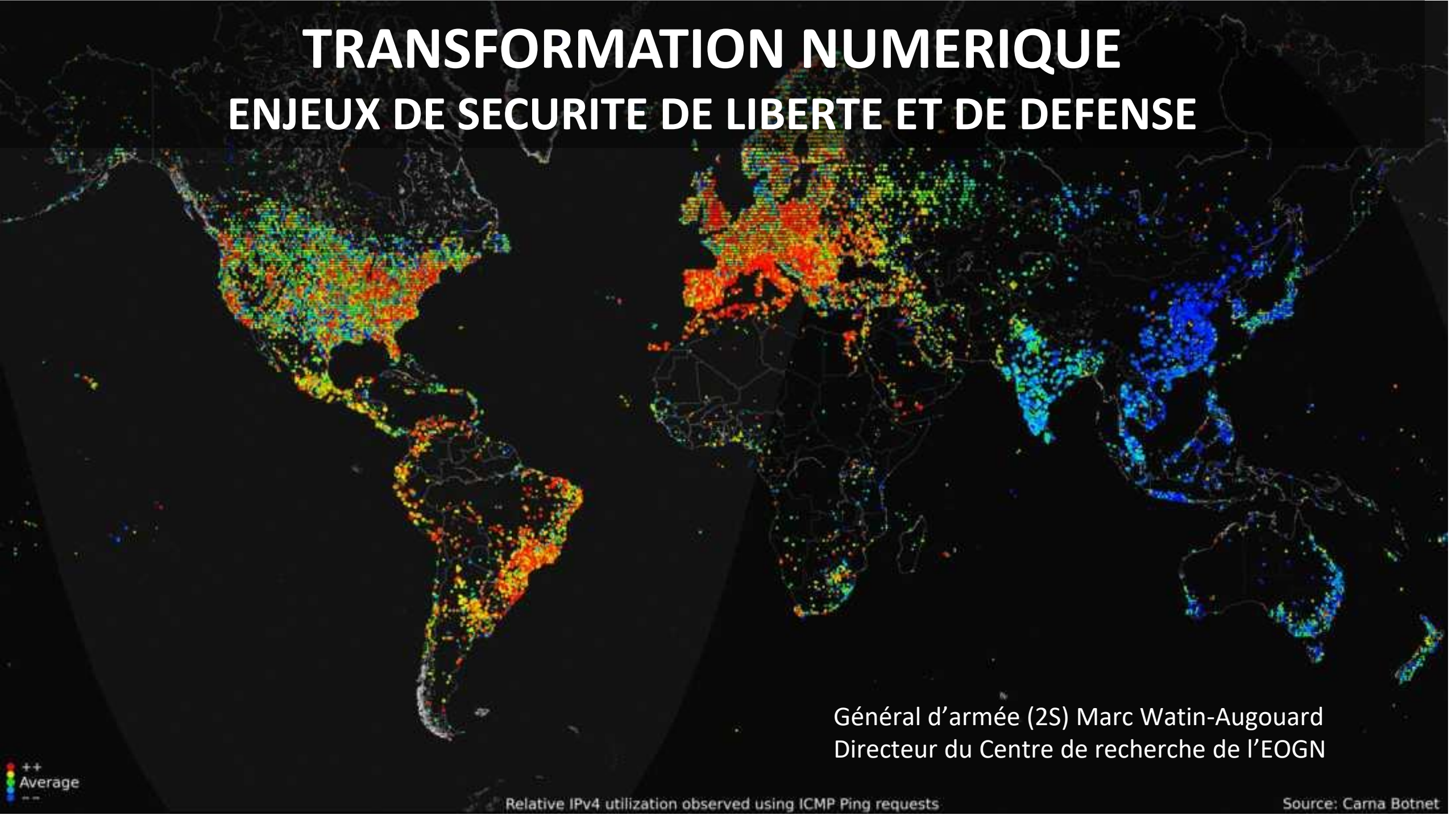


TRANSFORMATION NUMERIQUE

ENJEUX DE SECURITE DE LIBERTE ET DE DEFENSE



Général d'armée (2S) Marc Watin-Augouard
Directeur du Centre de recherche de l'EOGN

++
Average
--

Relative IPv4 utilization observed using ICMP Ping requests

Source: Carna Botnet



10^{ème} Forum International
de la **Cybersécurité**

FIC 2018

HYPERCONNECTION | THE RESILIENCE CHALLENGE



23 & 24 JANVIER 2018
LILLE GRAND PALAIS





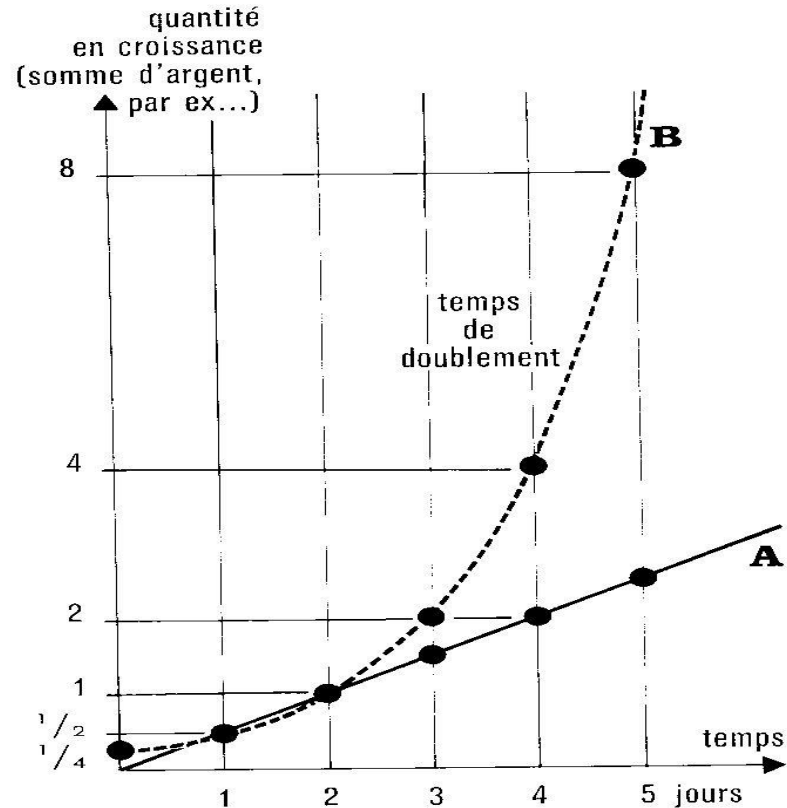
Sécurité et liberté



**Les
« libertaires »**

**Les
« sécuritaires »**

Le « non-perceptible »



**Comparaison des croissances
linéaire (A)
et exponentielle (B)**

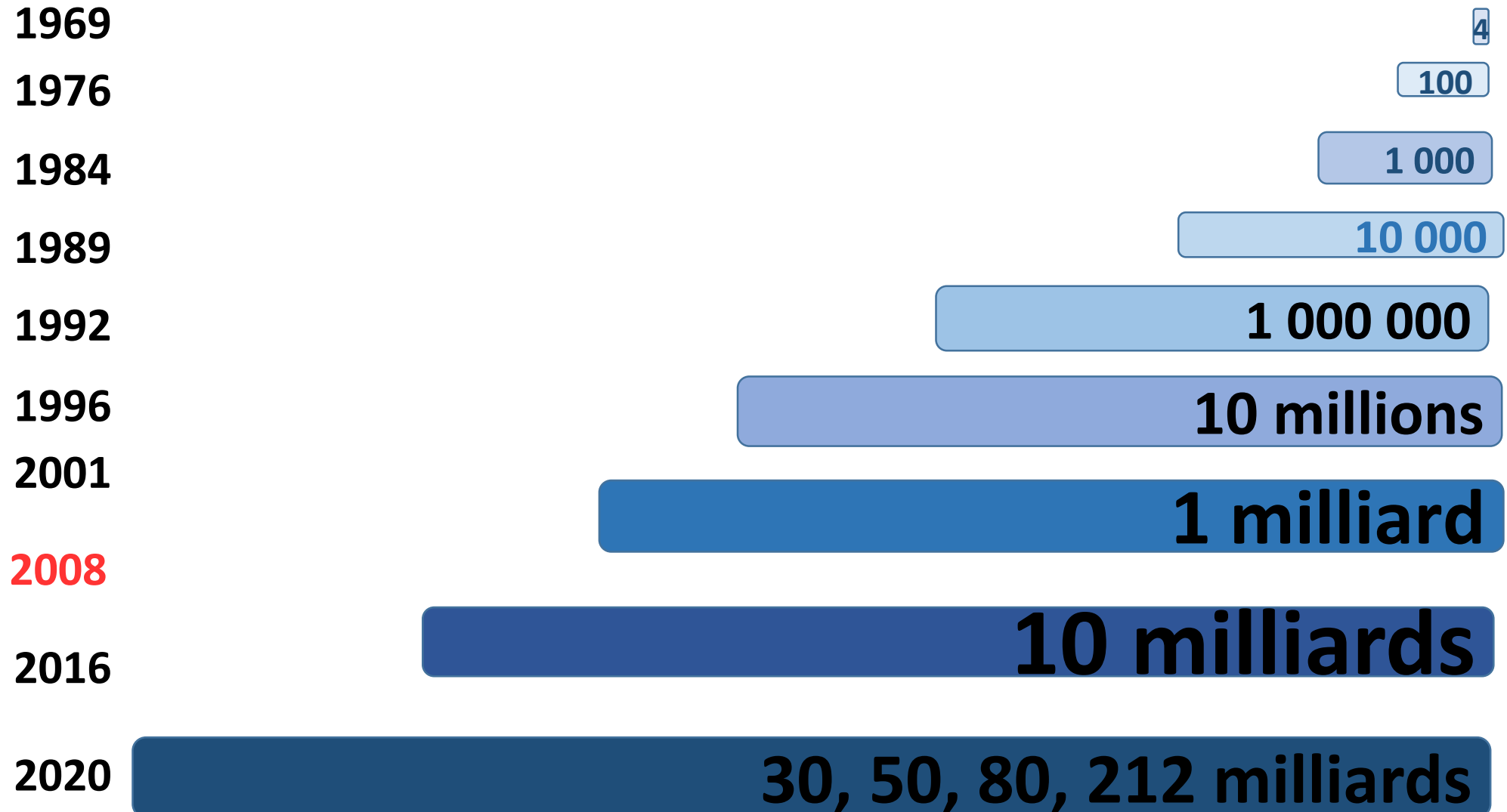
Infiniment rapide

Infiniment grand

Infiniment petit



L'infiniment rapide





Dynamique démographique du cyberspace

3,7
milliards
d'internautes
2017

4 milliards
d'internautes
2020
(1 milliard de
Chinois)

5
milliards
d'internautes
2025

Internaute francophone
2017: 3% 2050: 8%



L'infiniment grand

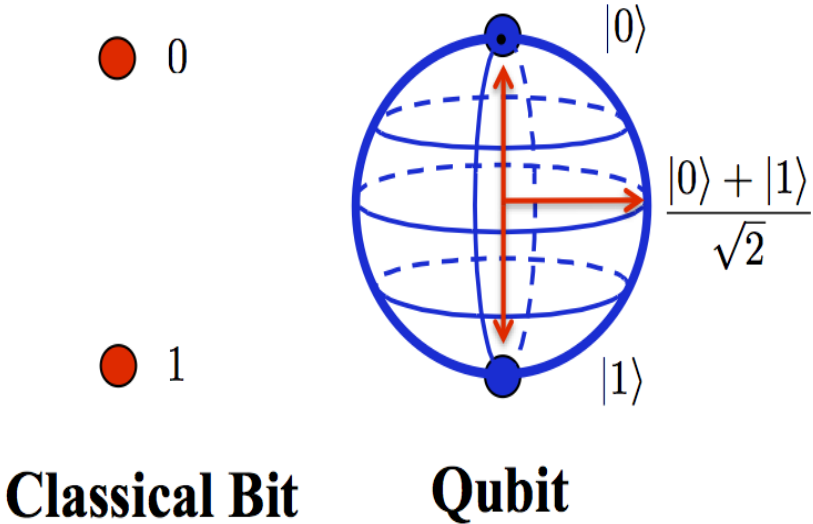
- **Des origines de l'humanité jusqu'à 2003 = 2 jours d'Internet**
- **Les pages Web = 200 000 fois l'Empire State Building**
- **Adresses IPV6 = 700 millions de milliards/mm²**
IPV4 xxx.xxx.xxx.xxx de 0 à 255 = 2³²
IPV6 XXXX :XXXX :XXXX :XXXX :XXXX :XXXX :XXXX :XXXX, hexadécimale
(de 0 à 9 et les lettres de a à f). On élargit ainsi à 2¹²⁸
- **Production annuelle de données : 8x10²¹ ➔ 10²⁴ en 2030**
Soit 1000 milliards de disques durs d'1 teraoctet
- **Capacité des machines x 1 000**
Capacité des algorithmes x 43 000 } **En 15 ans, vitesse globale de calcul x 43 millions**



L'infiniment petit

➔ **Taille des transistors : 1970 = 12 micromètres**
2013 = 12 nanomètres (12 milliardièmes)
Nota: taille de l'atome environ 5 nanomètres

➔ **Ordinateur quantique :**
10 000 ans en 1 seconde



➔ **Ordinateur biologique : ordinateur dans la cellule vivante (ADN)**



Les trois « couches » de l'espace numérique

- ➔ **Couche matérielle: *hardware, data centers*, câbles sous-marins**
- ➔ **Couche logique: logiciels, code, algorithmes, etc.**
- ➔ **Couche sémantique: le sens, les contenus, les données**



Les leviers de la transformation numérique

- **L'informatique dans les nuages (*le cloud computing*)**
- **Les méga-données (*le Big Data*), IA, analyse prédictive**
- **Les systèmes connectés: *domotique, immotique, smart grids, espaces, infrastructures intelligentes, transports intelligents, marétique, usine 4.0, etc.***
- **La réalité augmentée**
- **La robolution: droit des robots ou droit sur les robots? Droit de l'IA?**
- **La technologie Blockchain: dispositif d'enregistrement électronique partagé. *Vers la fin des tiers de confiance?***
- **L'impression « 3 D »**
- **NBIC (*Nano-Biotechnologies, Informatique, sciences Cognitives*)**

Smart cities/countries: une approche systémique





La donnée : matière première de la transformation numérique

Données à caractère personnel

- Loi du 6 janvier 1978
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27/04/2016
- Arrêt CJUE du 13/05/2016 : droit à l'oubli
- Arrêt CJUE du 6/10/2015 : fin du Safe Harbor ➔ Privacy Shield 12/07/2016

Données stratégiques pour l'Etat, l'entreprise

- Secret défense nationale
- « Secret des affaires »
- Propriété intellectuelle



Données à caractère personnel: un trésor à protéger



Règlement UE 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. RGPD ou *General Data Protection Regulation*.

Remplace la directive 95/46/CE du 24 octobre 1995. Entrée en vigueur le 25 mai 2018

173 « considérants », 99 articles...



Futur règlement « e-Privacy » (remplace la directive vie privée et communications électroniques 2002/58/CE)



Données à caractère personnel:

➔ **« toute information se rapportant à une *personne physique identifiée ou identifiable*; est réputée être une «personne physique identifiable» une personne physique *qui peut être identifiée, directement ou indirectement*, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (art.4 RGPD)**



Données à caractère personnel:

➔ **Art.4. Données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne**



Données à caractère personnel:

- ➔ **Art.9 Sensibilité de certaines catégories particulières de données à caractère personnel** qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé (déjà visées par l'article 4) ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.



Données à caractère personnel:

- ➔ **Entrent dans le champ du règlement**
- « les données à caractère personnel qui ont fait l'objet d'une *pseudonymisation* et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».**



Traitement de données

➔ « Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la **collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction** ».



Données à caractère personnel: 3 objectifs du RGPD



Le renforcement des droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;



La responsabilisation des acteurs, qu'ils soient responsables de traitement ou sous-traitants ;



L'amélioration de l'efficacité de la régulation, grâce à une coopération renforcée entre les autorités de protection des données (CEPD/G29).



Données à caractère personnel: Conformité *accountability*

- **Tenue d'un registre des traitements mis en œuvre (article 30) ;**
- **Notification de failles de sécurité aux autorités et aux personnes concernées (articles 33 et 34) ;**
- **Adhésion à des codes de conduites et la certification de traitements (articles 40 et 42) ;**
- **Désignation d'un délégué à la protection des données - DPO (articles 37 et suivants) ;**
- **Etudes d'impact sur la vie privée (EIVP).**



Données à caractère personnel: Conformité *accountability*



Privacy by design: garantie dès la conception d'une technologie du plus haut niveau de protection des données



Privacy by default: minimiser le traitement de données (pseudonymisation, mécanisme de purge, etc.)



Données à caractère personnel:

➔ **Traitement loyal et transparent:** *toute information et communication relatives au traitement des données à caractère personnel sont aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples » art.12*

➔ **Information de tout profilage:** *«évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements, dès lors qu'il produit des effets juridiques concernant la personne en question ou qu'il l'affecte de façon similaire de manière significative »*



Gouvernance et Internet

Gouvernance de l'Internet

Gouvernance sur Internet

**Echec de la conférence de Dubaï
6th World Conference on International
Telecommunications
(3 – 12 décembre 2012)**



Gouvernance et Internet

Groupe d'Experts Gouvernementaux
(Group of governmental experts –GGE)

25 Etats ONU

« Stabiliser le cyberspace »

- **Un constat: le droit international public s'applique au cyberspace**
Dont l'art.51 de la Charte des Nations Unies
- **Mission: évaluer la menace cyber – forger des normes comportementales**
- **Echec du GGE 2017: voir discours ONU de Jean-Yves LeDrian**
(72^e AG du 13/09/2017)



Le retour de l'Etat face aux prédateurs du cyber espace



Un espace de souveraineté interne et externe
Un espace de compétition
Un espace de confrontation, voire de conflictualité



Une stratégie de cybersécurité :



La lutte contre la cybercriminalité



La cyberdéfense



La cybercriminalité : de quoi parle-t-on ?

Cyber-infractions: apparaissent avec le cyberspace

- Traitement illégal de données à caractère personnel.
- Atteinte aux Systèmes de Traitement automatisés de données.
- Usurpation d'identité

➡ **Le cyberspace est la cible des cyberdélinquants.**

Infractions facilitées par le cyber: préexistent mais connaissent une autre ampleur

- Infractions de contenu.
- Escroqueries, chantage, abus de confiance.

➡ **Le cyberspace est le vecteur, l'amplificateur de la délinquance.**

Infractions complexe, « hybrides »: exemples du rançongiciel ou du Botnet





- ➡ **Rançongiciel = atteinte à un STAD (mod. Frauduleuse par chiffrement de données) + extorsion)**
- DDoS par Botnet = saturation par requêtes multiples et extorsion**

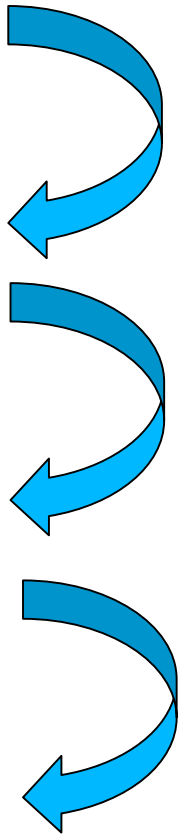
A glowing blue skull is centered on a computer monitor. The skull is rendered in a digital, wireframe style with bright blue highlights. A hand cursor, also glowing blue, is positioned over the skull's eye area. The background is dark, and the overall aesthetic is futuristic and digital.

Cybercriminalité, criminalité du XXIème siècle



La cybercriminalité, criminalité du XXIème Siècle

Secteur primaire	Agriculture	Meurtre, assassinat, viol, coups et blessures, Traite des êtres humains.	
Secteur secondaire	Industrie Artisanat	Vol, recel, dégradations.	
Secteur tertiaire	Services	Fraude, escroquerie, tromperie, abus de confiance, blanchiment.	
Secteur quaternaire	Numérique	Cybercriminalité.	





La transhumance du prédateur vers l'espace numérique

Le meilleur rapport « gain/risque pénal »

Jamais il n'a été aussi près de sa victime; jamais il n'a été aussi loin de son juge en agissant à distance

Le « chiffre noir »: on ne maîtrise pas la connaissance du phénomène



La donnée : cible des prédateurs

Extraction, « vol » de données », introduction, falsification – article 323-3 du code pénal (arrêt Cass.crim Bluetooft , loi du 13/11/2014)

« Rançongiciels » : articles 323-2 et 312-1 du code pénal **Wannacry, NotPetya**



La donnée : cible des prédateurs Wannacry 12 mai 2017

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! French



Qu'est-ce qui s'est passé avec mon ordinateur?

Vos fichiers importants sont chiffrés. Beaucoup de vos documents, photos, vidéos, bases de données et autres fichiers ne sont plus accessibles car ils ont été chiffrés. Peut-être que vous êtes occupé à chercher un moyen de récupérer vos fichiers, mais ne perdez pas votre temps. Personne ne peut récupérer vos fichiers sans notre service de décryptage.

Puis-je récupérer mes fichiers?

Sûr. Nous vous garantissons que vous pouvez récupérer tous vos fichiers en toute sécurité et facilement. Mais vous n'avez pas assez de temps. Vous pouvez décrypter certains de vos fichiers gratuitement. Essayez maintenant en cliquant sur <Decrypt>. Mais si vous souhaitez décrypter tous vos fichiers, vous devez payer. Vous n'avez que 3 jours pour soumettre le paiement. Ensuite, le prix sera doublé. En outre, si vous ne payez pas dans 7 jours, vous ne pourrez pas récupérer vos fichiers pour toujours. Nous aurons des événements gratuits pour les utilisateurs qui sont si pauvres qu'ils ne pouvaient pas payer en 6 mois.

Comment je paye?

Le paiement est accepté uniquement dans Bitcoin. Pour plus d'informations, cliquez sur <About bitcoin>. Veuillez vérifier le prix actuel de Bitcoin et acheter des bitcoins. Pour plus

Payment will be raised on
5/15/2017 20:57:50
Time Left
02:23:57:50

Your files will be lost on
5/19/2017 20:57:50
Time Left
06:23:57:50

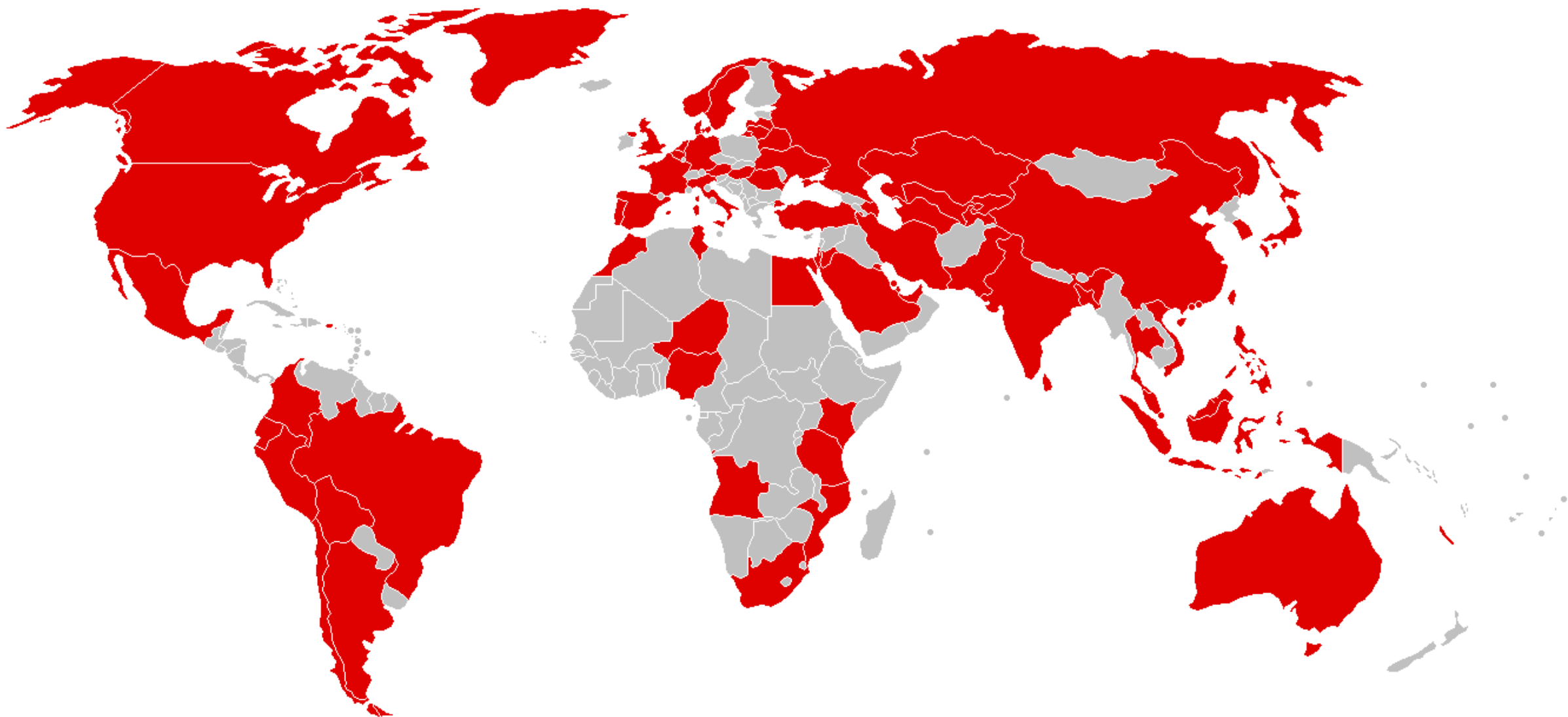
[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **Send \$300 worth of bitcoin to this address:**



La donnée : cible des prédateurs

Wannacry 12 mai 2017





Un corpus « Mille feuilles »

- Loi relative à l'informatique, aux fichiers et aux libertés (1978)
- Loi Godfrain (1988)
- Loi relative à la sécurité quotidienne (2001)
- LOPSI (2002),
- Loi pour la sécurité intérieure (2003)
- Loi Perben II (2004)
- Loi pour la confiance dans l'identité numérique (2004)
- Loi relative à la prévention de la délinquance (2007)



Un corpus « Mille feuilles »

- **LOPPSI (2011)**
- **Loi relative à la protection de l'identité (2012)**
- **Loi sur l'égalité réelle entre la femme et l'homme (2014)**
- **Loi renforçant la lutte contre le terrorisme (13 novembre 2014)**
- **Loi sur le renseignement (24 juillet 2015)**
- **Loi relative aux mesures de surveillance des communications électroniques internationales (30 novembre 2015)**



Un corpus « Mille feuilles »

- Loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme
- Loi du 7 octobre 2016 « pour une République numérique »
- Lois sur l'état d'urgence des 20 novembre 2015 et 21 juillet 2016
- Loi relative à la sécurité publique (28 février 2017)
- (Projet de) Loi renforçant la sécurité intérieure et la lutte contre le terrorisme (oct 2017?)



Les infractions « cyber »

Les infractions à la loi informatique et liberté

Les atteintes aux systèmes de traitement automatisé de données

L'usurpation d'identité sur internet



Loi Informatique et libertés (code pénal)

Article 226-16

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet d'une des mesures prévues au 2° du I de l'article 45 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article 226-17-1

Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34bis de la loi n°78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-18

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende.



Les infractions « cyber »

Les infractions à la loi informatique et liberté

Les atteintes aux systèmes de traitement automatisé de données

L'usurpation d'identité sur internet



Loi Godfrain

Accès ou le maintien frauduleux dans un STAD (323-1CP)

3ans d'emprisonnement

Violation de la volonté du « maître du système »

Aggravation si suppression ou modification de données contenues dans le système, soit une altération du fonctionnement de ce système. Cette atteinte aux données ou au fonctionnement est dans ce cas involontaire et résulte, par exemple, d'une manœuvre accidentelle.

Entrave au fonctionnement d'un STAD (323-2 CP)

5 ans d'emprisonnement

Malware, « bombe logique », attaque par déni de service (Distributed Denial of Service DDoS) par un botnet qui met en action plusieurs milliers d'ordinateurs « zombies », chiffrement malveillant.

Atteinte aux données (323-3 CP)

5 ans d'emprisonnement

Introduction, suppression, reproduction, extraction ou modification frauduleuse de données dans les STAD.



Pénétration frauduleuse: les « Menaces persistantes avancées »

Connus sous l'acronyme APT ("*Advanced Persistent Threat* ")

Attaque pouvant durer plusieurs mois (entrée dans réseau TV5 Monde 2 mois avant). Utilisation fréquente de l'ingénierie sociale pour accéder au réseau. Cible choisie de manière délibérée et non par « opportunité ».

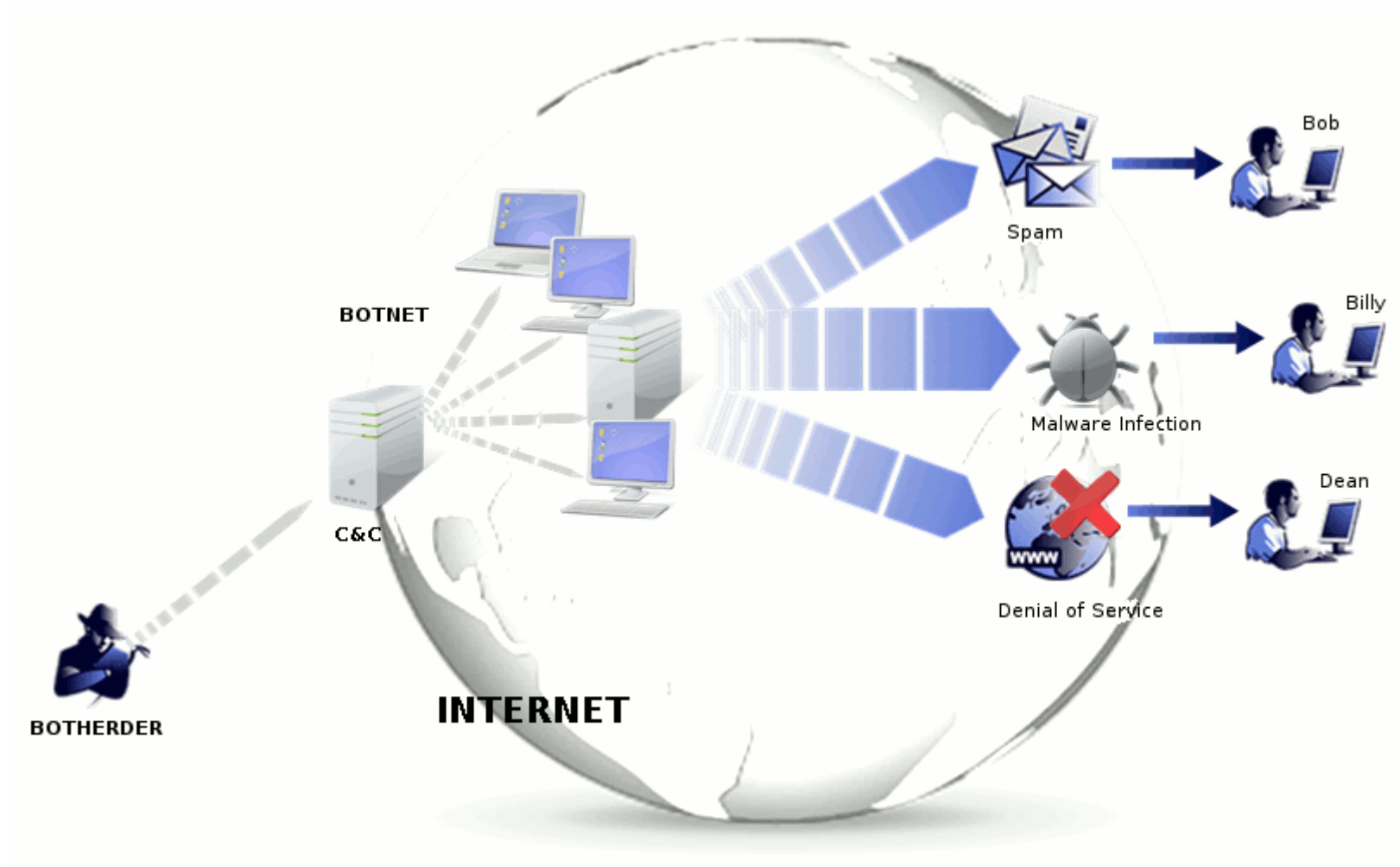
Persistante: l'attaquant va essayer de manière répétée d'atteindre son objectif en restant « sous les radars ».

Avancée: vulnérabilités non encore connues/corrigées (« *zero day* »), compromission de plusieurs technologies.

Exemples: Elysée et Bercy (2008), Stuxnet



Les Botnets





La détection en amont des cyberattaques

***Threat intelligence:* étude du contexte, des mécanismes et élaboration d'indicateurs pour agir en amont d'une cyberattaque**

Cybersécurité cognitive: *Watson for cybersecurity:* interprétation de données non structurées pour repérer les activités cybermalveillantes



Loi Godfrain et « hacker éthique »

Le contrat de *bug bounty*

- Délimite clairement dans le temps et dans l'espace le périmètre des investigations sur l'infrastructure, les sites ou les logiciels permises au *pentester*.
- Exclut toute altération du système, toute destruction de données. Les contraintes sont d'autant plus fortes que des données à caractère personnel sont en jeu.
- Obligation de confidentialité.
- Une obligation de moyens mais pas de résultat.
- Généralement, la découverte d'une faille est rémunérée selon son importance. Le montant de sa rémunération est d'autant plus élevé que la faille découverte est critique et assortie de recommandations (*Proof of Concept*).



Loi Godfrain « contournée »

STAD et article 40 du CPP (Art. L 2324-1 code de la défense)

« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ».



Les infractions « cyber »

Les infractions à la loi informatique et liberté

Les atteintes aux systèmes de traitement automatique de données

L'usurpation d'identité sur internet



Usurpation d'identité sur internet

L'usurpation d'identité « numérique » (article 226-4-1 al. 2 du code pénal), est commise sur un réseau de communication au public en ligne: courriers électroniques, sites web, messages publiés en ligne, profils en ligne sur les réseaux sociaux (Facebook, Twitter, etc.)

deux formes d'usurpation d'identité selon le mobile.

* **l'usurpateur souhaite nuire à la réputation de la personne:** faux profil sur les réseaux sociaux, blog, ou commentaires sous l'identité de sa victime.

* **l'usurpateur** envoie à sa victime un message en se faisant passer pour un organisme public ou privé connu, et **recupère à partir d'un faux site des informations personnelles.**

- - accéder à des comptes sécurisés et effectuer des opérations sous l'identité de la victime.
- - pirater des comptes de messagerie électronique ou des comptes RS de particuliers et les utiliser comme support pour des arnaques.



Les infractions de contenus

- - Délits réprimés par la loi du 29 juillet 1881 et « commis par tout moyen de communication au public par voie électronique ».
- - Atteinte à la dignité ou à la personnalité.
- - Atteinte à la réputation.
- - Contenus à caractère terroriste (dont consultation habituelle).
- - Contenus à caractère pédophile (dont consultation habituelle).

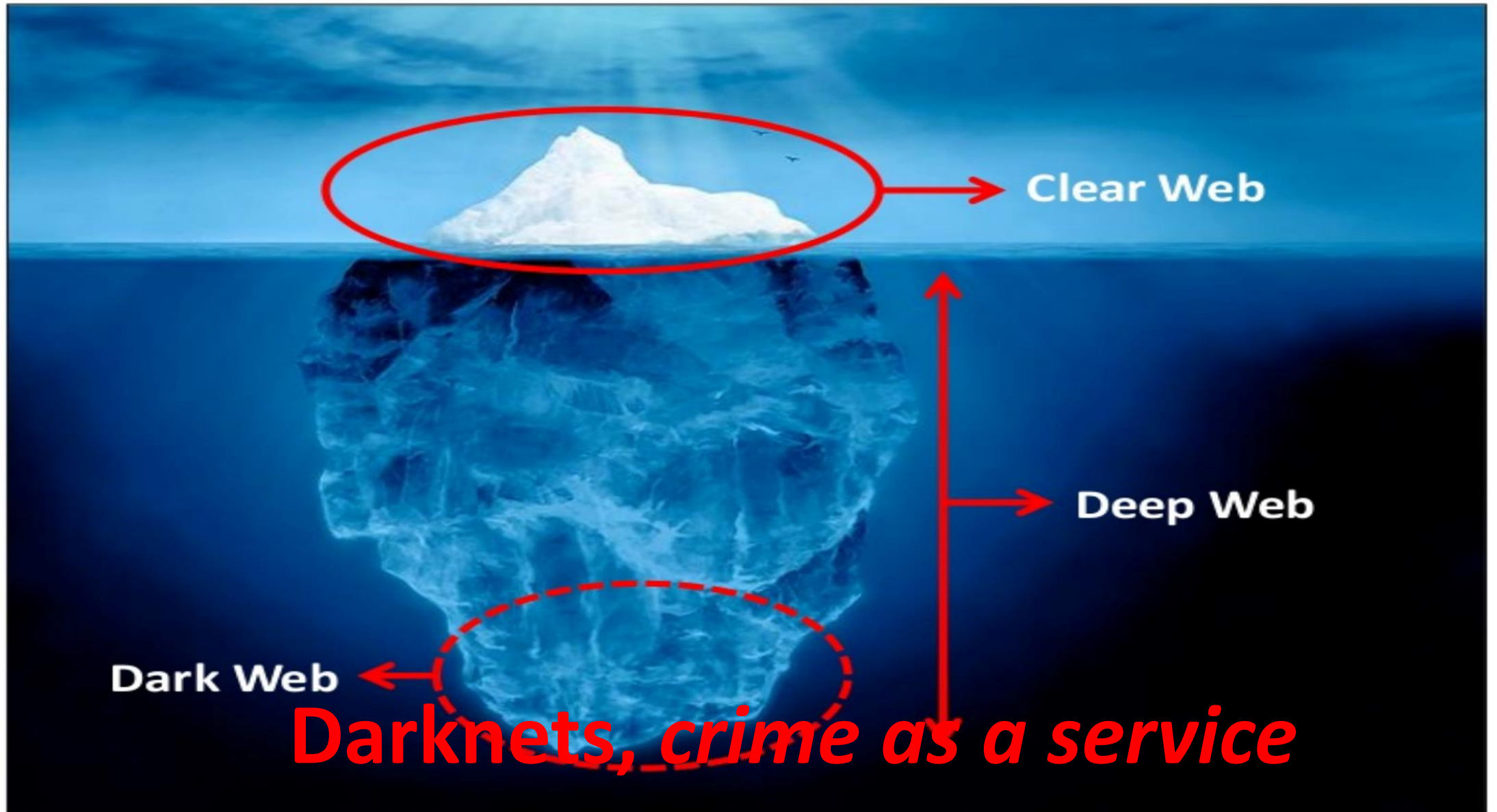


Infractions facilitées par internet

- **Les atteintes à la confiance**
- **Le chantage, l'extorsion.**
- **Les trafics de produits contrefaits.**



web surfacique/web profond





Cybermenaces sur les entreprises

- **Déni de service(DDoS).**
- **« Vol » modification de données (propriété intellectuelle, avantage compétitif).**
- **Sabotage (SCADAS).**
- **Attaque en rebonds.**
- **Atteinte à l'e-réputation (réseaux sociaux).**
- **Escroqueries, fraudes etc.**



Cybermenaces sur les entreprises

- **Quels sont les principaux actifs « critiques » (physiques, incorporels, espaces virtuels) à protéger ?**
- **Comment sont protégés les principaux actifs ?**
- **Quel est le niveau de risque acceptable en matière d'exposition au risque de cybercriminalité ?**
- **Quels contrôles sont en place pour surveiller les espaces réseaux (y compris cloud) et ceux des fournisseurs, ainsi que les installations sur les appareils de la société comme les appareils mobiles**
- **Qui est responsable de leur protection ?**
- **L'organisation compte-t-elle dans ses rangs du personnel formé et expérimenté en matière de prévention des cyber-risques ?**
- **Les ressources allouées à la cybersécurité (budget, RH) sont elles suffisantes ?**
- **Comment l'organisation réagirait-elle face à un incident majeur ? (COMEX, DSI, RSSI)**



La lutte contre la cybercriminalité



Les acteurs publics



Du préfet Cyber vers la délégation ministérielle aux industries de et de lutte contre les cybermenaces (décret du 25 janvier 2017).



La gendarmerie nationale.



La police nationale.



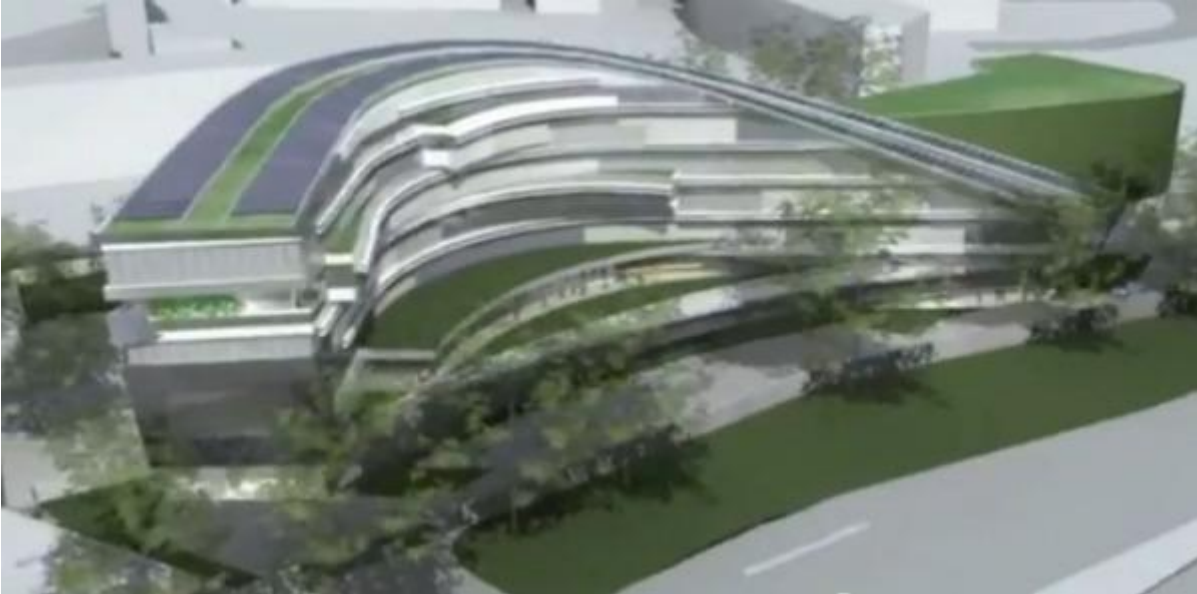
La cyber-douane.



La Direction générale de la concurrence, de la consommation et de la répression des fraudes – DGCCRF.



La lutte contre la cybercriminalité



Interpol : *Interpol global complex for innovation* – IGCI – Singapour

3 Axes

- Sécurité numérique.
- Renforcement des capacités de formation.
- Appui opérationnel et soutien aux enquêtes.

5 domaines

- Renforcement de la cybersécurité et lutte contre la cybercriminalité.
- Développement de la PTS en lien avec le numérique.
- Recherche sur les cyberattaques.
- Partenariat public/privé.
- Gouvernance de la sécurité d'Internet.



La lutte contre la cybercriminalité



3 Priorités

- Fraude en ligne par des organisations criminelles.
- Exploitation sexuelle des mineurs sur Internet.
- Attaques contre les infrastructures critiques et les SI de l'UE.

3 Focal Points

- Cyborg : enquête sur la cybercriminalité.
- Twins : abus de l'enfance en ligne.
- Terminal : fraude à la carte bancaire.



La lutte contre la cybercriminalité



Coopération transfrontalière contre la cybercriminalité

Animation du réseau des équipes communes d'enquête



De la cybercriminalité à la cyberconflictualité

- **2007 : Estonie**
- **2008 : Géorgie**
- **2006 – 2010 : Stuxnet**
- **2012 : Aramco**
- **2013 : Target**
- **2014 : Aciérie RFA - Sony**
- **2015 : TV5 Monde**
- **2016 : Botnet *Mirai***
- **2017 : Wannacry, Notpetya**

etc. etc. etc. etc. etc. etc. etc. etc. etc. etc. etc.



Les textes fondateurs de la cyberdéfense

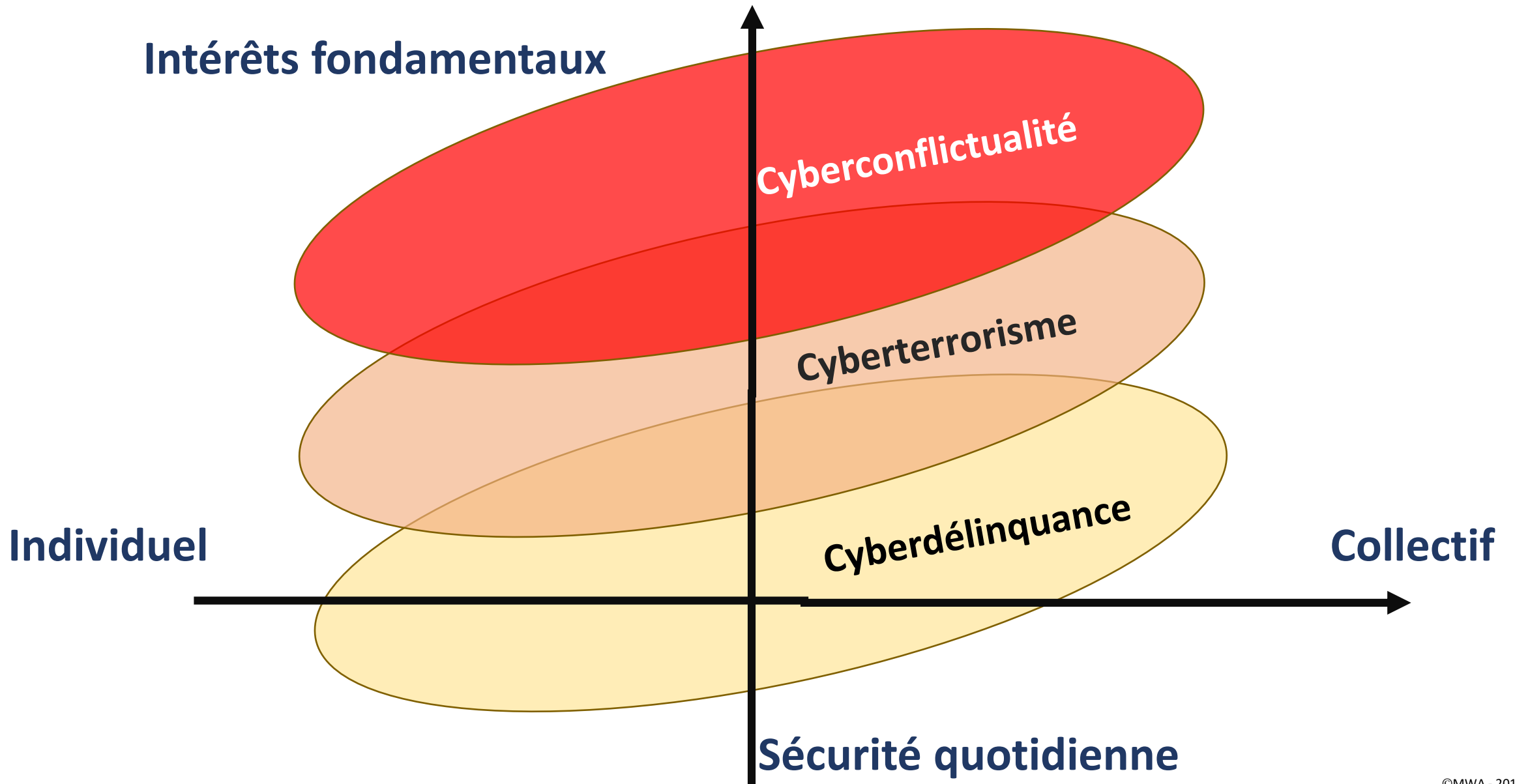
- **Livre blanc sur la défense et la sécurité nationale** **2008**
- **Stratégie de la France en matière de défense et de sécurité des systèmes d'information** **2011**
- **Rapport d'information du sénateur Bockel** **2012**
- **Livre blanc sur la défense et la sécurité nationale** **2013**
- **Loi de programmation militaire du 18 décembre** **2013**
- **Stratégie nationale pour la sécurité du numérique** **2015**
- **Décret du 5 mai sur le commandement cyberdéfense** **2017**

Cyberguerre: le mythe et la réalité





De la cyberdélinquance à la cyberconflictualité





Les caractéristiques du continuum

Un territoire unifié

- Ce n'est pas un champ de bataille.
- Ce n'est pas une Zone de Sécurité Prioritaire.

Des méthodes similaires

- Attaque par Ddos.
 - Crapuleuse.
 - Terroriste.
 - « Etatique ».
- Défacement.
 - e-réputation.
 - Provocation et apologie.
 - Subversion.

Un marché commun : les *darknets*

Un « prêt de main forte »

- Action par « tiers attaquant ».
 - Crime organisé, mafia.
 - Groupe paramilitaire.

Un « brouillage des pistes »

- Attribution « *c'est pas moi, c'est ma sœur...* »
- Pourquoi ?



Les exigences du continuum

Une réponse maillée



Pompier

« Soldat »



« Gendarme »

Diplomate





Les exigences du continuum

- **Une coopération public/privé renforcée – Rôle particulier des assurances**
- **Une stratégie Ressources Humaines**
 - Formation
 - Recrutement, gestion des carrières
- **Une Recherche/ Développement centrée sur les sciences forensiques**
 - Preuves
 - Attributions
- **Le partage du renseignement : le RIC et le ROC**



Les cyberattaques en temps réel



map.ipvicking.com

NORSE

ATTACK ORIGINS

#	COUNTRY
170	China
80	United States
41	Bulgaria
37	Russia
36	Mil/Gov
36	France
17	Taiwan
16	Turkey
16	Hong Kong
14	Netherlands

ATTACK TARGETS

#	COUNTRY
382	United States
109	Mil/Gov
39	Philippines
15	Russia
14	Saudi Arabia
11	Cyprus
8	Taiwan
6	France
5	Liechtenstein
2	Hong Kong

LIVE ATTACKS

TIMESTAMP	ATTACKER	LOCATION	IP	TARGET	TYPE	PORT
2015-06-01 12:53:52.00	TELEFÔNICA BRASIL S.A	Ribeirão Preto, Brazil	187.35.70.102	unknown, Philippines	ms-wbt-	3389
2015-06-01 12:53:52.24	ChinaNet Guangdong	Guangzhou, China	14.23.154.202	unknown, Mil/Gov	ms-wbt-	3389
2015-06-01 12:53:52.95	City Telecom (H.K.) Ltd.	Central District, Hong	59.148.126.71	Seattle, United States	telnet	23
2015-06-01 12:53:52.97	Chinanet Jiangsu Province	Changzhou, China	61.160.224.128	Seattle, United States	http	80
2015-06-01 12:53:52.99	Sweden Networks	unknown, Sweden	46.29.248.181	Kirkville, United	http-alt	8080
2015-06-01 12:53:53.98	Philippine Long Distance	Philippine, Philippines	49.148.173.106	Kirkville, United	telnet	23
2015-06-01 12:53:54.01	FortressITX	Clifton, United States	65.98.108.226	Dallas, United States	ntp	123
2015-06-01 12:53:54.23	LLC INTK	unknown, Russia	37.18.51.154	Seattle, United States	https	443

ATTACK TYPES

#	SERVICE	PORT
70	telnet	23
38	csd-mgmt-port	3071
33	microsoft-ds	445
29	ntp	123
29	unknown	27017
25	mysql	3306
24	http-alt	8080
23	ms-wbt-server	3389



Vers la déconnexion ?

La marétique
L'informatique et la mer



La marétique L'informatique et la mer



« Ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'utilisation des opérations relatives aux activités maritimes, fluviales et portuaires.

Livre Bleu cluster Marétique 2012



La marétique

Projet de « cloud maritime »

Projet porté par l'Organisation Marine Internationale (OMI)



« Une infrastructure de communication assurant le transfert autorisé sans frontière à bord des navires, entre les navires, entre les navires et la terre et entre les autorités à terre »



La marétique

L'informatique et la mer



- * **Navires**
- * **Ports**
- * **Systemes de navigation et de communication**
- * **Outils de gestion et de contrôle du trafic maritime et des cargaisons**



- * **Marine militaire**
- * **Marine marchande**
- * **Marine de plaisance**
- * **Marine de pêche**
- * **Marine scientifique**
- * **Installations off shore (plateformes, villes, etc.)**



Les menaces sur les navires



α Navigation électronique obligatoire avec la convention SOLAS (sauvegarde de la vie en mer): système ECDIS (visualisation des cartes électronique et d'information/

*radars

*AIS (Automatic Identification System), système facilement contrefait (projet ANR DéAIS)



α Systèmes de contrôle industriels: propulsion, manœuvre, énergie, surveillance du fret, alarmes incendies, voies d'eau, etc.

Tous systèmes reliés dans la « passerelle intégrée »



Les menaces sur les navires

- ➔ **▣ systèmes connectés aux réseaux de communication qui relient le navire à la terre**
- ➔ **▣ systèmes servant aux communications professionnelles, aux échanges privés de l'équipage, des passagers, voire de conteneurs connectés par Wifi du bord**
- ➔ **▣ systèmes servant aux communications professionnelles, aux échanges privés de l'équipage, des passagers, voire de conteneurs connectés par Wifi du bord**
- ➔ **Augmentation de la surface d'attaque (connexion satellitaire, clef USB, voiture connectée, etc.)**

Norme IEC 61162-460 (2018) pare-feu entre le navire et l'extérieur



Les menaces sur les ports



α numérisation des procédures et des services portuaires pour automatiser et fluidifier les échanges. Interconnexion croissante des systèmes d'information portuaire et partage des bases de données



α concept de « smart port »

-Fluidifier les contrôles de police et de douanes

-Coordonner les mouvements des navires, des passagers, du fret

-Coordonner les moyens de manutention, de transport terrestre

-Disponibilité des services portuaires (pilotage, avitaillement, etc)

-Disponibilité des quais et des aires de stockage, etc.



Exemples d'actions



⌘ agir sur un navire en pleine mer:

déni de service sur les systèmes de positionnement, sur les systèmes d'aide à la navigation



⌘ agir sur la manœuvre dans des eaux resserrées:

Prise de contrôle ou dérèglement des équipements de conduite



⌘ agir sur les systèmes de sécurité maritime

Modifier les informations de sécurité à destination des navires (SMDSM, Météo, SAR, MSI service, e-navigation, futur Maritime cloud.



⌘ agir sur la sécurité du port



N'ayons pas peur!

1/ Confiance

2/ Loyauté

3/ Solidarité

4/ Responsabilité