FRC 2017
10ème édition

LA GENDARMERIE D'ALSACE
& LES OFFICIERS DE LA RÉSERVE CITOYENNE

AD HONORES
Réseau ALSACE

10ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

2008 - 2017 : L'ODYSSÉE DU CYBER

www.frc.alsace

@cybermenaces

10ème FORUM DU RHIN SUPERIEUR DU LES CYBERMENACES

10e FRC 2017
Animation

M. Gilbert GOZLAN

Directeur de la Sûreté - la Poste Nord & Est
Président de l'association AD Honores Réseau Alsace
Lieutenant-Colonel (RC) de la gendarmerie nationale

FRC 2017
Discours d'ouverture

M. P. GÉRARD

Directeur de l'Ecole Nationale d'Administration

10e FRC 2017
Discours d'ouverture

Général Stéphane OTTAVI

Commandant Adjoint de la région de gendarmerie Grand Est,
Commandant le groupement de gendarmerie départementale du Bas-Rhin

10e FRC 2017
Discours d'ouverture

M. Jean-Luc HEIMBURGER

Président de la CCI Alsace Eurométropole

10e FRC 2017
Discours d'ouverture

M. François SCHRICKE

Adjoint au secrétaire général
pour les affaires régionales et européennes
auprès du préfet de la région Grand Est

10e FRC 2017 - PROGRAMME

Salle de conférence de l'ENA FRC 2017

13h00 — ACCUEIL DES PARTICIPANTS

13h30 — DISCOURS D'OUVERTURE

Général Stéphane OTTAVI
Commandant adjoint de la région de gendarmerie Grand Est.
Commandant le groupement de gendarmerie départementale du Bas-Rhin.

Monsieur Jean-Luc HEIMBURGER
Président de la CCI Alsace Eurométropole.

Monsieur François SCHRICKE
Adjoint au secrétaire général pour les affaires régionales et européennes auprès du préfet de la région Grand Est.

■ Animation
Monsieur Gilbert GOZLAN
Directeur de la Sûreté - la Poste Nord & Est.
Président de l'association AD HONORES Réseau Alsace.
Lieutenant-Colonel (RC) de la gendarmerie nationale.

14h00 — CONFERENCE PLENIÈRE

INTERNET : DE LA RECHERCHE A BIG BROTHER

Monsieur Louis POUZIN
Président Open-Root.
Inventeur du datagramme et concepteur du réseau à commutation de paquets.
Queen Elizabeth Prize for Engineering - 2013.

14h30 — TABLE RONDE #1

LA CYBERSECURITE OPERATIONNELLE

Monsieur Michel ROCHELET
Délégué ANSSI Région Grand-Est.

Monsieur Fabrice STALTER
Responsable Sécurité des Systèmes d'Information aux Hôpitaux Universitaires de Strasbourg.
Chargé d'enseignement à l'université de Strasbourg et à l'université d'Angers.

Monsieur Jean-Marc MISERT
Service PGCS – La Banque Postale.
Président du Clusir-Est.

Messieurs Kevin BROU BONI et Axel RIBON
Etudiants à l'Ecole Nationale Supérieur d'Ingénieurs Sud Alsace, université de Haute Alsace.

15h40 — PAUSE / DÉTENTE

10e FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

16h20 — TABLE RONDE #2

LES ATTEINTES A LA REPUTATION

Colonel Nicolas DUVINAGE
Chef du Centre de lutte Contre les Criminalités Numériques de la gendarmerie nationale (C3N) - Pôle Judiciaire de la Gendarmerie Nationale (PJGN).

Monsieur Daniel GUINIER
Expert en cybercriminalité et crimes financiers près la Cour pénale internationale de la Haye.
Colonel (RC) de la gendarmerie nationale.

Monsieur Ludovic HAYE
Maire de Richeim, Délégué régional ANAJHEDN Alsace.
Chef d'escadron (RC) de la gendarmerie nationale.

Lieutenant-Colonel Gilles LE GAL
Officier professeur au Centre d'Enseignement Supérieur de la Gendarmerie (CESG) de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN).

17h20 — CONFERENCE DE CLÔTURE

Général d'armée (2S) Marc WATIN-AUGOUARD
Ancien inspecteur des armées-gendarmerie,
Directeur du Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN).

18h30 — COCKTAIL

2008 2017
L'ODYSSÉE DU CYBERESPACE

www.frc.alsace
@cybermenaces

10e FRC 2017 - NOS SPONSORS

l'ena
ÉCOLE NATIONALE D'ADMINISTRATION

FRC 2017 - NOS SPONSORS

CCI ALSACE EUROMÉTROPOLE

FRC 2017 - NOS SPONSORS

FRC 2017 - NOS SPONSORS

Atheo

INGENIERIE | HUMAN INSIDE

10e FRC 2017 - NOS SPONSORS

AXA

Julien ROHFRITSCH

Agent Général

10e FRC 2017 - NOS SPONSORS

BANQUE POPULAIRE

BANQUE POPULAIRE
ALSACE LORRAINE CHAMPAGNE

ADDITIONNER LES FORCES, **MULTIPLIER LES CHANCES**

BANQUE POPULAIRE

FRC 2017 - NOS SPONSORS

CLUSIR EST

10e FRC 2017 - NOS SPONSORS

CRCC

COMPAGNIE
REGIONALE DES
COMMISSAIRES AUX
COMPTES

COLMAR

Partenaire de la marque Alsace

FRC 2017 - NOS SPONSORS

KASPERSKY lab

FRC 2017 - NOS SPONSORS

LCR

LES CONSTRUCTEURS REUNIS

10 FRC 2017 - NOS SPONSORS

SOCIETE GENERALE

10e FRC 2017


BAC PRO METIERS DE LA SECURITE
SECURITE
BPMS
68
LYCEE CHARLES DE GAULLE

10e FRC 2017

Notre objectif

Connaitre et partager les enjeux
Adopter et faire adopter les bons comportements
et les bonnes actions à mettre en œuvre

10e FRC 2017

Conférence plénière

Internet : de la recherche à Big Brother

M. Louis POUZIN

Président Open-Root
Inventeur du datagramme et concepteur du réseau à commutation de paquets
Queen Elizabeth Prize for Engineering – 2013

10e FRC 2017

Conférence plénière

Internet : de la recherche à Big Brother

Quels moyens de souverainetés numériques ?

10 FRC 2017


X-25
CYCLADES
COST 11
TELENET
EPSS
ARPANET
TYMNET
SITA
CIRCUITO

EN TRÈS BREF

1969 – CTNE réseau dédié interbanques espagnol

1971 – ARPANET USA recherche

1971 – SITA FR réservation internationale de places d'avion

1971 – TYMNET USA 1er réseau international d'accès à serveurs

1973 – **CYCLADES** FR premier réseau de **datagrammes**

1975 – EPSS UK prototype de réseau public (abandonné)

1975 – TELENET USA concurrent de TYMNET

1976 – UIT X25 standard mode paquet: **TRANSPAC** (obsolète)

1983 – INTERNET USA TCP IPv4

1988 – **TOILE** WEB, **CERN**

SERVEURS DE DONNÉES

- SOUVENT AU NIVEAU BETA
- FORMATS & PROTOCOLES PROPRIÉTAIRES
- INTEROPÉRABILITÉ RESTREINTE
- NON RESPONSABLE
- SÉCURITÉ INCERTAINE
- UTILISATION INCONTRÔLÉE DES DONNÉES PERSONNELLES
- FONT PEU DE CAS DES LOIS NATIONALES

10e FRC 2017

Conférence plénière

Internet : de la recherche à Big Brother

INTERNET GÉOPOLITIQUES

MULTINATIONALES / LOBBIES

- PLUS PUISSANTS QUE LES ÉTATS
- ÉCRIVENT LES LOIS & ACHÈTENT LES VOTES DES POLITICIENS
- RESSOURCES IMPOSANTES POUR PROPAGANDE CONTINUE & PROCÈS COÛTEUX
- TENTENT CONSTAMMENT DE LÉGALISER LEURS INTÉRÊTS
- AMENDES INFÉRIEURES À $100 M SONT INEFFICACES (RGPD?)

LAISSER - FAIRE

- SOLUTIONS PROPRIÉTAIRES
  - SYSTÈMES FERMÉS
  - NOMMAGE HÉTÉROGÈNE
  - SECURITÉ DOUTEUSE
- MARCHÉS CAPTIFS
- ARCHITECTURE OBSOLÈTE
- DÉPENDANCE DES USA

SURVEILLANCE MASSIVE

- DÉJA EXPLOITÉ PAR NOMBREUX (50 ~ 60) ÉTATS
  AUTORITAIRES OU DÉMOCRATIQUES

- À SUPPOSÉ POUR
  IP PROPRIÉTÉ INTELLECTUELLE
  PROTECTION DES ENFANTS
  SÉCURITÉ NATIONALE
  CYBERCRIME
  ORDRE SOCIAL
  RELIGION Etc..

- INTELLIGENCE (ESPIONNAGE) ÉCONOMIQUE

- CONTRÔLE POLITIQUE

- etc.

LASSITUDE DE L'UNILATÉRALISME US

- LES GOUVERNEMENTS NE SONT PLUS IGNORANTS
- EXPERTISE LOCALE DISPONIBLE
- LES USA RESTENT DOMINANTS
- AUTRES ÉTATS VEULENT PLUS D'AUTONOMIE
- BRICs, SPÉCIALEMENT CHINE – RUSSIE
- USA CIBLE LE BRÉSIL COMME UN LIEN FAIBLE
- FAIBLE POUVOIR DE L'EUROPE

ÉTAT DES LIEUX

QUE FAIRE DE L'INTERNET ACTUEL ?

SUR-PATCHÉ vs TABLE RASE

FRAGMENTATION EN EXPANSION

POLITIQUE + LINGUISTIQUE + SÉCURITÉ + ARMEMENT

APPLE - GOOGLE - FACEBOOK - TWITTER . . .

RISQUES EN EXPANSION

COMPLEXITÉ + ÉCHELLE + FRAUDE + SABOTAGE

FUTURS INTERNET

USA-Europe: RINA – IRATI – PRISTINE – ARCFIRE …

INTERNET CONSTRUIT COMME EXPÉRIMENTATION

IL L'EST RESTÉ

QUE FAIRE ?

APPEL AUX DROITS DES CITOYENS

- VOTE, PÉTITION, GRÈVE, BOYCOTT, MÉDIAS

UTILISER L'EXPERTISE DES INTERNAUTES

- ANONYMAT, CHIFFREMENT

ORGANISER LA PROFESSION DES TICs

- ÉTHIQUE, CHARTES, RÈGLES DE CONDUITE

PUBLIER LES ABUS ILLÉGAUX / EXCESSIFS

Etc ...

RACINES ouvertes

(http://en.wikipedia.org/wiki/Alternative_DNS_root)

- INDÉPENDANTES DU MONOPOLE ICANN
  - Antérieures à l'ICANN, depuis 1995
- RÉSEAUX PRIVÉS – LIBERTÉ DE NOMMAGE
- ENTREPRISES STYLE *JEUNES POUSSES*
- ACCÈS À L'INTERNET HISTORIQUE
- PLUS TLDs MULTIPLES
- TOUS LES SCRIPTS DE LANGUES
- **DOUBLE SOURCE**

RÉALISABLE SANS L'ACCORD DU GOUV. US

- **Appliquer les lois nationales/régionales à l'évasion fiscale;**
- **Imposer des amendes substantielles pour abus de position dominante;**
- **Exclure les monopoles illégitimes des principaux contrats;**
- **Ouvrir la compétition entre les Racines DNS multiples;**

RÉALISABLE SANS L'ACCORD DU GOUV. US (suite)

- **Conditions générales de vente invalides si non conformes au droit national;**
- **Juridiction nationale ou Européenne en cas de désaccord sur clauses contractuelles;**
- **Choix optionnel ou impératif de logiciels libres (open source);**
- **Absence ou carence de maintenance de logiciel entraîne suspension de propriété intellectuelle;**

10e FRC 2010

Merci de votre attention

SAVOIR-FAIRE
RCS 535 199 228 Paris

www.open-root.eu

contact@open-root.eu

Louis POUZIN
Chantal LEBRUMENT

TABLE RONDE #1

LA CYBERSECURITE OPERATIONNELLE

10e FRC 2017

La cybersécurité opérationnelle

M. Michel ROCHELET
Délégué ANSSI Région Grand-Est

M. Fabrice STALTER
Responsable Sécurité des Systèmes d'Information
aux Hôpitaux Universitaires de Strasbourg,
Chargé d'enseignement à l'université de Strasbourg
et à l'université d'Angers

M. Jean-Marc MISERT
Service PGCS – La Banque Postale
Président du Clusir-Est

10e FRC 2017

La cybersécurité opérationnelle

M. Michel ROCHELET

Suivi permanent du risque et du lien opérationnel

10e FRC 2017

La cybersécurité opérationnelle

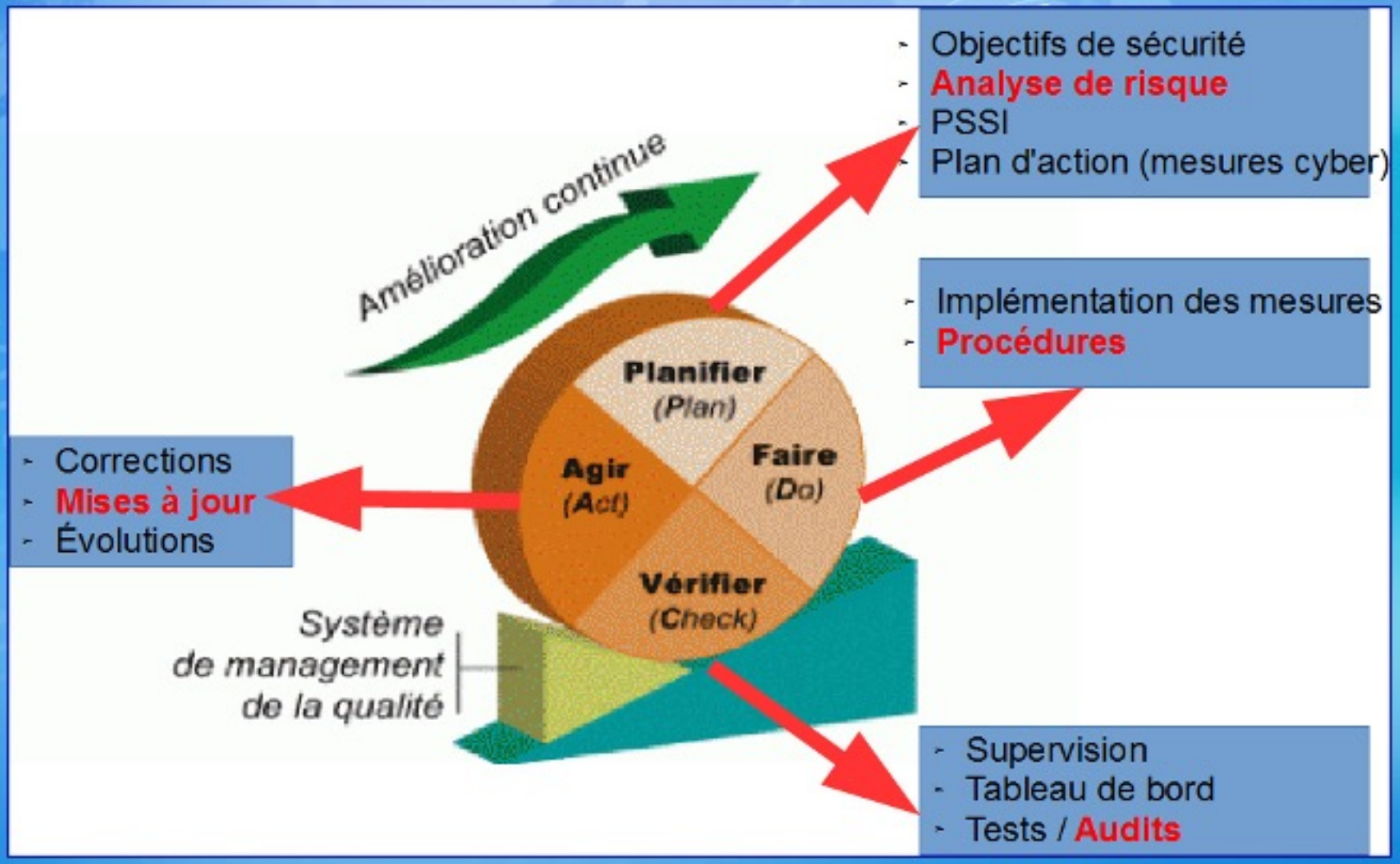
La théorie :

➢ mise en place d'un système de management de la sécurité de l'information (**SMSI**)

- ❑ **ISO 27002** (2013) : 114 mesures techniques et organisationnelles
  - ✓ *préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information*

10e FRC 2017

La cybersécurité opérationnelle



10e FRC 2017
La cybersécurité opérationnelle

La pratique :

- Guide d'hygiène informatique
  42 mesures pour les RSSI
  https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

- Guide des bonnes pratiques de l'informatique
  12 règles pour les PME
  https://www.ssi.gouv.fr/administration/bonnes-pratiques/

10e FRC 2017

La cybersécurité opérationnelle

Quelques fondamentaux :

- désigner un RSSI
- cartographier les informations sensibles
- évaluer les risques
- séparer les usages
- cloisonner (besoin d'en connaître)
- filtrer les flux
- mettre à jour les logiciels
- contrôler les accès physiques et logiques au SI
- sécuriser les supports amovibles
- chiffrer les informations sensibles
- sauvegarder les données
- sensibiliser le personnel

10e FRC 2017

La cybersécurité opérationnelle

L'autoformation des RSSI :

- MOOC de l'ANSSI : SecNum Académie

https://secnumacademie.gouv.fr/

La cybersécurité opérationnelle

<u>Quand la prévention a échoué</u> :
https://www.cybermalveillance.gouv.fr/

10e FRC 2017

La cybersécurité opérationnelle

Michel ROCHELET

Délégué de l'ANSSI pour la région Grand Est

michel.rochelet@ssi.gouv.fr

10e FRC 2017

La cybersécurité opérationnelle

M. Fabrice STALTER

Gestion des mises à jour de logiciels

10e FRC 2017

La cybersécurité opérationnelle

Objectifs

Enjeux

Continuité des activités vitales
Qualité des soins
Maîtrise des risques juridiques
Confiance dans le SI et maîtrise de l'image
Maîtrise des coûts

Contraintes et limites

SI conventionnel et SI industriel interconnectés
Prestataires « industriels » proposant une offre de service limitée en SSI
Prestataires « industriels » d'envergure internationale

Objectifs

Assurer la disponibilité des services vitaux du SIH
Exactitude et fiabilité de l'information
Empêcher toute intrusion au SIH et/ou divulgation, interne ou externe, d'information sensible
Garantir le respect des lois et règlements applicables à la sécurité de l'information

Comment ?

Etendre la démarche SSI au SI Biomédical

Renforcer la démarche SSI en intégrant les spécificités du contexte « biomédical »

Au commencement ...

	Forces	Faiblesses
Interne	Démarche SSI existante - Outils et méthodes - Organisation de la SSI - Soutien DG SSI sur SI « conventionnel » Expertise technique de la DSI	Contexte biomédical peu maîtrisé Faible crédibilité du RSSI sur le sujet
Externe	**Opportunités**	**Menaces**
	Quelques ingénieurs biomédicaux intéressés	Absence de soutien de la Direction du Biomédical Métiers ne se sentent pas concernés ou hostiles Fournisseurs indifférents ou hostiles

« Le plus probable, c'est qu'on va plutôt où on ne veut pas, et que l'on fait plutôt ce que l'on ne voudrait pas faire. » [Arthur Rimbaud]

… c'était compliqué !

Démarche SSI opérationnelle et technique. Objectifs atteints ?

	Forces	Faiblesses
Opportunités	~~Démarche SSI existante~~ Quelques ingénieurs biomédicaux intéressés Expertise technique de la DSI	Contexte biomédical peu maîtrisé Faible crédibilité du RSSI sur le sujet ~~Quelques ingénieurs biomédicaux intéressés~~
Menaces	~~Démarche SSI existante~~ Expertise technique de la DSI Absence de soutien de la Direction du Biomédical Métiers ne se sentent pas concernés ou hostiles Fournisseurs indifférents ou hostiles	Contexte biomédical peu maîtrisé Faible crédibilité du RSSI Absence de soutien de la Direction du Biomédical Métiers ne se sentent pas concernés ou hostiles Fournisseurs indifférents ou hostiles

Risques résiduels

L'expertise technique permet de traiter partiellement le positionnement des fournisseurs

Ce qui devait se passer, arriva

2009 | 2010 | 2011 | 2013 | 2016

Sécurité exclusivement opérationnelle et technique

Pack de sécurité des équipements biomédicaux

Isolement et filtrage des flux des équipements non maitrisés

Conformité Loi I&L

Et puis, avec pas grand-chose …

Interne

Forces

Démarche SSI existante
- Outils et méthodes
- Organisation de la SSI
- Soutien DG SSI sur SI « conventionnel »

Expertise technique de la DSI

Faiblesses

Contexte biomédical peu maîtrisé

Faible crédibilité du RSSI sur le sujet

Externe

~~« Je vous l'avais bien dit »~~

Opportunités

Quelques ingénieurs biomédicaux intéressés

Conficker

Groupe de travail « SSI Biomédical »

Menaces

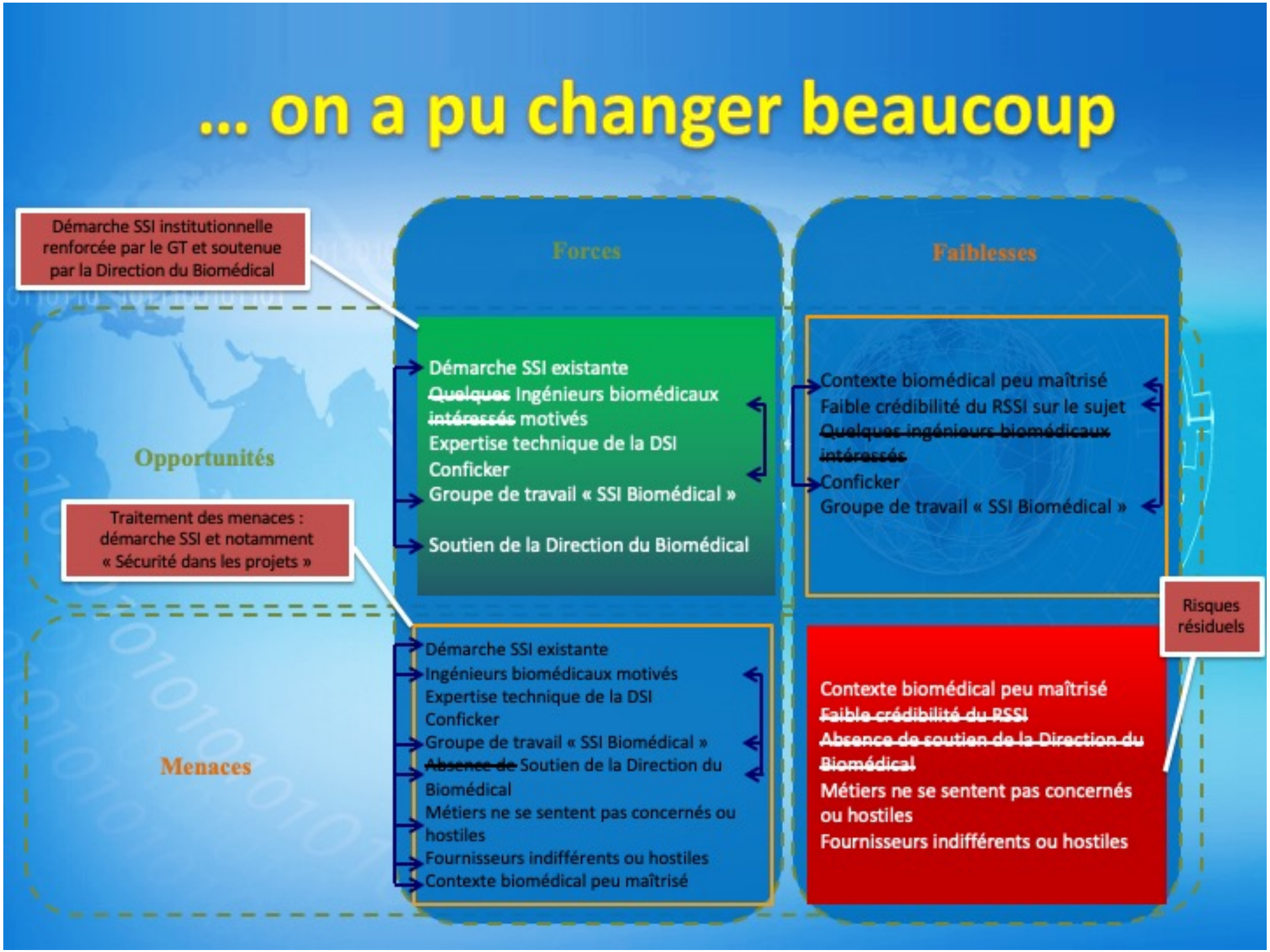
Absence de soutien de la Direction du Biomédical

Métiers ne se sentent pas concernés ou hostiles

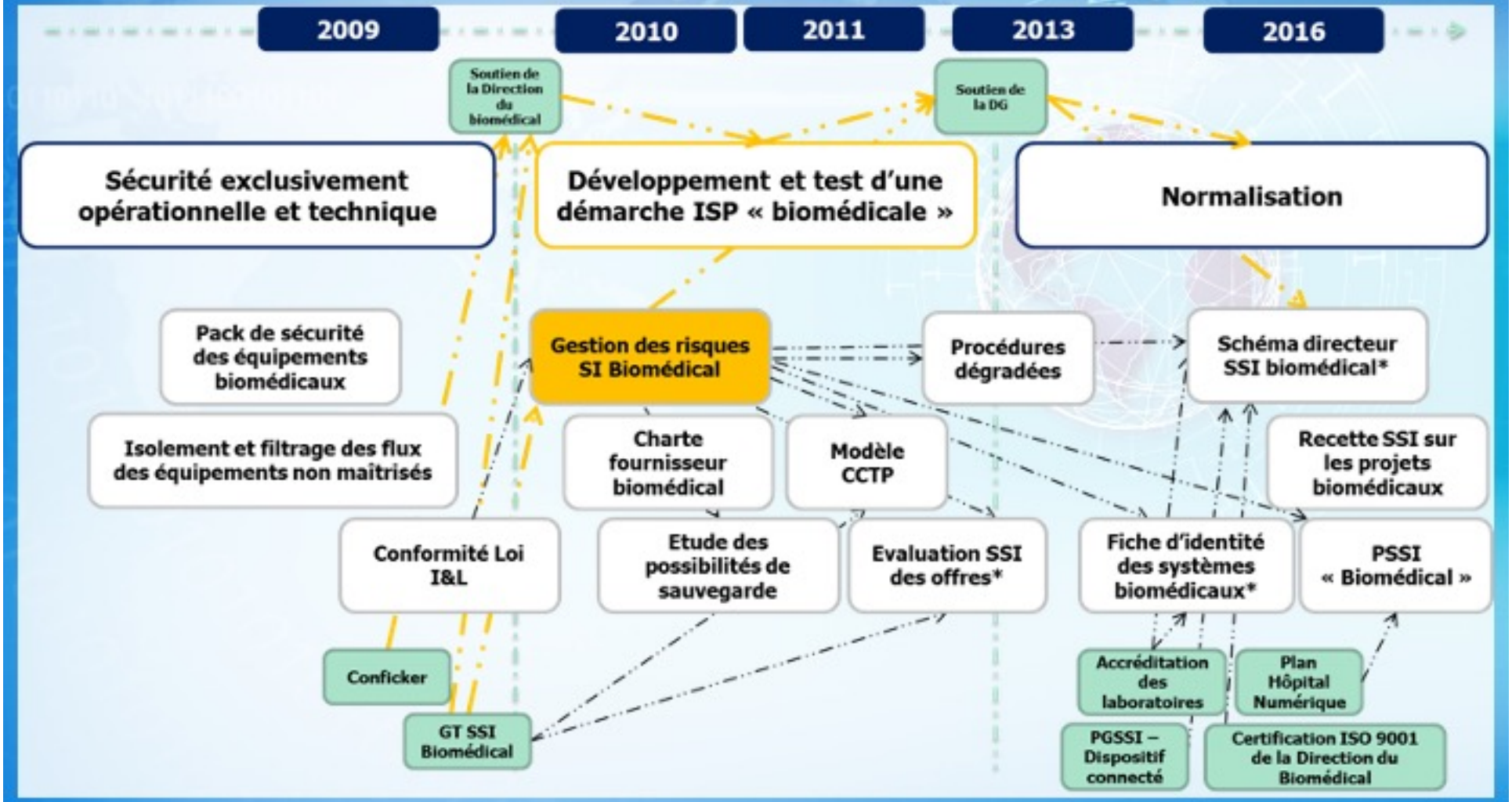
Fournisseurs indifférents ou hostiles

«Il faut toujours être prêt à négocier, mais ne jamais négocier sans être prêt. »
[Richard Nixon]

… on a pu changer beaucoup



Et en plus, ça marche !



Merci !

« Le sage poursuit l'absence de douleur et non le plaisir. »

[ARISTOTE]

10e FRC 2017

La cybersécurité opérationnelle

M. Jean-Marc MISERT

Socle de sécurité opérationnel et relation avec la production

La filière SI du groupe

Introduction

Répartition géographique et par branche des effectifs de la filière SI

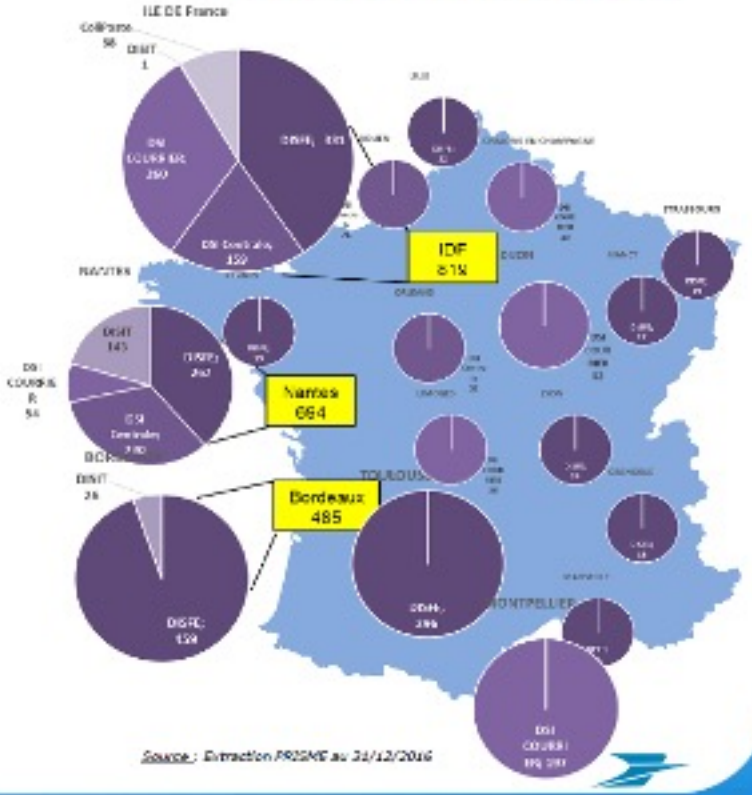
Répartition des effectifs par Branche

A fin décembre 2016, la filière SI du Groupe La Poste regroupait 4 436 EUTC

Effectifs à fin décembre 2016 par Branche (en EUTC)	
DSEM	1146
DISFE	1676
DSI BSCC	892
GROUPE (*)	672
Numérique	50
TOTAL Groupe	**4436**

(*) DSI Centrale, DISIT, DSI Groupe

Répartition des effectifs hors DSEM



Source : Extraction PRISME au 31/12/2016

Zoom sur le département sécurité de la production informatique

Nos missions :

- Garantir la sécurité opérationnelle : prévention, détection, réaction
- Garantir la continuité des SI

Quelques unes de nos contraintes

- Lois et règlements : LPM, NIS, RGPD, Bâle 3, ..
- La PSSI du groupe, de la banque
- L'effet volume
- La variété technologique
- Les compétences à maintenir ou développer

Mais surtout

- La production doit « tourner »

On fait comment ? Illustration avec quelques cas d'usage

- En phase de construction
  - Comment maintenir à jour la PSSI ?
  - Comment intégrer la sécurité dans les projets ?
- En phase récurrente
  - Comment surveiller nos SI et réagir ?
  - Comment assurer une veille sur les vulnérabilités ?
  - Comment garantir le « MCS » ?

Comment maintenir à jour la PSSI ?

- Un process est appliqué
- Périodiquement les RSSI émettent des propositions de mises à jour
- Au sein de la DPI, **une dizaine** de référents sur nos activités clés sont sollicités

- Chacun doit estimer **l'impact et la faisabilité** des maj
- Une réunion de concertation aboutit sur une synthèse
- Le PLUS : une PSSI plus en prise avec la réalité du terrain, qui peut mieux s'appliquer **de bout en bout**.

Comment intégrer la sécurité dans les projets ?

- La sécurité est « fondue » dans la méthode de conduite de projets
- Les ADR sont systématiques, ceci est validé en comité (CVP)
- Lors des phases de conception, il est demandé aux CDP de nous fournir un fichier « SecuOp »

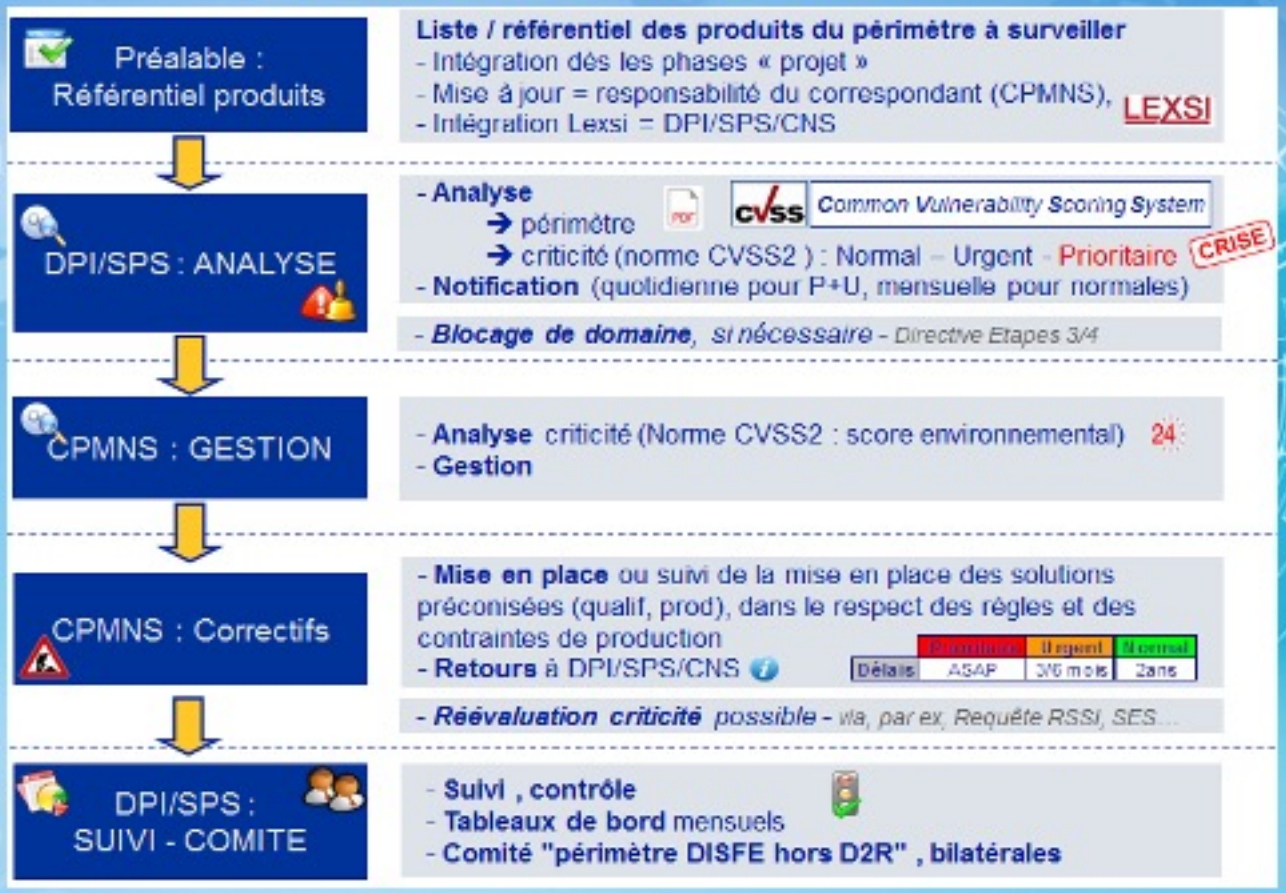
- Ce fichier nous permet de savoir lesquels de nos outils vont être mis en œuvre
- Le PLUS : **une vision de bout en bout** en assurant le lien entre exigences de sécurité et capacité à faire

Comment surveiller nos SI et réagir ?

- Nous disposons d'un CERT et SOC interne (24/7)
- Ce qu'il faut surveiller est défini dans la PSSI, et mis en œuvre par les architectes

- Chaque typologie d'alerte fait l'objet d'une « DTS »
- Une alerte est à minima un incident (ITIL) mais peut être un déclencheur de crise (cellule dédiée)
- Le PLUS : **le bout en bout** entre une description « littérale » dans la PSSI jusqu'aux actions précises de réaction(s)

Comment assurer une veille sur les vulnérabilités ?



Le PLUS : process **de bout en bout** de la déclaration d'un composant sur notre SI au suivi de ses mises à jour

Comment garantir le MCS ?

- La **double** problématique de base, avoir un niveau de sécurité de départ « conforme » **et** qui ne se dégrade pas dans le temps !
- Pour le niveau de sécurité de départ, chaque nouveau serveur voit l'affectation d'une tâche ITIL
- Pour les serveurs déjà en production : des campagnes de contrôles « massives » 4 fois par an.
- *Le PLUS : **le bout en bout** du contrôle sur l'ensemble du cycle de vie de l'équipement*

Conclusion et remerciements

Au **bout** de cette présentation, un message :

« raisonner de **BxxT en BxxT** »

Merci pour votre attention !

10e FRC 2017

QUESTIONS RÉPONSES

10e FRC 2017

La cybersécurité opérationnelle

M. Kevin BROU BONI
M. Axel RIBON

Exploitation d'une faille de sécurité web

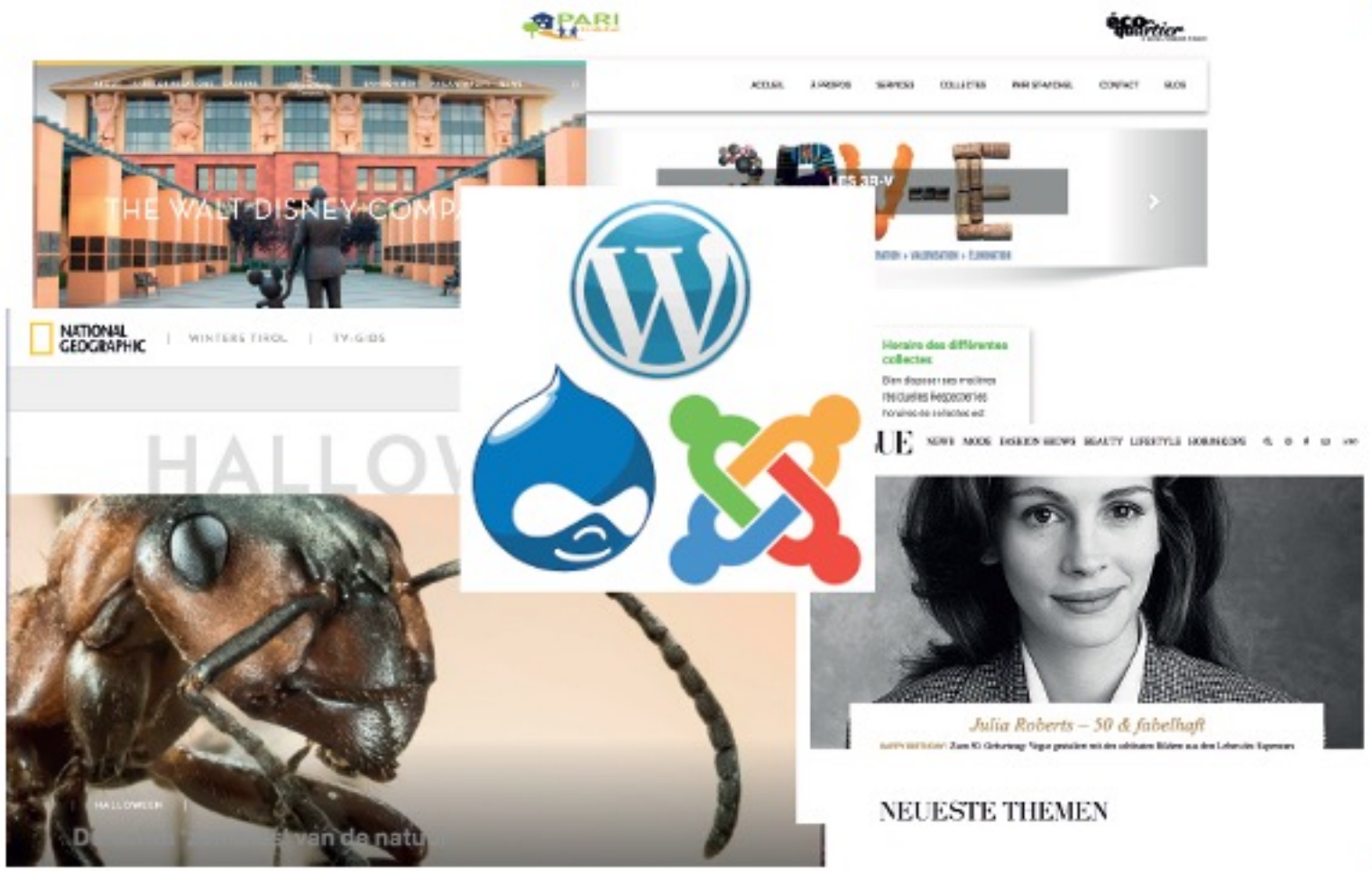
FRC 2017
Content Management System

Conception dynamiques de site Web

- Accessible aux non programmeurs
- Nombreux templates disponibles
- Maintenance décentralisée
- Gestion des droits d'accès
- Multitude de modules
- ...

10e FRC 2017

La cybersécurité opérationnelle



FRC 2017

TABLE RONDE #2

LES ATTEINTES A LA REPUTATION

10e FRC 2017

Les atteintes à la réputation

Capitaine Romain LEMARIE

Officier expert en criminalistique

Centre de lutte contre les criminalité numérique (C3N)

M. Daniel GUINIER

Expert en cybercriminalité et crimes financiers près la Cour pénale internationale de la Haye, Colonel (RC) de la gendarmerie nationale

Lieutenant-Colonel Gilles LE GAL

Officier professeur au Centre d'Enseignement Supérieur de la Gendarmerie (CESG) de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN)

M. Ludovic HAYE

Ingénieur en systèmes informatiques industriels

Maire de Rixheim, Chef d'escadron (RC) de la gendarmerie nationale

10e FRC 2017

Les atteintes à la réputation

Capitaine Romain LEMARIÉ

Les enjeux en matière de e-réputation

Exposition au risque (1/2)

Propos diffamatoires, dénonciation, fausses informations

Diffusion d'informations sur l'entreprise par les salariés
Dénonciation / mise en cause d'un salarié
(corruption, stupéfiants, pédophilie...).

Mauvaise publicité

Sites de consommateurs (UFC, Que Choisir?), presse

Prolongement dans la sphère privée

Ciblage salariés de votre entreprise via les réseaux sociaux :
Linkedin + infos sur réseaux sociaux / vie privée (famille / extorsion) / levier

Réseaux sociaux

Exposition au risque (2/2)

Pénétration des systèmes

Attaques sur site web (DDOS, défacement)
Attaques impliquant les employés ("phishing")
Attaque sur les systèmes de l'entreprise (malware, ransomware)

Cyber-escroqueries liées à votre entreprise

Typosquatting
Création de faux comptes *Twitter*
Usurpation d'identité : fausses offres d'emploi.
Vente de produits acquis frauduleusement (billets transport, luxe, abonnements, etc.)

E-réputation : vecteurs de diffusion

Web 1.0

- Forums de discussion : anciens employés, stagiaires (diffamations ou remontée de dysfonctionnements internes), consommateurs (60 millions, UFC, etc.)
- Presse en ligne, sites parodiques, diffusion fake news (legorafi.fr, actualites.co)
- Plateformes de partage de contenu (repository)

Web 2.0

Réseaux sociaux : Facebook, Twitter, Youtube, Instagram (photo sur site), Periscope, Facebook live (finalité différente en fonction du réseau social utilisé : diffusion contenu/image/vidéos/Live)
Linkedin/viadeo : ciblage de profils professionnels stratégiques

Typologie des attaquants

Concurrents

Groupes de pression (APT, Anonymous, Hacktivistes)

Anciens employés / stagiaires

Animalistes (secteurs viande, cosmétique, pharmaceutique, maroquinerie, etc.)

Zadistes (environnement, énergie, sécurité, transports)

Extrémismes (néo-nazis, radicalisés)

Un cercle vertueux (1/2)

1. Évaluer le risque d'exposition

Veiller, anticiper, cartographier des données les plus sensibles

2. Connaître l'environnement de son entreprise

Mesures de sécurité élémentaires (MAJ, antivirus, sauvegarde quotidienne, etc.)
Guide d'hygiène informatique ANSSI, etc.
Environnement utile : suivi des recommandations Europol/EC3, ENISA, ANSSI, Gendarmerie nationale, Police nationale.
Sensibiliser ses collaborateurs

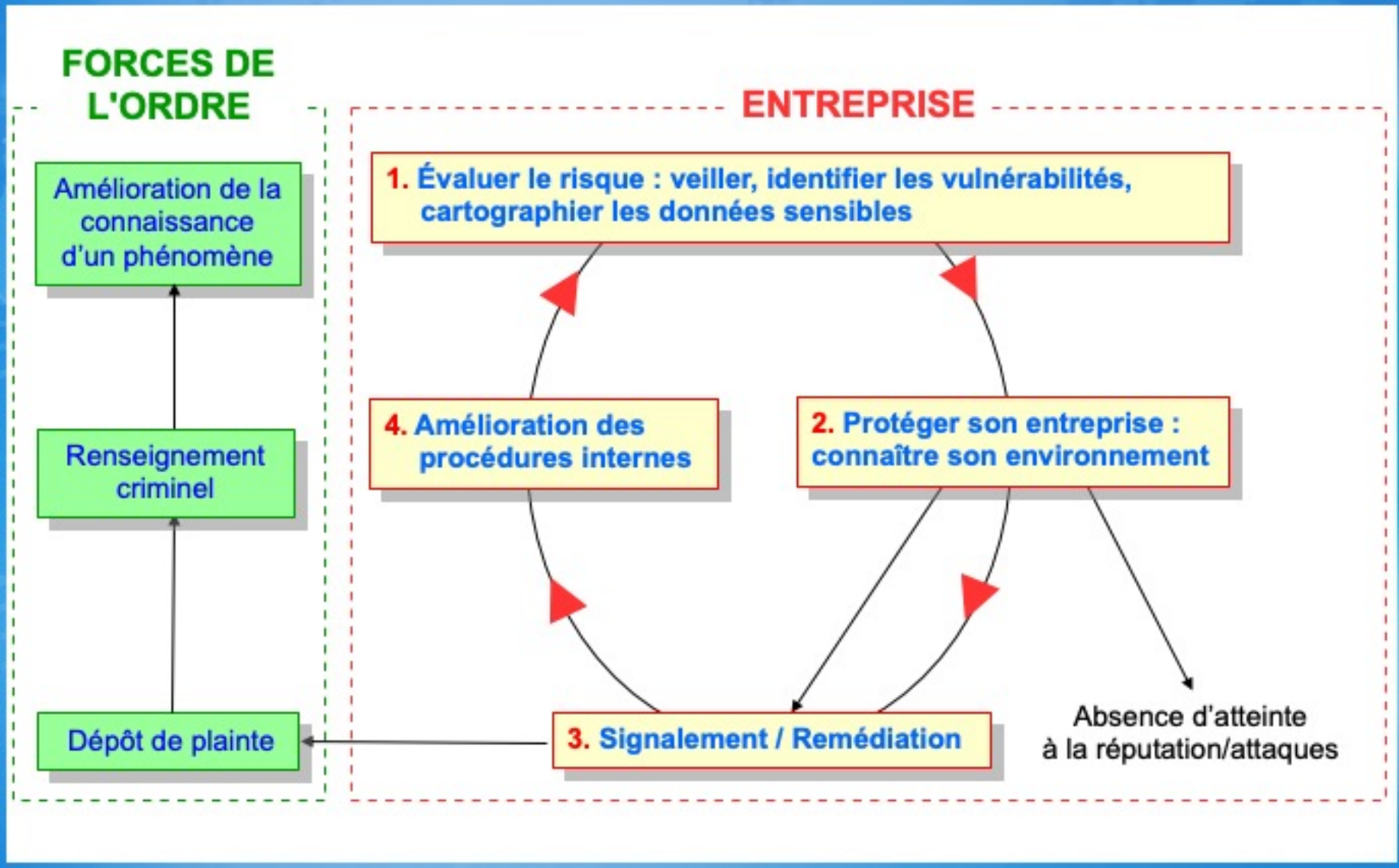
3. Signaler et remédier

Demander le retrait d'un contenu
Dépôt de plainte
ACYMA, Nomoransom

4. Améliorer les procédures internes

Correction d'un dysfonctionnement signalé
Signature d'une charte informatique/utilisation des réseaux sociaux
Clause de confidentialité

Un cercle vertueux (2/2)



10e FRC 2017

Les atteintes à la réputation

M. Daniel GUINIER

Les « bots » sociaux malveillants, une nouvelle menace sérieuse

LES ATTEINTES A LA REPUTATION

Les *"bots"* sociaux malveillants : une nouvelle menace sérieuse

par M. Daniel GUINIER

Expert en cybercriminalité près la Cour Pénale Internationale de La Haye
Colonel (RC) de la gendarmerie nationale

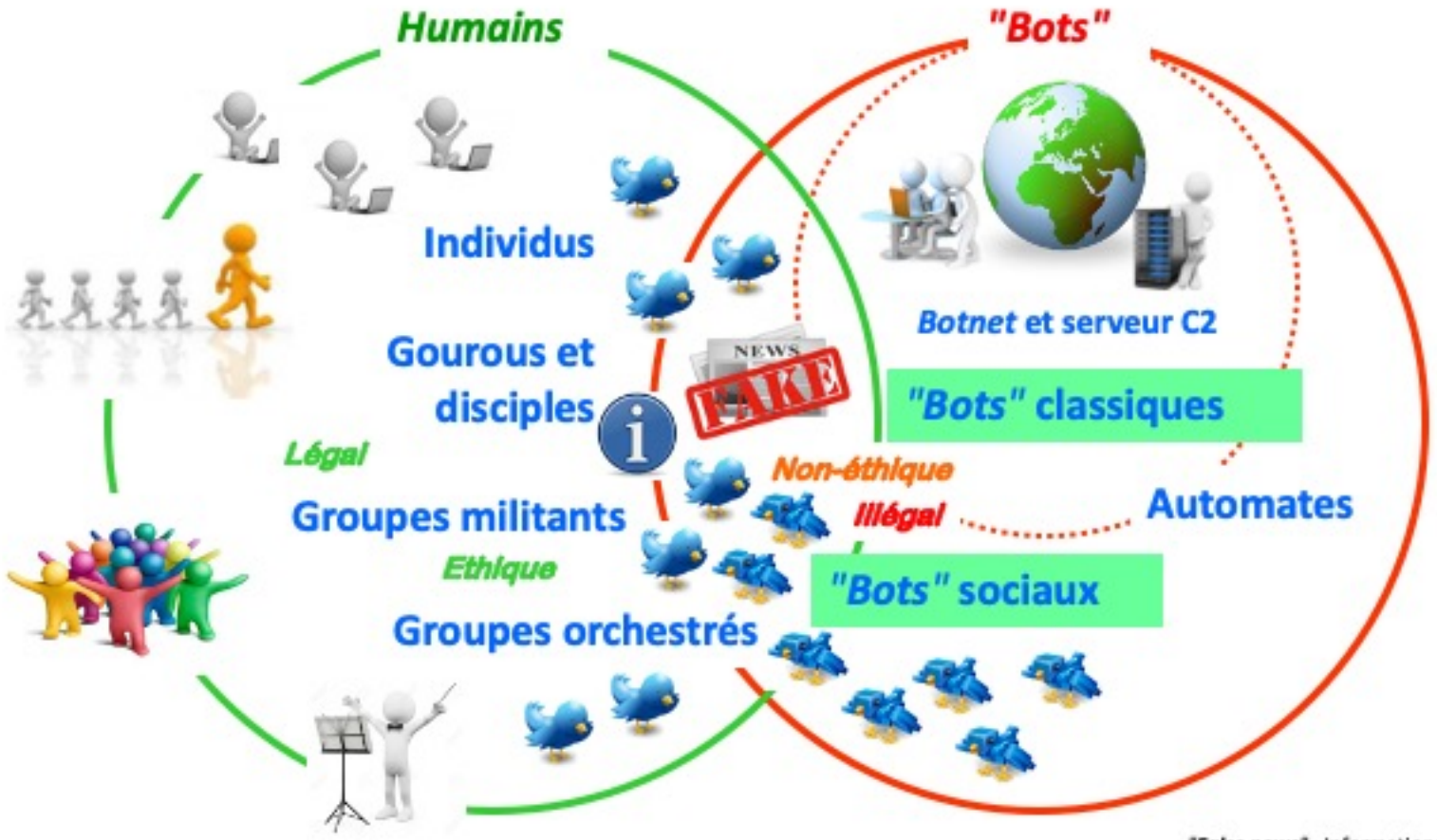
LES UTILISATEURS DES RESEAUX SOCIAUX

33 millions		2 milliards
29 millions		1,5 milliard
16 millions		330 millions

Twitter permet l'envoi spontané de brefs messages (140 car. max), **les *tweets***, par messagerie instantanée sur Internet ou par SMS, **en réaction immédiate**.

Le nombre d'utilisateurs actifs des trois principaux réseaux sociaux, indique qu'ils sont de très bon candidats pour les *"bots"* en servant de vecteurs.

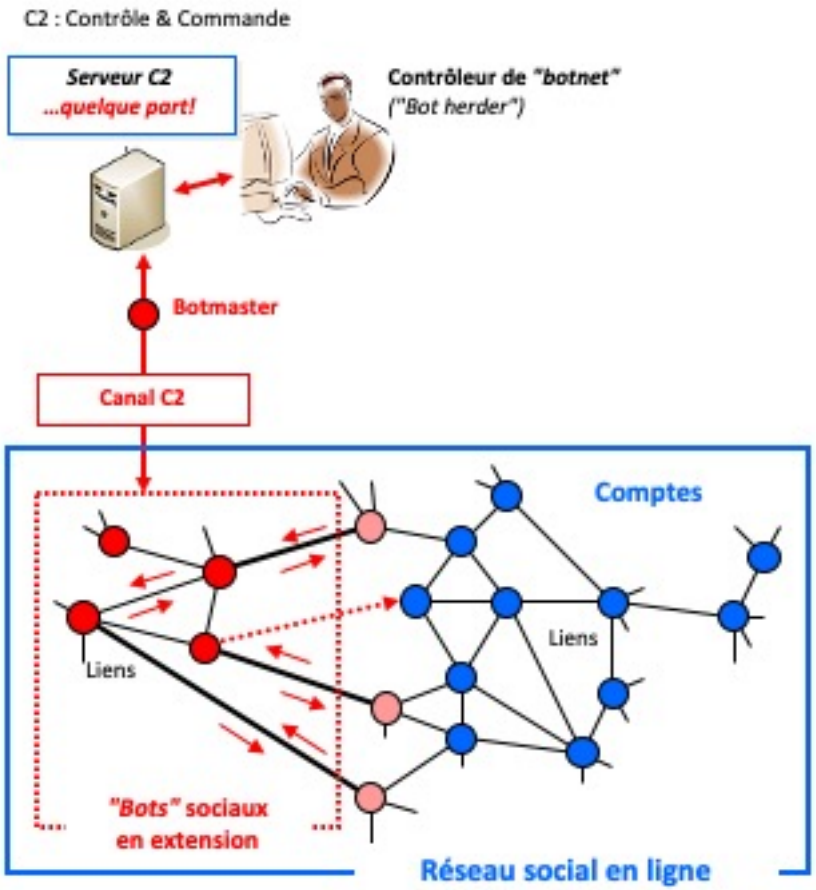
L'ECOSYSTEME DE L'INFLUENCE EN LIGNE



"*False news*" : Informations inexactes
"*Fake news*" : Fausses informations

Cet écosystème d'influence permet ainsi l'interférence et l'amplification des messages des différentes sphères, avec l'appui d'outils et de services légaux ou illégaux pour obtenir et diffuser des informations, vraies, inexactes ou fausses.

LES *"BOTS"* SOCIAUX



Les *"bots"* sociaux sont destinés à interagir en temps réel avec des humains sur les réseaux sociaux en produisant automatiquement du contenu de façon coordonnée mais incontrôlée par les plateformes, *telles que Facebook ou Twitter*.

En simulant le comportement humain ils peuvent créer et diffuser de fausses informations de façon massive, visant à atteindre la réputation.

Un *"bot"* social est lié à un compte d'appartenance à un réseau social, tandis qu'un *"bot"* classique se rapporte à une machine compromise d'adresse IP.

APPEL AUX SCIENCES COGNITIVES

Réseaux

sociaux humains

et "bots" sociaux

d'influence

Modélisation
Perception
Langage
Mémoire
Connaissances
Raisonnement
Émotions

Simulation
Acquisition
Transmission
Utilisation

Système d'IA
Algorithmes

"Bots" sociaux

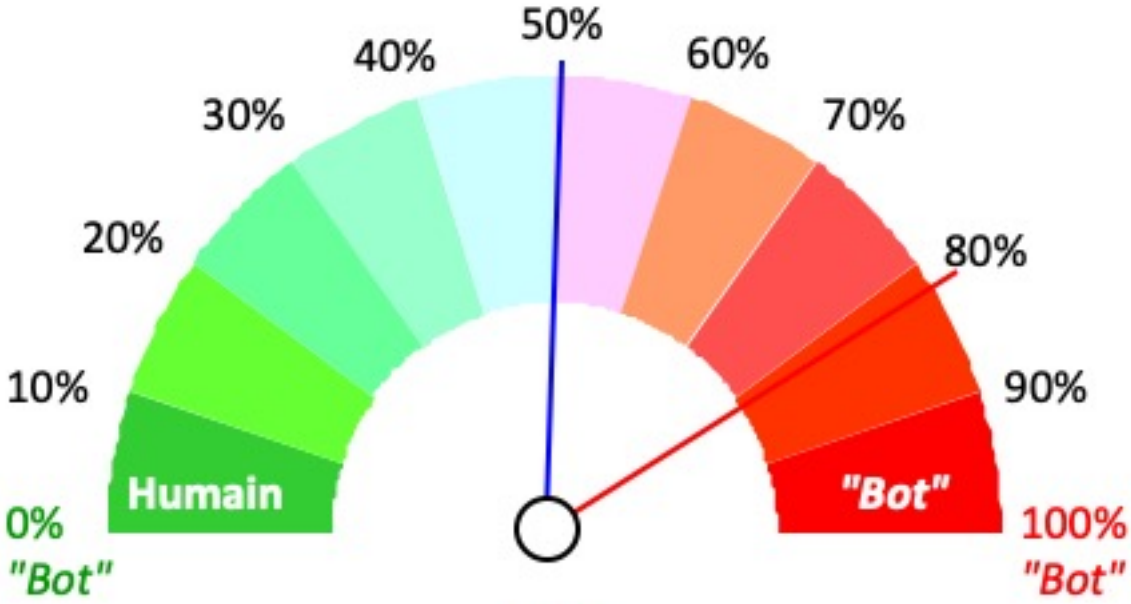
Action
Comptes sociaux :
Infiltration Création,
etc.
Informations :
Elaboration
Diffusion, etc.

Manipulations : leviers d'influence, biais cognitifs ; alimentées par des rumeurs.

IA : Intelligence Artificielle

Les sciences cognitives : *neurosciences, linguistique, psychologie, philosophie, anthropologie, et IA,* seront requises en traitant conjointement leurs données pour réaliser les *"bots"* évolués visant à simuler la pensée humaine.

DETECTION *Tweet* HUMAIN *versus* "BOT"



82%

40% : Réseau
45% : Temps

85% : Utilisateur
83% : Contacts
71% : Contenu
54% : Sentiments

Exemple

Après acquisition de l'historique, scores obtenus avec le système *BotOrNot* pour un compte *Twitter* @..... ; déterminant clairement un *"bot" social.*

ATTAQUES AVANCEES SUR LA REPUTATION

Préparation

Renseignements par tous moyens

Conception de stratégies

Experts en techniques d'influence pour bâtir des scénarii
Elaboration de fausses informations cohérentes et peu vérifiables

Exploitation de failles humaines et techniques

Moyens légaux ***Moyens illégaux***

Corruption Espionnage

Ingénierie sociale

Intrusion : furtivité, *"botnet"*

Experts

Cyberattaque

Exfiltration de fichiers et **accès en ligne à des comptes sociaux compromis**

Exécution

Choix en fonction des **circonstances** et du **but**
Diffusion de fausses informations
Relais : réseaux et *"bots"* sociaux, communautés, etc.

Points particuliers

Groupes d'influence, ***identités et comptes multiples*** *pour* ***amplifier la portée*** *;* ***détournements*** *d'hashtag impliquant la victime : spams, défiguration ;* ***invasion*** *: retweets, reposts, etc.*

Réaction de la victime

Plainte, préservation des preuves, enquête
Informations mêlées pour disqualifier l'attaque
Relais : réseaux sociaux, sympathisants

Points particuliers

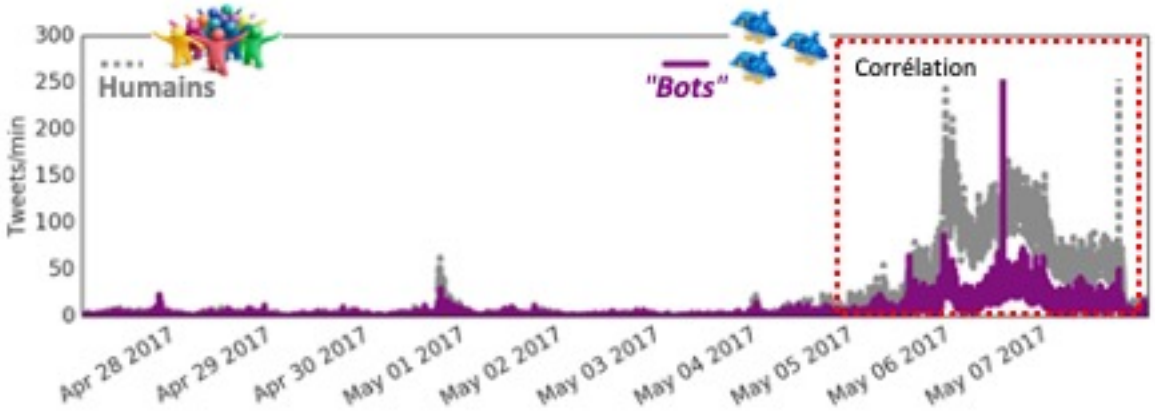
Compartimentation, chiffrement, messageries et protocoles ***sécurisés*** *;* ***détection précoce*** *:"honeypot" - "cloud" ;* ***veille active*** *:* ***réseaux et "bots" sociaux*** *;* ***PSI - plan d'action****, etc.*

La diffusion de fausses informations mêlées à d'autres, réelles, donneront de la crédibilité ou jetteront le doute, selon le cas de chacun : *attaquant ou victime*.

MacronLeaks : LES *"BOTS"* EN MARCHE ...

Réf. : Ferrara E. (2017)

La campagne de déstabilisation débute le 5 mai 2017, quelques heures avant l'entrée dans la période de réserve électorale avec **un pic important de *tweets* dus à des *"bots"* le dimanche 7 mai.**



Les *tweets* de désinformation de *"bots"* sociaux précèdent les cascades de *tweets* humains qui sont suscités par un **phénomène d'induction** permettant l'**amplification de la portée de l'influence.**

L'élection présidentielle française de 2017 a été liée aux *MacronLeaks*, par leur diffusion importante via *Twitter*.

Origine *"bots"* sociaux de la campagne : 18%

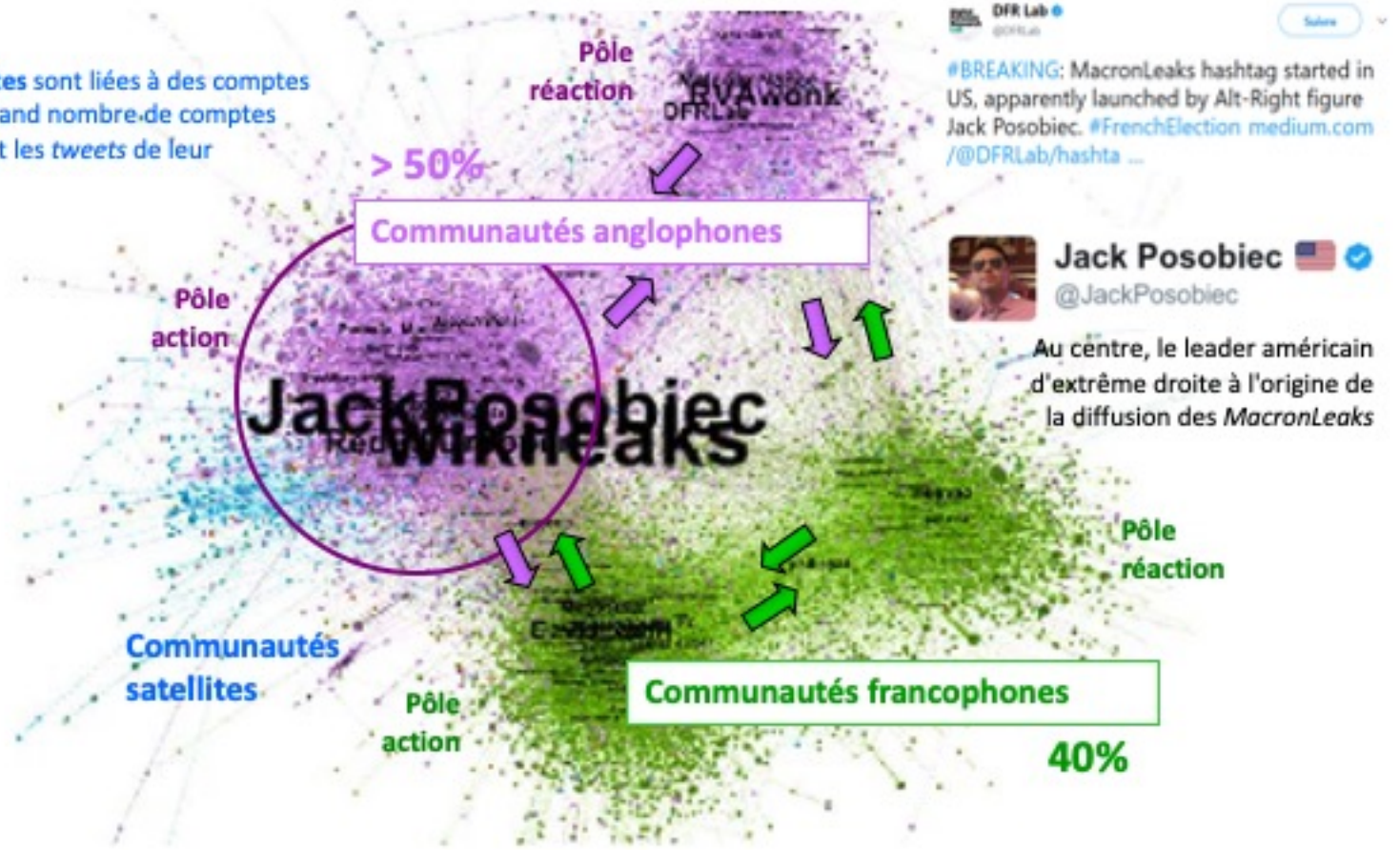
Origine anglophone de la campagne > 50%

Langue majoritaire : l'Anglais
Vocabulaire anglais et français

Il faut s'attendre à voir apparaître sur les *"darknets"* un marché de *"bots"* sociaux, sinon d'automatismes de désinformation, réutilisables à diverses fins.

LES RESEAUX DE COMMUNAUTES

Réf. : Gu L. et al. (2017)



Le diagramme du réseau du *hashtag #MacronLeaks* permet d'observer les interactions entre les communautés de comptes ou de *"bots"* sociaux utilisés pour amplifier le trafic de propagande ou pour diffuser les *MacronLeaks*.

CONCLUSION SUR LES *"BOTS"* SOCIAUX

- ❑ Les réseaux sociaux sont aussi un lieu de désinformation
- ❑ Les campagnes menées sont un risque pour la réputation
- ❑ Des *"bots"* sociaux ont d'ores et déjà été engagés
- ❑ D'autres seront plus sophistiqués et offerts sur les *"darknets"*
- ❑ Des actions de plus grande ampleur sont attendues
- ❑ Elles seront le fait d'organisations structurées ou d'États

Les *"bots"* sociaux sont de nouveaux vecteurs de menaces sérieuses

Les autorités ont à anticiper l'ampleur du phénomène et de ses conséquences, aux fins de prévoir des contremesures efficaces jusqu'au niveau international.

10e FRC 2017

Les atteintes à la réputation

LCL Gilles LE GAL

La cellule et la communication de crise en cas d'atteinte à la réputation

FRC 2017

Les atteintes à la réputation

1. Définition et missions de la cellule de crise
2. La répartition des rôles au sein de la cellule
3. Les phases de communication de gestion de crise
4. La diffusion du récit et les pièges à éviter pour le dirigeant

Le bestiaire de la réputation

L'autruche

- Peu ou pas de présence sur les réseaux sociaux
- Tendance à mettre la tête dans le sable = n'écoute pas ce qui se dit sur sa marque

Le coucou

- Présence sur les réseaux sociaux mais sans veille sur son marché et son entreprise
- Pas de connaissance des pratiques propres à chaque réseau / ni d'engagement conversationnel ou relationnel

Le caméléon

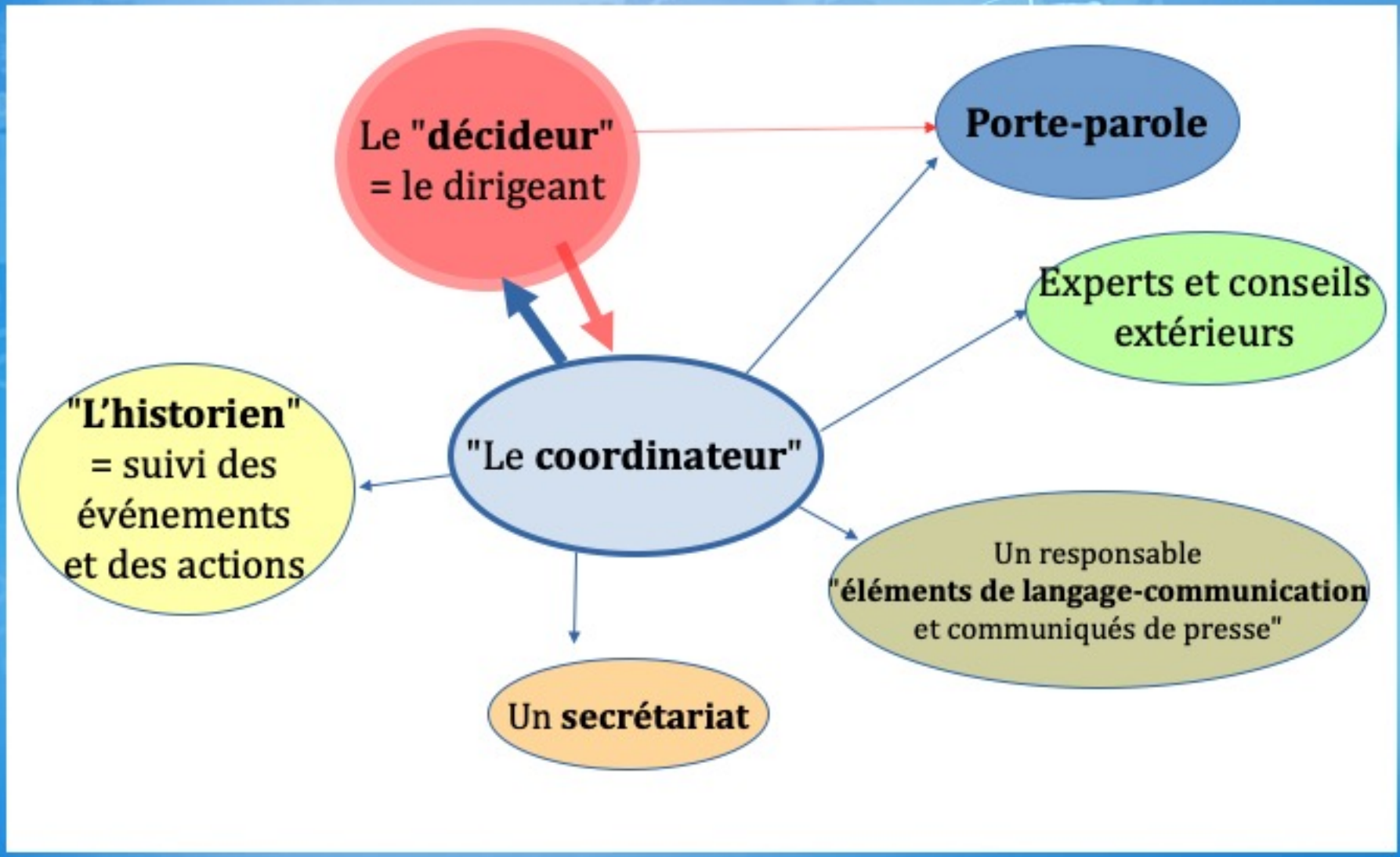
- S'adapte aux nouvelles pratiques pour s'y fondre
- Développe l'engagement / clients / prospects via les réseaux sociaux avec un investisssement sur la veille, les contenus et dans le conversationnel

La cellule de crise

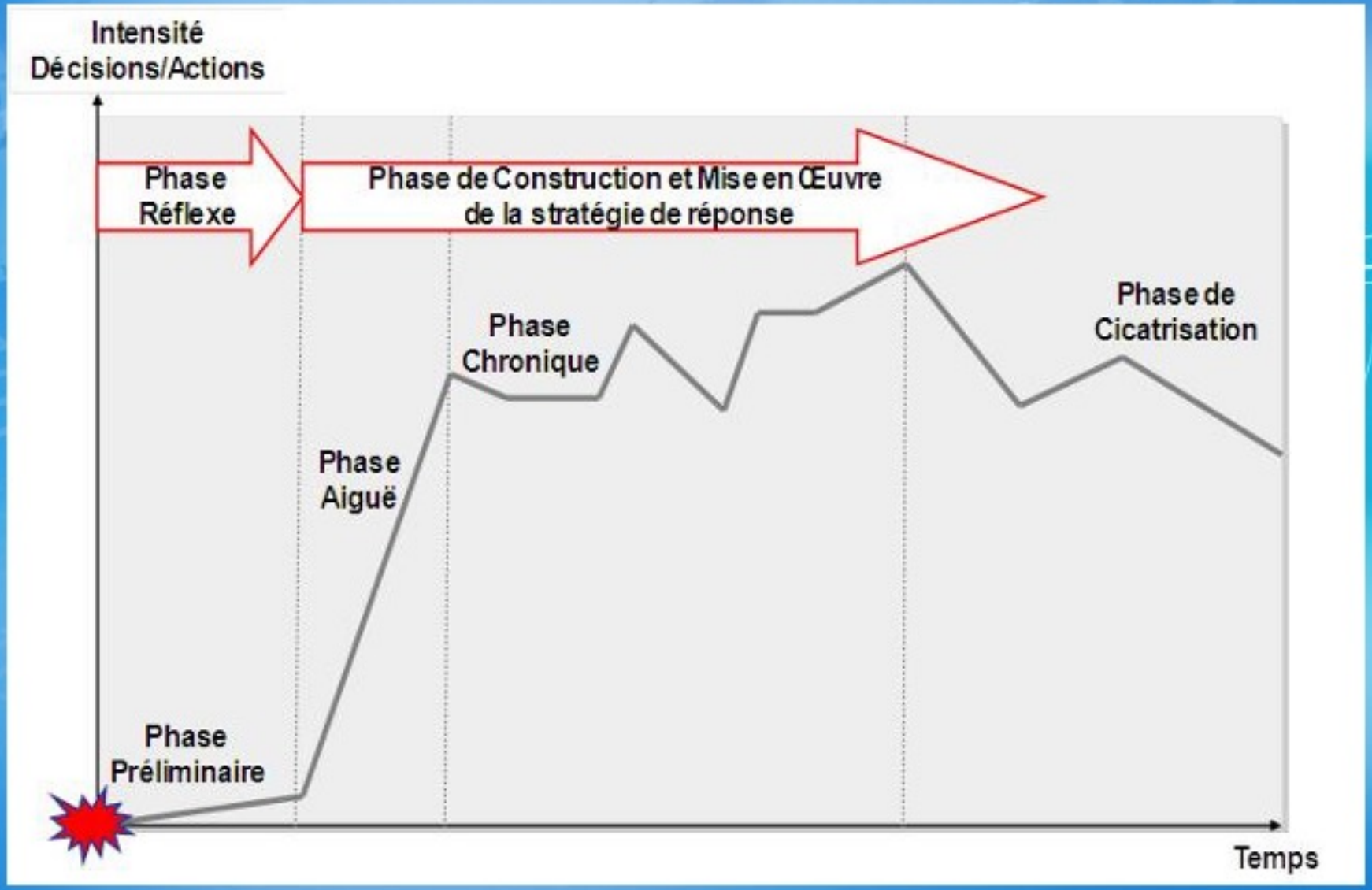
*"Une cellule de crise est un **endroit central** à partir duquel est organisée la gestion de crise pour faire face à une **situation critique** de toute nature. C'est depuis cet endroit que se construisent les politiques et stratégies de **réplique**...*

...elle regroupe par ailleurs des individus chargés de décider et de mettre en œuvre les actions de communication devant limiter la crise et ses effets sur l'entreprise et sa marque"

Composition de la cellule de crise



Les phases de la crise



Les phases de communication de la gestion de crise

La phase d'**empathie**

↓

Le choix de la **stratégie**

↓

La phase de **pédagogie**

↓

La phase du **récit**

↓

La phase de **conclusion**

Les 4 grandes formes de diffusion du récit

1. Le communiqué de presse
2. Le post Facebook ou le tweet
3. La conférence de presse
4. L'interview

10e FRC 2017

Les atteintes à la réputation

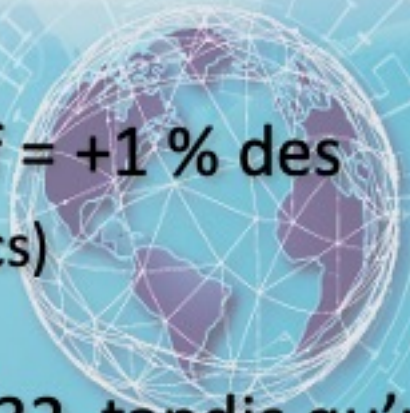
M. Ludovic HAYE

Les conséquences directes et indirectes d'atteinte à la réputation

LA REPUTATION

QUELQUES CHIFFRES

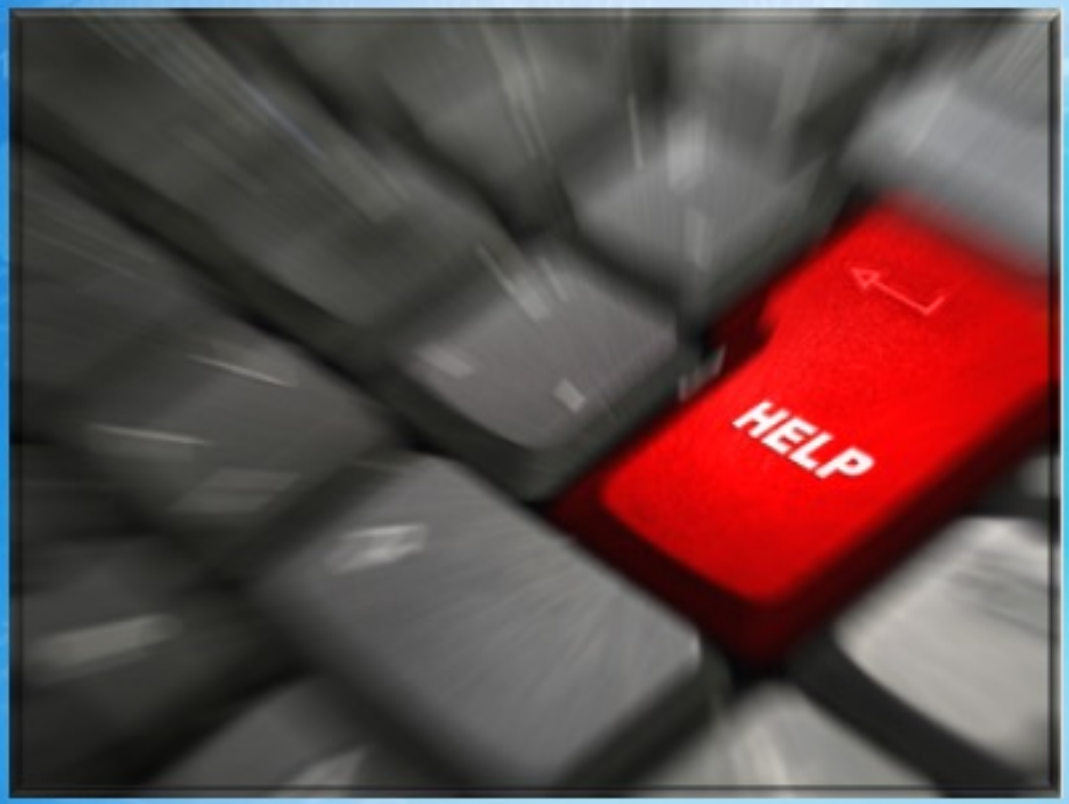
- ✓ +5 points à sa réputation = +7 % la prescription des consommateurs
- ✓ -2 % de bouche-à-oreille négatif = +1 % des ventes. (London School of Economics)
- ✓ Un client promoteur rapporte $32 tandis qu'un client détracteur coûte $57 (Dell)
- ✓ 85 % des internautes recherchent des informations avant un achat sur internet. (Baromètre Fevad, 2017)



QUELQUES CHIFFRES

- ✓ **80%** de ce qui se dit à propos d'une marque sur Internet ne provient pas de la marque
- ✓ 1 publication en ligne est potentiellement vue par **2,5 milliards** de personnes.
- ✓ **55%** des entreprises touchées par un bad buzz ne retrouvent pas leur cours en bourse 1 an plus tard.
- ✓ **85 %** de la valeur d'une PME réside dans sa réputation.

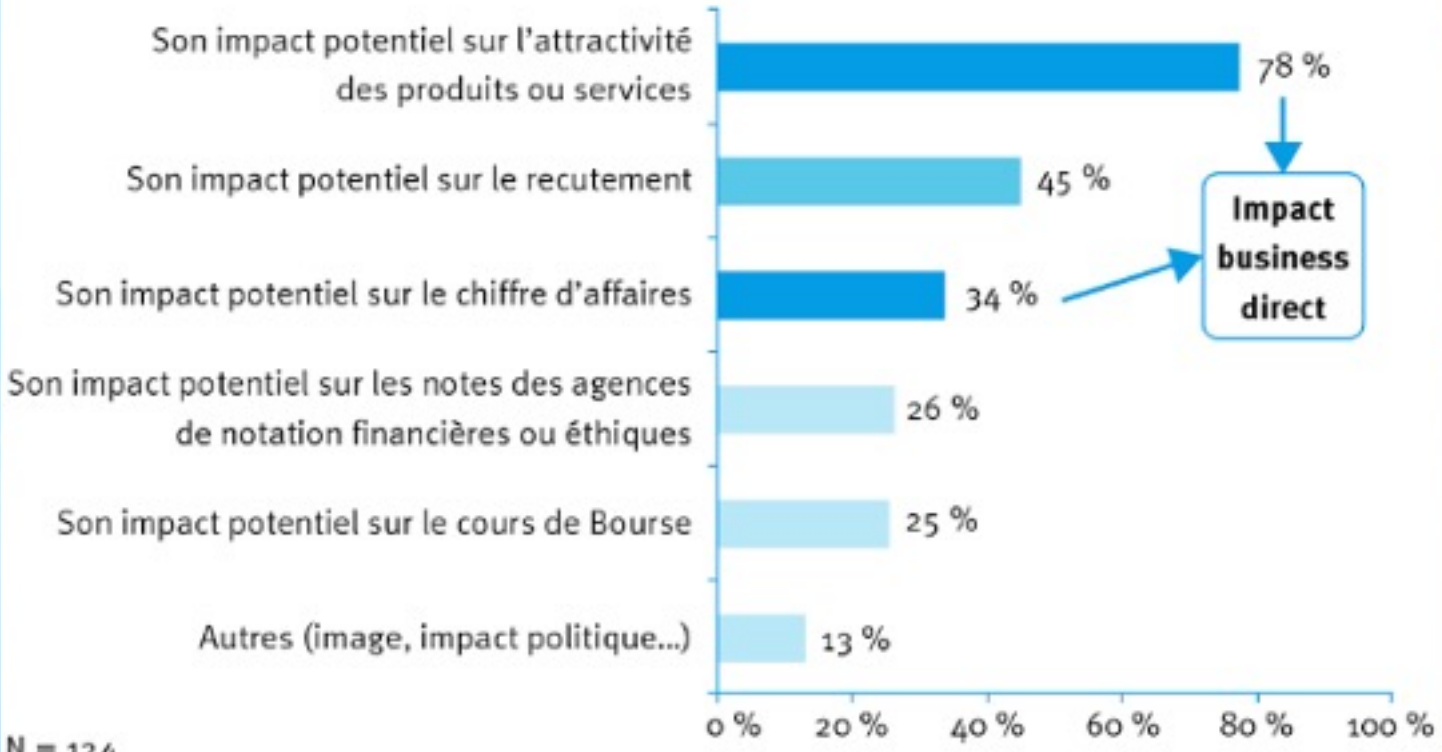
LES CONSEQUENCES D'ATTEINTES A LA REPUTATION



LES CONSEQUENCES DIRECTES ET INDIRECTES

Les raisons d'agir dans le domaine de l'e-réputation

Question : *Selon vous, quelles sont les raisons principales d'agir dans le domaine de l'e-réputation ?*



Sources : e-marketing[1] ; IDC/SAS, Enquête Entreprises, 2011

LES CONSEQUENCES DIRECTES

- ✓ Impact sur les produits et les services (baisse de productivité)

- ✓ Impact financier / boursier
  - Immédiat avec une perte de business
  - Parts de marché (actuelles et futures)
  - Alliances

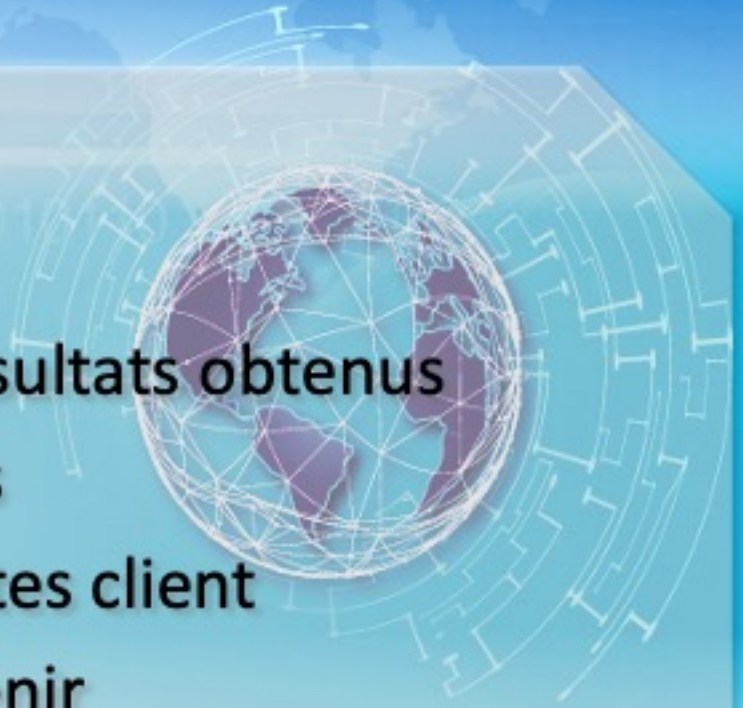
- ✓ Exposition médiatique du personnel
- ✓ Démotivation, baisse de qualité

LES CONSEQUENCES INDIRECTES

- ✓La réputation de la marque / référencement (durabilité internet)
- ✓Les notations des agences
- ✓Poursuites judiciaires
- ✓Difficultés de recrutement
- ✓ Mise en place de nouvelles cellules (internes)

LES SOLUTIONS

LES SOLUTIONS



- ✓ Veille quotidienne
- ✓ Analyse approfondie des résultats obtenus
- ✓ Valorisation des avis positifs
- ✓ Réponse adaptée aux attentes client
- ✓ *"War-Room"* prête à intervenir

FRC 2017

QUESTIONS RÉPONSES

10e FRC 2017

Conférence de clôture

Synthèse et prospective

Gal Marc WATIN – AUGOUARD

Ancien inspecteur des armées-gendarmerie,
Directeur du Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN)

10e FRC 2017
REMERCIEMENTS

AD HONORES

Réseau

ALSACE

10e FRC 2017
REMERCIEMENTS

L'équipe d'organisation

Emmanuelle Haaser
Camille Mungra
Véronique Wadel
Colonel Patrick Da Costa
Daniel Guinier
Stéphane Jeangérard
Ludovic Haye
Johan Moreau

Mjr Serge Seyfritz
Manuel Spraul
Didier Scherrer
Jonathan Weber

10e FRC 2017
REMERCIEMENTS

Acteurs Inédit Théâtre

M. MEYERL Marko

Mme. DE RENDINGER Antonia

Technique

M. GOUBET Gabi

Dessinateur

M. SALLES Laurent

10e FRC 2017

FICHE D'EVALUATION

10e FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Prénom : Nom :

Fonction: Entreprise :

	++	+	-	--
Accueil				
Je suis satisfait des conditions d'accueil du forum :	☐	☐	☐	☐
Table ronde « La cybersécurité opérationnelle »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « Les atteintes à la réputation »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Bilan				
J'accède aux supports pédagogiques mis à ma disposition à l'issue du forum :	☐	☐	☐	☐
Je suis globalement satisfait de ce forum sur les cybermenaces :	☐	☐	☐	☐
Ce forum a répondu à mes attentes :	☐	☐	☐	☐
Je conseillerai ce forum à mon entourage :	☐	☐	☐	☐

J'ai participé au forum l'année dernière ? oui ☐ non ☐

Si oui, j'ai mis en place une (des) actions de prévention dans mon entreprise ? oui ☐ non ☐

Lesquelles ? .....

Je souhaite voir traiter au 11ème forum en 2018, le(s) thème(s) suivant(s) :

.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.

FRC 2017

10e FRC 2017

Documents à votre disposition dans le Hall à la sortie

FRC 2017

www.frc.alsace

@cybermenaces

FRC 2017

Nos prochains rendez-vous

FIC 2018

10ème Forum International de la Cybersécurité

HYPERCONNECTION | THE RESILIENCE CHALLENGE

10 YEARS ANNIVERSARY

23 & 24 JANVIER 2018
LILLE GRAND PALAIS

Nos prochains rendez-vous

FER 2018

Forum Emploi Reconversion

Forum Emploi Reconversion
Au CREF à Colmar
Le 22 MARS 2018

10 Nos prochains rendez-vous

PETIT DÉJEUNER CYBER

www.frc.alsace

2ème petit déjeuner cyber

Printemps 2018

10 Nos prochains rendez-vous

FRC 2018

11ème édition

11ème Forum du Rhin Supérieur sur les cybermenaces

Le 6 NOVEMBRE 2018