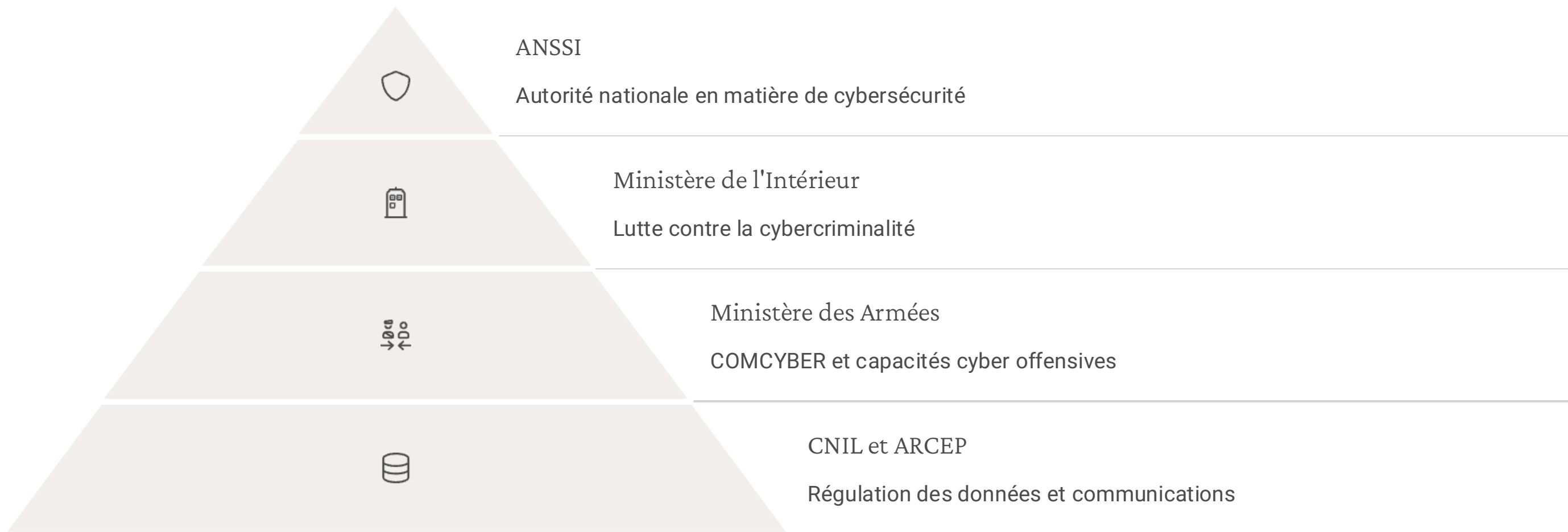


# Enjeux de la sécurité pour la société numérique

**SL** par Stéphane LARCHER



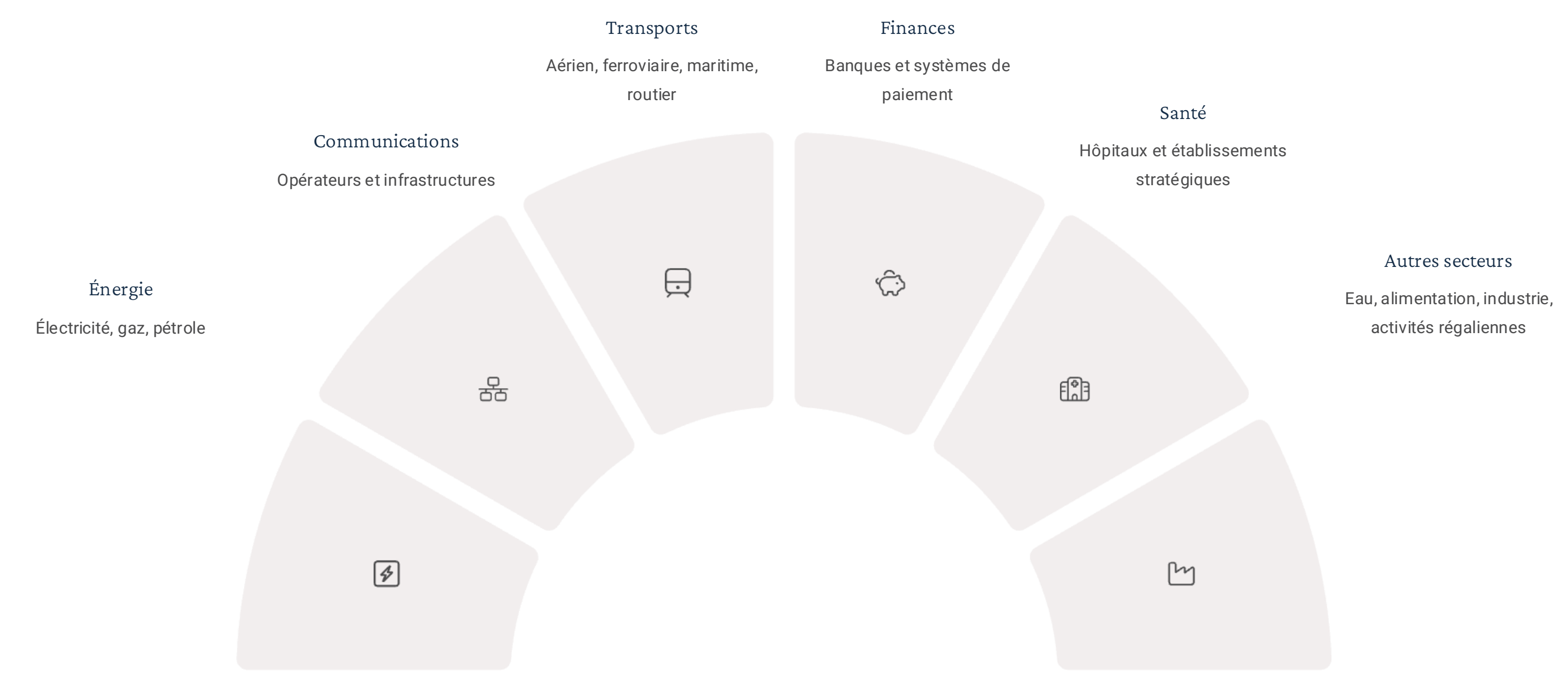
# Architecture institutionnelle de la cybersécurité en France



L'ANSSI constitue l'autorité nationale en matière de cybersécurité. Créée en 2009 et rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), elle remplit plusieurs missions essentielles : prévention et protection, détection et réaction, qualification et certification, sensibilisation et formation.

Le Ministère de l'Intérieur intervient via l'OCLCTIC et la BEFTI pour lutter contre la cybercriminalité, tandis que le Ministère des Armées développe des capacités cyber offensives via le COMCYBER. La CNIL régule la protection des données personnelles et l'ARCEP assure la sécurité des réseaux de communications.

# Les Opérateurs d'Importance Vitale (OIV)



Les OIV sont des organisations publiques ou privées dont les activités sont jugées indispensables au maintien du potentiel de guerre ou économique, à la sécurité ou à la survie de la Nation, et à la santé ou à la vie de la population. La désignation comme OIV entraîne des obligations légales strictes définies par la Loi de Programmation Militaire (LPM) et ses décrets d'application.

Ces obligations incluent la désignation d'un RSSI-IV, l'établissement d'une politique de sécurité, la cartographie des systèmes d'information, l'application de règles de sécurité minimales, des audits réguliers et la notification des incidents dans les 24h.

# La sécurité dans les différents secteurs d'activité

Secteur de la santé	Secteur financier	Secteur industriel
Transformation numérique avec le DMP, la télémédecine et les dispositifs médicaux connectés.	Écosystème complexe incluant banques, assurances, fintech et systèmes de paiement.	Spécificités : systèmes SCADA, automates programmables, protocoles industriels, contraintes temps réel.
Vulnérabilités spécifiques : systèmes legacy non patchables, équipements biomédicaux obsolètes, personnel peu sensibilisé.	Menaces spécifiques : APT (Lazarus, Carbanak), fraude, DDoS, supply chain, insider threats.	Vulnérabilités : systèmes non conçus pour la sécurité, impossibilité de patcher, protocoles sans authentification.
Menaces majeures : ransomware (Hôpital de Corbeil-Essonnes), vol de données (tests COVID), sabotage de dispositifs médicaux.	Incidents marquants : Bangladesh Bank (81M\$ volés), NotPetya sur BNP Paribas, ransomware sur Crédit Mutuel.	Attaques emblématiques : Stuxnet, Triton/Trisis, Industroyer, Colonial Pipeline.

# Les métiers de la cybersécurité



## Gouvernance et pilotage

RSSI, Risk Manager Cyber, Compliance Officer



## Protection et défense

Architecte Sécurité, Ingénieur Sécurité, Administrateur PKI



## Détection et réaction

Analyste SOC, Threat Hunter, Expert Réponse à Incident



## Audit et tests

Auditeur Sécurité, Pentester, Analyste Vulnérabilités



## Expertise transverse

Expert Forensique, Cryptologue, DPO

Les parcours professionnels en cybersécurité incluent des formations initiales (Masters spécialisés, Licences professionnelles) et des certifications professionnelles (CISSP, CISM, CEH, OSCP). L'évolution de carrière type passe par les étapes Junior (0-3 ans), Confirmé (3-7 ans), Senior (7-12 ans) et Expert (12+ ans).

# Fondements conceptuels de l'identité numérique

## Identité déclarative

- Informations volontairement fournies
- Profils sur réseaux sociaux
- Formulaires d'inscription
- CV en ligne
- Biais de présentation de soi

## Identité agissante

- Comportements en ligne observables
- Historique de navigation
- Interactions sociales numériques
- Transactions effectuées
- Patterns comportementaux

## Identité calculée

- Données déduites et inférées
- Scoring et profilage
- Prédictions algorithmiques
- Corrélations big data
- Shadow profiles

## Identité subie

- Données publiées par des tiers
- Tags et mentions
- Photos non consenties
- Données vendues/échangées
- Fuites de données

L'identité numérique représente l'ensemble des traces, données et attributs qui caractérisent un individu ou une entité dans l'espace numérique. Elle se compose de plusieurs couches interconnectées et comprend des attributs primaires (identifiants uniques), secondaires (pseudonymes), comportementaux (géolocalisation) et sociaux (graphe social).



# Enjeux de la vie privée à l'ère numérique



## Privacy Paradox

Contradiction entre préoccupations exprimées et comportements réels de partage d'informations, expliquée par des biais cognitifs, l'asymétrie d'information, les coûts de transaction élevés, les effets de réseau et le design manipulateur.



## Risques pour la vie privée

Surveillance de masse (programmes étatiques, surveillance commerciale), profilage et discrimination (redlining numérique, discrimination algorithmique), vol et usurpation d'identité (phishing, deepfakes), atteintes à la réputation (revenge porn, cyberharcèlement).



## Nouveaux paradigmes de protection

Privacy by Design (proactif, préventif, intégré dès la conception), minimisation des données (collecte limitée, anonymisation), souveraineté des données personnelles (self-sovereign identity, consentement granulaire).







# Technologies de gestion de l'identité



## Authentification moderne

Évolution des paradigmes du mot de passe à l'authentification sans mot de passe, de la sécurité par l'obscurité à la transparence, de l'authentification statique à continue.



## Facteurs d'authentification

Ce que je sais (mots de passe), ce que j'ai (tokens), ce que je suis (biométrie), où je suis (géolocalisation), comment je me comporte (dynamique de frappe).



## Standards modernes

FIDO2/WebAuthn (authentification sans mot de passe), OAuth 2.0/OpenID Connect (délégation d'autorisation), SAML 2.0 (fédération d'identité).



## Gestion des identités et des accès

Architecture IAM moderne avec Identity Provider, Service Provider, Identity Broker, et modèles d'autorisation RBAC, ABAC, PBAC.



# Protection avancée de la vie privée



## Chiffrement et cryptographie

Chiffrement homomorphe (calculs sur données chiffrées), Secure Multi-party Computation (calculs distribués confidentiels), Zero-Knowledge Proofs (preuves sans révélation).



## Anonymisation et pseudonymisation

Differential Privacy (bruit statistique calibré), K-anonymité et extensions (indistinguabilité dans un groupe), Tokenisation (remplacement réversible).



## Communications privées

Messagerie chiffrée de bout en bout (Signal Protocol), Réseaux d'anonymisation (Tor, I2P), Blockchain et privacy (adresses pseudonymes, mixing services).





# Cadre juridique et éthique



## Le RGPD : révolution réglementaire

Principes fondamentaux : licéité/loyauté/transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité et confidentialité.



## Accountability et gouvernance

Privacy by Design et by Default, Analyse d'impact (DPIA/PIA), Registre des traitements, DPO (Data Protection Officer).



## Droits des personnes concernées

Droit d'accès, de rectification, à l'effacement, à la limitation, à la portabilité, d'opposition.



## Enjeux éthiques émergents

Intelligence artificielle et vie privée (biais algorithmiques), surveillance biométrique, profilage prédictif, neurotechnologies, Internet of Bodies, métavers et identités virtuelles.



# CYBER THREAT ACTIONS

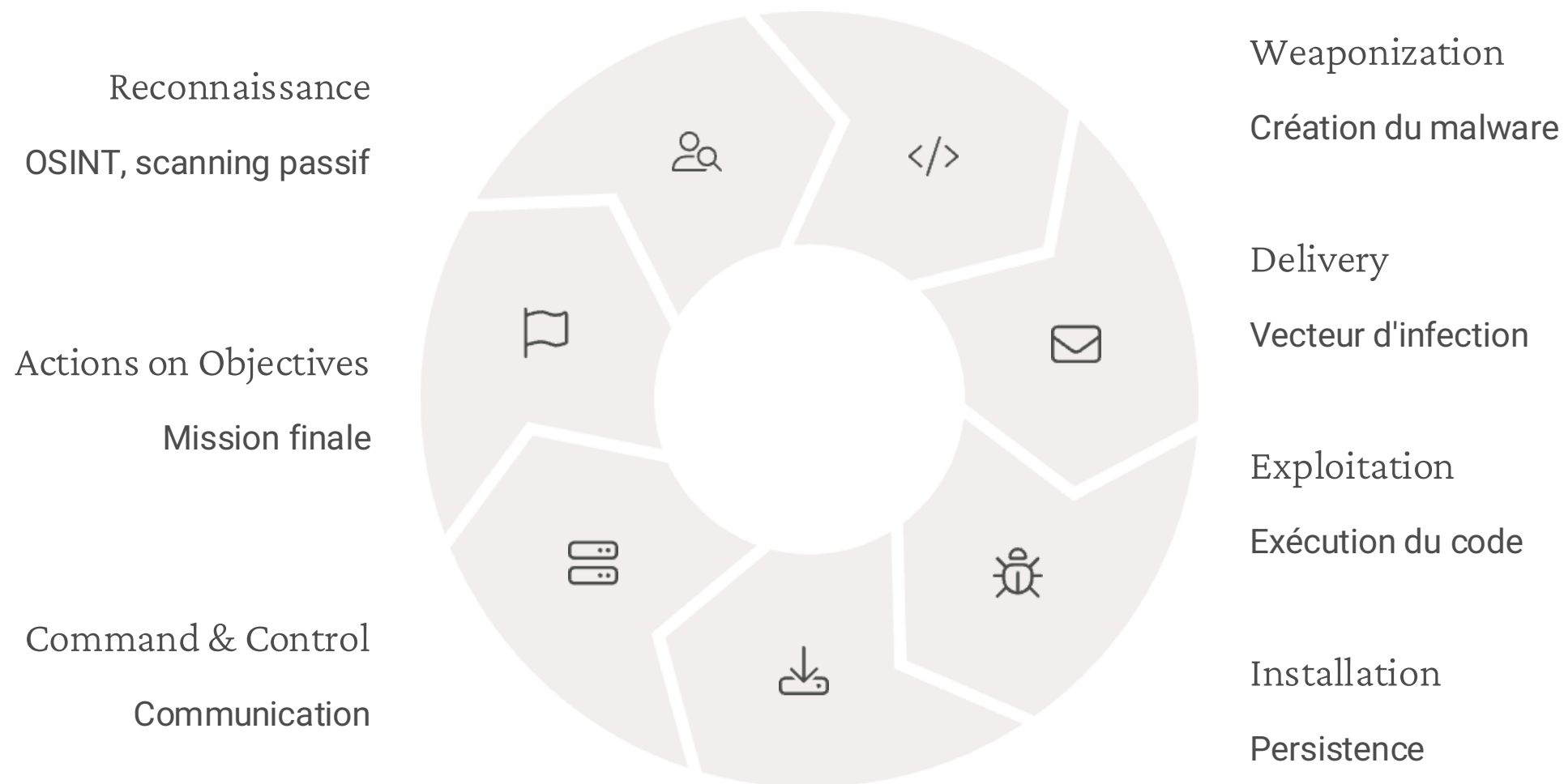
An angry, clandestine disinformation campaign able to frighten cyber operations were the result of a concerted effort to force or for the sake of the world's most powerful cyber powers. The threat actors are the most powerful cyber powers and the most powerful cyber powers. The threat actors are the most powerful cyber powers and the most powerful cyber powers.



# Panorama des acteurs de la menace

Type d'acteur	Motivations	Exemples	Techniques
États-nations (APT)	Espionnage, sabotage, influence	APT28 (Russie), APT41 (Chine), Lazarus (Corée du Nord)	0-day, supply chain, persistance avancée
Cybercriminels	Profit financier	Conti/Ryuk, REvil, LockBit	Ransomware-as-a-Service, phishing, exploitation
Hacktivistes	Idéologie, causes politiques	Anonymous, Killnet, DragonForce Malaysia	DDoS, defacement, doxing, leak de données
Menaces internes	Vengeance, espionnage, profit	Employés mécontents, espions infiltrés	Abus de privilèges, vol de données, sabotage

# Techniques d'attaque avancées



Parmi les techniques d'attaque sophistiquées, on trouve les Supply Chain Attacks (compromission via la chaîne d'approvisionnement), le Living Off The Land (utilisation d'outils légitimes du système) et les attaques sur l'IA et ML (empoisonnement des données, évasion de détection).



# Intelligence économique approfondie

## Cycle du renseignement économique

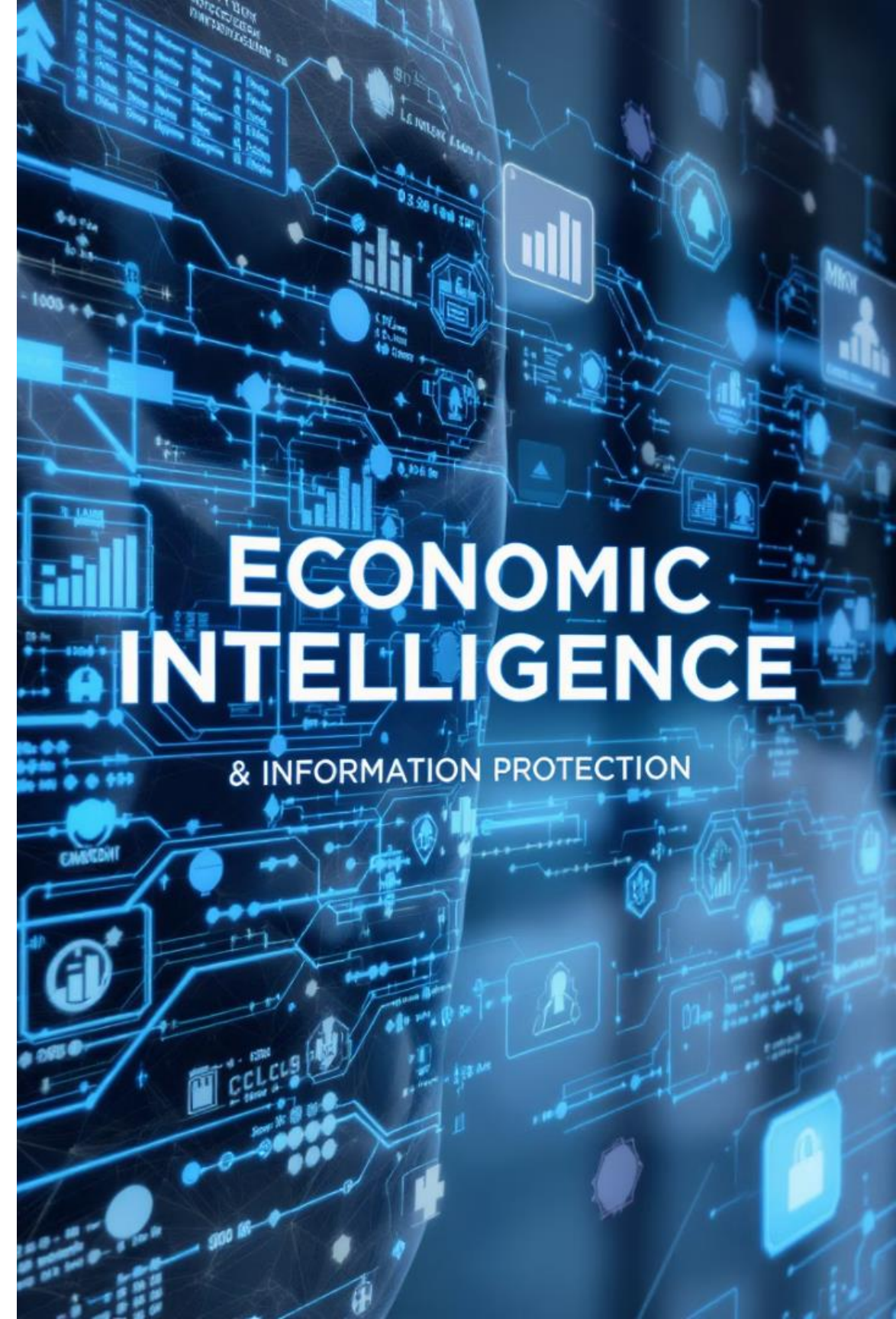
Orientation (définition des besoins), Recherche (collecte multi-sources), Exploitation (analyse et synthèse), Diffusion (communication adaptée), Feedback (amélioration continue).

## Guerre économique moderne

Stratégies offensives incluant la déstabilisation concurrentielle, la manipulation de l'information, le lawfare, la prédation économique et l'influence normative. Cas d'études : Affaire Alstom-GE, guerre des semi-conducteurs, TikTok et souveraineté des données.

## Protection du patrimoine informationnel

Classification de l'information (public, interne, confidentiel, secret, très secret) et contre-intelligence économique (compartimentation, cover stories, désinformation contrôlée, honeypots informationnels).

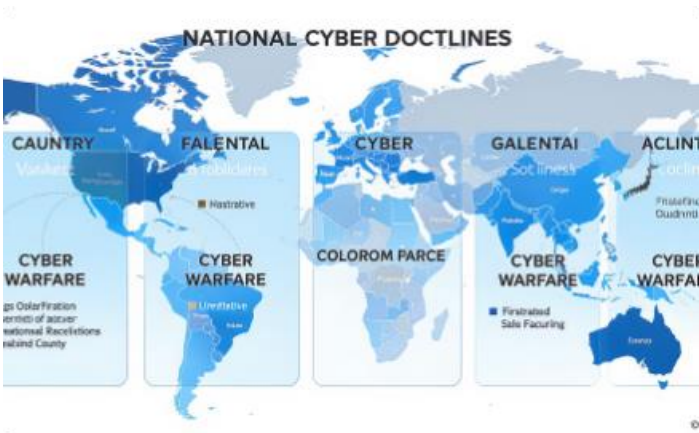


# Dimension géopolitique du cyberspace



Le cyberspace comme 5ème domaine

Caractéristiques uniques : absence de frontières physiques, vitesse de la lumière, asymétrie des coûts attaque/défense, attribution complexe, dommages réversibles/irréversibles.



Doctrines nationales cyber

États-Unis (persistant engagement, defend forward), Russie (guerre de l'information, zones grises), Chine (stratégie des "Trois Guerres", fusion civilo-militaire), France (autonomie stratégique, cyber-dissuasion).



Conflits cyber majeurs

Estonie 2007 (premier cyber-conflit d'ampleur), Géorgie 2008 (coordination cyber-cinétique), Ukraine 2014-présent (laboratoire de cyber-guerre), Moyen-Orient (Stuxnet game-changer).



# Panorama réglementaire et normatif

20

Règles LPM

Obligations pour les OIV

72h

Délai RGPD

Pour notifier une violation

150K

Entités NIS2

Concernées dans l'UE

10M€

Sanction max

Ou 2% du CA mondial

L'architecture réglementaire française repose sur la Loi de Programmation Militaire (LPM) pour les OIV, le Référentiel Général de Sécurité (RGS) pour les administrations, et des réglementations sectorielles comme l'Hébergement de Données de Santé (HDS) pour la santé ou la DSP2 pour la finance.

Au niveau européen, la directive NIS2 étend massivement le périmètre des entités concernées par rapport à NIS1, avec des obligations renforcées et des sanctions plus lourdes. Le Cybersecurity Act établit un cadre de certification européen avec trois niveaux d'assurance (Basic, Substantial, High).

Les standards internationaux incluent la famille ISO/IEC 27000 (notamment 27001 pour les SMSI), le NIST Cybersecurity Framework 2.0 avec ses six fonctions (Govern, Identify, Protect, Detect, Respond, Recover), les CIS Controls et COBIT 2019.

La mise en conformité pratique nécessite une démarche structurée en quatre phases : assessment initial, planification, implémentation, maintien et amélioration. Elle s'appuie sur une documentation complète et des outils de GRC (Governance, Risk, Compliance).