Protéger et défendre le cyberespace militaire.

"Opérer en sécurité dans un environnement de plus en plus numérisé".




LE MINDEF en quelques mots

295 000 personnes, militaires et civils.

7000 personnes engagées en opérations extérieures, 80% au sein d'une coalition internationale (février 2012).
Des forces pré positionnées (DOM/COM, Afrique de l'ouest, EAU..)
Une Posture Permanente de Sureté (PPS)

- dissuasion,
- défense de l'espace aérien,
- défense des espaces maritimes,
- protection des événements internationaux.

Plus de 1500 systèmes d'information divers et très variés,
Un opérateur mondial de télécom (Satellites, VLF à SHF, VPN..),
Des niveaux de classifications très divers nationaux/multinationaux.
De nombreux liens vers des partenaires (alliés, industrie…)

Une activité opérationnelle H24 tout autour du globe.

LE MINDEF en quelques images











UN CONSTAT SIMPLE

Les attaques sont une réalité de tous les jours, le monde militaire bien que résilient par nature n'est pas à l'abri :

- un fond de cybercriminalité et de « cyber-pollution » qui peut gêner la bonne marche des systèmes et organisations ;
- des attaques qui ciblent les individus et les organisation, d'ampleur et de discrétion variables, fruit d'une préparation et d'un ciblage précis ;

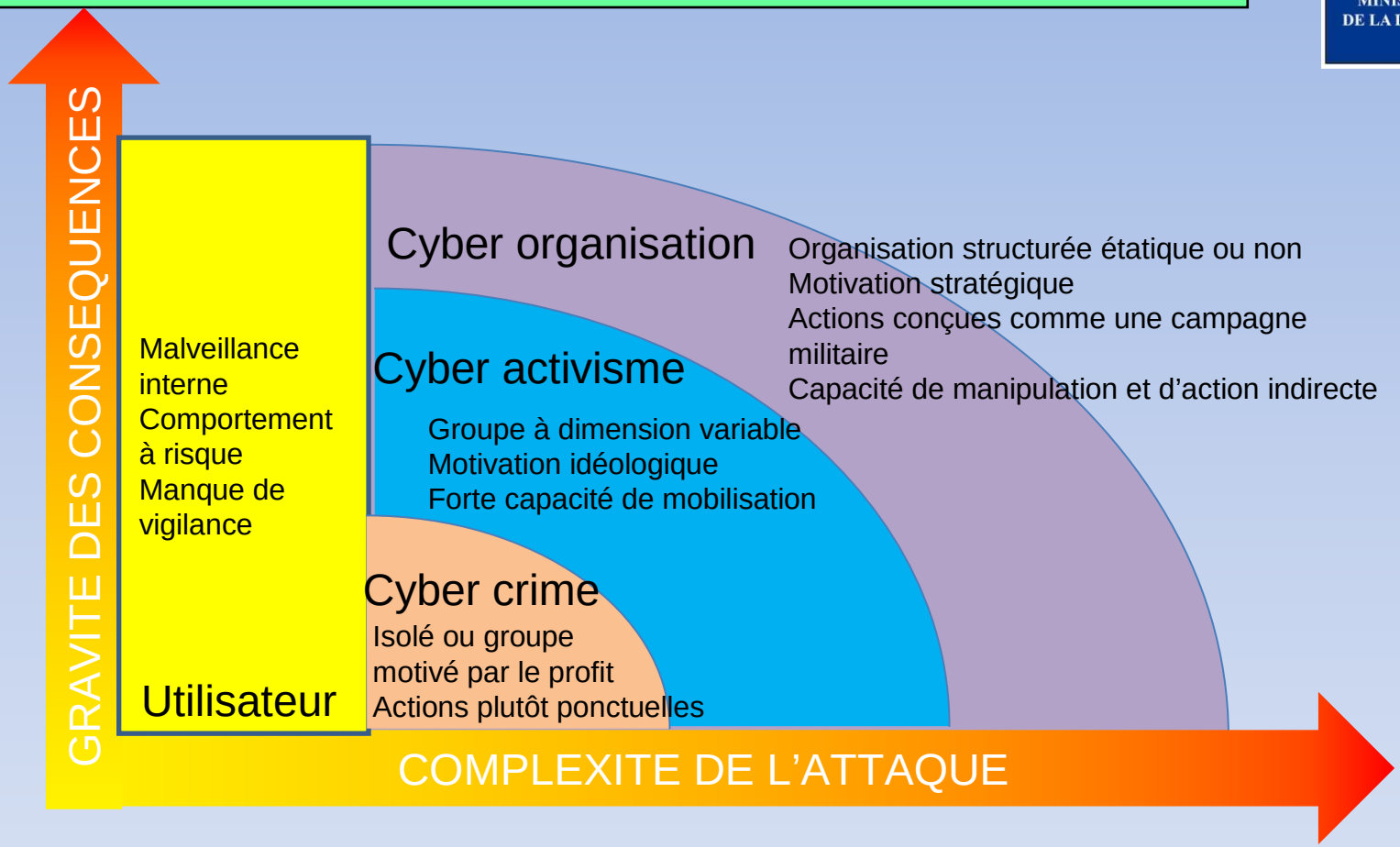
Les séparations physiques ne sont plus un rempart suffisant ; les failles et les vulnérabilités sont en trop grand nombre ; les protections pourtant indispensables se font contourner.

Un lieu de confrontation et de contestation

- Quelques dates symboliques :
  - mai 2007 : Estonie, hackers patriotiques russes ;
  - sept. 2007 : raid aérien israélien en Syrie ;
  - août 2008 : accompagnement action russe en Géorgie ;
  - juil. 2009 : attaques Corée du sud ;
  - mi. 2010 : , Olympic Game (Stuxnet) en Iran
  - 2012 : Duqu, Flame
- Des actions « tout azimut »
  - Anonymous sur tous les fronts de la contestation,
  - Hacking patriotique ;
  - Activisme : fuites d'information wikileaks,
  - Cyber espionnage,
  - Réseaux sociaux lors des révolutions arabes,
  - Cyberattaques en toile de fond Israël-Iran,

➔ Un foisonnement de cyber-(contestation, activisme, espionnage, influence, menace, censure……)

TYPOLOGIE DES ATTAQUANTS



Il faut pouvoir **détecter, contenir** et **contrer** des attaques de grandes ampleurs, particulièrement **discrètes** et pouvant aller jusqu'à cibler les capacités opérationnelles.

CHAMP D'APPLICATION

Les actions malveillantes portent :

- sur les systèmes et constituants SIC ;
- sur les systèmes d'armes et l'informatique embarquée ;
- sur les infrastructures et les plateformes de combat.

Les objectifs sont similaires aux confrontations classiques mais avec l'effet amplificateur, la prolifération et l'impunité propres au cyberespace :

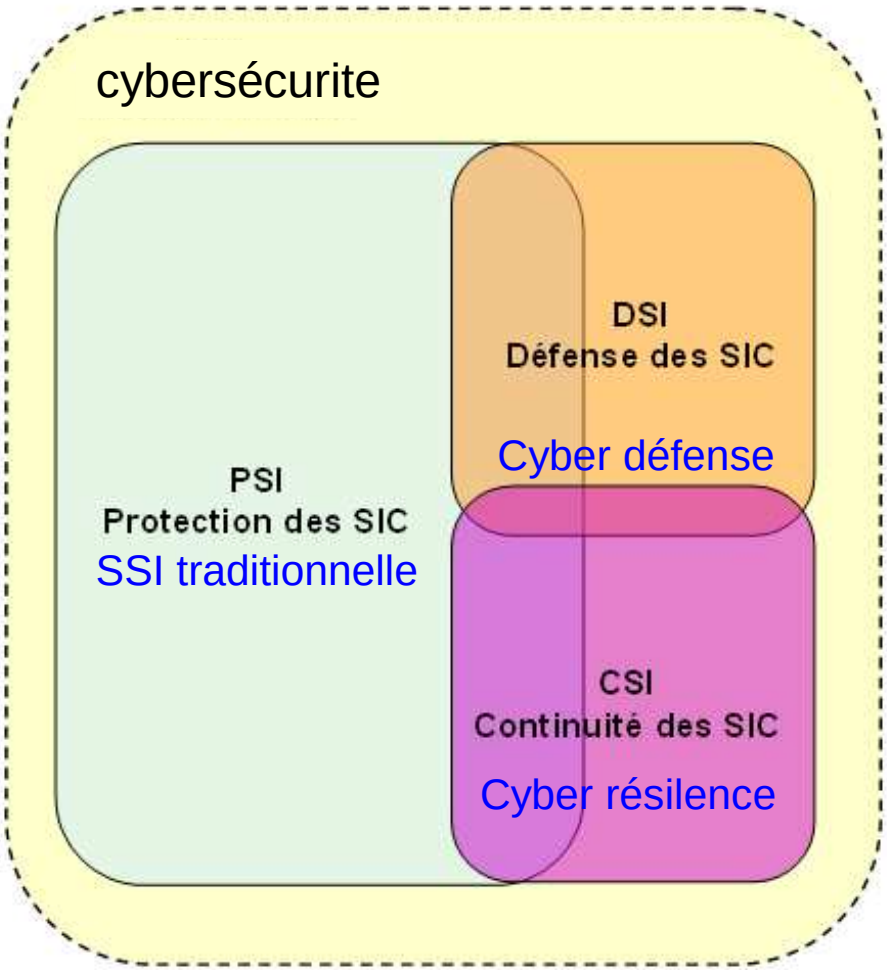
- l'espionnage et les fuites de données sont fréquentes ;
- les autres effets sont techniquement possibles et des prémices d'emploi sont observés.

Très forte dualité civilo-militaire et dilution des frontières, il faut renforcer :

- coopération et pilotage gouvernementaux,
- relations avec les nations alliées,
- discussions pour faire émerger un droit spécifique,
- concertation et coopération avec l'industrie et le monde académique.

LA CYBER SECURITE

Une approche globale au travers de la gestion de crise Cyber et des plans de continuité d'activité et informatique.



Reproductible évolutive
Confiner et caractériser
Reconquérir
Combattre un agresseur

Cyber-attaques

Défense active en profondeur

Manœuvre SIC

Gestion de crise Cyber

Sinistres accidentels

Fait ponctuel
Cause circonscrite
Restaurer
Gérer des risques

COMMENT S'ADAPTER (MINDEF)

Compléter la posture de protection par une posture de défense active.

La Cyberdéfense des armées et du ministère de la Défense.

Ensemble des activités conduites dans le cyberespace, pour garantir l'efficacité de l'action des armées, la réalisation des missions, et le bon fonctionnement du ministère.

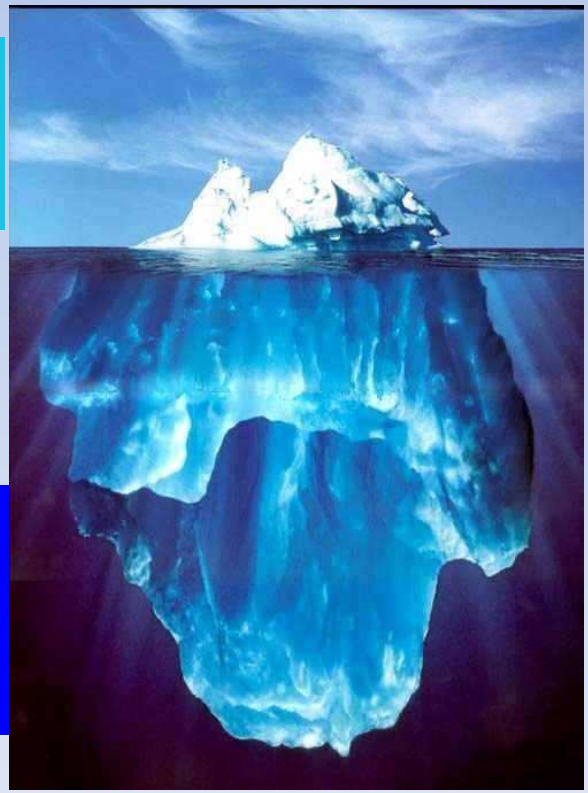
Défense des SI.

LID ou CND

Repose sur

Protection des SI.

SSI ou IA



Défense active en profondeur soutenue par une posture de protection robuste

Gestion de crise Cyber
Unicité chaine LID

UNE COOPERATION SGDSN/ANSSI - MINDEF

<u>Une autorité gouvernementale unique l'ANSSI</u> pour la protection et la défense des SI avec un mandat vis-à-vis des ministères, mais aussi vis-à-vis des « opérateurs d'importance vitale ». Une structure de plus en plus opérationnelle.

<u>Un rôle particulier joué par le MINDEF et une relation très étroite ANSSI-MINDEF</u> :

Complémentaire dans les relations internationales,
Pleinement responsable de ses systèmes : un grand opérateur qui se doit d'être fortement résilient (SIC, Armements, Plateformes, Infrastructures, Emprises….),
Délégataire en matière d'homologation,
Contribue aux crises sur le territoire national.

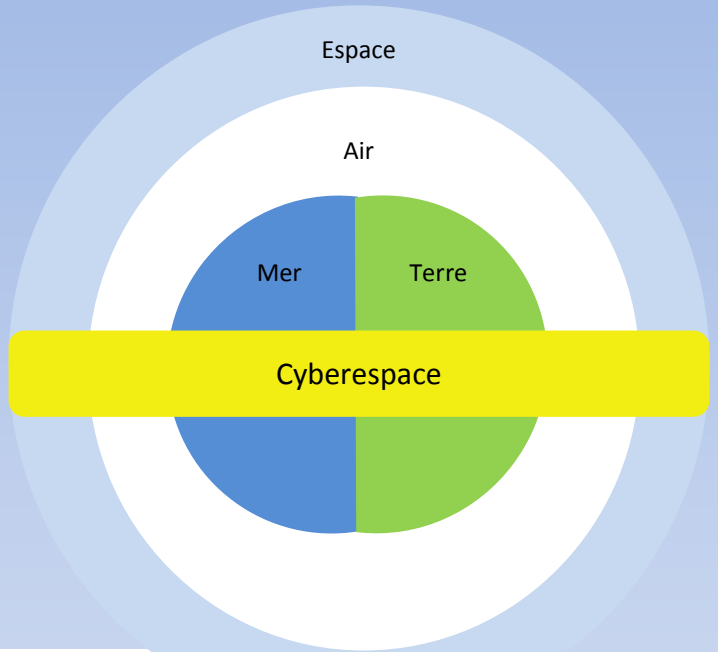
«Centres LID (CERT)» ANSSI et MINDEF colocalisés en 2013,

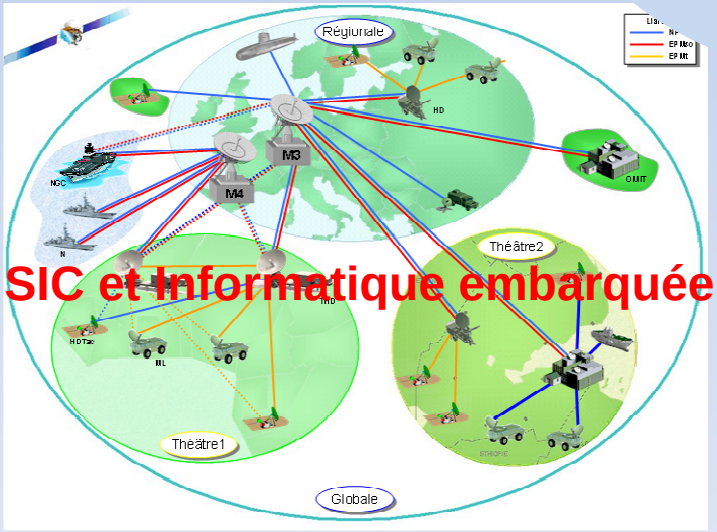
LA DOCTRINE CYBER MINDEF

Les 7 piliers :

Connaître le cyberespace et ses menaces : renseignement d'intérêt « cyberdéfense » ;
Anticiper les cyber attaques potentielles : anticipation stratégique, évaluation de la menace et plan de continuité d'activité ;
Surveiller et apprécier la situation : une situation « cyber » globale des systèmes à protéger ; partagée par tous les acteurs ; des niveaux d'alerte et une capacité de montée en puissance ;
Commander la défense des SI : une haute autorité de cyberdéfense pour le Mindef et les forces déployées ; unicité du commandement
Se protéger en permanence : « bonne hygiène des réseaux » ; formation, entrainement, préparation des forces ;
Investiguer et se défendre : défense dynamique, investigation et intervention rapide, contenir et caractériser une attaque, Forensic ; unités cyber (Calid et renforts)
Restaurer les capacités : cyber-résilience et gestion de crise cyber, capacité de mobilisation pour renforcer les entités attaquées.

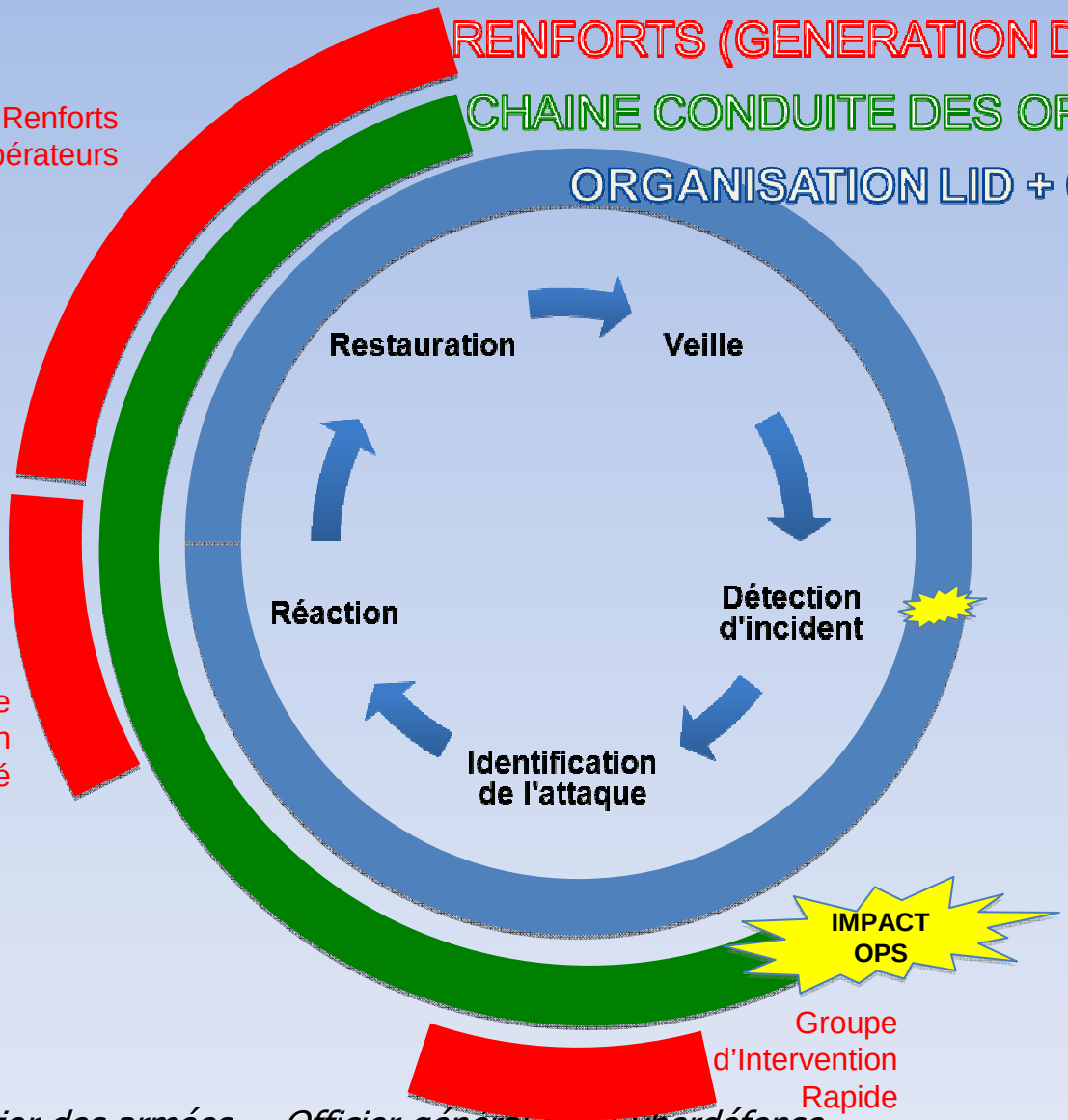
UN MILIEU TRANVERSE ET SUBSTRAT DES AUTRES





SIC et Informatique embarquée

CYCLE LID ET ACTEURS CYBERDEFENSE



La formation du personnel : un axe majeur à accélérer

Facteur essentiel de la robustesse de la posture.

1 – L'esprit de cybersécurité : des fondamentaux pour un comportement sain dans un espace sain.

hygiène cybernétique : tous et toute la carrière

simple : les 10 commandements pour utilisateurs / administrateurs

➔ 295 000 « sources de risque mais aussi acteurs de sécurité »

2 - La compétence spécialisée de la filière « SI » au sens large

des modules SSI/LID amplifiés dans toutes les formations « SI »

des généralistes et des experts SSI-CYBER

de nouveaux métiers : enquêteurs, traqueurs, patrouilleur….

un pôle d'excellence Mindef à Rennes : DGA, ETRS, ESCC et de nombreux partenaires.

3 - La formation au commandement et à la conduite dans le domaine Cyber

doctrine, tactique, commandement, conception de la manœuvre cyber, conduite d'intervention

décideurs, officier d'état major OPS, planificateurs….

En conclusion

La sécurisation du Cyberespace et la maîtrise des zones essentielles aux opérations relèvent d'une nouvelle forme de confrontation.

L'attaquant y a un avantage certain, il sait être discret et surtout exploiter nos faiblesses.
Il va falloir traquer ce que l'on ne connaît pas encore en recherchant des indices ou « signaux faibles » à investiguer.

La dimension humaine est fondamentale, l'utilisateur est le 1er niveau de défense.

Il est à la fois une source de risques, un acteur de la protection, et un déclencheur d'alerte.

Il faut absolument améliorer le comportement des individus en développant et contrôlant l'état d'hygiène et de préparation cybernétiques des unités.

Au-delà de la technique, le rôle et l'implication du commandement y sont particulièrement importants.