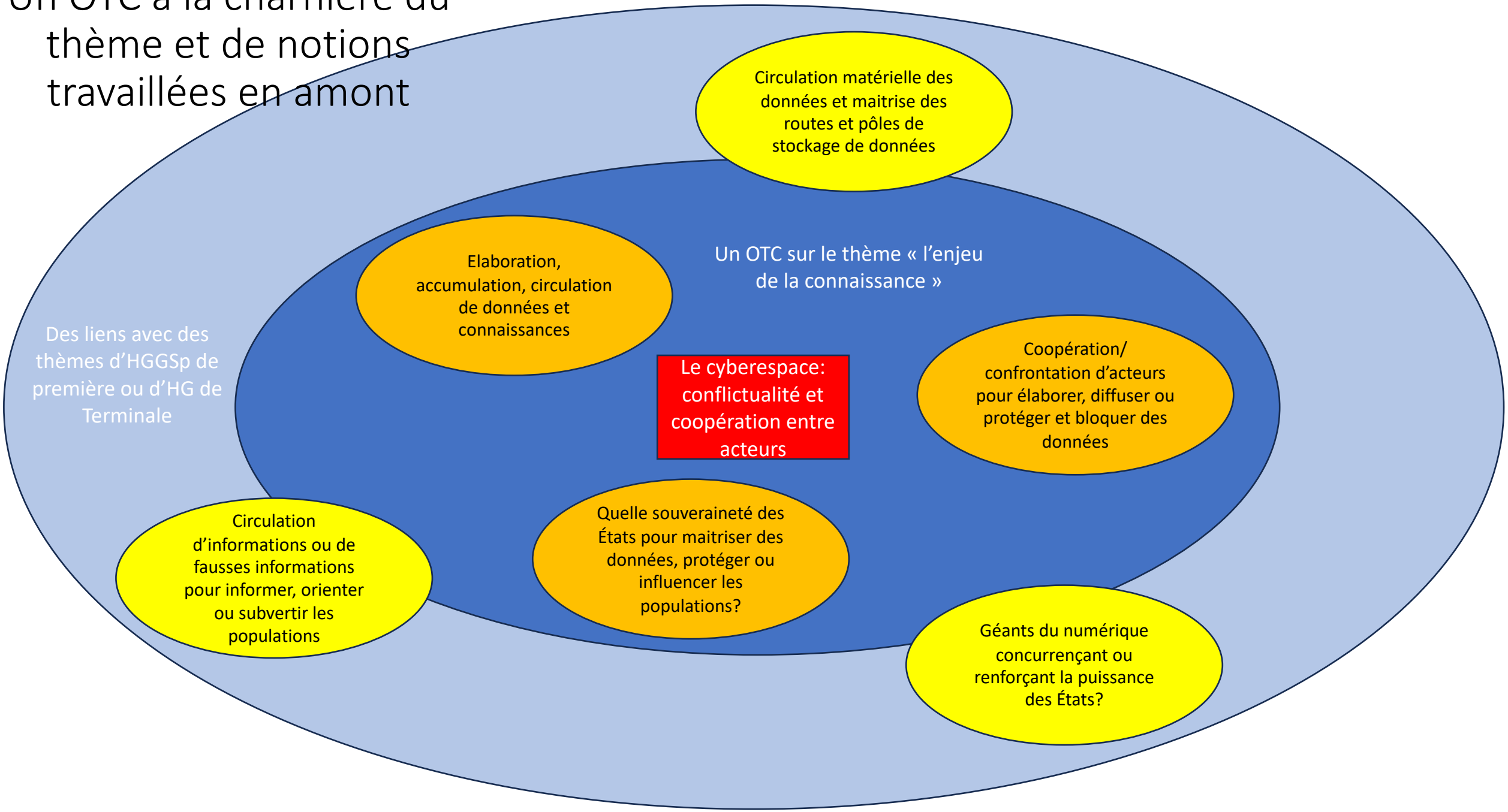
Enseigner un objet de travail conclusif. Le cyberespace: conflictualité et coopération entre les acteurs

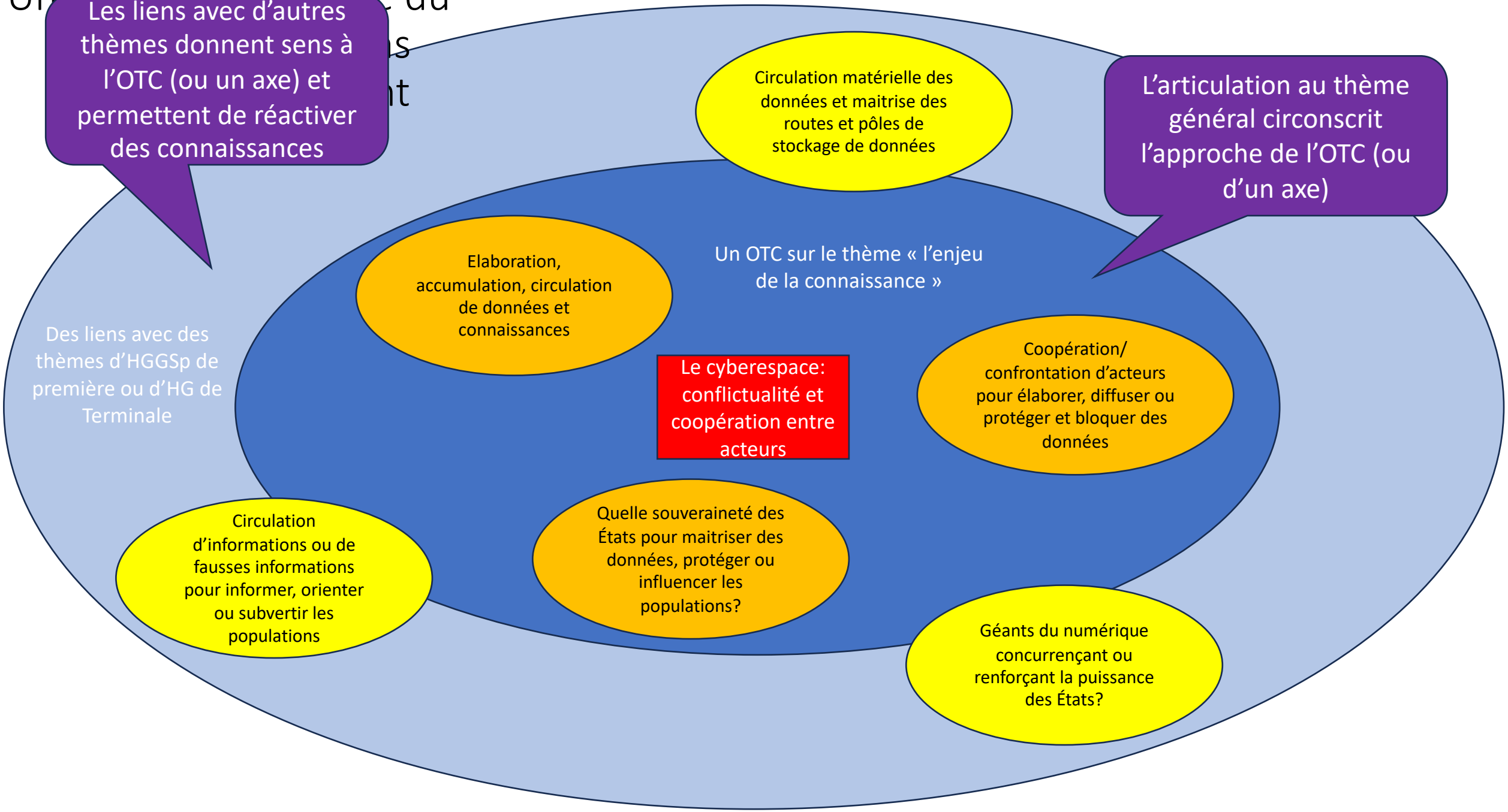
ROOU David-Pierre

IA-IPR histoire géographie

Un OTC à la charnière du thème et de notions travaillées en amont



Un OTC à la charnière du [illegible]

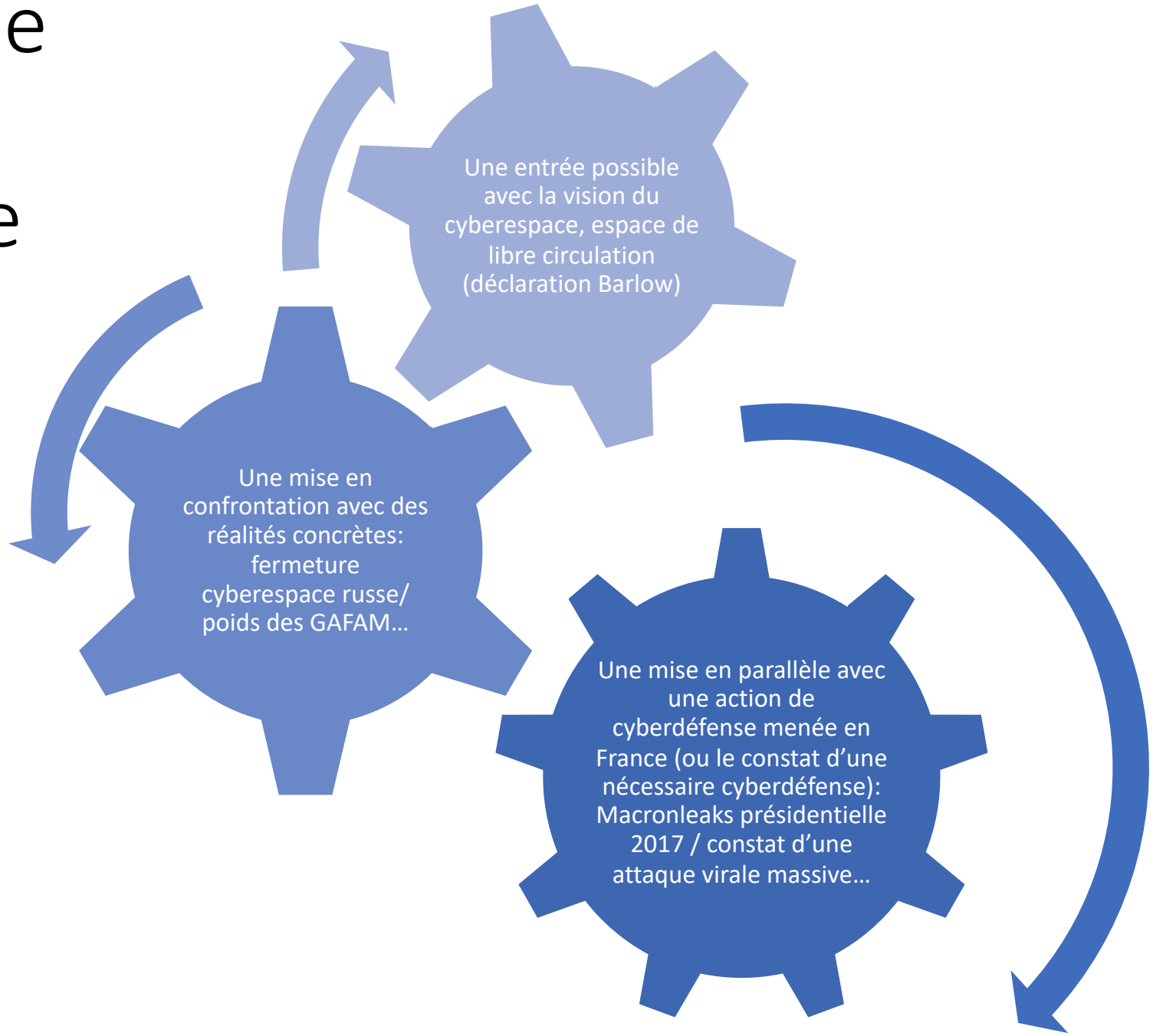


Articuler jalons et axe dans la perspective du thème sur la connaissance

Objet de travail conclusif	**Jalons**
Le cyberespace : conflictualité et coopération entre les acteurs.	- Le cyberespace, entre réseaux et territoires (infrastructures, acteurs, liberté ou contrôle des données…) - Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.

- le cyberespace comme lieu d'élaboration, de circulation et d'accumulation de données, qui sont autant de connaissances, selon les cas et les acteurs impliqués dans leur circulation
  - mises à disposition des usagers,
  - mises à profit pour orienter les comportements et agir sur les sociétés,
  - Visant à gêner le fonctionnement des sociétés ;
- le cyberespace comme lieu de coopération et de confrontation d'acteurs publics et privés, aux objectifs divers. Il s'agira d'envisager
  - la place de ces acteurs dans le cyberespace et leurs interactions,
  - questionner les formes d'élaboration, de diffusion ou de protection de la connaissance ;
- le cyberespace comme lieu interrogeant la réalité de la souveraineté des États quant à leur capacité à
  - Maitriser les flux de données
  - Protéger leurs populations et leurs intérêts.

Entrer dans le thème du cyberespace



Articuler jalons et axe dans la perspective du thème sur la connaissance

Objet de travail conclusif	**Jalons**
Le cyberespace : conflictualité et coopération entre les acteurs.	- Le cyberespace, entre réseaux et territoires (infrastructures, acteurs, liberté ou contrôle des données…) - Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français.

- Une problématique générale possible :

- Comment la structuration du cyberespace parvient-elle à combiner quasi-infinité d'usagers et de réseaux et domination ou contrôle de celui-ci par quelques acteurs en nombre limité ? Comment les interactions entre acteurs de natures et de capacités d'influences très différentes peuvent-elles faire évoluer les relations et les rapports de force entre territoires ? Comment, pour un État mettre en œuvre des politiques de défense prenant pleinement en compte le cyberespace et permettant de préserver les personnes, les activités ainsi que les fondements et les valeurs d'une société ? »

Les deux jalons sont ainsi articulés autour d'une problématique amenant à poser la conflictualité du cyberespace et, en lien l'importance pourun État de créer de nouvelles formes de défense.

Aborder le jalon le cyberespace entre réseaux et territoires

- Problématique possible (par exemple au regard des documents déjà travaillés en introduction):

- Comment le cyber espace, pensé par nombre de ses promoteurs comme un lieu d'échanges ouvert et sans frontières, a-t-il pu devenir un espace de luttes d'influences, de rivalités, et parfois de cloisonnements ? En quoi les interventions des différents acteurs aux objectifs et aux poids très différents dans le cyber espace participent à la définition des rapports de force et de pouvoir entre territoires susceptibles de générer des formes de conflictualité ?

Le cyberespace entre réseaux et territoires: la structuration des données

Les couches du cyberespace (contexte)

- La couche infrastructurelle
- La couche logicielle
- La couche cognitive

Lien th 1. géo terminale

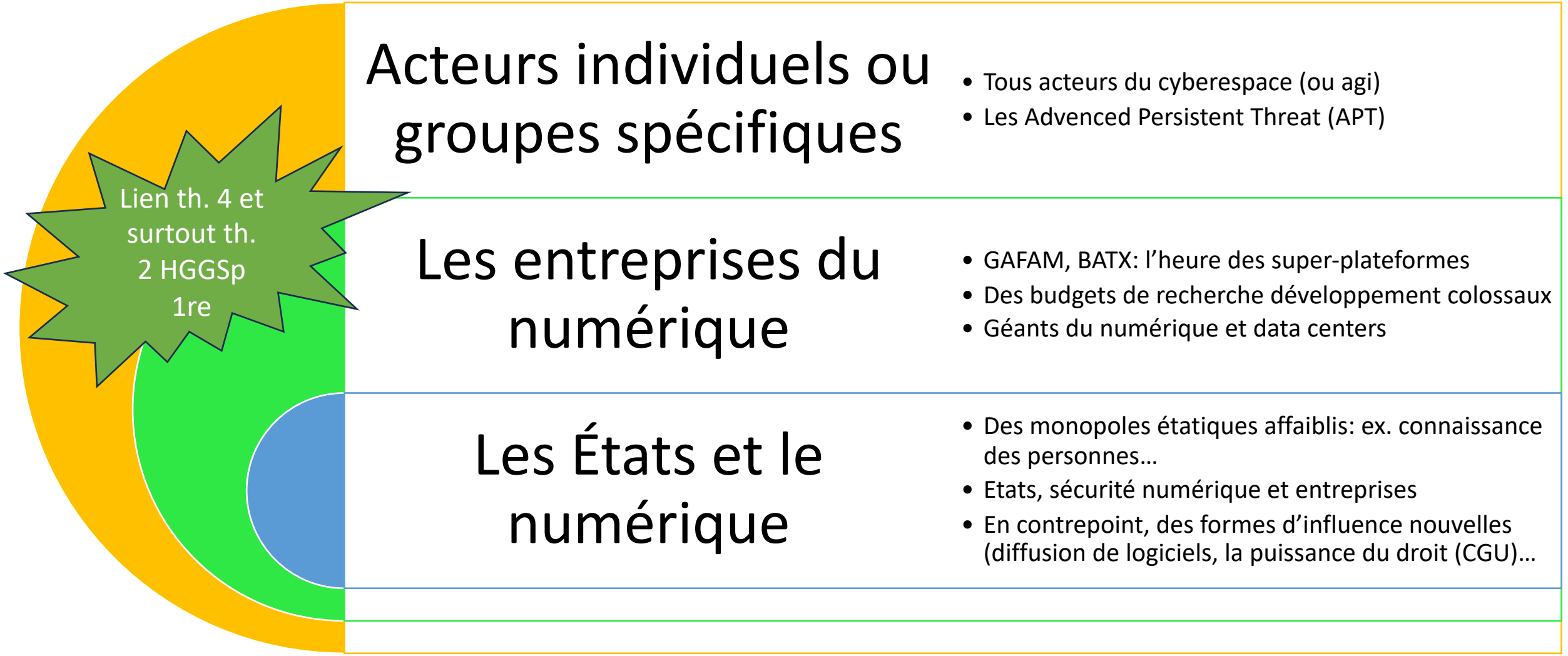
Les données: data ou capta?

- Le monde à l'heure de la « datafication »
- Progrès de la connaissance, progression de la surveillance
- Des données toujours sélectionnées (l'idée de capta)

La territorialisation des données

- Territorialisation des données et *cloud computing*
- Les data center : les Etats-Unis… et quelques autres
- Le routage des données: ouvertures/ fermetures

Le cyberespace entre réseaux et territoires: la diversité des acteurs



Le cyberespace entre réseaux et territoires: marqueurs territoriaux et difficile gouvernance du cyberespace

Stratégies Étatiques

- Le « modèle chinois et ses épigones: « Décider seul comment règlementer son cyberespace »
- Le cyberespace vu des États-Unis ou de l'Union européenne: libre circulation mais protection des populations et surveillance

Quelle gouvernance du cyberespace?

- ICANN vs UIT : gouvernance non Étatique ou interétatique?
- Quels engagements internationaux pour réguler les comportements dans le cyberespace?

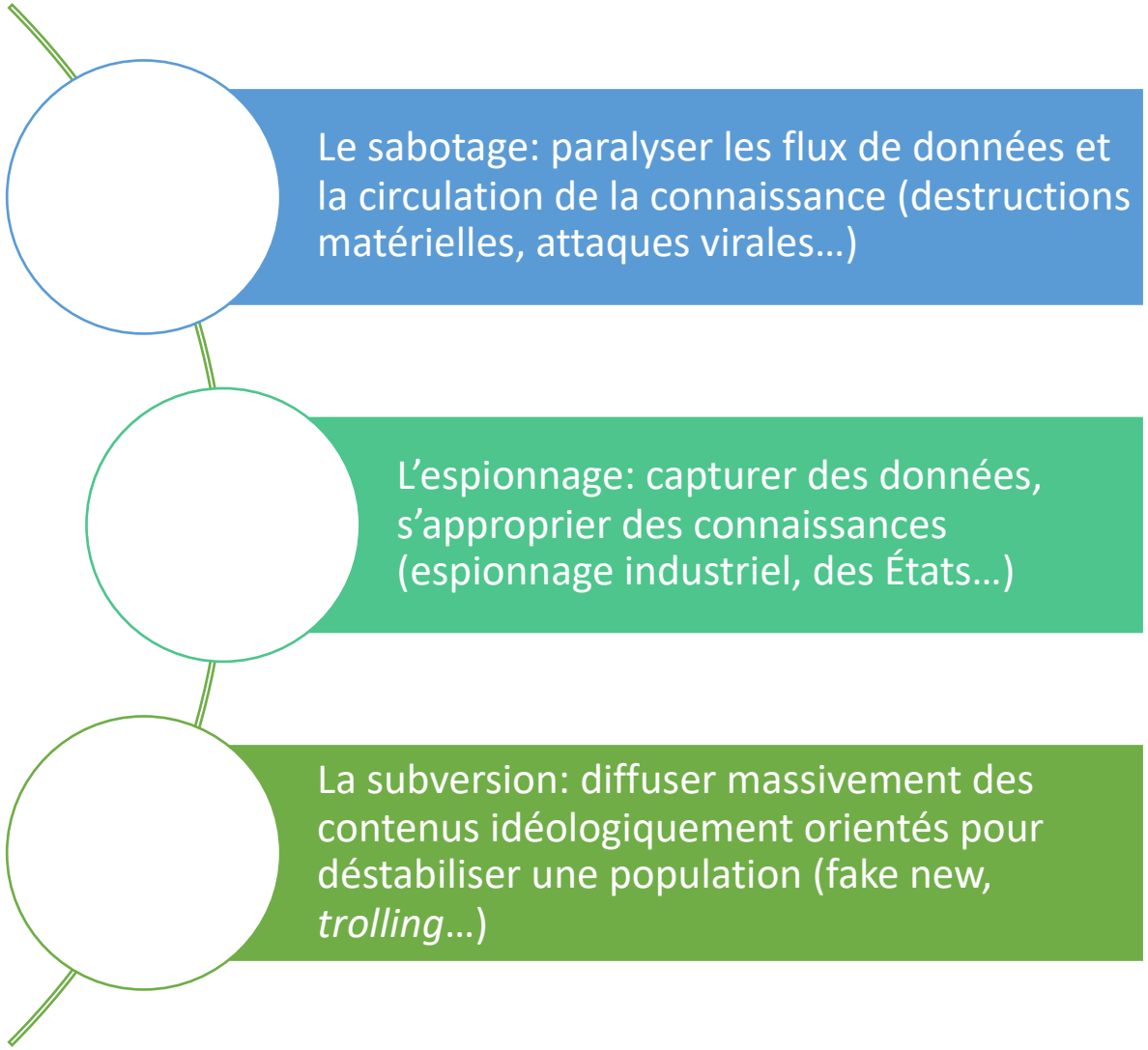
Aborder le jalon: la cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français

- Problématique possible (par exemple au regard des documents déjà travaillés en introduction):

- Comment penser la souveraineté d'un État dans un cyber espace ouvert et avec des outils techniques largement dépendants d'acteurs non nationaux ? Comment est-il possible d'agir avec certains partenaires de confiance, ainsi les pays de l'Union européenne pour la France, afin de gagner en autonomie d'action ? Pourquoi malgré les risques d'escalade est-il nécessaire d'envisager des actions offensives en matière de cyberdéfense allant au-delà de la protection des personnes et des systèmes ?

La cyberdéfense…le cas français: la question des menaces

Couche cyber	Attaques et menaces potentielles
Couche physique	Coupure de câbles sous-marins, destruction de satellites, bombardements de bâtiments accueillant des serveurs, des infrastructures de communication…
Couche logicielle	Attaque par codes, hacking, logiciels malveillants (virus, cheval de troie…), déni de service…
Couche cognitive	Modification de l'affichage des ordinateurs, modification de la présentation d'un site web (defacement de site), vols ou destructions d'informations ou de données, introduction de messages modifiant les perceptions, opérations de propagande…



La cyberdéfense…le cas français: la question des menaces

Couche cyber	Attaques et menaces potentielles
Couche physique	Coupure de câbles sous-marins, destruction de satellites, bombardements de bâtiments accueillant des serveurs, des infrastructures de communication…
Couche logicielle	Attaque par codes, hacking, logiciels malveillants (virus, cheval de troie…), déni de service…
Couche cognitive	Modification de l'affichage des ordinateurs, modification de la présentation d'un site web (defacement de site), vols ou destructions d'informations o de d introduction de messages mo perceptions, opérations

Réinvestir des éléments du jalon 1

Le sabotage: paralyser les flux de données et la circulation de la connaissance (destructions matérielles, attaques virales…)

L'espionnage: capturer des données, s'approprier des connaissances (espionnage industriel, des États…)

La subversion: diffuser massivement des contenus idéologiquement orientés pour déstabiliser une population (fake new, *trolling*…)

La cyberdéfense… le cas français: l'enjeu de l'autonomie stratégique

Souveraineté ou autonomie stratégique?

- L'impossible maitrise des trois couches du cyberespace par un État
- Conserver une autonomie de décision et d'action
- L'importance de l'échelle européenne

L'importance de l'échelon européen

- L'importance de l'UE dans la définition de règles internationales propres au cyberespace
- Vers une stratégie de cybersécurité européenne ?
- La difficile émergence d'entreprises majeures du numérique en Europe

Un exemple de stratégie de défense: le cas du *cloud* français

- La volonté de développer un *cloud computing* avec les géants des télécoms
- Vers une stratégie passant par des entreprises plus spécialisées
- La recherche de solutions de sécurité plus modestes mais plus vite opérantes

La cyberdéfense… le cas français: rendre opérationnelle la cyberdéfense française

Une prise en compte progressive des menaces cyber

- L'émergence du risque cyber dans les différents *livres blancs* et *revues stratégiques* de défense depuis 2008
- Vers une hiérarchisation des menaces… et une adaptation des réponses

Les pôles structurant la cyberdéfense française

- La place de la défense civile et le rôle de l'ANSSI
- La cyberdéfense militaire et le rôle du COMCYBER
- Des liens étroits avec le renseignement civil et militaire DGSE/ DGSI

Trois axes dans la cyberdéfense française

- La lutte informatique défensive (LID)
- La lutte informatique offensive (LIO)
- La lutte informatique d'influence (L2I)