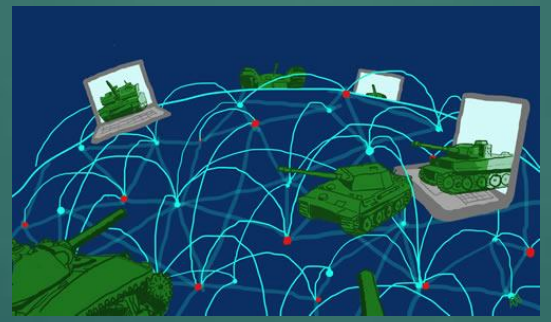
MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

SOUVERAINETE DU NUMERIQUE

Un champ numérique résilient et durci pour garantir les nouveaux champs de conflictualité







MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

1- SOUVERAINETE DU NUMERIQUE DANS SON ENSEMBLE

- La souveraineté numérique au sein des armées est un enjeu majeur pour les États modernes.

- Elle consiste à garantir l'indépendance et la sécurité des systèmes d'information et de communication des forces armées, ainsi que la protection de leurs données sensibles.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

2- SOUVERAINETE DU NUMERIQUE GENESE

La souveraineté numérique dans les armées s'est développée en réponse à l'essor des technologies numériques et aux menaces croissantes en cybersécurité.

Intégration des technologies numériques pendant la guerre froide et défis de sécurité liés à l'avènement d'Internet

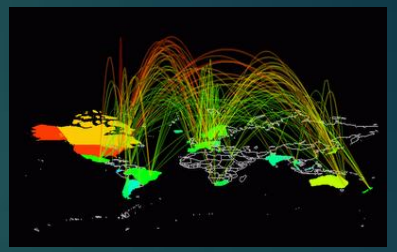
Cyberattaques et élaboration de stratégies de cybersécurité

Investissement dans la cybersécurité et la résilience des systèmes.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

3- Les enjeux de la souveraineté numérique pour les armées

- La souveraineté numérique fait référence à la capacité d'un État à contrôler ses infrastructures numériques, ses données et ses technologies. Dans le contexte militaire, cela implique la protection des systèmes d'information, des communications et des opérations numériques.



- Face à la hausse de cyber menaces croissantes, la souveraineté numérique est devenue un impératif stratégique pour les armées.

- Les cyberattaques peuvent en effet perturber les opérations militaires, compromettre les systèmes de commandement et de contrôle, ou encore exposer les données confidentielles des forces armées.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

4- Exemples de souveraineté numérique dans différents pays

- La France a créé l'Agence nationale de la sécurité des systèmes d'information (ANSSI) :
  renforcer la cyber sécurité de l'État et de ses opérateurs d'importance vitale, dont les armées.
- Les États-Unis ont créé l'United States Cyber Command (USCYBERCOM) :
  protéger les réseaux et les systèmes d'information du département de la Défense.
- Le Royaume-Uni a créé le National Cyber Security Centre (NCSC) :
  fournir des services de conseil, d'assistance et de formation en matière de cyber sécurité.
- L'Allemagne a créé le Bundesamt für Sicherheit in der Informationstechnik (BSI) :
  fournir des services de conseil, d'audit et de certification en matière de cyber sécurité.
- L'OTAN a créé le Centre d'excellence pour la cyber sécurité (CCDCOE) :
  fournir des services de conseil, d'assistance et de formation en matière de cyber sécurité.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

5- FOCUS sur La cybersécurité et les JO 2024 en France

- Stratégie de cybersécurité franco-JO 2024 : collaboration pour la sécurité numérique, protection d'infrastructures critiques, surveillance réseaux et réponse incidents.

- Collaboration, Investissement, Sensibilisation, Surveillance, et Protection.
- Ces mesures incluent : partage de bonnes pratiques, investissement dans capacités, sensibilisation et éducation, surveillance et détection des menaces, pour garantir cybersécurité et offrir un environnement sûr pour tous.

- Bilan CYBER des JO et JOP de Paris 2024 : ANSSI et partenaires ont aidé plusieurs victimes à résoudre incidents, aucun impact majeur sur cérémonies et épreuves.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

6- La cybersécurité dans les armées

- La cybersécurité est un enjeu crucial pour les armées, qui doivent protéger leurs systèmes d'information et de communication contre les cybermenaces.

- Les armées ont donc mis en place des mesures de cybersécurité pour garantir la confidentialité, l'intégrité et la disponibilité de leurs systèmes d'information et de communication.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

7- ALERTE ATTAQUE CYBER

- En cas de cyberattaque dans les armées la cellule ou direction dédiée à la cybersécurité :
  - analyse la menace
  - déclenche le plan de réponse à incident
  - informe les autorités et partenaires
  - évalue la situation pour éviter les récidives et renforcer la culture de cybersécurité.

- Cette gestion repose sur une approche collaborative et multidisciplinaire.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

8- Le métier de cyber dans les armées

Il consiste à :

assurer la sécurité des systèmes d'information et de communication de l'armée contre les cybermenaces.

Ce métier requiert :

des compétences techniques, organisationnelles et humaines, qui permettent de détecter, d'analyser, de prévenir et de répondre aux incidents de cybersécurité.

Métier dynamique et évolutif, qui offre de nombreuses opportunités de carrière et de spécialisation.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

9- L'Organisation des systèmes de sécurité de l'information au FAZSOI

SENSIBILISATION
des acteurs SSI de la zon

UTILISATEURS

CONSEILLE les CSSI des organismes et formations pour la cohérence de rs politiques de sécurité avec la SI-Armées et la PSSI FAZSOI.

Faire appliquer TXT

OSSIZ organise le prolongement de la voie fonctionnelle SSI OUTRE-MER

TRAITE LES INCIDENTS
SSI dans sa zone
En coordination avec la DIRISI,

CR incidents

CONTRÔLE
niveau général des SIC utilisés.
(contrôles programmés ou inopiné en cas de nécessité.)

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

10 -Les métiers de la cybersécurité dans les armées

Importance croissante de la cyber sécurité dans le domaine militaire.
La cybersécurité est essentielle pour la défense nationale.
Les métiers dans ce domaine offrent des opportunités passionnantes et un impact significatif.

1. ***Les analystes de la menace :***

- Surveillance des réseaux pour détecter des menaces.
- Analyse des incidents de sécurité.

2. ***Les ingénieurs en sécurité des systèmes d'information :*** -
- Conception et mise en œuvre de solutions de sécurité tels que les firewalls, les systèmes de détection et de prévention des intrusions, les systèmes de chiffrement et les systèmes de sauvegarde et de restauration des données.

- Évaluation des vulnérabilités des systèmes.

3. ***Les experts en numérique :***

- Gestion des incidents de sécurité.
- Coordination des efforts de réponse et de récupération.

4. ***Les formateurs en cybersécurité :***

- Sensibilisation et formation des personnels de l'armée aux enjeux de la cybersécurité,

- Apprendre à adopter des comportements responsables et sécurisés.

5. ***Les chefs de projet en cybersécurité*** :

- Coordonnent les projets de cybersécurité de l'armée,

- Veillent à leur bonne exécution dans le respect des délais, des coûts et de la qualité.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

11 -FOCUS sur La Réunion et la zone Océan Indien

L'océan Indien, une région stratégique pour la sécurité mondiale

- Formes de menaces : attaques DDoS, intrusions, vols de données, rançongiciels, logiciels malveillants
- Infrastructures critiques dans la zone : ports, aéroports, réseaux de télécommunications, systèmes de contrôle industriel
- Zone de commerce et logistique importante, attractive pour les cybercriminels

Mesures pour contrer les menaces :

- Mise en place de mesures de sécurité renforcées
- Surveillance en temps réel, détection et réponse aux incidents
- Formation des professionnels de la sécurité
- Coopération et collaboration entre États, entreprises et particuliers pour renforcer la cybersécurité et lutter contre les menaces

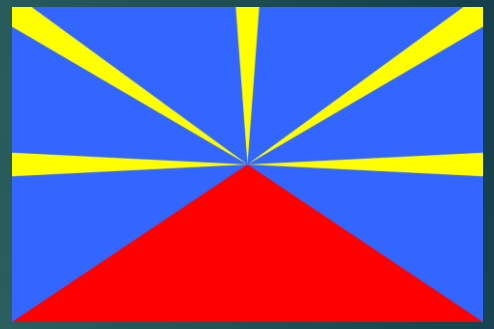
L'océan Indien et La Réunion doivent se préparer et se protéger contre les menaces cyber croissantes pour assurer leur sécurité et stabilité.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

11 -FOCUS sur La Réunion et la zone Océan Indien (suite)

La souveraineté numérique des armées à l'île de la Réunion est assurée par plusieurs initiatives et infrastructures :

- Les systèmes de communication sécurisés
- les réseaux informatiques dédiés
- les centres de données locaux.



Ces mesures visent à garantir :

- la confidentialité
- l'intégrité des données échangées
- à protéger les informations sensibles contre les cybermenaces.

La souveraineté numérique est essentielle pour maintenir une présence militaire efficace et réactive face aux enjeux régionaux dans cette zone géographique stratégique.

Elle contribue également à renforcer la résilience des armées face aux défis contemporains et à assurer une meilleure coordination avec les autres forces militaires et les autorités locales.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Conclusion

Importance pour la Sécurité Nationale

La souveraineté numérique est cruciale pour garantir la sécurité des informations sensibles et des opérations militaires. Elle permet de réduire la dépendance vis-à-vis des technologies étrangères, qui peuvent être vulnérables à des cyberattaques ou à des manipulations.

Défis à Surmonter

Les armées doivent faire face à des défis tels que la rapidité de l'évolution technologique, la nécessité de former le personnel aux nouvelles compétences numériques, et la gestion des risques liés aux cybermenaces.

Pour conclure

La souveraineté numérique est un enjeu stratégique pour les armées modernes. En développant des capacités numériques autonomes et en protégeant leurs infrastructures, les États peuvent mieux se préparer aux défis de la guerre moderne et garantir leur sécurité nationale.

Merci pour votre attention

Des questions?