Sécurité Informatique
Synoptique

ISIMA MI2 – S2 2019/20 – CM 16h

Thomas LEFAURE

Sommaire

Introduction

Introduction

- Thomas LEFAURE
  - thomas.lefaure[at]gmail.com
  - Vous pouvez me contacter sur LinkedIn
- Parcours
  - IFMA 2000 & Telecom SudParis MS-SSR 2016
  - Développement Informatique
    - 2001-2007 : Analyste Développeur C/C++/CAA (IAO)
    - 2007-2010 : Manager équipe de développement PLM (France & Inde)
  - Sécurité Informatique
    - 2010-2012 : Officier & Analyste Sécurité SI dans le domaine R&D
    - 2012-2018 : Architecte et Chef de projet Sécurité SI
    - Depuis 2018 : Architecte Cybersécurité d'Entreprise

Introduction

- Règles de vie du cours
  - Si vous ne voulez pas venir … ne venez pas !
  - Vous pouvez à tout moment m'interrompre pour poser une question pertinente.
  - Bien connaître le support de cours (en libre accès) permet d'avoir au moins la moyenne au partiel (QCM), et pour avoir plus que la moyenne il faudra de toute façon suivre le cours.

  - Il y aura un appel impromptu lors d'un de mes cours. Les personnes présentes ce jour là auront le bénéfice d'un point sur leur note de partiel.
  - Ce support de cours sera disponible au téléchargement après chaque session, et dans son intégralité après la dernière.

Introduction

- Cours sous licence Creative Common BY-NC-ND
  - **Paternité [BY]** : ce cours peut être librement distribué et utilisé, à condition de m'en attribuer la paternité en citant mon nom et en conservant le slide n°4 intact.
  - **Pas d'utilisation commerciale [NC]** : j'autorise par défaut tous les types d'utilisation, sauf les utilisations à but commercial qui sont soumises à mon autorisation explicite.
  - **Pas de modification [ND]** : je me réserve la faculté de réaliser des œuvres de type dérivées, les traductions restant soumises à mon autorisation explicite.
  - La plupart des images illustrant ce document sont sous **123RF STANDARD LICENSE** et ne peuvent pas être extraites et redistribuées sous licence Creative Common.

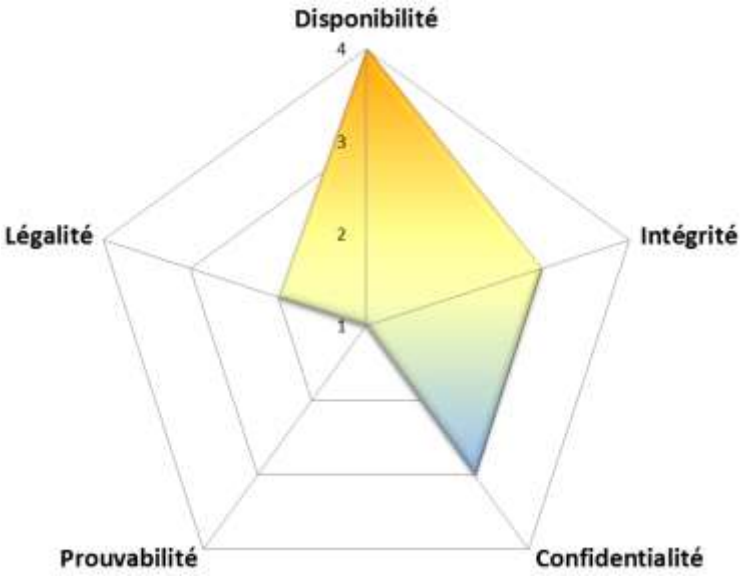
Introduction

- **Sécurité Informatique** : ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information. [Wikipédia]
- **Synoptique** : (adj.) qui permet d'embrasser, de saisir d'un même coup d'œil les diverses parties d'un ensemble, qui en offre une vue générale. [Wiktionnaire]

Chapitre I
Historique de la Cybersécurité
Notions de base

Notions de base

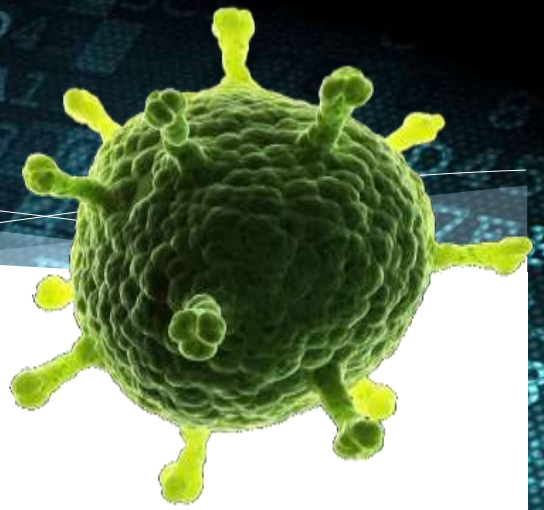
- On formalise les besoins de sécurité selon cinq axes (les DICPL) :
  - Disponibilité : garantir la continuité de service
  - Intégrité : garantir la non-falsification de l'information
  - Confidentialité : garantir le respect du besoin d'en connaître
  - Prouvabilité (ou Preuve) : garantir la traçabilité et l'imputabilité des actions
  - Légalité : garantir le respect des lois et règlements
- C'est sur cette base que sont définis et mis en œuvre les moyens de sécurisation.



Notions de base

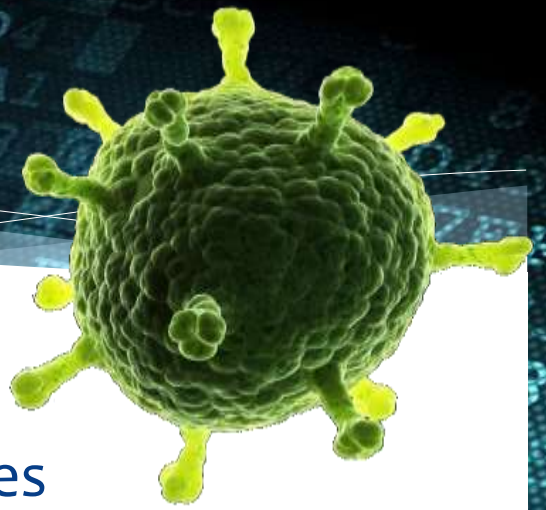
- Le terme hacker apparaît en 1959 au MIT :
  - ***« Personne qui se délecte de la compréhension approfondie du fonctionnement interne d'un système, en particulier des ordinateurs et réseaux informatiques » RFC1983 (1996)***
- La notion de chapellerie permet de distinguer leur éthique :
  - Le **whitehat** agit légalement, pour le bien de la communauté ou pour celui de ses clients. Il se rémunère par la prestation de services (tests d'intrusion, cyberdéfense, « bug bounty ») … ou pas (recherche).
  - Le **greyhat** agit généralement sans malveillance, mais assurément en dehors du cadre légal ou éthique. Lorsqu'il a la volonté de nuire, c'est souvent pour la « bonne cause » (cyberespion, hacktiviste).
  - Le **blackhat** a lui clairement choisi le côté obscur, qu'il soit à son propre compte, au service du cybercrime ou du cyberterrorisme.

Notions de base



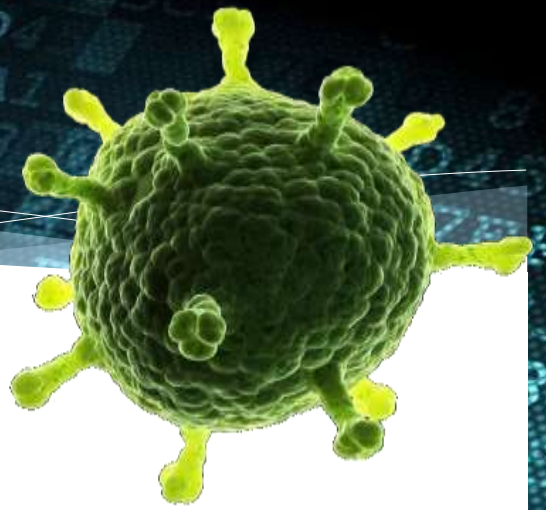
- Le terme malware (ou maliciel) désigne un logiciel malveillant classé en fonction de trois caractéristiques :
  - Un **vecteur de propagation**, qui lui permet de se diffuser.
  - Un **mécanisme déclencheur**, qui conditionne son action.
  - Une **charge utile**, le plus souvent offensive.
- Les malwares peuvent être assimilés à des **armes logicielles**.
- Les virus sont les plus anciens malwares. Ils ont été théorisés en 1949 par John von NEUMANN, et se caractérisent par un vecteur de propagation orienté autoréplication et parasitisme logiciel.
- Les vers se propagent eux sans parasitisme logiciel, souvent par l'intermédiaire de services réseau vulnérables.

Notions de base



- Les troyens, ou chevaux de Troie, sont des logiciels malveillants dont le vecteur de propagation consiste à abuser de la crédulité des utilisateurs en se faisant passer pour des programmes légitimes.
- Le spam, ou pourriel, est un message électronique (courriel, SMS, …) non sollicité, généralement à visée publicitaire.
- Le phishing, ou hameçonnage, est une technique d'ingénierie sociale visant à manipuler un utilisateur en se faisant passer pour un service légitime afin de lui soutirer des informations.
- Un botnet est un réseau de « machines zombies » connectées à Internet qui communiquent avec un ou plusieurs serveurs de contrôle, voire même entre elles (P2P).

Notions de base



- Une vulnérabilité est une faille permettant à un attaquant de nuire à la disponibilité d'un système informatique, à la confidentialité ou l'intégrité des données qu'il héberge.
- Les CERT ou CSIRT (Computer Emergency/Security Incident Response Team) sont des équipes chargées de la prévention et du traitement des attaques informatiques dans les entreprises et administrations.
- Un DoS (Denial of Service), ou Déni de Service, est une attaque portant préjudice à la disponibilité d'un système.
- Une APT (Advanced Persistent Threat), ou Menace Avancée Persistante, est une forme très sophistiquée d'intrusion.

Chapitre I
Historique de la Cybersécurité
Un peu d'Histoire

Un peu d'Histoire

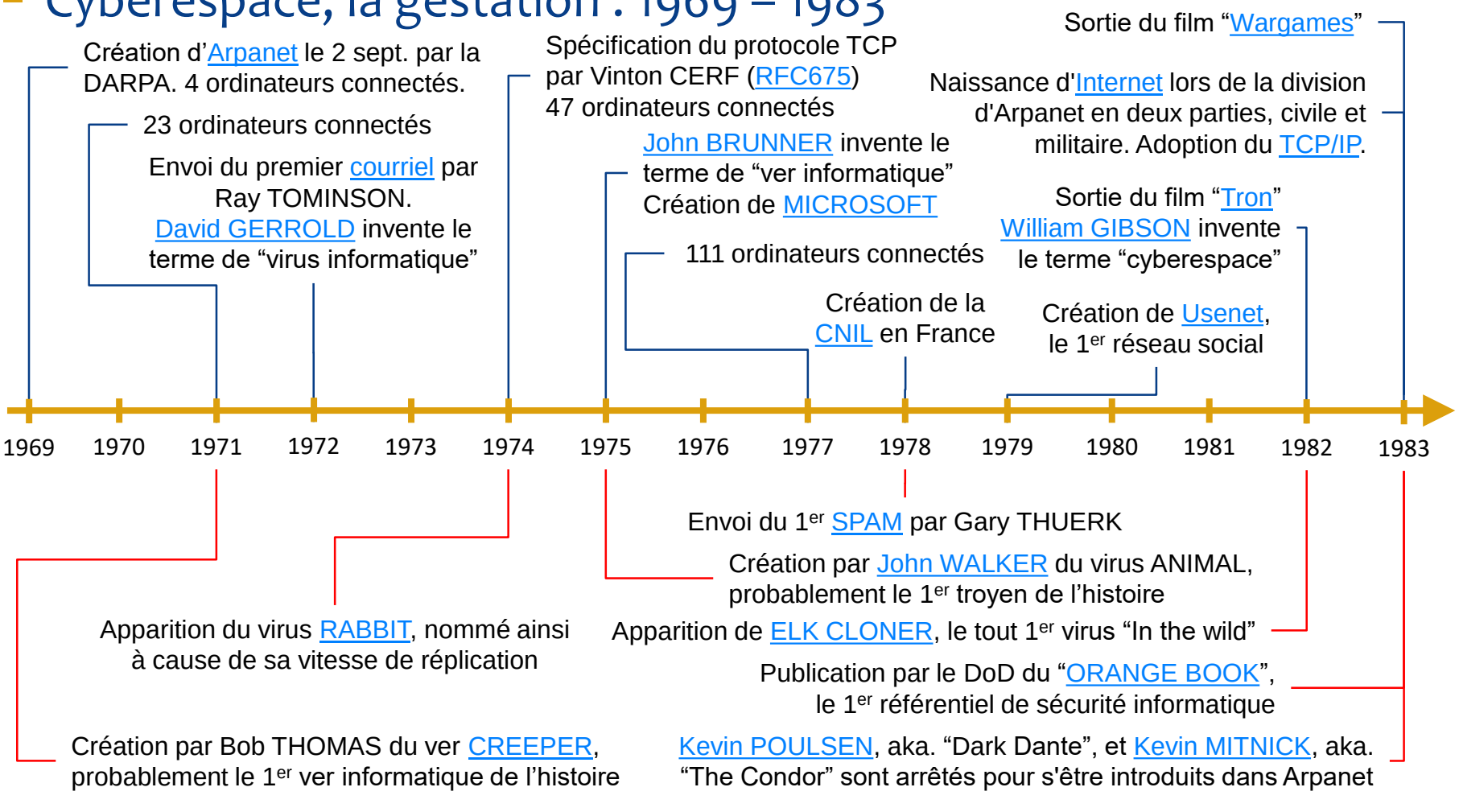
- La Cybersécurité peut-être biologiquement comparée au système immunitaire des SI auxquels elle se rattache.
- Elle s'est donc développée de concert avec « l'organisme » que l'on nomme le Cyberespace, constitué de l'interconnexion mondiale des ordinateurs.
- Le Cyberespace a connu 4 âges majeurs au cours desquels les menaces (la cyberinsécurité) et les réponses (la cybersécurité) se sont simultanément développées, avec des enjeux économiques et sociaux de plus en plus élevés.

Un peu d'Histoire

- Cyberespace, la gestation : 1969 – 1983
  - Période d'intense foisonnement intellectuel (naissance de la cyberculture) et technique (définition des fondations d'Internet avec les RFC).
  - Les hackers sont déjà là : ils sont à la fois les pères fondateurs du Cyberespace, et les créateurs des premiers virus.
  - Expérimentations techniques tous azimuts, pour le meilleur et pour le pire, mais sans volonté de nuire.
  - Cohabitation difficile entre militaires « méfiants » (guerre froide) et universitaires « libertaires » (évènements de 1968) qui aboutira à la partition du réseau et la création d'Internet.

Un peu d'Histoire

Cyberespace, la gestation : 1969 – 1983



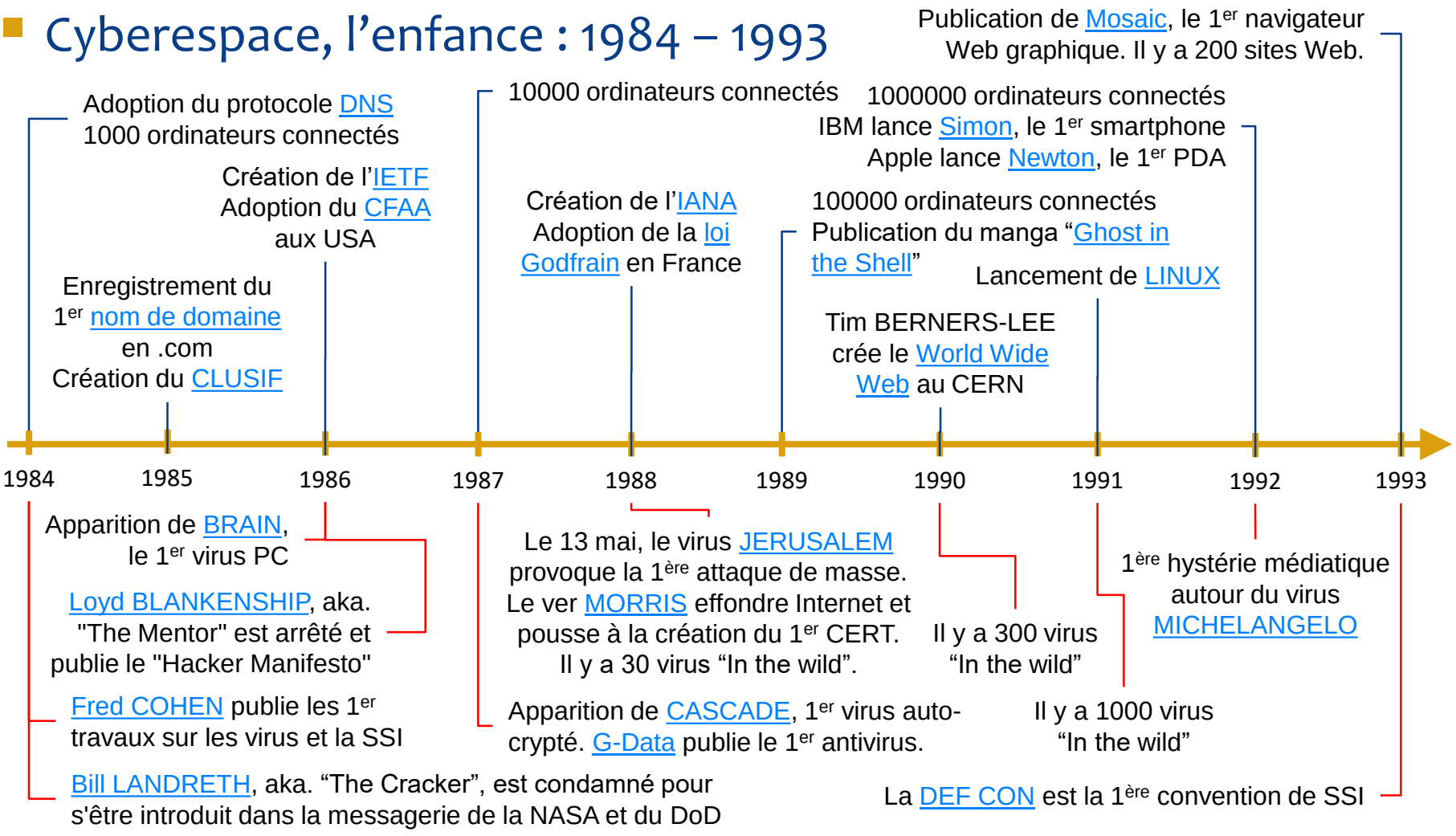
Un peu d'Histoire

- Cyberespace, l'enfance : 1984 – 1993
  - Période d'augmentation très rapide du nombre de machines connectées au réseau : leur nombre est décuplé tous les 30 mois.
  - Formalisation des principes fondateurs de la Sécurité Informatique.

  - Promulgation des premières lois relatives au cybercrime.
  - Création des principaux organes de régulation et de gouvernance.
  - Internationalisation du réseau par ouverture aux pays européens.
  - La communauté hacker se développe et se structure. La plupart ne sont pas malveillants et recherchent le défi technique et épique.
  - Apparition des premiers virus dotés de charges offensives.

Un peu d'Histoire

Cyberespace, l'enfance : 1984 – 1993



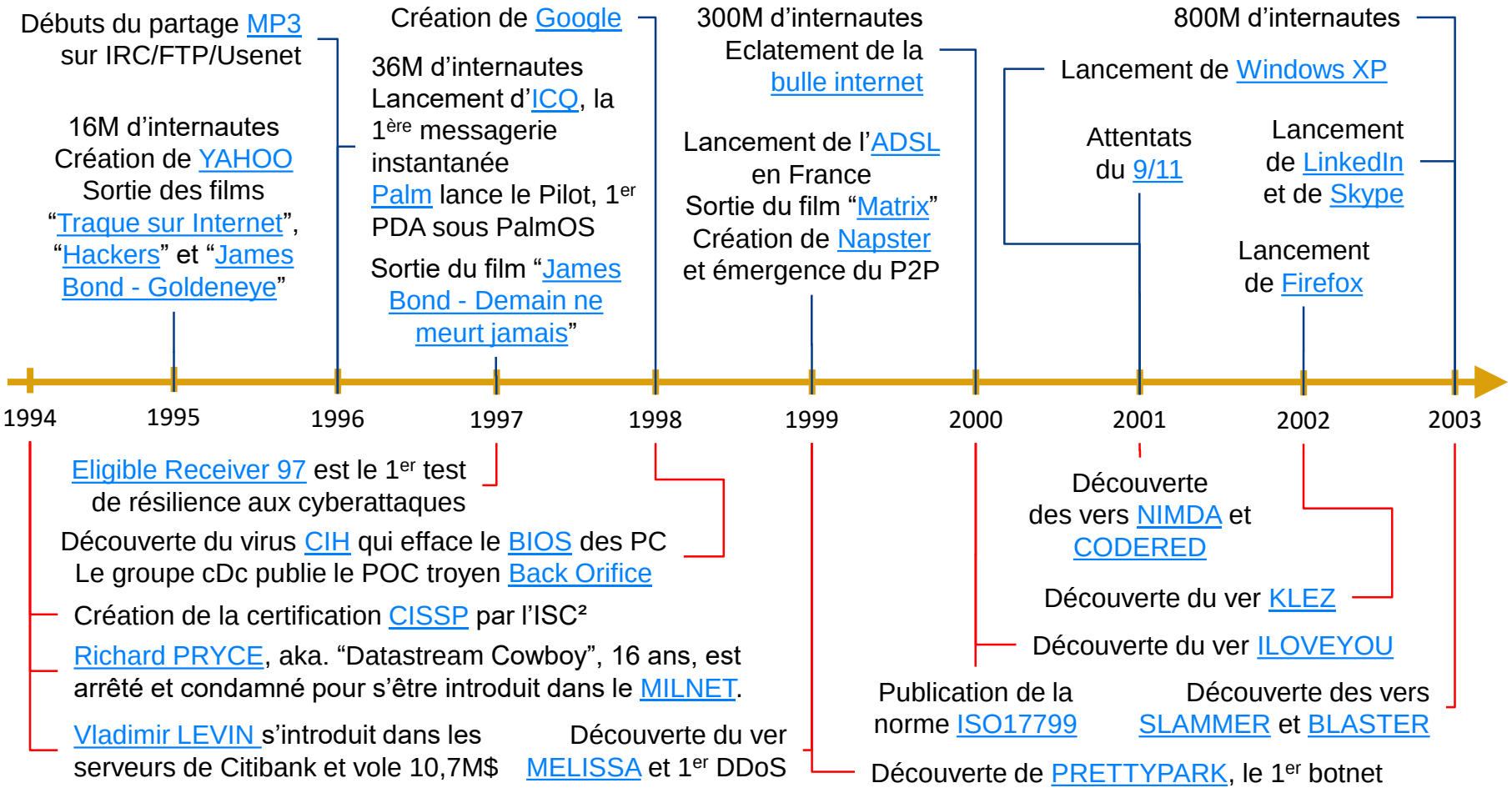
Un peu d'Histoire

- Cyberespace, l'adolescence : 1994 – 2003
  - Croissance soutenue par le développement de l'accès grand public dans les pays industrialisés, et par l'ouverture du réseau aux activités commerciales.
  - Le cyberespace devient moins élitiste et se fait une place dans la culture populaire.

  - La Nouvelle Economie s'éveille puis s'emballe jusqu'à éclatement de la bulle spéculative.
  - Les grandes entreprises prennent conscience de leur dépendance informatique avec le Bug de l'An 2000 et les Attentats du 9/11.
  - Les black hats sortent du bois et recherchent le profit.
  - Le nombre de malwares et le spam explosent.

Un peu d'Histoire

Cyberespace, l'adolescence : 1994 – 2003

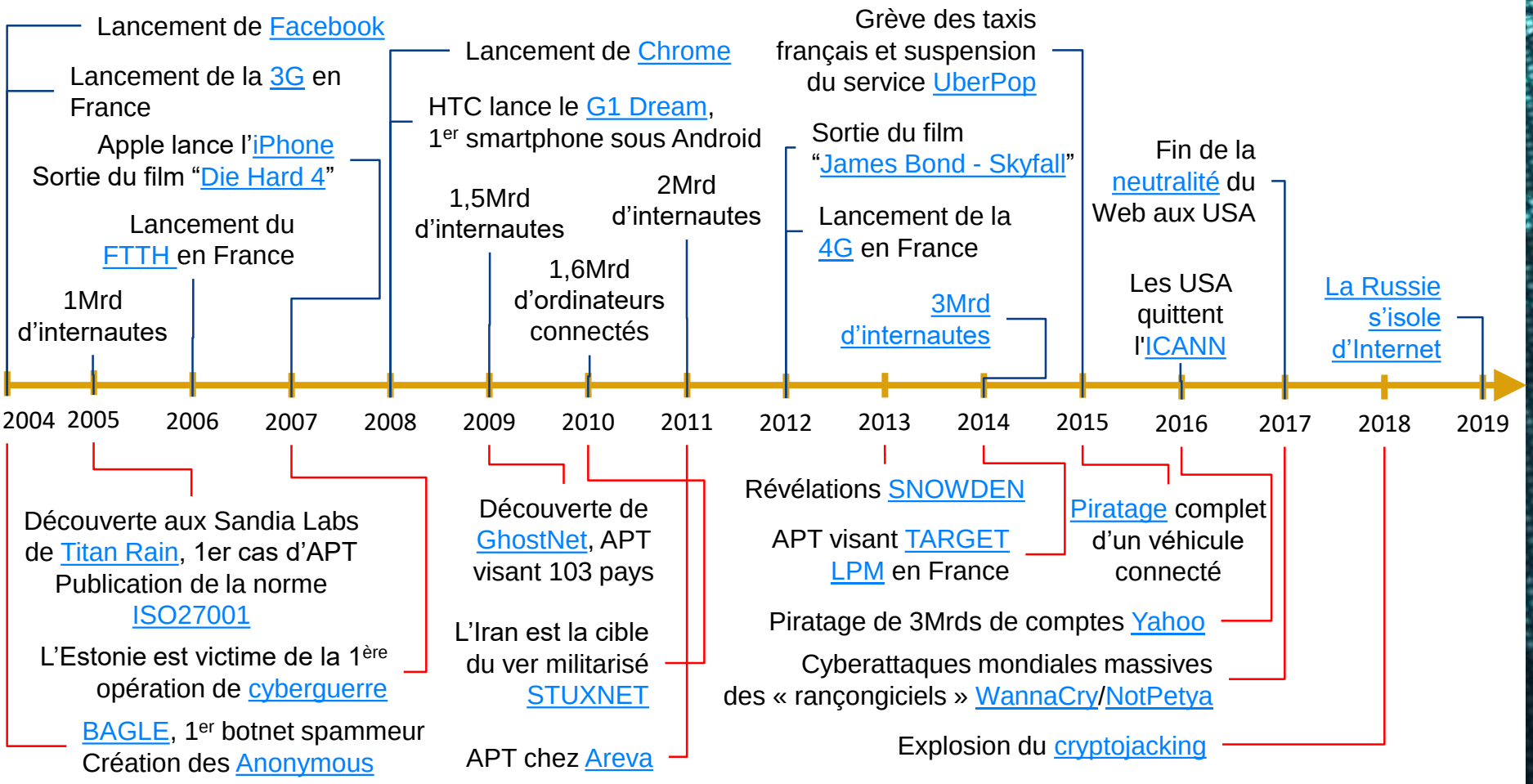


Un peu d'Histoire

- Cyberespace, l'âge adulte : 2004 – aujourd'hui
  - Croissance du réseau soutenue par le développement des connexions haut débit permanentes dans les pays industrialisés, et par l'accès mobile (smartphone) dans les pays en voie de développement.
  - Augmentation très sensible de l'hacktivisme.
  - La culture populaire découvre la notion de cyberterrorisme.
  - Militarisation fulgurante du cyberespace et révélation des premières opérations de cyberespionnage et de cyberguerre.
  - Structuration et professionnalisation de la cybercriminalité.
  - La sophistication et la malveillance des attaques explosent avec la multiplication des botnets, des DDoS, et des APT.

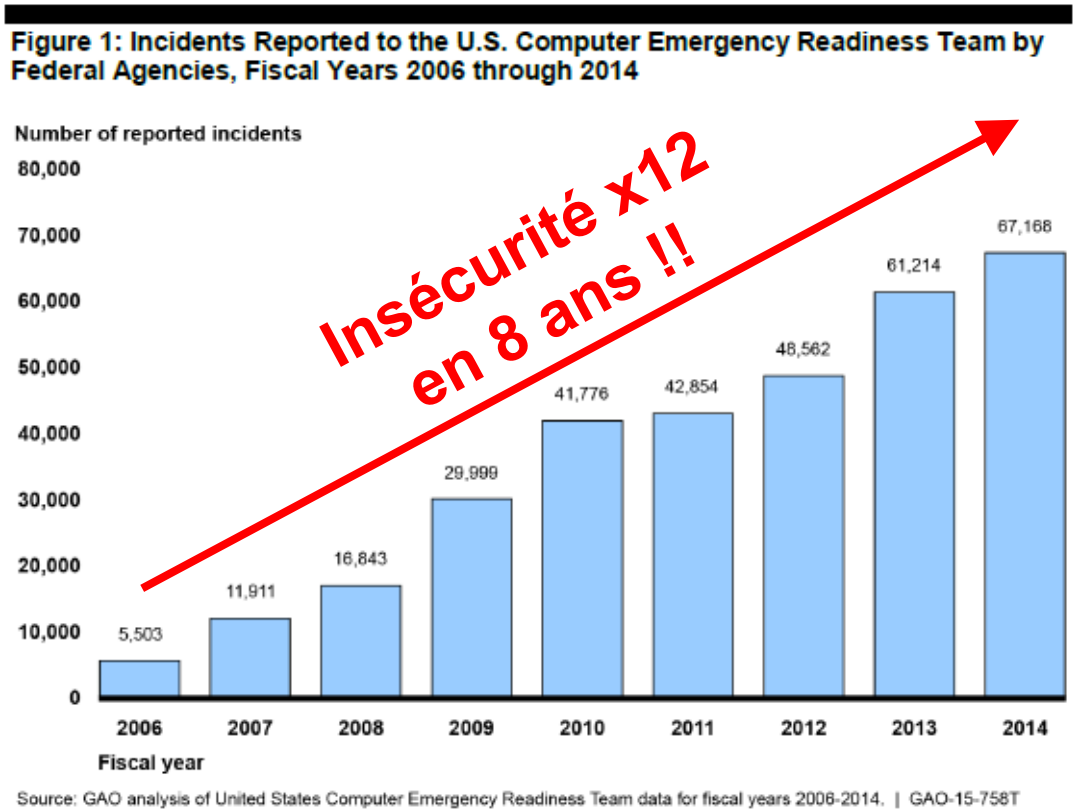
Un peu d'Histoire

- Cyberespace, l'âge adulte : 2004 – aujourd'hui



Un peu d'Histoire

- Cyberespace, l'âge adulte : 2004 – aujourd'hui



Source : [US Government Accountability Office]

Questions ?

http://bit.ly/355XPBp