MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

la souveraineté numérique

vue de la DIRISI Saint-Denis de la réunion

Mercredi 30 avril 2025

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Plan de la présentation

DIRISI
Unir nos forces

- La DIRISI Saint Denis de la Réunion et mes fonctions
- La Cyberprotection
- La menace cyber et focus sur La Réunion et la zone Océan Indien.
  - Constellations de basse altitude et frugalité numérique
  - Câbles sous-marins
- La souveraineté Numérique
  - Confiance VS Souveraineté
  - Moyens souverains
  - Résilience

(15 minutes + 5 minutes d'échanges) :

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

DIRISI Saint Denis de la Réunion

DIRISI
Unir nos forces

- DIRISI: Direction interarmées des Réseaux d'infrastructure et des Systèmes d'information:
- L'opérateur des Systèmes d'informations et de communications des armées et directions de services.
  - S'intègre au 1/9/2025 dans une nouvelle entité: le Commissariat au Numérique de la Défense.
- Les 80 personnels de la DIRISI Saint Denis de la Réunion ont pour mission de :

  fournir des SIC en tous lieux et en toutes circonstances, garantir la sécurité et la capacité d'action des forces armées sur toute la ZRP des Forces Armées de la zone Sud de l'Océan Indien (FAZSOI);
  - Périmètre technique:
    - de la radio « à l'ancienne » aux DataCenter et à l'IA, via les connexions satellites souveraines

Mes fonctions

- La sécurité en général
  - La cybersécurité en particulier
    - Quand on parle de souveraineté, la protection des éléments secrets (clés de chiffrement) est un point d'attention permanent.

La Cyber protection

4 phases de protection:

- **Prévoir** (l'imprévisible)
  - Plan de continuité d'Activités: Prévoir un plan B pour éviter un Planté
  - Sauvegarder ses données, les protéger en les isolant et tester leur restaurabilité.
  - Concevoir des systèmes résilients
- **Détecter**
  - La phase cruciale: on ne peut pas se protéger contre une menace indétectable
    - 1920: Radiations ionisantes
    - 2010: StuxNet
    - 2019: COVID19
      - Tant qu'on ne sait pas détecter, on ne peut pas débuter la lutte.
      - Particularité de l'emploi militaire: Tant qu'on ne sait pas maitriser la diffusion, on n'utilise pas
- **Protéger**
  - Protéger les organismes/organes sains
    - Vacciner une fois qu'on a créé le vaccin / le patch correctif
- **Reconquérir**
  - Stuxnet:
    - patcher les systèmes
  - COVID 19:
    - Inventer un protocole de soins efficace / une procédure de désinfection et éliminer les protocoles fantaisistes

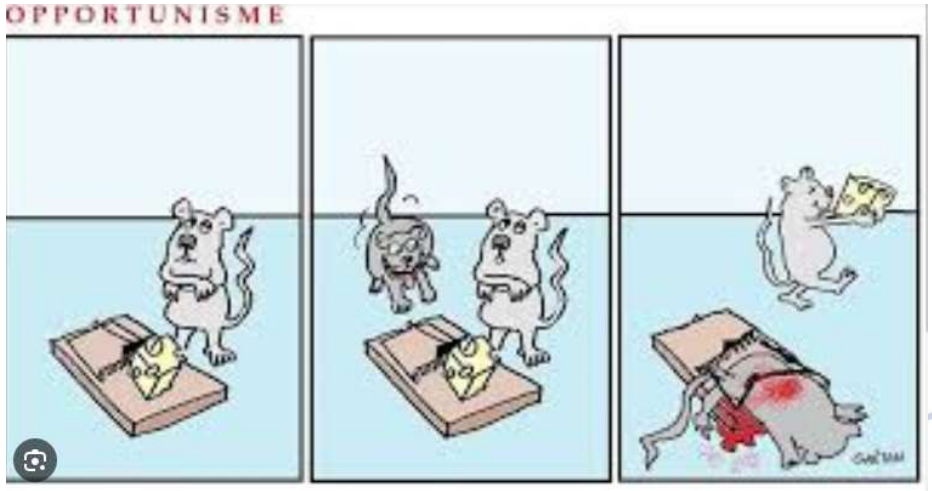
MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

La menace Cyber

DIRISI
Unir nos forces

- Le Phishing
  - **Toujours** un effet d'aubaine et une notion d'urgence
    - « Nous n'allons pas pouvoir vous livrer », régularisez immédiatement
    - « Votre remboursement n'arrivera pas », régularisez aujourd'hui
    - « Votre compte Paypal bloque votre commande »
  - **Souvent** sans date précise pour conserver une bonne longévité
    - « le mois dernier »
    - « courant juillet »

L'activation des circuits de l'urgence évite l'éveil de l'esprit critique.



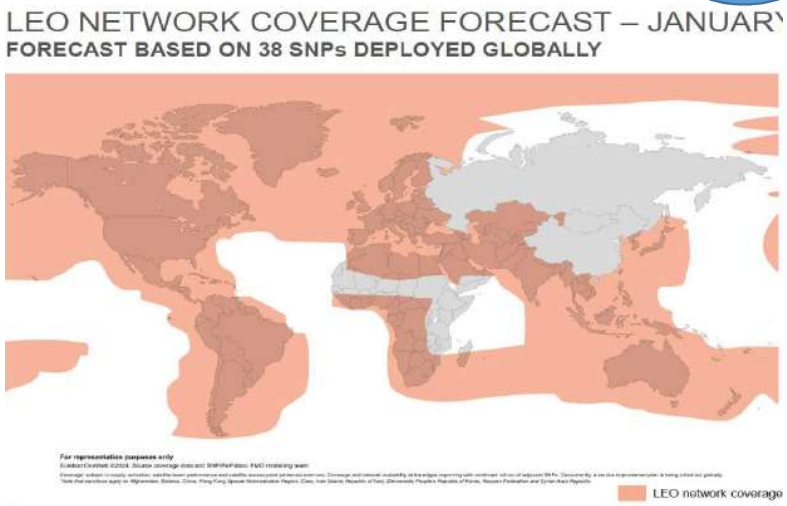
La menace Cyber

- Notre position géographique fragilise les liaisons vers l'Hexagone ou Mayotte.

Menace Peï

- Peu de câbles sous-marins nous desservent

- Les constellations « Basse altitude », commerciales, visent les zones les plus denses en clients potentiels
  - Exemple ONE WEB (Europe + Inde)



- Nous conduisons des exercices sur le thème:

<u>« c'est bien avec, mais vérifions que nous savons encore faire sans »</u>

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

La Menace

DIRISI
Unir nos forces

Menace Peï

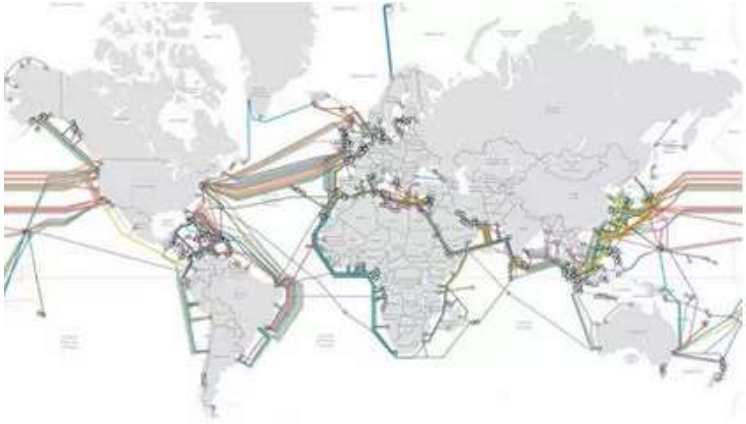
- Les câbles sous-marins
- **Zone maritime Atlantique - mer Baltique**
- Le 23 novembre, dans le cadre de l'enquête sur la rupture des câbles sous-marins *C-LION1* et *BCS*, un patrouilleur suédois a rejoint la zone à proximité du YI PENG 3 (pavillon chinois), vraquier soupçonné d'avoir saboté les câbles,
- Des dégâts inhabituels aux pattes de son ancre bâbord, accréditent l'hypothèse selon laquelle il l'aurait draguée sur le fond sur une distance de plus de 85 Nq, provoquant la rupture des deux câbles.
    - Le navire est actuellement mouillé en dehors des eaux territoriales danoises et suédoises ce qui empêche les autorités de ces pays de conduire leur enquête à bord sans l'accord de l'État du pavillon.
    - Le Kattegat étant suffisamment large, le YI PENG 3 peut reprendre sa route vers le large sans pénétrer dans les eaux territoriales des pays riverains de la Baltique.

La Menace

Menace Peï

- Le flux est une menace de déni de service distribué (DDOS)
  - Il suffit de perturber une bonne partie du lien, pour provoquer un engorgement total du reste (exple: Barachois à St Denis)

- Avec quelques câbles sectionnés, le report de trafic sur provoquer un Déni De Service Distribué (DDOS)



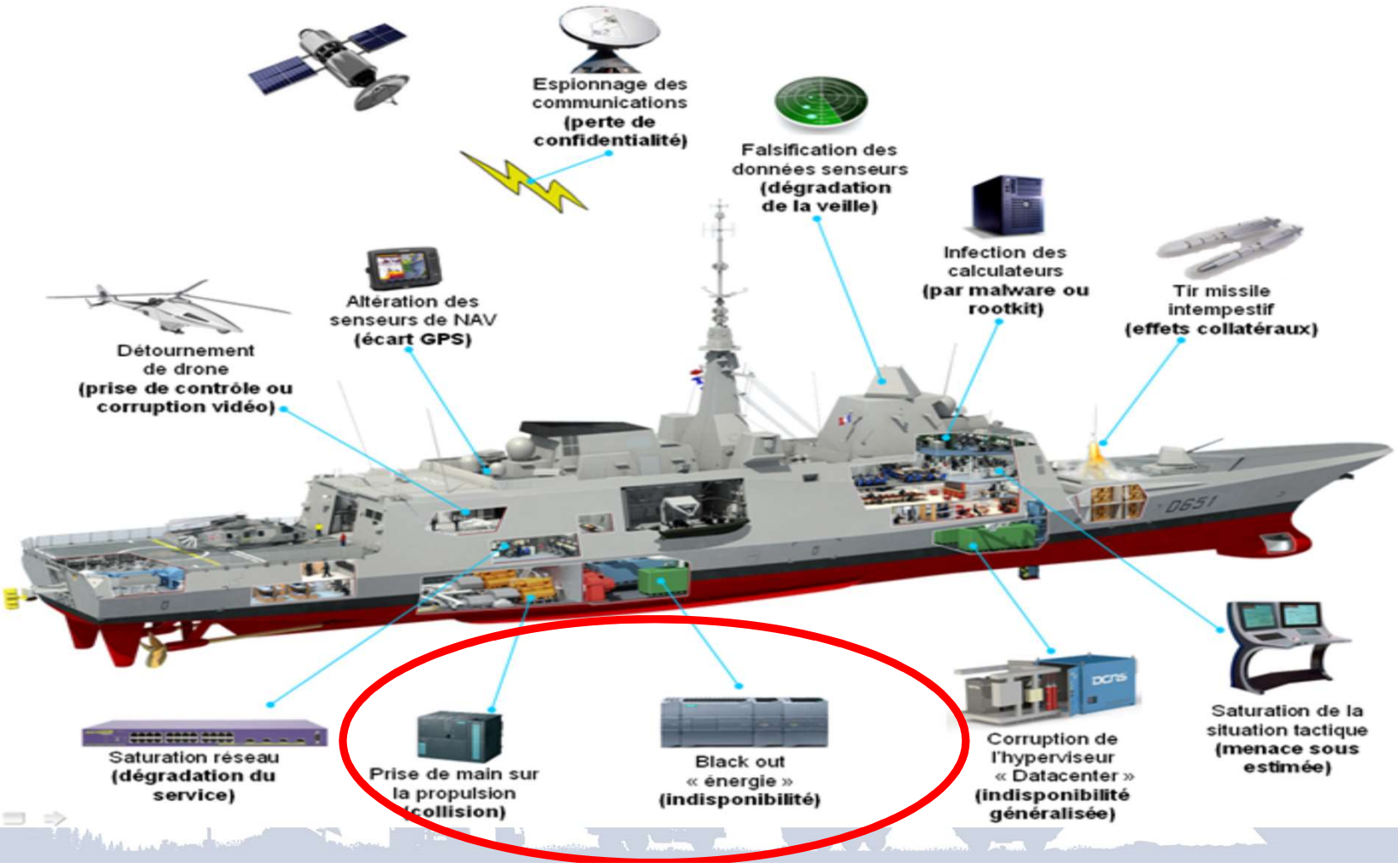
- Faire courir une rumeur d'attentat peut suffire à provoquer un DDOS sur le réseau des tph mobiles dans une zone de concentration de foule (salle de spectacle, stade, festival,…)

- On peut aussi provoquer un DDOS en jouant avec les peurs:
  - 2022 - 2023: Menace d'approvisionnement sur le carburant
  - Tous les gens se ruent sur les stations services et provoquent le DDOS.
  - Les réservoirs de tous les véhicules sont pleins, notamment ceux des gens qui n'en ont pas besoin pour leur vie quotidienne.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

La menace Cyber

DIRISI
Unir nos forces



MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

La souveraineté

DIRISI
Unir nos forces

Confiance numérique vs Souveraineté numérique pour nos actifs vitaux:

- Confiance = assurance d'un niveau de protection limité de mes données et process
  - Défaut => pénalités pour le fautif.
- SOUVERAINETÉ = niveau de protection renforcé de mes données et process
  - Le défaut n'est pas indemnisable.

- Choisissons bien nos offres et plateformes:
  - Souverain, SecNumCloud, sans menace d'extraterritorialité.
  - Infrastructure as a service (Iaas): le prestataire fournit le serveur virtuel
    - Offre salle blanche
  - Container as a service (Caas): le prestataire fournit le serveur virtuel avec un OS
  - Plateforme as a service (Paas): le prestataire fournit le serveur virtuel avec un OS et ses accessoires (anti-virus, agents de supervision, …)
    - Offre VPS
  - Software as a service (Saas): le prestataire fournit le serveur virtuel avec des SGBD, des applications métiers prêtes à l'emploi
    - Offre Infogérance
- Les prestataires peuvent devenir défaillants ou malveillants.
  - C'est historiquement un voie de pénétration des sites sensibles (ménage, nourriture, …)

- N'oublions pas les systèmes de sauvegarde et de restaurations (on premise ou off-premise)

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

La souveraineté

DIRISI
Unir nos forces

CHIDO a montré que la souveraineté c'est aussi assurer le fonctionnement de l'état dans les vents contraires

- Nous assurons la souveraineté sur les systèmes stratégiques,
  - son coût oblige à des renoncements sur les autres:
    - Être résilient c'est être malins.
    - Pour être résilients, il faut maitriser notre environnement
  - Quand on doit la partager, la souveraineté c'est dépendre du moins d'alliés possible
    - Ne pas mettre tous ces œufs dans le même panier, mais diversifier avec intelligence pour diminuer notre dépendance à un acteur.
    - Constellations LEO: One-Web (Eur + Inde) plutôt que Starlink

- Constellations de basse altitude et frugalité numérique
  - Nous avons des services puissants et économiques, mais non maitrisés
    - Coupure de Starlink au dessus de l'Ukraine pour bloquer les attaques par drones sur les forces Russes.
  - Même si c'est si pratique, nous devons garder le savoir faire pour communiquer si c'est coupé quelle que soit la menace.

- Nous avons donc des moyens souverains, mais à débit limité;
  - Satellites du programme SYRACUSE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Résilience

DIRISI
Unir nos forces

CHIDO/ GARANTE ont montré que nos moyens sont vulnérables.

La souveraineté c'est assurer le fonctionnement de l'état dans les vents contraires

Les données sont vitales: Sauvegardez-les, protégez-les, et testez-les

- Tout ce qui est accessible par le réseau est cible des attaques,
  - protégez-les en les isolant
- Testez votre capacité à les restaurer (une fois perdues, c'est trop tard)
- Les pannes, les négligences ou les vengeances sont assimilables à des attaques en disponibilité ou en intégrité,

Prévoir un plan de continuité d'activités pour les fonctions vitales.

« Prévoir un plan B pour éviter un Planté »

- C'est simple si et seulement si la direction détermine de quoi elle peut se passer,
  - Il faut accepter de perdre des fonctions, du temps et des données…
- Les systèmes sont résilients si c'est prévu lors de la conception, sinon il reste des points uniques de défaillance (SPOF).

MINISTÈRE DES ARMÉES
Liberté Égalité Fraternité

DIRISI
Unir nos forces

Conclusion

- La souveraineté numérique à un coût non négligeable, mais à chaque crise nous mesurons ses bénéfices.
  - Dans l'urgence, la communauté nationale sait se réunir pour faire face à l'adversité
  - Les sorties de crise sont des moments privilégiés pour la désinformation, l'influence

Nous sommes le maillon faible:

- Quand on fait appel à l'effet d'aubaine, soyons **vigilants**
- Quand ajoute de l'urgence, soyons **méfiants**.

Il faut prévoir avant qu'il ne soit trop tard: **la résilience, la continuité d'activités**

« **soignez votre pouvoir d'HA** » (High Availibility)