Ch. 4 Cyber-Combat

UE Master 2 : Sécurité des Systèmes d'Information

Sébastien Duval

D'après vous ?

Qui sont les cyber-combattants ?

Pourquoi se battent-ils ?

D'après vous ?

C'est quoi le cyber-combat ?

cyber-combat = cyber-attaque + cyber-défense ?

D'après vous ?

C'est quoi le cyber-combat ?

cyber-combat = cyber-attaque + cyber-défense ?

- combat = **militaire**
- différence majeure par rapport à la cybersécurité civile : **pas les mêmes objectifs**

Contenu

Première partie I

Définition et Enjeux

Contenu Partie I : Définition et Enjeux

Quelles entités se battent ?

Attaque

- armées
- services d'espionnage
- groupes idéologiques violents (terroristes...)
- groupes idéologiques non-violents (lobbys...)
- individus

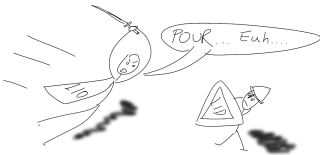
Défense

- armées
- services de contre-espionnage
- police
- sécurité des entreprises
- individus

Pourquoi ?

D'après vous ?

Pour/quoi se battre ?

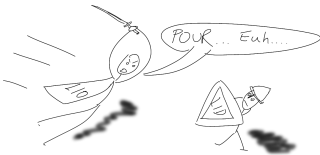


Pourquoi ?

D'après vous ?

Pour/quoi se battre ?

- **infuence** (politique, économique, idéologique, destabilisation...)
- intérêts nationaux (guerres...)
- intérêts économiques (concurrence de marchés, sabotage...)



Cible principale : l'influence

L'**influence** est un sujet vaste : toute personne qui s'exprime influence.

Influence (définition du cnrtl)

Action (généralement prolongée dans le temps et non brutale) qu'une personne ou un groupe exerce sur les opinions politiques, morales, intellectuelles, artistiques d'une personne ou sur ses modes d'expression.

Objectif : changer l'opinion

Moyens :

- **convaincre** (arguments)
- **persuader** (émotions)

Tout le monde influence.
Certains en font leur **métier**.

Résumé

Attaque

Personnes

- armées
- services d'espionnage
- groupes idéologiques violents (terroristes...)
- groupes idéologiques non-violents (lobbys...)
- individus

Armes

- menace, déstabilisation (sabotage, rançons)
- sondes d'espionnage (logicielles, matérielles, individus)
- propagande (média sociaux et nationaux, publicité)
- distraction, anti-réflexion (logiciel, matériel, médiatique...)

Défense

Protections

- protection anti-intrusion
- protection anti-intrusion
- propagande (média sociaux et nationaux, publicité)
- information (journalisme, science)

Personnes

- armées
- services de contre-espionnage
- police
- sécurité des entreprises
- individus

Résumé

Attaque

armées, terroristes
espions
lobbys
individus

menace, déstabilisation
sondes d'espionnage
propagande
distraction

Défense

anti-intrusion
anti-intrusion
propagande
information

armées, police, SSI civile
contre-espions
lobbys
individus, journalistes

Deuxième partie II

Rôles

Contenu Partie II : Rôles

Les trois axes du cyber-combat

L'armée française inclut aujourd'hui trois types de luttes distincts :

- LIO : Lutte informatique offensive ($\sim$ Red Team)
- LID : Lutte informatique défensive ($\sim$ Blue Team)
- L2I : Lutte informatique d'influence

LIO - Lutte informatique offensive

- sabotage
- espionnage
- déstabilisation

Mais attention ! Il y a des règles à respecter ! (cf. Section Règles)

LID - Lutte informatique défensive

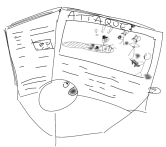
- mise en place de protections
- mise à jour des protections
- monitoring
- contre-espionnage
- réponse à incident

L2I - Lutte informatique d'influence

C'est l'objectif final, à ne pas perdre de vue !

- utilise les informations remontées par les LIO et LID pour générer du soutien de l'opinion publique, politique, économique
- inclut deux sous-axes d'attaque et défense sur les réseaux sociaux et nationaux :
  - information vs désinformation
  - faits vs mensonges
  - utilisation/destruction de bots sur les réseaux sociaux
- récupère des informations utiles pour les LIO et LID (informations sur des entreprises, des personnes...)

Ici aussi, la partie offensive doit respecter les règles ! (cf. Section Règles)



L2I - Informatique ou SHS ?

Les collègues de SHS qui font de la L2I ne sont pas experts en informatique.

L2I - Informatique ou SHS ?

Les collègues de SHS qui font de la L2I ne sont pas experts en informatique.

Mais ils ont besoin d'informaticiens !

L2I - Informatique ou SHS ?

Les collègues de SHS qui font de la L2I ne sont pas experts en informatique.

Mais ils ont besoin d'informaticiens !

- pour créer/détecter des bots sur les réseaux sociaux
- pour gérer du big data (les réseaux sociaux c'est des milliards de messages par jour)
- pour créer des sites Web
- pour authentifier des informations (*e.g.* signatures électroniques d'images)
- pour détecter des fausses informations (idem)
- ...

C'est majoritairement du développement logiciel, parfois spécialisé.

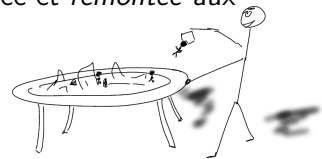
Contenu Partie II : Rôles

Management

- cadre militaire : très hiérarchisé
- management vertical (tout remonte vers les supérieurs)
- commandement spécialisés en gestion de crise
- soldats spécialistes techniques
- commandement et soldats ne sont pas sur les mêmes lieux
- LID, LIO et L2I communiquent peu

Quelques règles fondamentales :

- toute **information** doit être *communiquée* avec l'équipe et résumée et *remontée* aux supérieurs
- toute **action** doit être *formalisée* et *validée* par les supérieurs
- toute **opération** donne lieu à un *rapport*



Communication

Principe : C'est un monde encore jeune, avec des gens de formations différentes dans un cadre militarisé : rien de tout ça ne favorise la communication.

Pourtant la communication est **essentielle**, vous le verrez dans CHE ! Vous êtes capables de faire mieux que les pros sur la communication, n'hésitez pas à le faire (et allez révolutionner le cyber-combat si ce domaine vous intéresse) !

- dialogue LIO $\leftrightarrow$ LID
- dialogue LIO $\leftrightarrow$ L2I
- donner au commandement une **vision précise** de la situation (autant que possible !)
- l'**information** est notre force, on la *protège* mais on l'*utilise* aussi !

Troisième partie III

Règles

Contenu Partie III : Règles

Règles

Ça va être court : c'est majoritairement confidentiel.

- comme pour toute armée, l'armée cyber suit des **règles d'engagement**
- depuis peu, l'armée a publié une doctrine de la L2I (cf. Arche)
- la France n'est pas en guerre
- la France est en **conflit ouvert permanent** dans le monde numérique

Quelques éléments (propres à l'armée française) :

- la **désinformation** est une *arme interdite*
- la **maîtrise du périmètre d'attaque** est essentielle pour éviter les *dégâts colatéraux*
- la branche de l'armée dédiée est le COMCYBER
- respect de la Charte des Nations unies et du principe de non-ingérence
- respect du Droit international humanitaire

Quatrième partie IV

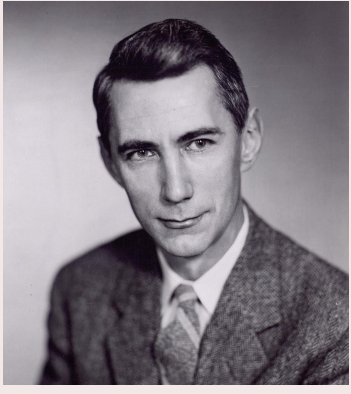
Un peu de théorie de la communication

Contenu Partie IV : Un peu de théorie de la communication

Claude Shannon

D'après vous ?

Claude Shannon, c'est qui ?



Claude Shannon

- père de la **théorie de l'information** / de l'**informatique** (années 40)
- articles fondateurs :

Claude Shannon

- père de la **théorie de l'information** / de l'**informatique** (années 40)
- articles fondateurs :
  - 1948 - *A Mathematical Theory of Communication*
    point de départ de l'informatique
    information et signal, numérique et analogique, transmission, correction, canaux de communication, ...

Claude Shannon

- père de la **théorie de l'information** / de l'**informatique** (années 40)
- articles fondateurs :
  - 1948 - *A Mathematical Theory of Communication*
    point de départ de l'informatique
    information et signal, numérique et analogique, transmission, correction, canaux de communication, ...
  - 1949 - *Communication Theory of Secrecy Systems*
    point de départ de la cryptographie moderne
    one-time pad, sécurité inconditionnelle, sécurité calculatoire, principes fondateurs de la cryptographie symétrique

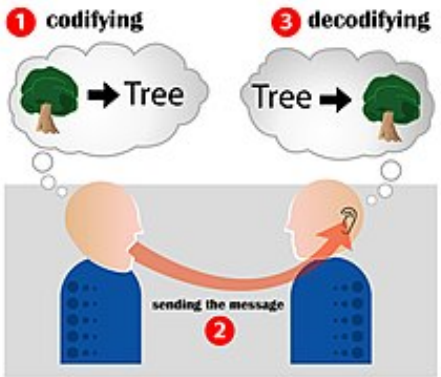
Claude Shannon

- père de la **théorie de l'information** / de l'**informatique** (années 40)
- articles fondateurs :
  - 1948 - *A Mathematical Theory of Communication*
    point de départ de l'informatique
    information et signal, numérique et analogique, transmission, correction, canaux de communication, ...
  - 1949 - *Communication Theory of Secrecy Systems*
    point de départ de la cryptographie moderne
    one-time pad, sécurité inconditionnelle, sécurité calculatoire, principes fondateurs de la cryptographie symétrique
  - 1950 - bases de l'intelligence artificielle

Shannon et la théorie de la communication

- Shannon a tenté de formaliser l'information dans la communication (1948)
- il a formalisé les concepts de
  - canaux de communication
  - bruit, erreur et correction d'erreur
  - émetteur et récepteur
- en électronique, mais aussi dans une conversation **orale** ou **écrite**
- c'est un article fondateur de la *théorie de la communication* (SHS)

Éléments de théorie de la communication



Éléments de théorie de la communication

Quelques éléments de théorie pour tous les jours :

- il y a du **bruit** à **chaque étape** de la communication
- une grosse part du bruit vient du fait que l'éméteur et le receveur
  - n'ont **pas les mots parfaits** pour décrire le concept à exprimer
  - n'ont **pas la même interprétation** des mots
- pour corriger l'erreur :
  - l'émetteur **répète** avec des **mots différents**
  - le récepteur **répète** ce qu'il a compris
  - choisir les mots les plus **précis** possible
  - faire des phrases **courtes**

Bref, communication

- les militaires se vantent d'avoir de bons canaux de communication
- c'est vrai, dans une certaine limite * :
  - le commandement reçoit bien toute l'information
  - les soldats n'ont presque pas d'information
  - ça fonctionne bien quand le soldat n'a **pas besoin d'information** (*e.g.* a un rôle physique, pas intellectuel)
  - en cyber, le soldat a besoin d'information, et là côté militaire ça pêche
- pendant Cyber Humanum Est, **communiquez** !
- si vous voulez bosser dans l'armée, je compte sur vous pour les déranger sur ce sujet !

*. Ceci est mon opinion.

Cinquième partie V

Dans le monde professionnel

Contenu Partie V : Dans le monde professionnel

Branches de l'armée qui font du cyber

Gendarmerie : force armée chargée de missions de police pour les civils + un peu d'opérations extérieures

- gestion de la défense civile
- travail avec la police (l'effectif cyber de la gendarmerie est bien plus important)

COMCYBER : commandement de la cyberdéfense

- gestion de la protection nationale

DGA : Direction Générale de l'Armement

- référent technique de l'armée pour la cybersécurité
- $\sim$ ANSSI militaire

Tout le monde travaille avec les équivalents des autres pays, le numérique est par essence **international**.

Sixième partie VI

La coopération civil-militaire

Contenu Partie VI : La coopération civil-militaire

Le rôle classique des militaires

- le rôle des militaires est de protéger les **frontières** contre les menaces **extérieures**
- la protection face aux menaces intérieures est du ressort de la **police** (exception : gendarmes en renfort)

Le cas cyber

Les menaces cyber n'ont pas de frontières physiques bien définies !
Point-de-vue militaire : Où protéger ? Comment, quand on ne peut pas faire barrière et filtrer les entrées ?

Conclusion : Dans le cas cyber, les militaires ne peuvent pas tenir la menace à l'écart des civils ! Ils **coopèrent** avec les civils et soutiennent la montée en compétence de la cybersécurité civile !

Info : Comme dans le civil, en cyber, beaucoup de gens font quelques années dans l'armée comme n'importe quel job et changent de job ensuite.

Références utiles liées au chapitre

https://cyber.gouv.fr/publications/
anticiper-et-gerer-sa-communication-de-crise-cyber