Notion de cybersécurité

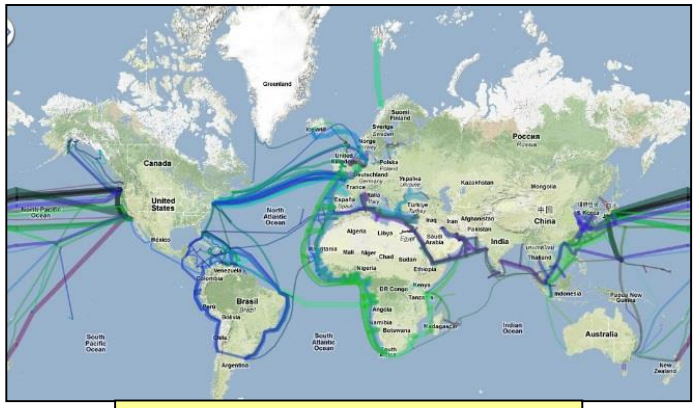

Cyberespace

Cyberespace

- Espace virtuel qui réunit tous les vecteurs d'informations numériques accessibles par ordinateurs.
- Source de « pollutions », de tensions voire de conflits.
- Pénètre tous les autres milieux et les relie.
- On y définit généralement 3 niveaux.

La couche physique

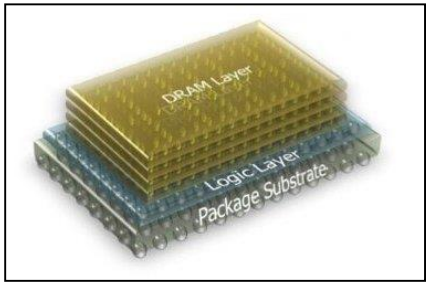
- Hardware au sens large du terme
- Matériels et infrastructures de réseau (ordinateurs, routeurs, serveurs, câbles et fibres optiques)
- Possibilité de protection physique



Câbles sous-marins

La couche logique

- Permet le fonctionnement des ordinateurs et réseaux, d'en exploiter les ressources et d'en gérer les flux d'information (software).

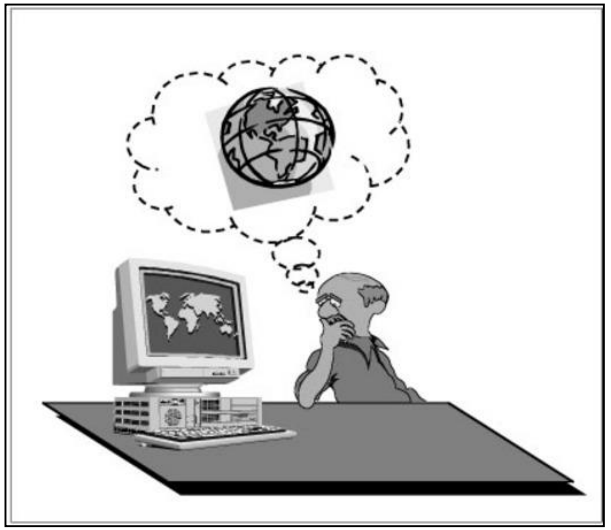


- Permet l'utilisation du cyberespace :
  - par le dialogue homme-machine ;
  - par le codage ;
  - par le dialogue entre machines.

- Ce niveau est sujet aux attaques informatiques.

La couche cognitive

- Aussi connue sous le nom couche sémantique ou informationnelle.



- C’est la couche haute où se mêlent les perceptions de la réalité et les capacités de gestion de la connaissance.

- Cette couche traite du contenu des informations dont il faut protéger l’intégrité.

Caractéristiques du cyberespace

- Intangible (*plus approprié que virtuel*)
- Opaque même si en apparence, c'est un espace public. C'est un avantages stratégiques, car cela rend possible des actions cachées et anonymes.
- Artificiel car il est une création de l'humain. Un autre espace qui présente des caractéristiques analogues est celui de l'arme nucléaire.
- Fugace et poreux : rapidité des flux et des menaces difficiles à saisir
- Complexe : technologie, multi dimensions,

Notion de système de systèmes

Internet

Technologie IP

Systèmes Wireless

Services Internet multi et inter réseaux

Internet des objets (Liaisons GPS, Bluetooth, étiquettes RFID, etc.)

Systèmes de positionnement et de chronologie

Un aéronef est un système de systèmes

- Systèmes mécaniques composés de différents sous ensembles ;
- Systèmes numériques interconnectés par un bus ;
- Systèmes d'information logistiques ;
- Liaisons de données externes ;
- Système humain !

CYBER…*notions*

"Si certains pensent que les scénarios de cyber-attaques relèvent du fantasme, alors avec ce que nous voyons tous les jours, nous pouvons dire que la réalité dépasse la fiction",

Jean-Michel Orozco,

Président de Cassidian Cyber Security

EADS*

* Devenu Airbus Defence and Space, le 1 janvier 2013

Cybersécurité

Cyberespace

Cyberattaques

Cyberarmes de rétorsion

Cyberarmes d'agression

Cyberdéfense
(Lutte informatique défensive et offensive)

Cyberpolice
(Lutte contre la criminalité)

Cyberprotection
(SSI, comportements, etc.)

Les cyberarmes

- Une « cyberarme » est une capacité destinée à perturber les systèmes informatiques et les réseaux.
- Elle peut être définie comme un élément logique (un code) capable de mettre hors service :
  - les systèmes d'information adverses ;
  - les équipements qui en sont dotés (systèmes administratifs et industriels, systèmes d'armes et de C2, systèmes d'informations logistiques, etc.).

Les cyberarmes

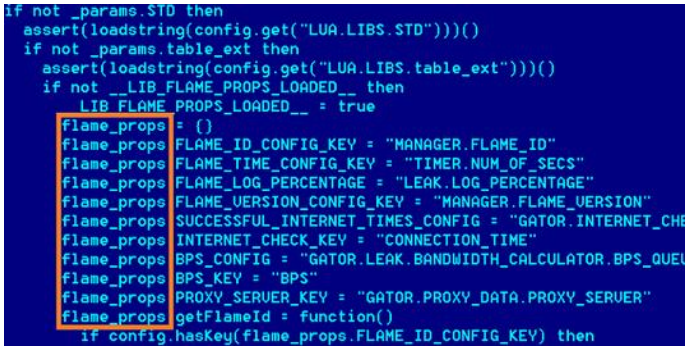
3 constituants

- un vecteur (page web, mail, logiciel, clé USB…)
- un pénétrateur pour déjouer les défenses informatiques
- une charge utile à effet (code malveillant)

Les cyberarmes

L'exemple du virus Flame

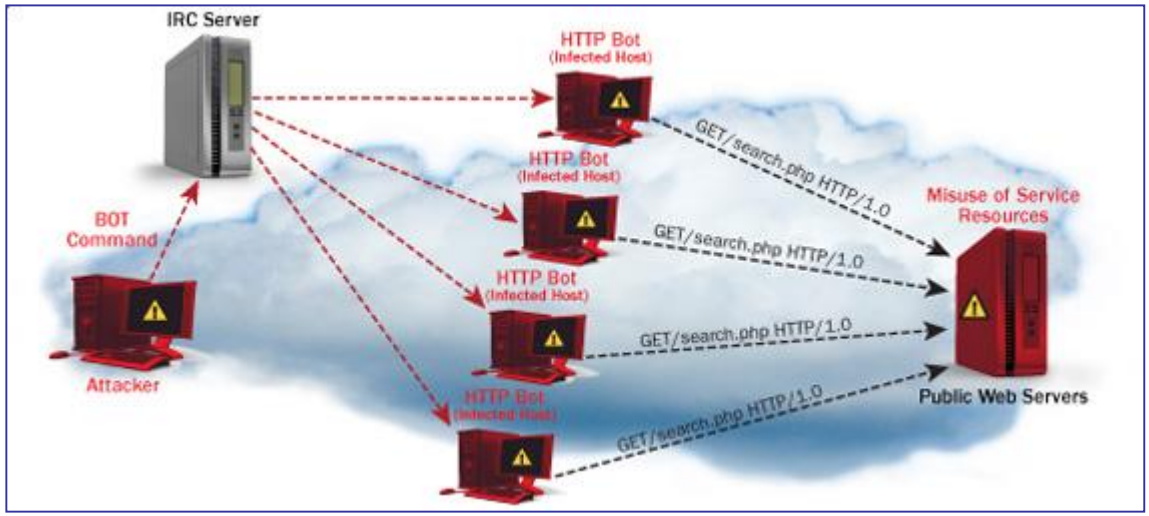
- Vecteur : clé USB/ accès au réseau
- Pénétration : faille de windows
- Subtilise des données
- Allume le micro
- Utilise le bluetooth pour « puiser » dans les appareils proches
- Effectue des captures d'écran, etc..



Catégories d'attaques

Attaque par déni de service (*Denial of Service* ; DOS).

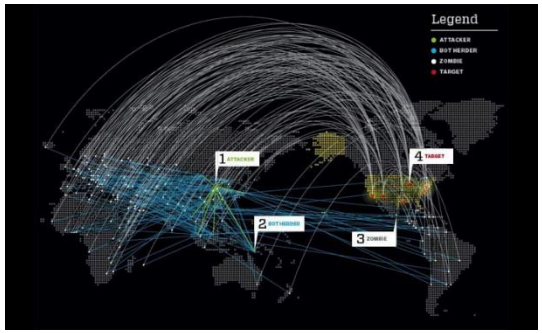
➲ Saturation du serveur par un nombre de requêtes supérieur à ses capacités de traitement

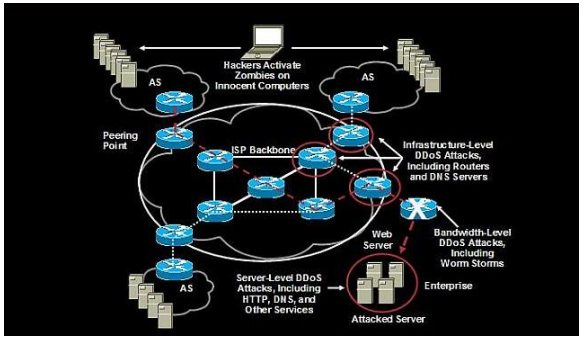


Catégories d'attaques

Attaque par déni de service distribué (DDOS).

- Principe identique au DOS mais à partir d'un très grand nombre d'ordinateurs qui participent à la même attaque
- On parle de *Botnets* (contraction de *robot* et de *network*, réseaux de robots ou de machines zombies)





Dans les deux cas (DAS et DDOS, l'attaque peut être insidieuse sans que le propriétaire de l'ordinateur en soit conscient

Catégories d'attaques

Attaques par intrusion (Malware)

- Ces programmes s'installent discrètement et accèdent à une information protégée et confidentielle sans autorisation
- Ils « sniffent » les paquets de données sensibles puis se les approprient (système DPI - *Deep packet inspection*)

Catégories d'attaques

Attaques par intrusion (Malware)

– « Cheval de Troie » : trompe les anti-virus et capture des données (mot de passe, infos sécurisées, identifiants).

– « Porte dérobée » (*backdoor*) : fonctionnalité introduite secrètement sur un logiciel et qui le transforme en cheval de Troie.

– « Vers » : programme qui peut détruire les informations classifiées, détourner des données ou entraîner des dysfonctionnements.

Catégories d'attaques

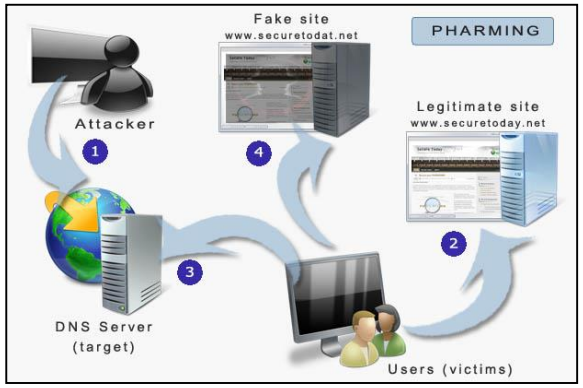
Attaques par prise de contrôle (RAT)

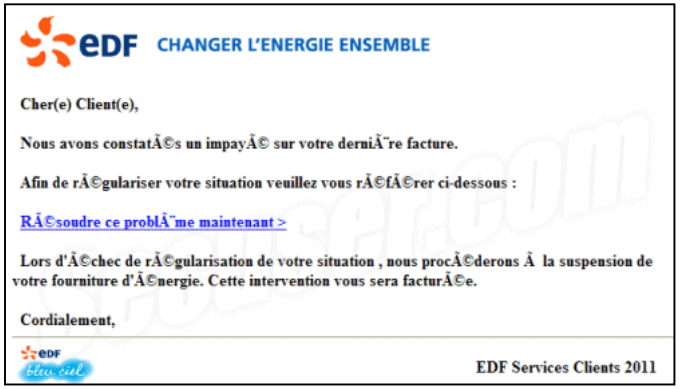
- Les RAT sont des spyware qui s'installent furtivement dans un répertoire où il ont peu de chance d'être repérés
- Ils modifient les systèmes d'exploitation pour se mettre en route à chaque démarrage de l'ordinateur
- Ils permettent la prise de contrôle à distance de l'ordinateur

Catégories d'attaques

Exploitation du facteur humain (social engineering)

- Hameçonnage (*phishing ou vishing*) : usurpation de l'identité pour obtenir de la victime des informations confidentielles (écrit ou audio)
- Dévoiement (*pharming*) : piégeage des utilisateurs orientés à leur insu vers des serveurs frauduleux
- Rançongiciels (*ramsomware*): prise en otage des internautes




EDF CHANGER L'ENERGIE ENSEMBLE

Cher(e) Client(e),

Nous avons constatÃ©s un impayÃ© sur votre derniÃ¨re facture.

Afin de rÃ©gulariser votre situation veuillez vous rÃ©fÃ©rer ci-dessous :

RÃ©soudre ce problÃ¨me maintenant >

Lors d'Ã©chec de rÃ©gularisation de votre situation , nous procÃ©derons Ã la suspension de votre fourniture d'Ã©nergie. Cette intervention vous sera facturÃ©e.

Cordialement,

EDF bleu ciel

EDF Services Clients 2011

Catégories d'attaques

Neutralisation physique

➲ Atteinte physique aux systèmes connectés aux réseaux par arrêt, perturbation, divergence, etc.

Les motivations

Cyber……militants

The Anynomous attaquent des cibles désignées ennemies car attentant à la liberté d'expression :

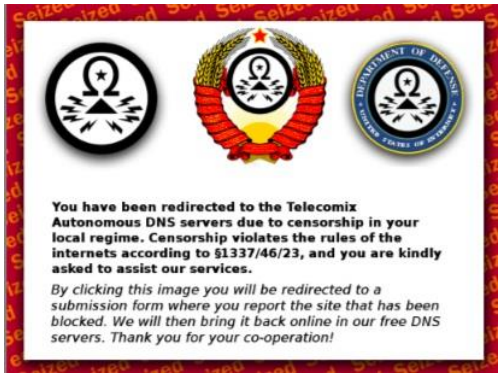
- Entreprises et organismes qui combattent les hackers
- Pays considérés comme des dictatures anti-internet
- Eglise de scientologie
- Opposants à leur action (Présidence, Express)

Depuis 2006
Pas de leadership

Attaques DDOS
Piratage,
Divulgation d'infos confidentielles

Cyber…..indignés

- « Hacktivistes » politiques du Net
- Actions vers les états qui utilisent la censure (printemps arabes)
- Actions de formation pour apprendre à déjouer la censure (ex: Egypte) ou s'initier à la crypto (ONG Reporters sans frontières), etc.
- Groupe structuré qui utilise les réseaux sociaux pour s'organiser



Cyber…..weakers

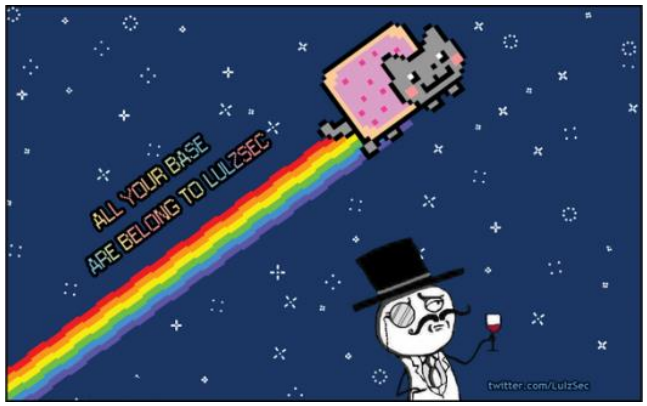
Weakyleaks diffuse de manière anonyme, non identifiable et sécurisée, des infos de nature sociale, politique, voire militaire, pour « *assurer une transparence planétaire* ».

Ne fonctionne pas comme un wiki

- Salutaire pour les uns, menace pour les autres
- N'agit pas par attaque mais par divulgation d'infos confidentielles
- Cibles de nombreuses attaques

Cyber…..challengers

Lulz Security ou **LulzSec** est un groupe de hackers responsable de plusieurs intrusions informatiques



- Intrusions/compromission de réseaux (Sony, Sénat US, Sécu UK, Site Présidence du Brésil, etc.).
- Attaque site web de la CIA.

Actif à partir de mai 2011, le groupe annonce la fin de ses activités le 25 juin 2011. Les membres du groupe sont arrêtés le 6 mars 2012.

Cyber……espions

- Entre intelligence économique, concurrence, influence et sabotage

«Nous arrêtons des attaques tous les jours mais nous arrêtons que les attaques que l'on détecte. » ***Airbus***

- Attaques de milliers de hackers mandatés ou d'Etat (Aramco, Areva, Sony, Hadopi, Elysée, Médias, etc.)

Affaire NSA/Snowden

Cyber……terroristes

Al-Qassam Cyber Fighters, un groupe autoproclamé d'hactivistes musulmans a attaqué des dizaines de banques US dans une opération nommée Ababil

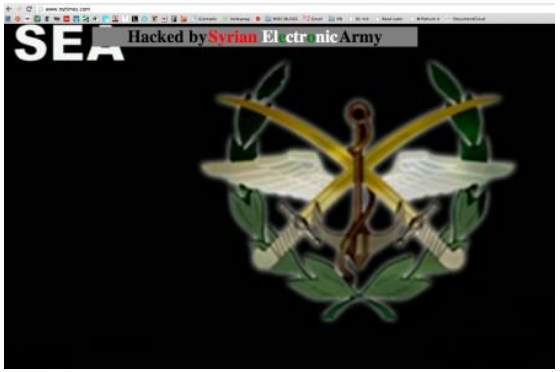
OPERATION ABABIL

Tunisian Cyber Army et
Al-Qaeda Electronic Army (AQEA)

"We and #Electronic-Al-QAEDA got access to one of the most largest american gaz companies,"
Tweet from the @TN_Cyberarmy account

Cyber…. « groupes paramilitaires »

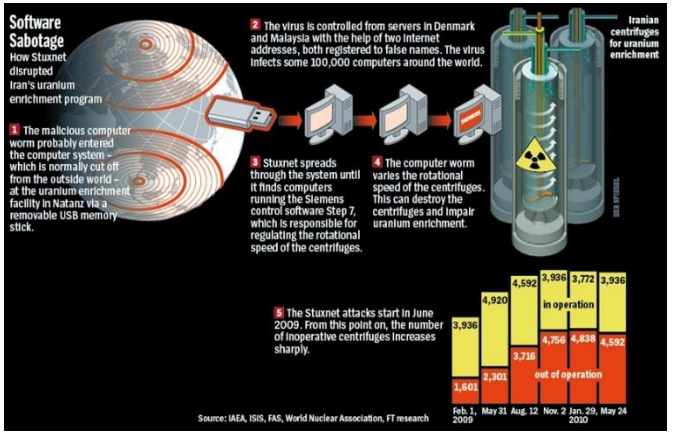
- Groupes à vocation « poltico-militaire »
- Lien non avoué avec les états mais probable
- Attaques contre des intérêts « politiques » (banques, médias, etc.), déstabilisation

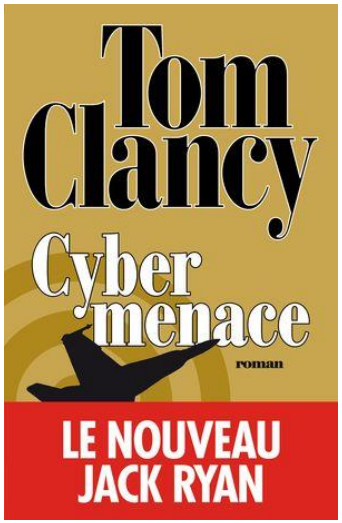


Cyber…..armées

Actions contre-Etat

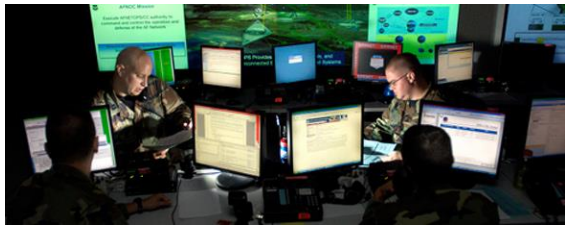
- Vs France (espionnage)
- Vs Estonie (saturation)
- Vs Géorgie (influence)
- Vs Iran (sabotage)
- Israël ⟺ Palestine (nuisance)
- Etc.





Cyber…..armées

Guerre numérique



- Intrusion sur les systèmes C4ISR
- Manipulation du champ de bataille
- Sabotage des systèmes d'armes
- Perturbation des progiciels de *supply chain*
- Psy Ops

Cyberdéfense : les Rafale, Tigre, Leclerc sont-ils vulnérables aux cyber-attaques ?

LA TRIBUNE

Organisation Cyber en France

Organisation cyber

Premier Ministre

ANSSI

Ministère de la Défense

Armées

DGA

DGSE

Ministère de l'intérieur

Gendarmerie nationale

200 Opérateurs d'importance vitale (OIV) publics et privés

Cyberdéfense

La doctrine nationale

La cyberdéfense est l'ensemble des activités qui permettent d'intervenir dans le cyberespace pour garantir l'efficacité opérationnelle des forces armées, la réalisation des missions qui leur sont confiées et le bon fonctionnement du ministère.

La cyberdéfense complète les actions de protection menées par la voie fonctionnelle SSI afin de renforcer le niveau de sécurité global (cybersécurité).

La doctrine nationale

Défense active des systèmes d'information

+

Capacité de gestion de crise cybernétique

+

Capacités de lutte et de conduite d'opérations dans le cyberespace

La doctrine nationale

Posture robuste et résiliente de protection des SI de l'État, des opérateurs d'importance vitale (OIV) et des industries stratégiques, couplée à une organisation opérationnelle de défense de ces systèmes.

Capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et d'ampleur variées faisant (…) appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens (…) de la Défense, si les intérêts stratégiques nationaux étaient menacés.

ANSSI

- Agence nationale de la sécurité des systèmes d'information

- Créée le 7 juillet 2009, suite au Livre blanc sur la défense et la sécurité nationale (2008).
- Rattaché au Secrétaire général de la défense et de la sécurité nationale(SGDSN), organe rattaché au Premier ministre.
- ANSSI, autorité nationale en matière de sécurité et de défense des systèmes d'information
- Dispose d'un centre opérationnel (COSSI)

SGDSN

Missions ANSSI

- Détecter et réagir aux attaques informatiques (surveillance des réseaux sensibles et mise en œuvre de mécanismes de défense)
- Prévenir la menace (développement de produits de très haute sécurité pour les administrations et les acteurs économiques
- Conseiller et soutenir les administrations et opérateurs d'importance vitale (OIV)
- Informer le public sur les menaces

MINDEF- Armées

- Officier général en charge de la cyberdéfense (OG Cyber), secondé par un Officier en lutte informatique défensive central (OLID)

- Centre d'analyse de lutte informatique défensive (CALID) : alerte et réaction rapide face aux menaces sur le théâtre national et en opérations extérieures

- Des officiers LID (Lutte Informatique Défensive) dans les armées et des ALID (adjoints LID) dans les unités.

MINDEF- DGA

- Recherche et expérimentations
- Etudes amonts
- Développement de produits de sécurité avec l'industrie
- Moyens techniques de lutte informatique défensive (MTLID)
- Soutien au PME innovante (projets RAPID, techno. duale)

Division Maitrise de l'information

Site de Bruz (près de Rennes)

MINDEF- DGSE

Ministère de l'intérieur

- Lutte contre la cybercriminalité
- Institut de police criminelle
  - Laboratoire de police scientifique
- Service technique de recherche judiciaire et de documentation
  - Division de lutte contre la cybercriminalité
  - Centre d'analyse des images pédopornographiques
  - Enquêteurs technologie numérique (local)
- Recherche, cyberpatrouilles, piégeage, enquête, blocage ordinateurs, etc.

Opérateurs d'importance vitale (OIV)

- Un secteur d'activité d'importance vitale (SAIV) a trait à la satisfaction des besoins essentiels des populations ou peut présenter un danger grave pour elle

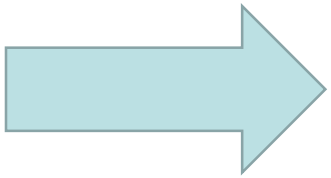
- Un opérateur d'importance vitale OIV gère ou utilise un ou des établissements, ouvrages, installations dont le dommage, l'indisponibilité, la destruction, le sabotage, etc. risque :
  - d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
  - ou de mettre gravement en cause la santé ou la vie de la population.

L'action de l'Etat pour l'industrie

- Octobre 2013, le Premier ministre installe le Comité de la filière industrielle de sécurité (COFIS)
- Janvier 2014, le ministre de la Défense annonce un pacte Défense Cyber dont, entre autres:
  - Renforcement de l'industrie ;
  - Développement d'une nouvelle génération d'équipements et de logiciels ;
  - Augmentation des crédits des programmes d'études amont à 30 Meuros par an.

Cyber et aéronautique

- Transformation digitale
- Interconnexion des systèmes
- Interconnexions externes
- Facteurs humains



- Altération du secret
- Vulnérabilité des systèmes
- Dérive des données

Questions