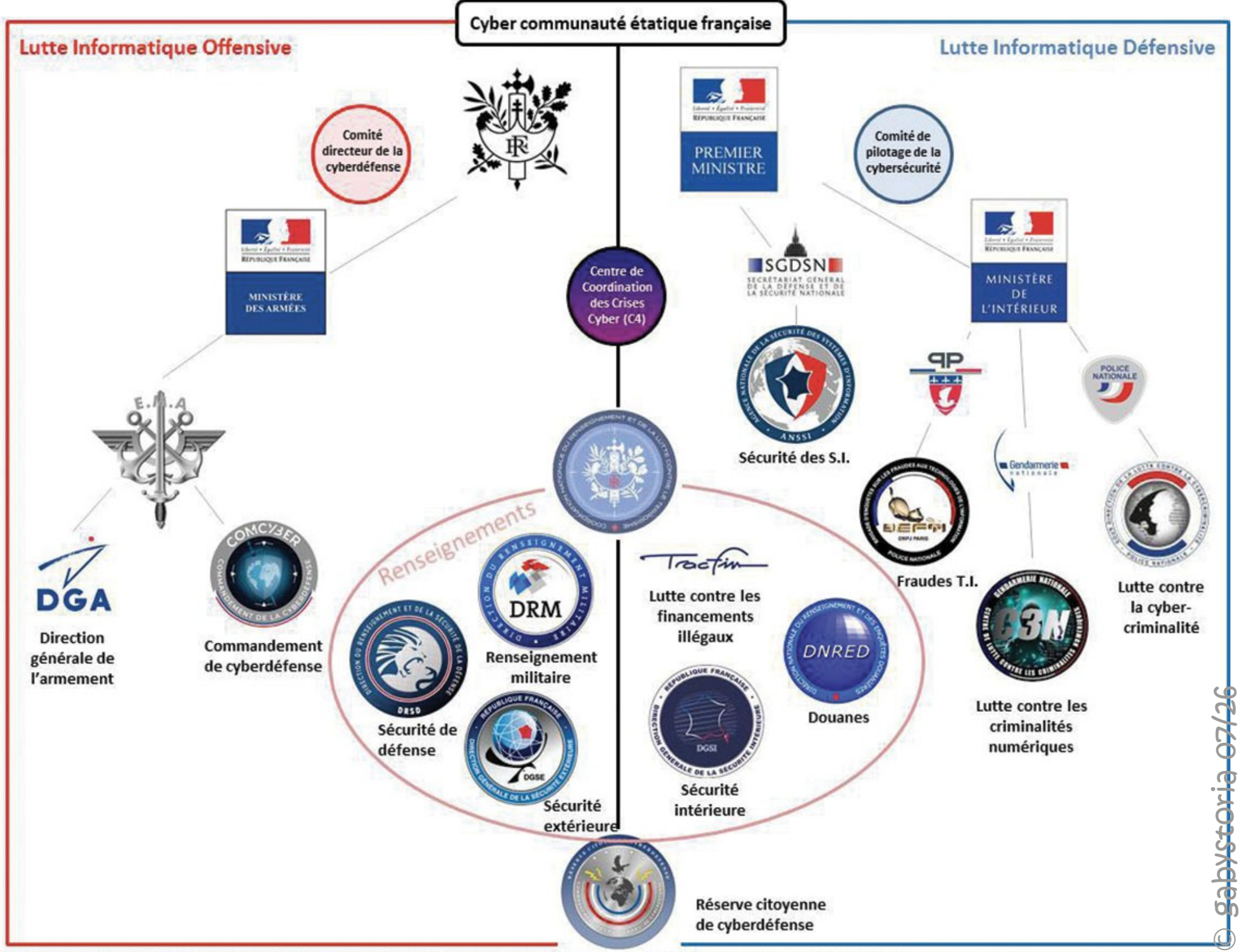


Illustration d'après «Organisation de l'Etat français en cas de crise cyber majeure », Martial Le Guédard, IHENSJ, 2019

Schéma n° 2 : Architecture simplifiée de la cyber-influence de l'État islamique en 2015

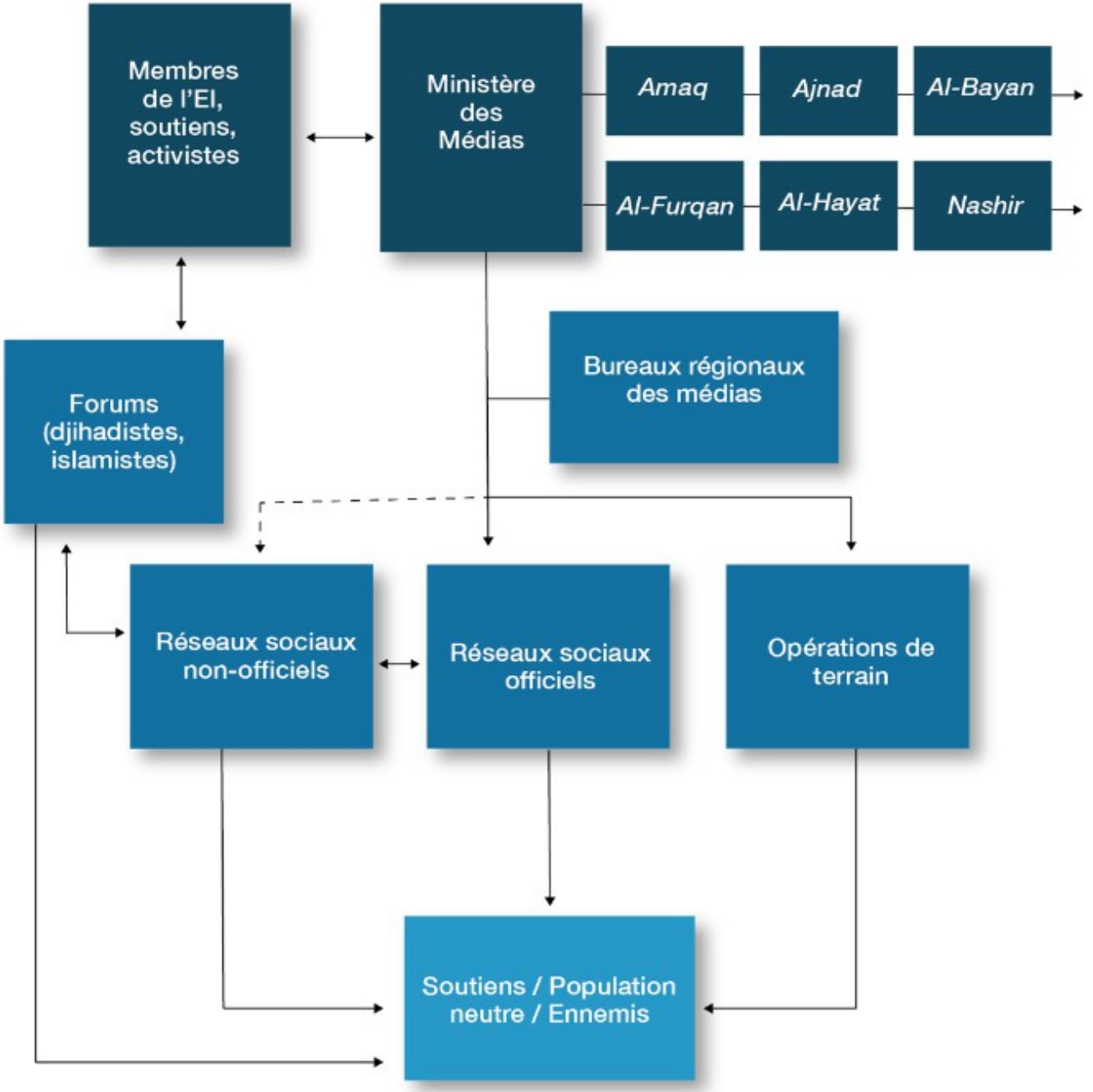


Schéma n° 3 : Architecture simplifiée de la cyber-influence aux États-Unis

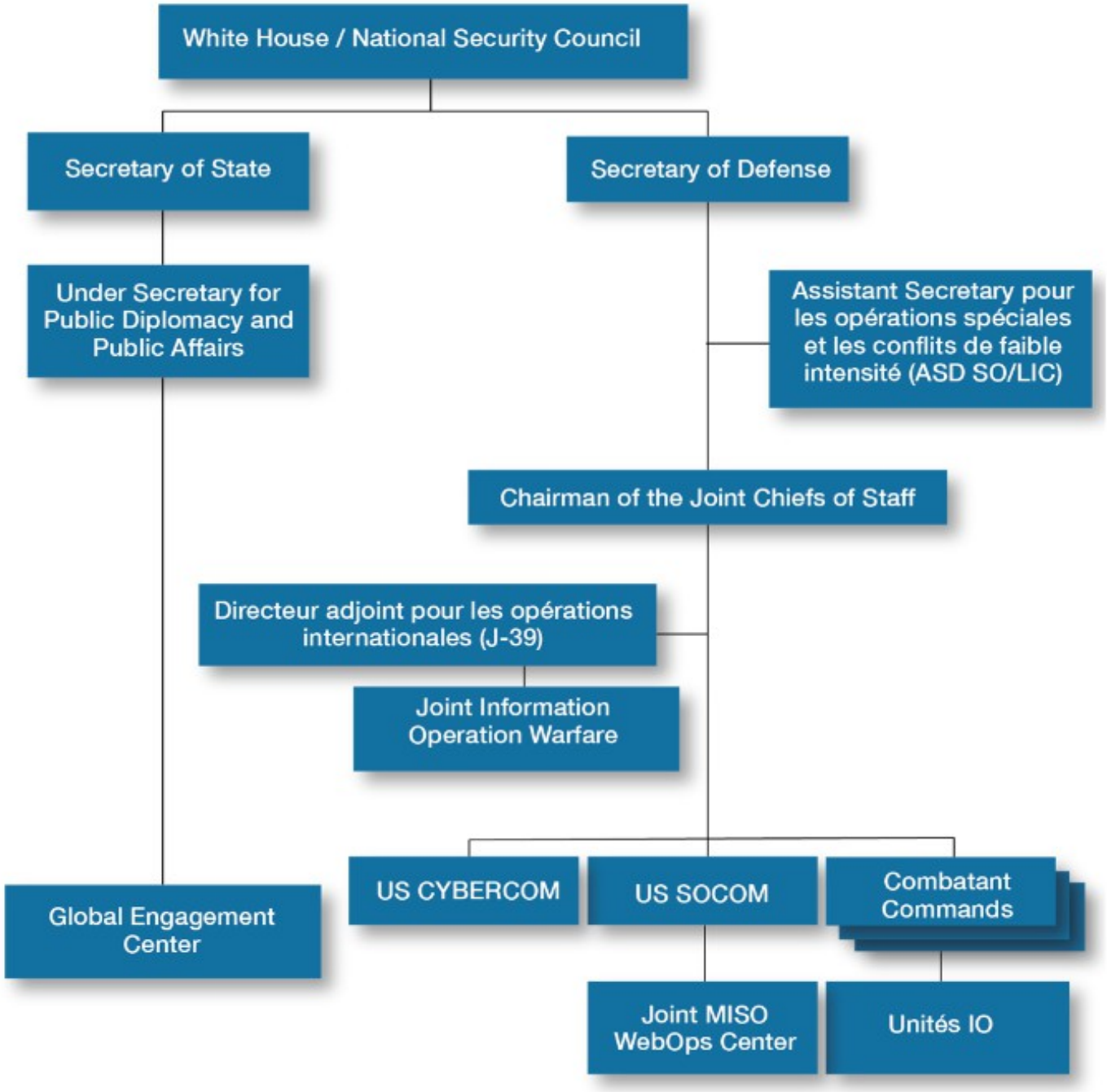
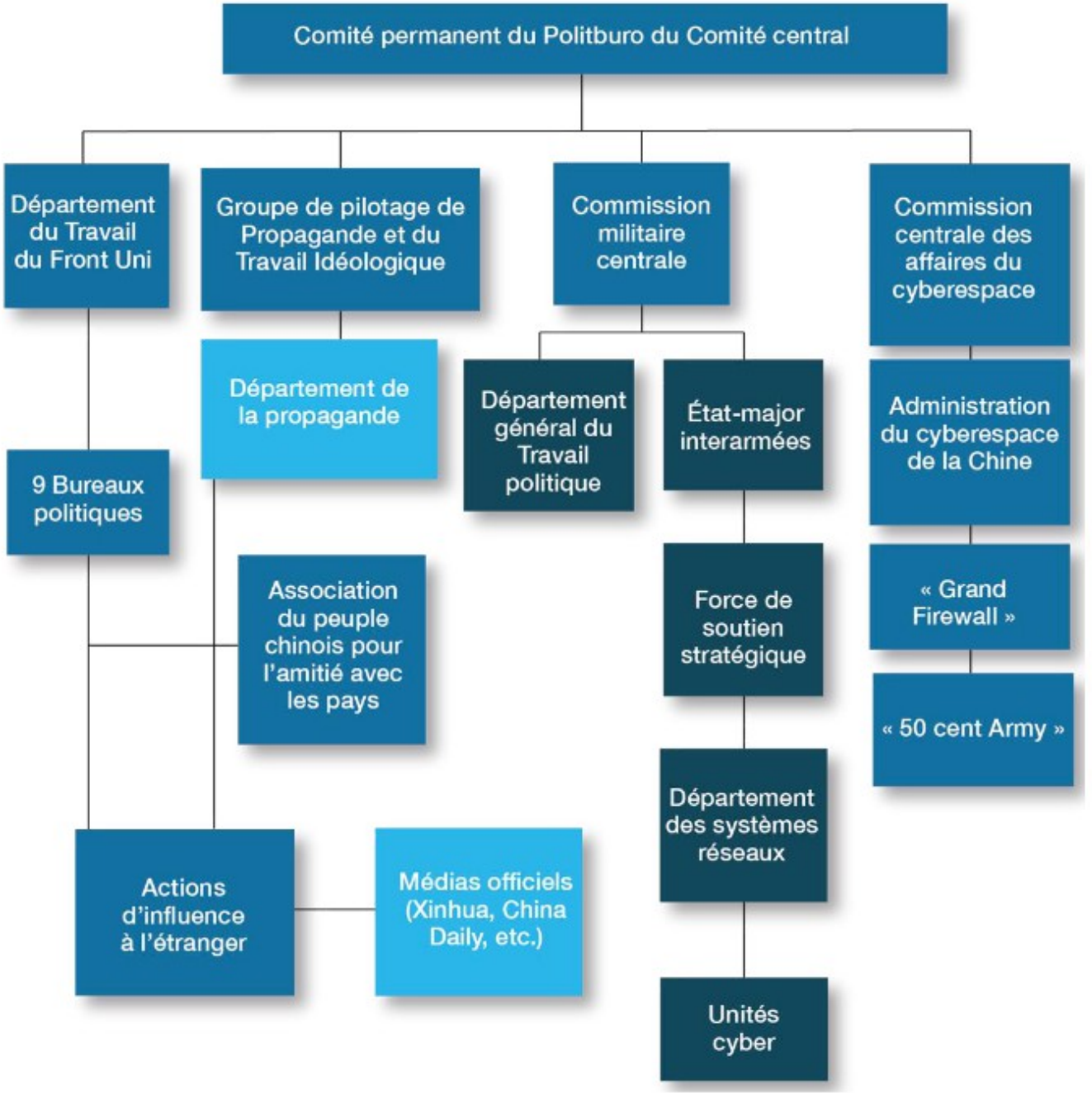
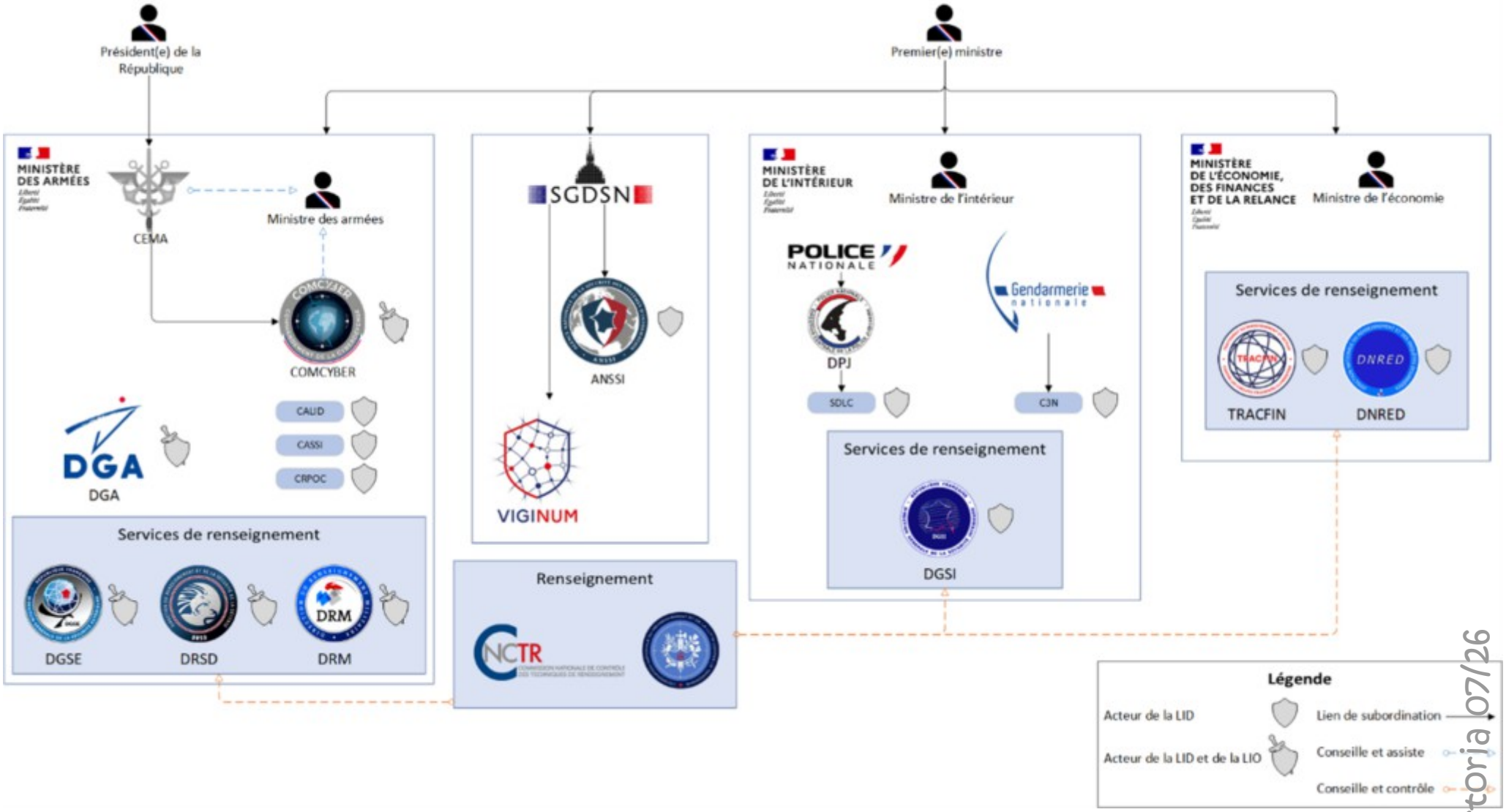


Schéma n° 5 : Architecture simplifiée de la cyber-influence en Chine



ANNEXES



Les opérations de « cyber-influence »
Les nouveaux enjeux de la lutte informationnelle

De l'influence à la lutte informationnelle dans le cyberespace

Stratégie militaire d'influence et opérations d'information

L'influence dans la doctrine OTAN

- **Communication stratégique (Influence)**
  - **Cohérence d'information (IMEI)**
    - **Action d'information**
    - **Soutien/ engagement**
    - **Opérations psychologiques (PSYOPS)**
  - **Affaires publiques**
    - **Contre-mesures informationnelles**

Campagnes d'influence

Connaissance de l'environnement informationnel

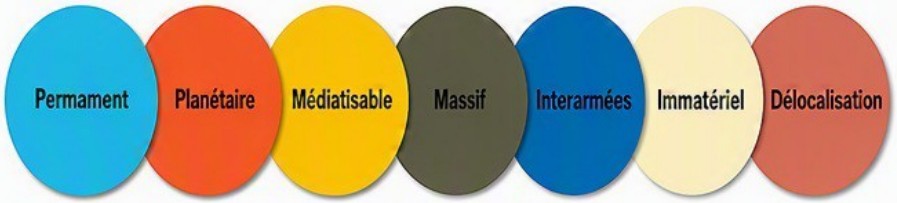
↓

Formulation de contenus et de la « story-informationnelle »

↓

Diffusion

Les caractéristiques de ce nouveau domaine de lutte



Enjeux militaires

Déception contre une force adverse

Actions sur l'environnement humain d'une opération

L'avenir de la guerre de l'information

Technologies clés

- **Intelligence artificielle** (ex. : bots plus authentiques, anticipation des tendances)
- **Hyperpersonnalisation** (ex. : ciblage individualisé, exploitation de l'IA conversationnelle)
- **Modélisation de contenus** (ex. : deepfakes, simulation de comportements)
- **Blockchain** (ex. : authentification des contenus, lutte contre la manipulation)

Enjeux pour la France

- Un aggiornamento nécessaire
- Faire émerger une chaîne de communication stratégique intégrée en mettant l'accent sur l'action interministérielle et l'action politique
- **Revaloriser la place de l'influence dans les armées** (soutien de connaissance, parcours de carrière, soulagement opérationnel)
- **Mobiliser le secteur privé et la société civile** (associer les acteurs de la communication et de l'intelligence économique, accroître la résilience sociétale)

Enjeux pour la France

- Un appauvrissement nécessaire
- Faire émerger une chaîne de communication stratégique intégrée en mettant l'accent sur l'action interministérielle et l'action politique
- **Revaloriser la place de l'influence dans les armées** (soutien de connaissance, parcours de carrière, soulagement opérationnel)
- **Mobiliser le secteur privé et la société civile** (associer les acteurs de la communication et de l'intelligence économique, accroître la résilience sociétale)

Infographie Ifri, 2021 | Source : M. Goya, "Théoriser le Malware", *Cyberdefense revue stratégique*, n° 15, printemps 2019 ; M. Goya, "La potion Cyber", *Cahiers de la pensée mili-terre*, n° 56, 2019 ; M. Yakemtchouk, "Désinformation, cyberdéfense et forces armées", *Revue de la Gendarmerie nationale*, n° 1, 2020.