

# La guerre numérique, une réalité !

Corentin CHÉDOTAL

30 Mars 2016

# Sommaire

- 1 Introduction
- 2 Les Acteurs
  - États
  - Non-étatiques
- 3 Possibilités Professionnelles
  - Secteur Public
  - Secteur Privé
- 4 Conclusion

# Préface

## Nota

La cyberguerre et ce qui l'entoure est fréquemment affiliée au monde des renseignements. Ainsi les informations sur celle-ci sont généralement entourées du film opaque de la classification des documents. De ce fait certains des éléments contenus dans cette présentation se révéleront peut être incomplets ou inexacts dans le futur suite à des déclassifications.

# Ouverture

*[Le Cyber], est un milieu à part entière, d'une complexité extrême. Et qui voit actuellement des combats d'une ampleur, je serais même tenté de dire d'une violence, inouïe.*

*Matrix n'est plus un film de science-fiction, nous y sommes.*

Jean-Yves LE DRIAN, Ministre de la Défense  
Janvier 2016

# La guerre du numérique, késako ?

Internet connecte presque tous les réseaux. Ainsi l'information peut être transmise d'un bout à l'autre de n'importe quel endroit sur Terre à n'importe quel autre. Les états comme les entreprises et les particuliers se servent donc d'Internet continuellement.

Cependant aucun réseau n'est infallible.

Les informations ont de la valeur.

De plus en plus de systèmes sont connectés à Internet, de la webcam de votre maison à des fonderies.

Alors des acteurs rivaux tenteront toujours d'employer tous les moyens à leur disposition pour contrer leurs nemesis.

## Divers termes pour décrire une même réalité

Partant du constat précédent le cyberspace est bien un champ de bataille.

L'OTAN préférera employer le terme de "cyberdéfense" et évitera à tout prix celui de "cyberguerre" qu'elle estime ne pas encore être une réalité pour diverses raisons.

La France depuis plusieurs années communique sur ce qu'elle qualifie de "4ème milieu" sur lequel se déroule des batailles aux effets parfois très réels. Le terme de "cyberguerre" étant alors employé parfois pour décrire ces conflits virtuels.

# Petit point de vocabulaire

## Petit point de vocabulaire

### Cyberespace

Monde virtuel dans lequel l'Utilisateur se plonge quand il rentre dans un réseau.



# Petit point de vocabulaire

## Cyberespace

Monde virtuel dans lequel l'Utilisateur se plonge quand il rentre dans un réseau.

## Sécurité des Systèmes d'Information

Ensemble des systèmes assurant à un SI

- sa confidentialité
- son intégrité
- sa disponibilité
- sa non-répudiation (authentification)

# Petit point de vocabulaire

Les faux semblants

# Petit point de vocabulaire

## Les faux semblants

### Cyberprotection

Ensemble des moyens mis en place pour la protection des SI par un pays.

# Petit point de vocabulaire

## Les faux semblants

### Cyberprotection

Ensemble des moyens mis en place pour la protection des SI par un pays.

### Cyberdéfense

Défense et attaque de SI et/ou de réseaux par un pays.  
Décrit aussi la mise en place des stratégies et tactiques liées à ces attaques sans qu'elles ne soient forcément mise en oeuvre effectivement.

# Petit point de vocabulaire

## Les faux semblants

### Cyberprotection

Ensemble des moyens mis en place pour la protection des SI par un pays.

### Cyberdéfense

Défense et attaque de SI et/ou de réseaux par un pays.  
Décrit aussi la mise en place des stratégies et tactiques liées à ces attaques sans qu'elles ne soient forcément mise en oeuvre effectivement.

### Cyberrésilience

Autonomie des SI et réseaux par rapports à des états/entreprises ou à la nature.

# Petit point de vocabulaire

Les faux semblants

# Petit point de vocabulaire

## Les faux semblants

Cybersécurité

Cyberprotection + Cyberdéfense + Cyberrésilience

# Sommaire

- 1 Introduction
- 2 Les Acteurs
  - États
  - Non-étatiques
- 3 Possibilités Professionnelles
  - Secteur Public
  - Secteur Privé
- 4 Conclusion



# "Five Eyes"

Qu'est-ce ?



Le "Five Eyes" est une alliance stratégique regroupant l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis d'Amérique. Les agences de renseignements des cinq états membres sont en lien direct et doivent partager leurs renseignements bruts avec leurs homologues étrangers.

Dans le domaine du cyber cette alliance fait majoritairement dans la collecte passive de renseignement et dans la défense des infrastructures connectées à Internet de leurs pays respectifs. Mais pas que. . .

# "Five Eyes"

Pas très offensif ? Vraiment ?

**ICSD**  
Intelligence, Defense, Effects

**EFFECTS: Definition**

**JTRIG**

- “Using online techniques to make something happen in the real or cyber world”
- Two broad categories:
  - Information Ops (influence or disruption)
  - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D's: Deny / Disrupt / Degrade / Deceive

**TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL**

FIGURE – Extrait d'une présentation interne des services secrets britanniques

# "Five Eyes"

## Le cas particulier des États-Unis d'Amérique

En plus de leur participation au "Five Eyes" les États-Unis sont un cas particulier.

Bien plus agressifs que le reste des pays participants ils organisent leur collecte de renseignements de façon bien plus offensive, cassant les réseaux internes de certaines ambassades par exemple.

De plus les Américains ne s'arrêtent pas simplement à la défense et aux renseignements. Ils seraient à l'origine de plusieurs malwares dont le but était bien stratégique, dont *Stuxnet*.

# L'État d'Israël



Au vu de l'histoire courte mais pourtant très belliqueuse d'Israël cela ne surprend personne de voir à quelle vitesse ce pays a pu utiliser l'informatique pas seulement pour la collecte d'information mais bien en tant qu'arme. Cependant très peu d'informations fuient dans le public sur leurs avancées.

# L'État d'Israël



Au vu de l'histoire courte mais pourtant très belliqueuse d'Israël cela ne surprend personne de voir à quelle vitesse ce pays a pu utiliser l'informatique pas seulement pour la collecte d'information mais bien en tant qu'arme. Cependant très peu d'informations fuient dans le public sur leurs avancées.

## Stuxnet

Ver informatique découvert en 2010. Spécifique à Windows, il s'est propagé sur Internet jusqu'à atteindre sa seule et unique cible : le programme nucléaire iranien. Il a provoqué la destruction de centrifugeuse d'enrichissement d'uranium et plusieurs explosions. Enfin il avait un mécanisme d'auto-destruction.

# La Fédération de Russie



La Russie est un des plus gros acteurs de la cyberguerre mais aussi l'un des mieux préparé à celle-ci. En effet, quand beaucoup d'états se satisfont simplement d'une cyberdéfense la Russie cherche elle une capacité offensive dans le Cyber et l'a, ce qui est en totale adéquation avec ses objectifs géopolitiques. De plus la Russie met un point d'honneur à rendre les liens entre les attaques et sont gouvernement extrêmement ténus. En effet elle emploiera des groupes et/ou des entreprises privés qui eux seront à l'origine des attaques.

# La Fédération de Russie

## Quelques exemples

# La Fédération de Russie

## Quelques exemples

### Attaques sur les pays baltes

En 2008 l'Estonie puis la Lituanie subissent une vague d'attaques informatiques. Du simple *defacing* à des tentatives d'accès à la banque centrale lituanienne. Les enquêtes pointent du doigt la provenance russe des attaques. Cependant elles proviennent de très nombreux particuliers et petits groupes, pas d'institutions gouvernementales. Aucune réelle sanction ne pourront être imposé par les états cibles.



# La Fédération de Russie

## Quelques exemples

### Attaques sur les pays baltes

En 2008 l'Estonie puis la Lituanie subissent une vague d'attaques informatiques. Du simple *defacing* à des tentatives d'accès à la banque centrale lituanienne. Les enquêtes pointent du doigt la provenance russe des attaques. Cependant elles proviennent de très nombreux particuliers et petits groupes, pas d'institutions gouvernementales. Aucune réelle sanction ne pourront être imposé par les états cibles.

### BlackEnergy

Trojan découvert d'abord en 2014, il est passé de la collecte de renseignements sur le gouvernement Ukrainien à la coupure temporaire récente du réseau électrique du pays.

# La République Populaire Démocratique de Corée



La Corée du Nord fait des efforts considérables depuis l'avènement des années 2000 pour maintenir une force offensive dans le Cyber. En effet, n'ayant que peu de capacités militaires conventionnelles elle se tourne vers d'autres moyens d'atteindre ses cibles principales : la République de Corée, le Japon et les États-Unis. Pour cela elle possède diverses institutions spécialisées dans le vol de renseignements et l'attaque de SI.

# La République Populaire Démocratique de Corée



La Corée du Nord fait des efforts considérables depuis l'avènement des années 2000 pour maintenir une force offensive dans le Cyber. En effet, n'ayant que peu de capacités militaires conventionnelles elle se tourne vers d'autres moyens d'atteindre ses cibles principales : la République de Corée, le Japon et les États-Unis. Pour cela elle possède diverses institutions spécialisées dans le vol de renseignements et l'attaque de SI.

## Bureau 121 et The Interview

L'une des actions nord-coréennes les plus médiatisées fut l'attaque des serveurs de Sony Pictures qui annula la diffusion du film en salle comme l'attaque était accompagnée de menaces.

# La République Française



La France comme beaucoup d'états démocratiques et se disant des Droits de l'Homme tend à limiter son action à la cyberprotection et à l'aspect plus défensif de la cyberdéfense. Cependant il n'est pas exclus que la France prépare ou ait préparé des capacités offensives à employer si un conflit ouvert avait lieu avec une autre puissance mondiale. De plus la Loi sur le Renseignement récemment promulguée ouvre un plus grand panel de possibilité pour la DGSE. Quant aux renseignements la France n'est pas en reste et utilise tous ses moyens à disposition pour faire de la collecte, y compris dans le cyberspace.

# La République Française


## Quand la France embête ses alliés

Overall Classification: TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, USA

Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada

### Attribution: Binary Artifacts

- ntrass.exe
  - DLL Loader uploaded to a victim as part of tasking seen in collection
  - Internal Name: Babar
  - Developer username: titi
- Babar is a popular French children's television show
- Titi is a French diminutive for Thierry, or a colloquial term for a small person



Safeguarding / Préserver la sécurité du Canada par la confidentialité de l'information

TOP SECRET // COMINT // REL TO CAN, AUS, GBR, NZL, USA

Canada

18

FIGURE – Rapport des services secrets canadiens sur Babar

# Sommaire

- 1 Introduction
- 2 Les Acteurs
  - États
  - Non-étatiques
- 3 Possibilités Professionnelles
  - Secteur Public
  - Secteur Privé
- 4 Conclusion

# Anonymous



Collectif anarchique d'*hacktivistes* qui malgré son fonctionnement volontairement sans réelles règles parvient à réaliser de nombreuses actions de très grandes envergures.

Utilise l'informatique pour lutter contre le non respect de droits qu'ils considèrent fondamentaux. Leurs cibles les plus connues sont les gouvernements occidentaux, Daesh et la Scientologie.

# Anonymous



Collectif anarchique d'*hacktivistes* qui malgré son fonctionnement volontairement sans réelles règles parvient à réaliser de nombreuses actions de très grandes envergures.

Utilise l'informatique pour lutter contre le non respect de droits qu'ils considèrent fondamentaux. Leurs cibles les plus connues sont les gouvernements occidentaux, Daesh et la Scientologie.

## Actions couramment entreprises

- Attaques DDoS
- *Doxxing* de personnalités importantes de leurs cibles
- *Defacing* des sites Internet de leurs cibles diverses



# Daesh

Organisation terroriste basée entre la Syrie et l'Irak, tristement célèbre en particulier suite aux attentats de Paris et de Bruxelles. Elle aurait une ou plusieurs "sections" dédiées à ce qu'elle qualifie de "cyberjihad". Cependant contrairement au reste de l'organisation leur "cyberjihad" est assez risible.

# Daesh

Organisation terroriste basée entre la Syrie et l'Irak, tristement célèbre en particulier suite aux attentats de Paris et de Bruxelles. Elle aurait une ou plusieurs "sections" dédiées à ce qu'elle qualifie de "cyberjihad". Cependant contrairement au reste de l'organisation leur "cyberjihad" est assez risible.

## Actions couramment entreprises

- *Defacing* de divers sites Internet
- Serait en train d'entreprendre des hacks bien plus importants

## 4chan

Forum de discussion anglophone basé sur l'anonymat, il est extrêmement controversé car on y trouve de tout, du bien (lieu de naissance d'Anonymous à priori) comme du mal (apologie du nazisme. . .). Malgré l'anarchie totale qui en transpire sa communauté est parfois à l'origine de "raids" qui bien que n'entrant pas forcément dans la définition de la cyberguerre il s'en approche parfois.

## 4chan

Forum de discussion anglophone basé sur l'anonymat, il est extrêmement controversé car on y trouve de tout, du bien (lieu de naissance d'Anonymous à priori) comme du mal (apologie du nazisme. . .). Malgré l'anarchie totale qui en transpire sa communauté est parfois à l'origine de "raids" qui bien que n'entrant pas forcément dans la définition de la cyberguerre il s'en approche parfois.

### Actions couramment entreprises

- *Trolling* de masse, s'apparentant parfois presque à du DDoS tant il peut rendre un site inutilisable.
- Attaques DDoS
- *Doxxing* de personnalités comme d'individus lambdas
- *Cyberbullying* de masse

# Possibilités Professionnelles

La cyberguerre et tout ce qui l'entoure peut être certes à l'origine de nombreuses questions et troubles en particulier quand autour de l'irrespect de droits fondamentaux comme les Droits de l'Homme ou certains fondements du droit international.

Cependant elle a aussi un bon côté. Elle crée de nombreux emplois tant dans le domaine public que privé.

# Sommaire

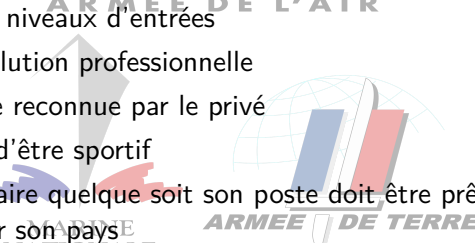
- 1 Introduction
- 2 Les Acteurs
  - États
  - Non-étatiques
- 3 Possibilités Professionnelles
  - Secteur Public
  - Secteur Privé
- 4 Conclusion

# Exemples de métiers

- Informatique
  - Recherche (lutte contre les attaques, recherches sur des SI plus défendables, recherches sur de nouvelles failles. . .)
  - Expert en Sécurité des Systèmes d'Information
  - Analyste
  - ...
- Mathématiques
  - Recherche (cryptographie, *codebreaking*. . .)
  - Analyste
  - ...
- Physique
  - Recherche (nouveaux matériaux, nouvelles techniques d'encodage matériel. . .)
  - Expert en Télécommunication
  - ...

# Quelques employeurs

## Les Armées

- 
- Nombreux niveaux d'entrées
  - Bonne évolution professionnelle
  - Expérience reconnue par le privé
  - Nécessite d'être sportif
  - Tout militaire quelque soit son poste doit être prêt à donner sa vie pour son pays



# Quelques employeurs

## La DGSE

- Entrée très restreinte
- Accepte autant des civils que des militaires
- Chargé du renseignement provenant de l'étranger
- Serait responsable des actions menées par la France sur des réseaux étrangers



# Quelques employeurs

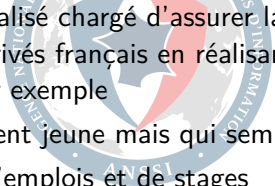
## La DGSJ

- Entrée très restreinte
- Service uniquement composé par des civils
- Originellement ses ancêtres étaient rattachés à la Police Nationale
- Chargé du renseignement provenant de l'intérieur et des éventuelles surveillances sur le territoire national



# Quelques employeurs

## L'ANSSI

- 
- Service très spécialisé chargé d'assurer la protection des SI publics comme privés français en réalisant des audits et des sensibilisation par exemple
  - Service relativement jeune mais qui semble très ouvert
  - Plusieurs offres d'emplois et de stages

# Quelques employeurs

## Les Universités

Le parcours parfait pour la recherche dans le Public, parcours que je ne détaillerai pas puisque vous avez déjà les pieds dedans.

# Sommaire

- 1 Introduction
- 2 Les Acteurs
  - États
  - Non-étatiques
- 3 Possibilités Professionnelles
  - Secteur Public
  - Secteur Privé
- 4 Conclusion

# Exemples de métiers

- Informatique
  - Auditeur
  - *Pen-tester*
  - Expert en Sécurité des Systèmes d'Information
  - ...
- Physique
  - Expert en Télécommunication
  - ...

# Quelques employeurs

## Les SSII

De très nombreux postes liés à l'informatique sont offerts dans les SSII puisqu'il s'agit de leur domaine d'action. Mais avec le nombre croissant d'attaques informatiques de plus en plus de postes ont attiré à la cyberprotection. Que ce soit dans la mise en place d'une (meilleure) sécurité de système d'information ou dans le conseil les SSII restent les maîtres incontestés des services liés au numérique.

# Quelques employeurs

## Les entreprises d'intérêt stratégiques

La cyberguerre est pour certaines entreprises un cauchemar duquel elle ne se réveilleront jamais. En effet pour les entreprises comme Dassault Aviation, DCNS, Total et tant d'autres elles représentent le summum des capacités stratégiques et technologiques de la France et sont donc des cibles de choix pour les différents acteurs de la guerre numérique. Ainsi elles doivent redoubler d'efforts pour se protéger des attaques et intrusions. Et ainsi elle sont particulièrement à la recherche de personnels qualifiés dans les domaines de la cyberprotection. Le seul défaut est qu'elles recherchent des personnes ayant déjà une grande expérience.



# Pour conclure

## Pour conclure

- Quoi qu'on en dise, quel que soit le nom qu'on lui donne **la cyberguerre est une réalité.**

## Pour conclure

- Quoi qu'on en dise, quel que soit le nom qu'on lui donne **la cyberguerre est une réalité.**
- Les acteurs sont **nombreux, plus ou moins dangereux et organisés** et chacun avec leurs agendas spécifiques.

## Pour conclure

- Quoi qu'on en dise, quel que soit le nom qu'on lui donne **la cyberguerre est une réalité.**
- Les acteurs sont **nombreux, plus ou moins dangereux et organisés** et chacun avec leurs agendas spécifiques.
- Cependant les gouvernements comme les entreprises s'en rendent compte et **la guerre numérique crée des emplois.**

# Remerciements

Merci beaucoup d'avoir suivi cette conférence.

Si vous avez des questions je vous invite à les poser maintenant.

# Remerciements

Merci beaucoup d'avoir suivi cette conférence.

Si vous avez des questions je vous invite à les poser maintenant.  
Cette présentation est maintenant terminée, en espérant qu'elle  
vous ait plu, des cookies devraient vous attendre à la sortie de  
l'amphithéâtre.

