

FRC 2021
14ème édition

14 ÈME EDITION

LES INVESTIGATIONS CRIMINELLES DANS LE CYBERESPACE

Auditorium de L'ENA de
Strasbourg
2 NOVEMBRE 2021



FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

2009



2010



2011



2012



2013



2018



2017



2016



2015



2014



2019



2020



2021

**FORUM DU RHIN SUPÉRIEUR
SUR LES CYBERMENACES**
LA GENDARMERIE ET LES OFFICIERS DE LA RÉSERVE CITOYENNE

14ème édition

**LES INVESTIGATIONS CRIMINELLES
DANS LE CYBERSPACE**

TABLE RONDE 1 – LA RÉACTION FACE À UNE CYBERATTAQUE
TABLE RONDE 2 – RETOUR D'EXPÉRIENCE ET PRÉVENTION

2 NOVEMBRE 2021
auditorium de l'ENA de Strasbourg

ENTRÉE LIBRE
Demande d'inscription sur
www.adhones-alsace.fr
formulaire en ligne

PARTENAIRES: ena, CCJ ALSACE, Atheo, LCR, SOCIÉTÉ GÉNÉRALE, CLUSIF EST, BANQUE POPULAIRE, CRCC

SPONSORS: FRC

FRC 2021

14ème édition



FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

LA GENDARMERIE ET LES OFFICIERS DE LA RESERVE CITOYENNE

14ème édition

LES INVESTIGATIONS CRIMINELLES DANS LE CYBERESPACE

TABLE RONDE 1 – LA RÉACTION FACE À UNE CYBERATTAQUE
TABLE RONDE 2 – RETOUR D'EXPÉRIENCE ET PRÉVENTION



ENTREE LIBRE
Demande d'inscription sur
www.adhonores.alsace
formulaire en ligne

2 NOVEMBRE 2021
auditorium de l'ENA de Strasbourg

FRC

14ème édition

EDITION 2021

ANIMATION

Madame Emmanuelle HAASER

Responsable veille et marketing
Direction Economie Numérique, Information,
Marketing
CCI Alsace Eurométropole

DISCOURS D'OUVERTURE

Général Jude VINOT

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

DISCOURS D'OUVERTURE

Monsieur Jean-Luc HEIMBURGER

Président de la CCI Alsace Eurométropole

DISCOURS D'OUVERTURE

Madame Josiane CHEVALIER

Préfète de la région Grand Est
Préfète du Bas-Rhin

FRC 2021 : NOTRE PROGRAMME

LES INVESTIGATIONS CRIMINELLES DANS LE CYBERESPACE

2 NOVEMBRE 2021
auditorium de l'ENA de Strasbourg



13H00 ouverture des portes

15h45 pause

13H30 discours d'ouverture

Général Jude VINOT - Commandant adjoint de la Région de Gendarmerie Grand Est
Commandant le Groupement de Gendarmerie du Bas Rhin

Jean Luc HEIMBURGER - Président de la CCI Alsace Eurométropole

Josiane CHEVALIER - Préfète de la Région Grand Est - Préfète du Bas Rhin

Emmanuelle HAASER - animation - CEN (RC) Gendarmerie Nationale
Responsable veille et marketing - Direction Economie Numérique, Information, Marketing
CCI Alsace Eurométropole

14H00 conférence d'ouverture

La lutte contre la cybercriminalité, un enjeu majeur commun

Colonelle Fabienne LOPEZ - Cheffe du Centre de lutte contre les criminalités numériques (C3N)
du Commandement de la gendarmerie dans le cyberspace (COMcyberGEND)

14h30 Table ronde # 1 : réactions face à une cyberattaque

L'intervention opérationnelle

Major Florent PEYREDIEU - Chef du Groupe Atteintes aux Systèmes de Traitement Automatisé de Données (ASTAD) Centre de Lutte Contre les Criminalités Numériques

La justice face à la cybercriminalité : enjeux et perspectives

Myriam QUÉMÈNER - Avocat général près la cour d'appel de Paris, docteur en droit

Intrusion informatique et traces

Madeleine DUFRASNE et Alexandre RADOS - Etudiants en troisième année de l'ENSISA
à Mulhouse - Spécialité Informatique et Réseaux

Comprendre les risques et les menaces pour mieux se protéger

Laurent VERDIER - Chargé de mission sensibilisation - risque cyber - cybermalveillance.gouv.fr

16H15 Table ronde # 2 - retour d'expérience et prévention

Témoignage d'un dirigeant d'une entreprise victime

Olivier PIQUET - Directeur général / CEO du groupe LISE CHARMEL

Les enjeux pour une collectivité locale

Cyrille BRAS - Responsable de la Sécurité des Systèmes d'Information (RSSI) - Grenoble
Alpes Métropole, Ville de Grenoble et CCAS

Retour d'expérience et prévention du risque cyber à Butachimie

Stéphane FACOTTI - Responsable des systèmes d'Information de la société Butachimie
(Fabrication d'intermédiaires Polyamide) – Chalampé (68)

17h45 conférence de clôture

Général Marc WATIN-AUGOUARD

Général d'armée (2S)

Fondateur du Forum International de la Cybersécurité (FIC)

Président de l'Institut National pour la Cybersécurité et la Résilience des Territoires

18H30 cocktail

entrée libre
pré-inscription en ligne obligatoire
présentation du pass-sanitaire à l'entrée du Forum



FRC 2021 : NOS PARTENAIRES



FRC 2021 : NOS PARTENAIRES



FRC 2021 : NOS PARTENAIRES



FRC 2021 : NOS PARTENAIRES



FRC 2021 : NOS PARTENAIRES



FRC 2021 : NOS SPONSORS



Atheo
INGENIERIE | HUMAN INSIDE

The logo for Atheo is displayed within a white rounded rectangle. The word "Atheo" is written in a bold, sans-serif font, with "Atheo" in red and "o" in grey. Below it, the tagline "INGENIERIE | HUMAN INSIDE" is written in a smaller, grey, all-caps sans-serif font.

FRC 2021 : NOS SPONSORS

BANQUE POPULAIRE
ALSACE LORRAINE CHAMPAGNE



FRC 2021 : NOS SPONSORS



Partenaire de la marque **Alsace**

FRC 2021 : NOS SPONSORS



FRC 2021 : NOS SPONSORS



**SOCIETE
GENERALE**

FRC 2021 : NOS SPONSORS



LA GENDARMERIE, LA RCDS & AD HONORES



FRC 2021 : NOTRE OBJECTIF

CONNAÎTRE ET PARTAGER LES ENJEUX

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

FRC 2021 : FICHE D'ÉVALUATION

**FORUM DU RHIN SUPERIEUR
SUR LES CYBERMENACES**
LA GENDARMERIE ET LES OFFICIERS DE LA RESERVE CITOYENNE

Prénom : _____ Nom : _____
Fonction : _____ Entreprise : _____

Accueil
Je suis satisfait des conditions d'accueil au forum : ++ + - ..

Table ronde « Mieux connaître les risques cyber »
Ce sujet est utile à l'exercice de mon métier :
J'ai trouvé réponse à mes questions :

Table ronde « La sécurité du site internet de l'entreprise »
Ce sujet est utile à l'exercice de mon métier :
J'ai trouvé réponse à mes questions :

Bilan
Je suis globalement satisfait de ce forum sur les cybermenaces :
Ce forum a répondu à mes attentes :
Je recommanderai 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 15^{ème} forum en 2022, 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 2021

FRC 2021 : NOTRE DESSINATEUR

Laurent SALLES





Connexion au réseau wifi : WIFI_ENA

Identifiant

gendarmerie

Mot de passe

WPy57qq4

Profil

EVENEMENT



N'hésitez pas à consulter notre site :

www.adhonores.alsace

CONFÉRENCE PLÉNIÈRE

Colonelle Fabienne LOPEZ

Cheffe du C3N

**« LA LUTTE CONTRE LA CYBERCRIMINALITE, UN ENJEU
MAJEUR COMMUN »**

Présentation du ComCyberGend



Com CyberGend



4 lignes directrices :



SIMPLIFICATION



COHERENCE

PERFORMANCE

LISIBILITE

Objectifs :



- Mieux anticiper les menaces de demain
- Favoriser la création d'un SCN cyber PN/GN
- Préparer un triplement des capacités cyber de la GN



Rattachement direct au DGGN, sous l'autorité du ministre de l'Intérieur



Positionnement transverse permettant de créer de la cohérence et d'animer l'ensemble des structures nationales et territoriales



Périmètre d'intervention large sur l'ensemble du territoire national et en appui des unités

Le réseau CyberGend : une allonge dans les territoires

4 piliers

Prévention et proximité numériques

Investigations et interventions numériques

Appui et opérations numériques

Stratégie et partenariats

NIVEAU DEPARTEMENTAL

- Une expertise de premier niveau
- 100 sections opérationnelles de luttres contre les cybermenaces (SOLC)
- **Coordination** des manœuvres départementales de prévention



NIVEAU REGIONAL

- Intervention sur des **investigations complexes**
- 11 antennes du C3N dans les territoires
- Structurer parcours évolutifs avec des responsabilités transverses, tant techniques que préventives



NIVEAU NATIONAL

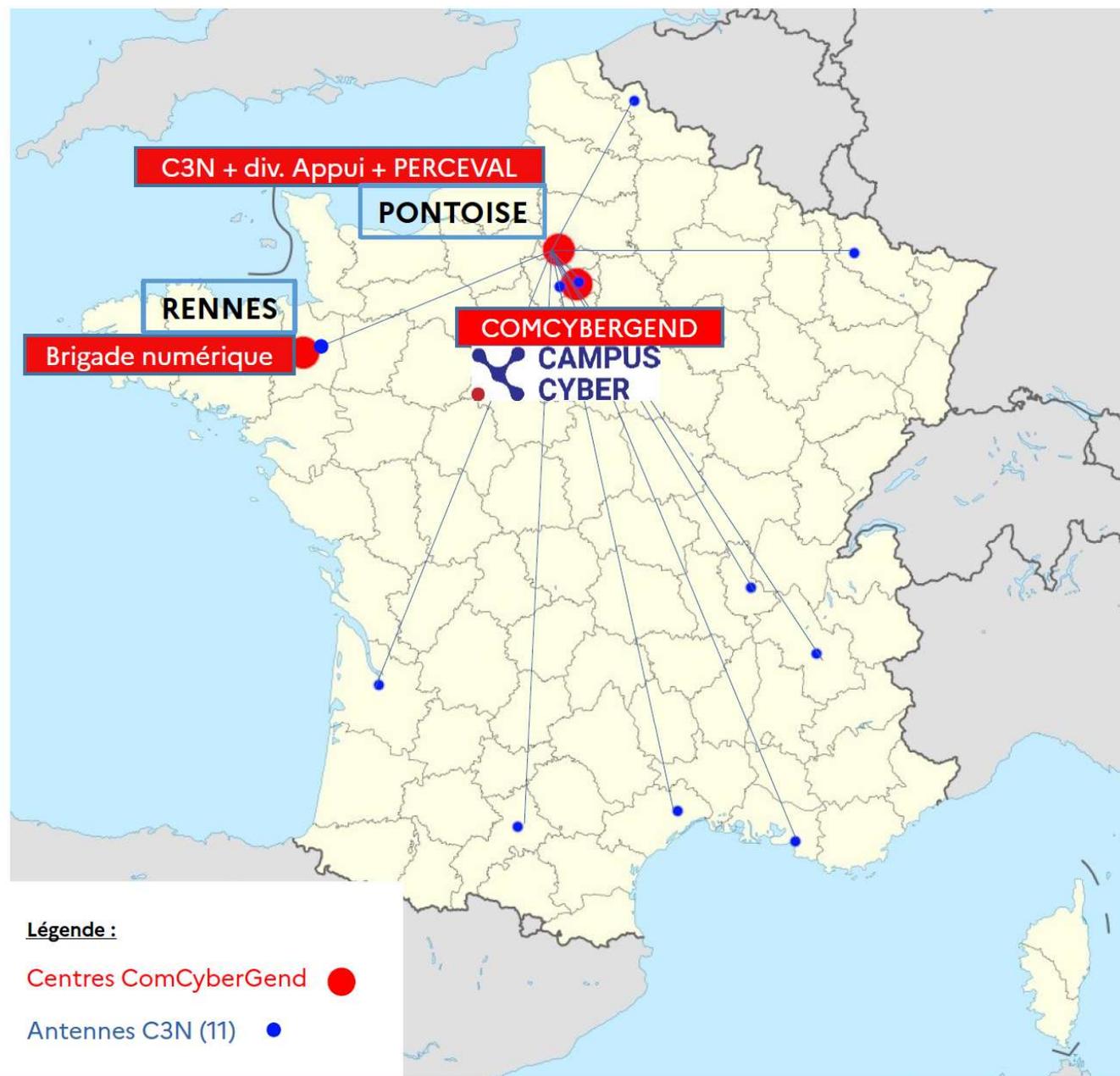
- Prise en charge et suivi des opérations du **très haut du spectre**
- Capacités d'investigations et de développement de pointe (C3N et DAONUM – central)

Une implantation géographique multisites

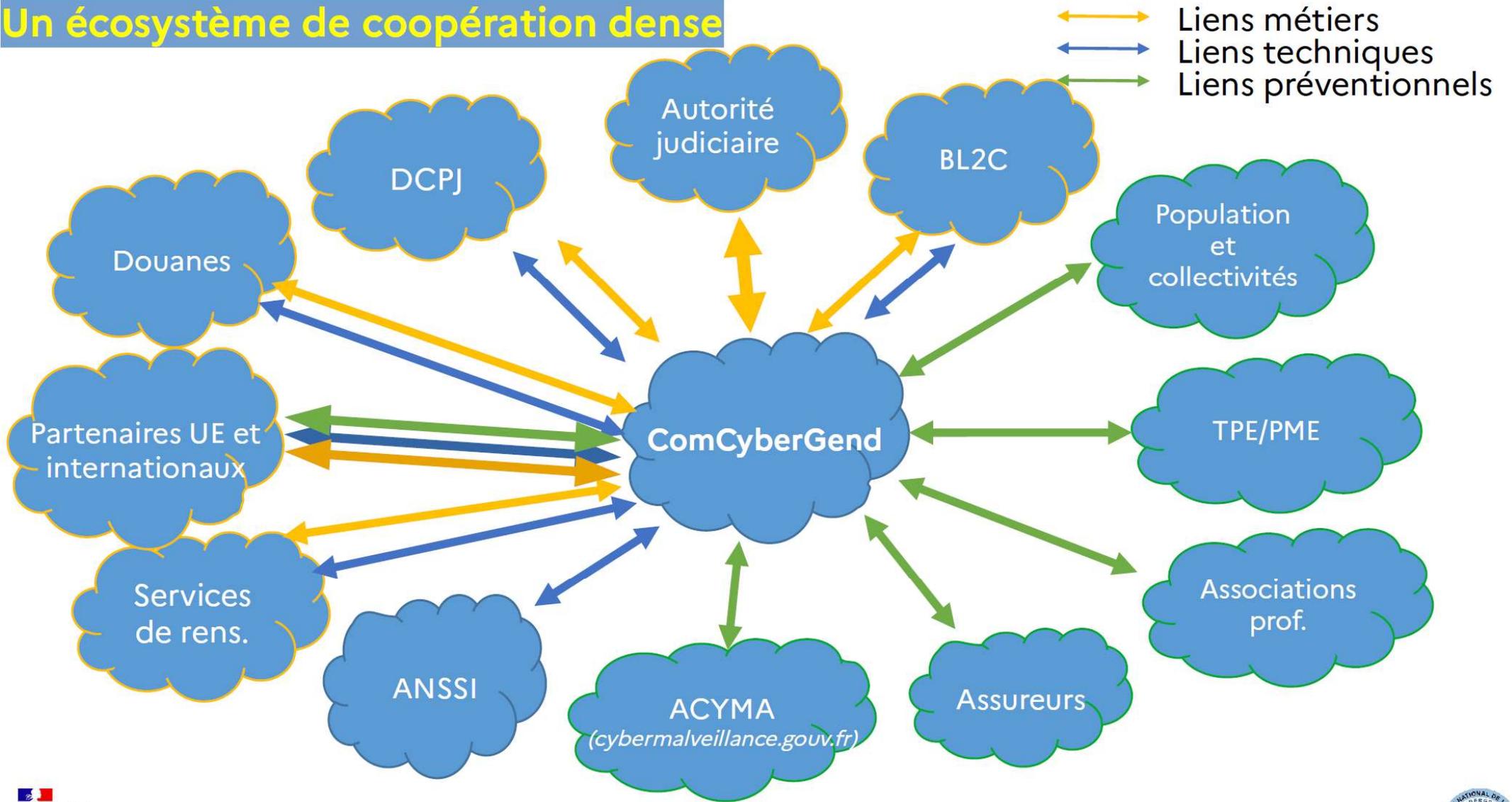
Un réseau de plus de 7 000 cyberenquêteurs (10 000 à terme)

Un réseau par ailleurs enrichi de réservistes cyber (200 aujourd'hui – 1000 à terme)

Une implantation dans tous les territoires, y compris en outre-mer



Un écosystème de coopération dense





MINISTÈRE DE L'INTÉRIEUR

*Liberté
Égalité
Fraternité*



CENTRE DE LUTTE CONTRE
LES CRIMINALITES
NUMERIQUES
- **C.3.N.**

COMCYBERGEND / C3N (Centre de Lutte Contre les Criminalités Numériques)

Organisation

30 personnels
3 départements



Département
Coordination
opérationnelle cyber

Département
Enquête cyber

Département
Enquêtes et
recherches en sources
ouvertes

Département Enquête
5 grandes thématiques traitées en relation étroite
avec EUROPOL

- G1 : Atteintes aux STAD
- G2 : Trafics illégaux sur le Darkweb (ESP)
- G3 : Crypto-actifs (FINTECH)
- G4 : Atteintes sexuelles sur mineurs (CNAIP)
- G5 : Enquêtes complexes



TABLE RONDE #1

LA RÉACTION FACE À UNE CYBER ATTAQUE

Madame Myriam QUÉMÉNER

Avocat général près de la cour d'appel de Paris, docteur en droit.

Madame Madeleine DUFRASNE

Monsieur Alexandre RADOS

Etudiants en 3ème année de l'ENSISA à Mulhouse en spécialité Informatique et Réseaux

Monsieur

Laurent VERDIER

Chargé de mission
Sensibilisation – risque cyber
– cybermalveillance.gouv.fr

Major

Florent PEYREDIEU

Chef du groupe
ASTAD – C3N

TABLE RONDE #1 LA RÉACTION FACE À UNE CYBER ATTAQUE

Major Florent PEYREDIEU

Chef du groupe ASTAD – C3N

« L'INTERVENTION OPERATIONNELLE »

Les Rançongiciels

- I. Les Rançongiciels
- II. La Cybercriminalité en chiffres
- III. La réponse face à une attaque
- IV. L'enquête judiciaire

- I Les Rançongiciels:

I. LES RANCONGICIELS



Le 1^{er} ransomware, ou rançongiciel en français, est apparu en 1989. Ce logiciel informatique malveillant, prend en otage les données.

Le rançongiciel chiffre et bloque les fichiers contenus sur un ordinateur et propose en échange d'une rançon une clé permettant de les déchiffrer.

- **Rançongiciel de verrouillage (Ransomware Lockers)** : blocage de l'accès à l'interface de l'ordinateur, toutefois il n'affecte pas les fichiers ni le système.
- **Rançongiciel bloqueurs de données (Ransomware Crypto)** : les fichiers individuels sont chiffrés

II. LES ACTEURS



- Les acteurs :

Trois types peuvent être mis en évidence :

- **Les A.P.T.** (Advanced Persistent Threat) financés et soutenus par des Etats Commanditaires
- Des **groupes cybercriminels** organisés
- Des **cyber délinquants**

III. LES TYPOLOGIES D'ATTAQUE



- Les typologies d'attaques :

Quatre types peuvent être mis en évidence :

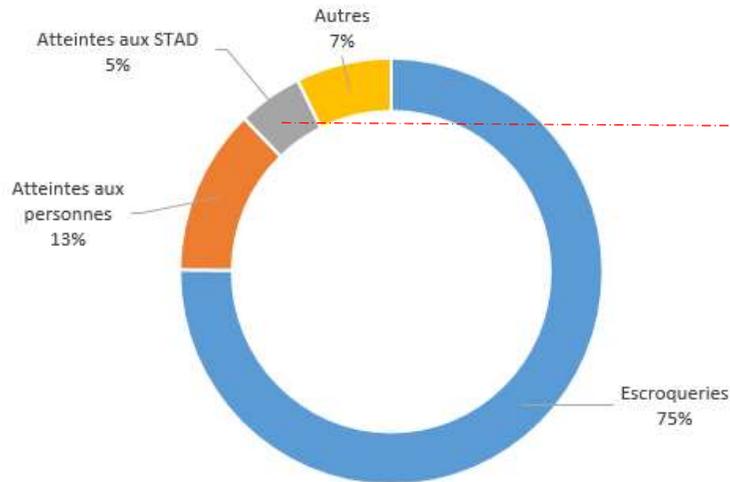
- **Attaque ciblée** dite Big Game Hunting (Chasse au gros gibier)
- **Attaque Massive**
- **La double extorsion**
- **RaaS (Ransomware-as-a-Service)**

II. LA CYBERCRIMINALITE EN CHIFFRES

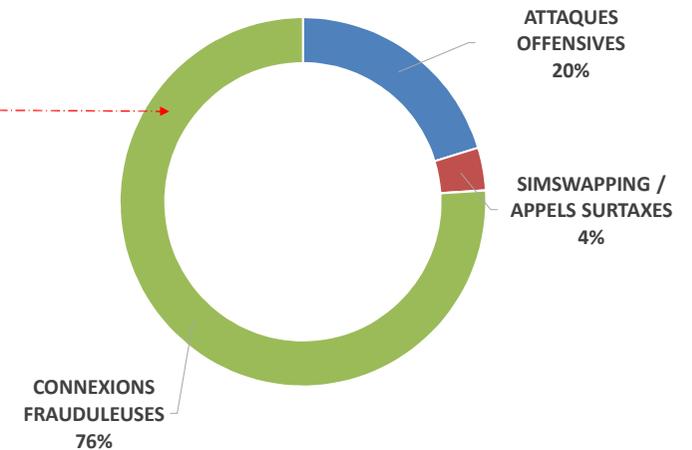


- II La CYBERCRIMINALITE:

II. LA CYBERCRIMINALITE EN CHIFFRES



Ensemble de la cybercriminalité



Atteintes aux STAD (2021)

- Les attaques par rançongiciel ne représentent que 0,5% de la cybercriminalité mais le préjudice économique et social le plus important.
- Un chiffre noir important estimé à un dépôt de plainte pour 267 attaques tentées ou réussies concernant les rançongiciels

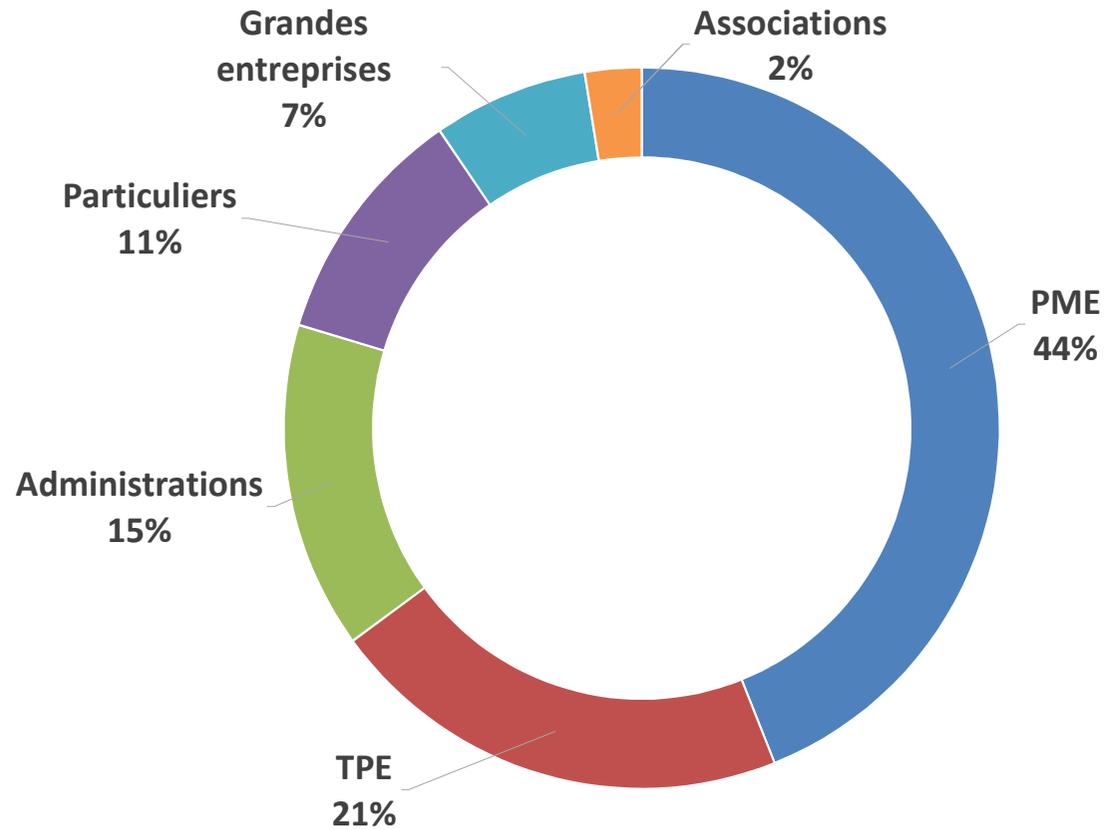
COMCYBERGEND / C3N (Centre de Lutte Contre les Criminalités Numériques)



II. LA CYBERCRIMINALITE EN CHIFFRES



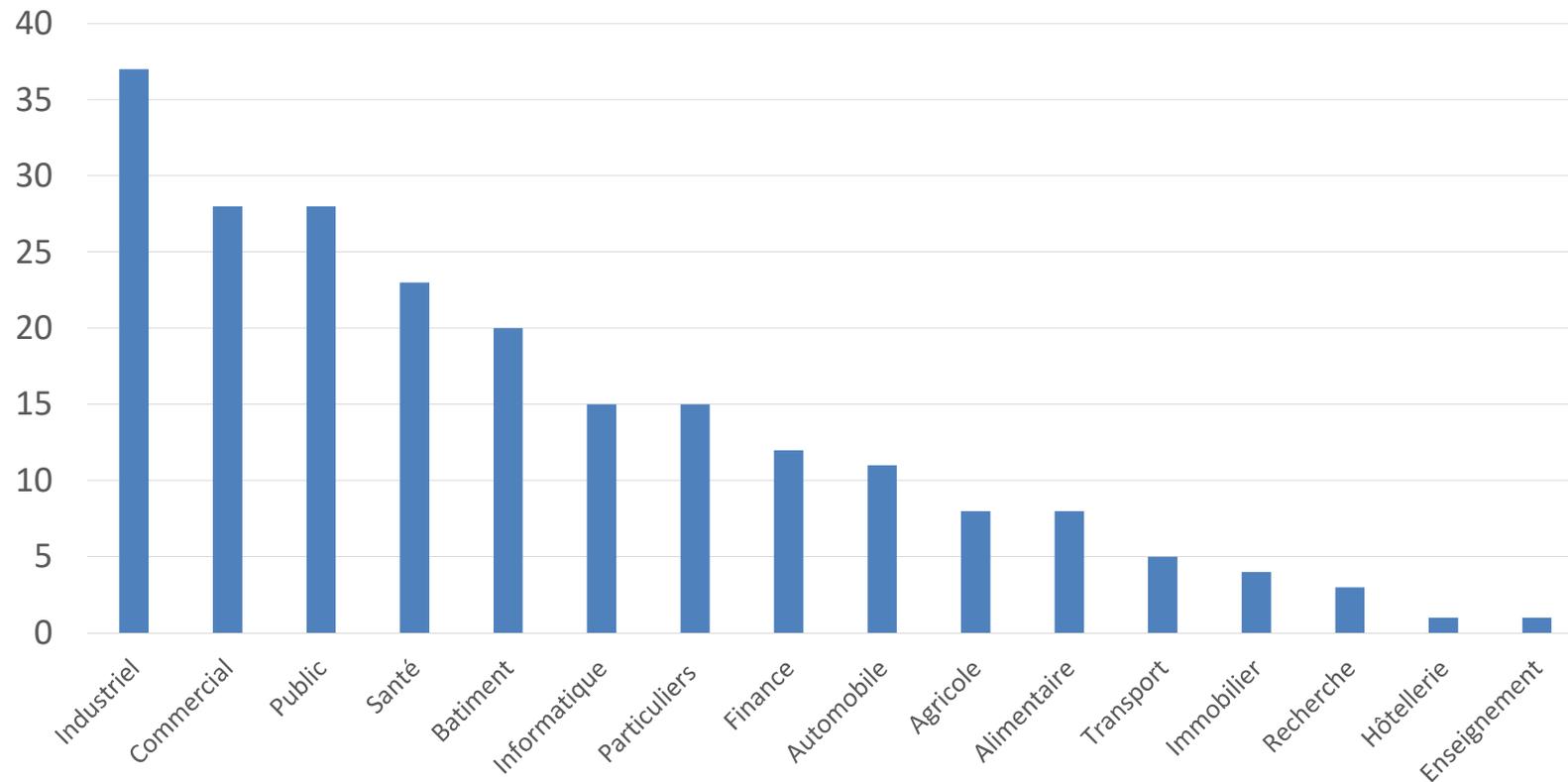
Typologie des victimes rançongiciels



II. LA CYBERCRIMINALITE EN CHIFFRES



Secteurs ciblés par les rançongiciels



- III La réponse face à une attaque :

III. LA REPONSE FACE A UNE ATTAQUE



- La réponse face à une attaque :
 - Arrêter la propagation (déconnexion du réseau des machines infectées et des sauvegardes)
 - Désinfecter l'ordinateur ou les machines
 - Ne pas payer la rançon
 - Trouver de l'assistance technique (interne ou externe)
 - Isoler les éléments techniques utiles ultérieurement (remédiation et enquête)
 - Signaler l'attaque aux autorités (Plainte, C.N.I.L., A.N.S.S.I.)
 - Consulter le site cyber malveillance

- IV L'Enquête judiciaire:

IV. L'ENQUETE JUDICIAIRE



Les enquêtes judiciaires en matière de cybercriminalité sont similaires aux enquêtes judiciaires classiques.

Elles répondent au même formalisme que ces dernières.

La particularité est qu'elles sont commises dans un univers dématérialisé, ou souvent les auteurs œuvrent depuis l'étranger.

- Délinquance internationale
- Organisation criminelle structurée
- Haute technicité

IV. L'ENQUETE JUDICIAIRE



Les leviers d'action :

- Proactivité
- Expertises techniques
- Techniques spéciales d'enquêtes
- Coopération internationale (BKA, FBI, NCA, INTERPOL, EUROPOL,.....)

Le C.3.N. :

- Direction des enquêtes à connotation cyber
- Accompagnement de la victime
- Préservation des données techniques
- Actes d'enquête utiles
- Saisie et exploitation des données techniques
- Mise en place de techniques spéciales
- Aide à la prise de décision

Merci de votre attention

TABLE RONDE #1 LA RÉACTION FACE À UNE CYBER ATTAQUE

Madame Myriam QUÉMÉNER

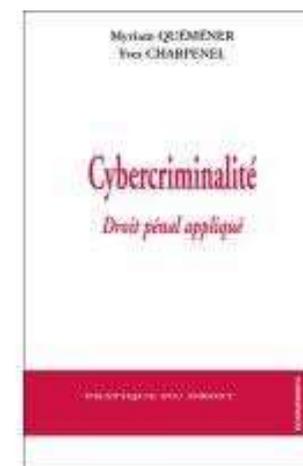
Avocat général près la cour d'appel de Paris

« LA JUSTICE FACE À LA CYBERCRIMINALITÉ :
ENJEUX ET PERSPECTIVES »



La justice face à la cybercriminalité Enjeux et Perspectives

- Myriam Quéméner avocat général près la Cour d'appel de Paris
- Docteur en droit



LES CYBERTENDANCES

- Cybercriminalité organisée et criminalité financière
- Une posture plus agressive des délinquants, avec des modes d'action relevant de plus en plus souvent de l'extorsion: *sextorsion*, rançongiciels chiffreurs de données(postes ou serveurs)
- La croissance du nombre et de l'ampleur des **détournements de données**,
- Les logiciels malveillants sont une menace croissante, avec une évolution dans le domaine des botnets bancaires
- Les FOVI qui touchent de nombreux pays occidentaux avec des formes de plus en plus sophistiquées d'accès aux informations permettant l'ingénierie sociale ;
- Les **attaques en déni de service** (DDoS) sont un mode opératoire en croissance, (requêtes massives, plus de réponse du serveur)
- Les **cryptomonnaies** (*bitcoin, ethereum monero...*) sont devenues un moyen transactionnel de choix car discret pour les échanges financiers entre cybercriminels
- **Explosion de la cybercriminalité durant la pandémie sanitaire**

Les réponses pénales : les infractions

Les accès et maintiens frauduleux dans un STAD, entrave, entente en vue de commettre une des infractions des 323-1 et ss CP

Collecte illégale de données à caractère personnel et divulgations, détournement de finalité de fichier 226-17 et ss CP

Contrefaçon de bases de données L 341-1 et L 343-4 du CPI

Escroquerie et Faux et usage de faux 313-1 et 441-1 ss CP

La fraude à la carte bancaire L.163-4 du code monétaire et financier

L'usurpation d'identité en ligne 226-4-1 CP

Le blanchiment en bande organisée 324-1 CP



Une politique pénale réaffirmée

- [Dépêche du 9 juin 2021](#) relative à la lutte contre la cybercriminalité
- Annexe 1 : [pcyberd final clean](#)
- Annexe 2 : [Compétences cyber final](#)
- Annexe 3 : [Fiche rançongiciels final v26 mai](#)
- Annexe 4 : [Canevas plainte Ransom](#)
- Annexe 5 : [Fiche Reflexe Ransom](#)
- Annexe 6 : [Jackpotting final](#)
- Annexe 7 : [Botnets final](#)
- Annexe 8 : [TheseePerc final](#)

Exemples d'affaires internationales

- **Crime organisé : un responsable du réseau crypté Sky ECC mis en examen en France**
- Un Canadien accusé d'avoir distribué des téléphones munis d'une messagerie cryptée utilisée par des réseaux criminels a été placé en détention à Paris avec son épouse.

Un des principaux distributeurs du réseau de téléphones cryptés Sky ECC, [au cœur d'investigations anticriminalité hors-norme à travers le monde](#), a été mis en examen et incarcéré vendredi à Paris, selon les informations de l'AFP, qui cite une source judiciaire. Arrêtés en Espagne début juin, le Canadien Thomas Herdman et son épouse, qui contestent les accusations, ont été mis en examen pour «*association de malfaiteurs, fourniture et importation de [moyen de cryptologie](#) en méconnaissance de la réglementation et blanchiment de trafic de stupéfiants*», a précisé la source judiciaire.

Exemples La loi du 3 juin 2016 au regard de la compétence territoriale

- ❑ Adaptation des règles de compétence territoriale du 43 CPP du PARQUET et des juridictions d'Instruction et de Jugement
 - En sus de la compétence classique (52,382,522 du CPP)
 - Domicile ou lieu d'arrestation ou de détention de l'auteur et le lieu des faits
 - tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique
 - au préjudice d'une personne résidant en France
 - est réputé commis sur le territoire national,
 - octroyant une compétence nationale concurrentes au parquet et juridiction de Paris (pôle de l'instruction, tribunal correctionnel et cour d'assises) pour l'ensemble des atteintes à un système de traitement automatisé de données.

Organisation du parquet de Paris

- **Deux nouvelles divisions**
- La troisième division, forte de dix-sept magistrats, est chargée des contentieux de très haut vol, d'une grande complexité à une très grande complexité. Elle regroupe en effet la juridiction interrégionale spécialisée, la juridiction nationale de lutte contre la criminalité organisée et la lutte contre la cybercriminalité. La deuxième division. J1 , est focalisée sur la criminalité organisée. J2 est dédiée à la criminalité financière la section dédiée à la cybercriminalité est désormais J3 , rattachée à **la Junalco**.

Quelques exemples d'affaires

- Jackpotting
- Blanchiment en bande organisée (affaire Vinnik)
- Escroquerie en bande organisée



Pour aller plus loin



Télécharger le rapport

Merci de votre attention

Myriam Quéméner - Frédérique Dalle - Clément Wierre

QUELS DROITS FACE AUX INNOVATIONS NUMÉRIQUES ?

—
LÉGISLATION, JURISPRUDENCES
ET BONNES PRATIQUES DU CYBERESPACE

—
DÉFIS ET PROTECTIONS
FACE AUX DÉRIVES DU NUMÉRIQUE

Préface de Agathe Lepage



Gualino un savoir-faire de Lextenso

TABLE RONDE #1 LA RÉACTION FACE À UNE CYBER ATTAQUE

Madame Madeleine DUFRASNE & Monsieur Alexandre RADOS

Etudiants ENSISA

**DÉMONSTRATION
« INTRUSION INFORMATIQUE ET TRACES »**

Les traces laissées par les attaques informatiques

Un ordinateur piraté est une scène de crime !



Et on ne touche pas à une scène de crime !

En revanche, il vaut mieux déconnecter l'ordinateur infecté du réseau.

Quelques traces laissées par un programme malveillant

The image displays three overlapping Windows utility windows that provide evidence of a malware program's activity:

- Observateur d'événements (Event Viewer):** Shows a log for the 'Installation' category with 76 events. The list includes several 'Information' level events from 20/10/2021, indicating the installation and execution of various files.
- Gestionnaire des tâches (Task Manager):** Shows the 'Applications' tab with a table of running processes. The process 'pirate.exe' is highlighted with a red box, showing it is using 0.5% of the CPU and 26.0 Mo of memory.
- LastActivityView:** Provides a detailed log of system activity. The entry for 'pirate.exe' is highlighted with a red box, showing it was executed at 20/10/2021 16:1... from the full path 'C:\Users\user\Dropbox\MON PC I...'. Other entries include 'instup.exe', 'AvEmUpdate.exe', 'atom.exe', 'node.exe', 'where.exe', 'WmiPrvSE.exe', 'python.exe', 'conda.exe', 'svchost.exe', and several 'POWERSHELL.EXE' instances.

Pourquoi conserver et rechercher les traces d'une intrusion ?

- Identifier la cause de l'infection ;
 - → **Donc éviter un 2e piratage utilisant la même faille !**
 - Savoir quels fichiers ou programmes ont été ciblés ;
 - → **Comprendre ce qui intéressait l'attaquant et quelles données doivent être modifiées ou considérées comme obsolètes.**
 - Avoir des informations sur l'origine de l'attaque.
 - → **Donc avoir une chance de retrouver l'attaquant et d'éviter d'autres intrusions.**
-
-

Et maintenant, une petite démonstration...



TABLE RONDE #1 LA RÉACTION FACE À UNE CYBER ATTAQUE

Monsieur Laurent VERDIER

Chargé de mission cybermalveillance.gouv.fr

« COMPRENDRE LES RISQUES ET LES MENACES
POUR MIEUX SE PROTÉGER »



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

Dispositif national de sensibilisation, prévention et d'assistance aux victimes

LES MISSIONS DU DISPOSITIF

- 1** **ASSISTER LES VICTIMES**
d'actes de cybermalveillance 
- 2** **INFORMER & SENSIBILISER**
à la sécurité numérique 
- 3** **OBSERVER & ANTICIPER**
le risque numérique 

QUI EST CONCERNÉ ?



CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES



53

**organisations
membres**
(publiques et privées)
du GIP ACYMA



1200

**prestataires
référéncés**
sur l'ensemble
du territoire



335 000

**victimes
assistées**
depuis fin 2017



47

**types d'incidents
traités**

LE PARCOURS VICTIME SUR CYBERMALVEILLANCE.GOUV.FR

DIAGNOSTIC

CONSEILS

MISE EN RELATION

TRAITEMENT

SATISFACTION

Cherche à comprendre son problème

Applique les conseils personnalisés proposés

Décide de se faire aider et sélectionne un prestataire

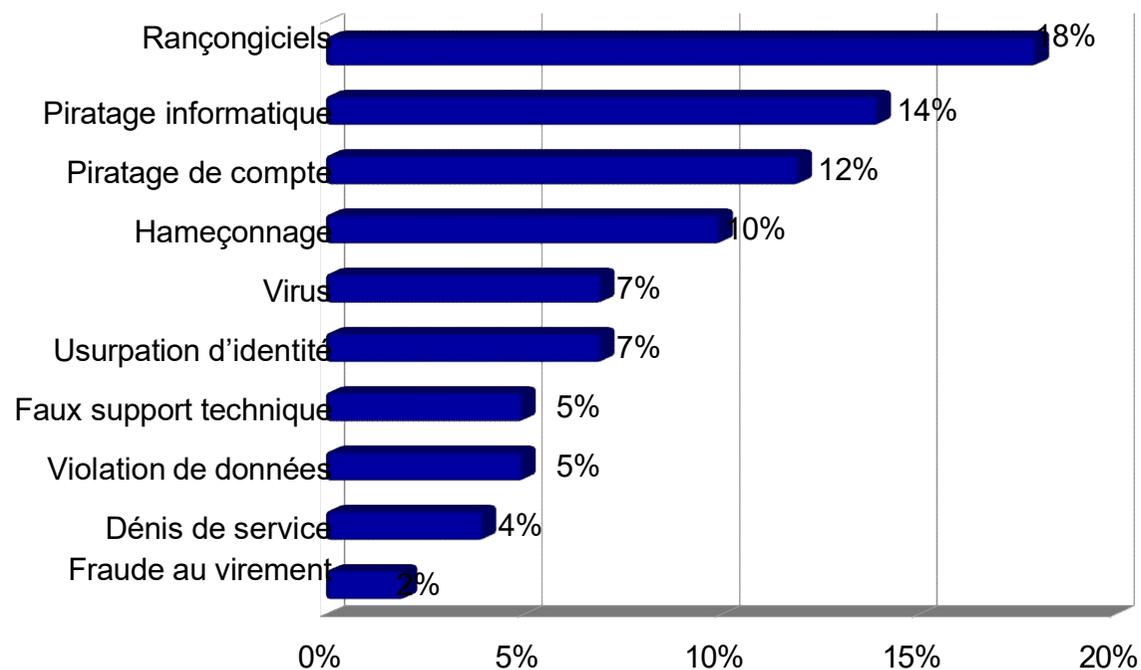
Suit la bonne exécution de la prestation

Note le service

The screenshot shows the website's navigation menu and a main content area. The navigation menu includes: LES MENACES ET BONNES PRATIQUES, L'ACTUALITÉ DE LA CYBERMALVEILLANCE, NOUS DÉCOUVRIR, and VICTIME D'UN ACTE DE CYBERMALVEILLANCE?. Below the menu, there are filters for 'DES SERVICES POUR : TOUS PUBLICS' and 'PROFESSIONNELS'. The main content area is divided into three columns: 1 - DIAGNOSTIC EN LIGNE (Victime d'acte de cybermalveillance? Nous vous aidons à qualifier votre problème), 2 - DES CONSEILS ET SOLUTIONS (Des conseils et solutions vous sont proposés pour résoudre votre problème. ET/OU Vous pouvez faire une demande de mise en relation avec un professionnel spécialisé.), and a 'CLIQUER ICI' button with a right arrow and the text 'Pour commencer' and 'En savoir plus →'.

PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Professionnels (entreprises, collectivités...) :



ALERTES ET GUIDES PRATIQUES

- Alertes régulières sur les réseaux sociaux pour nos publics

CYBERSÉCURITÉ 

**DES CENTAINES DE FAILLES DE SÉCURITÉ
CORRIGÉES DANS LES MISES À JOUR D'AVRIL**

Microsoft Windows, Exchange Server, Office, Edge, 365 Apps...
Linux Red Hat, Suse, Ubuntu
Apple iOS, iPadOS, watchOS
Google Android, Chrome, Chrome OS
Mozilla Firefox, Thunderbird
GitLab - Joomla! - OpenSSH - OpenSSL - Samba - WordPress
Cisco - Citrix - IBM - Juniper - SAP - VMware...

Mettez à jour sans tarder !
www.cybermalveillance.gouv.fr



- Publication d'articles et guides pratiques adaptés aux entreprises



PROGRAMME DE SENSIBILISATION A DESTINATION DES ÉLUS

Objectif : sensibiliser aux risques numériques et partager avec eux les bonnes pratiques

Démarche : s'inscrire dans la durée
(3 volets : octobre/février/mai)

Approche pragmatique : en contextualisant par rapport à leur quotidien pour réussir à les interpeller

Volet 1 : les principales menaces et les réflexes essentiels

Volet 2 : vigilance toutes les collectivités sont concernées !

Volet 3 : valorisation de collectivités ayant mis en place des actions de sensibilisation

Madame Sylvie Marsilly, maire de Fouras-Les-Bains (17) :

"Quelles sont les principales menaces numériques pour les collectivités ?"



Cybermalveillance.gouv.fr : en 2019, la première menace observée par le dispositif national Cybermalveillance.gouv.fr chez les collectivités et entreprises est l'hameçonnage qui représente près d'un quart des demandes d'assistance, suivi du piratage de comptes en ligne et des rançongiciels.

Madame Sylvie Marsilly : "Qui sont les auteurs de ces actes malveillants, que recherchent-ils, par où attaquent-ils ?"

Cybermalveillance.gouv.fr : les profils des cybercriminels sont très variés, suivant les finalités poursuivies : appât du gain, motivations idéologiques, politiques...
Au sein des collectivités, les principales cibles des attaques sont les systèmes d'information internes et les sites internet souvent insuffisamment sécurisés ou avec des failles de sécurité non corrigées par défaut d'application des mises à jour.

I.M.M.U.N.I.T.E. Cyber

Projet « I.M.M.U.N.I.T.É Cyber » Conjointement avec le Ministère Intérieur et l'AMF

- Outil d'autoévaluation de la sécurité numérique des collectivités
- Évaluation très rapide en 10 questions simples
- Permet une démarche proactive des collectivités
- Courrier envoyé par l'AMF à ses adhérents début septembre
- Diffusion générale de l'information au niveau de la gendarmerie

Évaluez la sécurité numérique de votre collectivité en 10 points

	OUI	NON ou NE SAIS PAS
1 Avez-vous un inventaire complet de tous vos systèmes numériques ?	<input type="checkbox"/>	<input type="checkbox"/>
2 Utilisez-vous des mots de passe solides et différents pour chaque service ?	<input type="checkbox"/>	<input type="checkbox"/>
3 Vos systèmes numériques sont-ils mis à jour en temps réel et faites-vous des sauvegardes régulières de toutes vos données ?	<input type="checkbox"/>	<input type="checkbox"/>
4 Avez-vous sensibilisé vos agents aux risques numériques ?	<input type="checkbox"/>	<input type="checkbox"/>
5 Vos postes et serveurs informatiques sont-ils protégés par un antivirus ?	<input type="checkbox"/>	<input type="checkbox"/>
6 Êtes-vous en règle vis-à-vis du Règlement Général sur la Protection des Données (RGPD) ?	<input type="checkbox"/>	<input type="checkbox"/>
7 Vos agents sont-ils équipés de matériels sécurisés pour le télétravail ?	<input type="checkbox"/>	<input type="checkbox"/>
8 Faites-vous réaliser régulièrement des évaluations de votre sécurité numérique par des outils techniques ?	<input type="checkbox"/>	<input type="checkbox"/>
9 Avez-vous un plan de secours face aux cyberattaques ?	<input type="checkbox"/>	<input type="checkbox"/>
10 ACTION À MENER	<p>Vous êtes dans le VERT : Bravo ! Votre collectivité met en œuvre les mesures essentielles. Pour aller encore plus loin et vous aider à perfectionner votre sécurité numérique, le réseau des cyber gardiens est à votre service.</p> <p>Vous êtes dans le ROUGE : Attention, votre collectivité est peut-être en danger. La gendarmerie peut vous aider à faire un état des lieux de votre sécurité numérique et à établir un plan d'actions pour renforcer votre protection.</p>	

UNE HÉSITATION ? UN DOUTE ?
Contactez votre GENDARMERIE pour un ACCOMPAGNEMENT DÉTAILLÉ

Le ministre
Le président des maires de France
Le directeur général du dispositif
cybermalveillance.gouv.fr

Paris, le

Madame la Maire, Monsieur le Maire,

Dans un souci constant d'accompagnement et de protection renforcée face aux nouvelles menaces numériques, nous avons souhaité mettre à votre disposition des outils pour vous soutenir très concrètement dans l'ouvrage de votre mandat.

Fidèlement engagé dans la stratégie gouvernementale de cybersécurité lancée en février dernier par le Président de la République, le ministre de l'Intérieur vous propose ainsi un support d'autoévaluation de la sécurité numérique de vos collectivités.

S'appuyant sur une infographie simple et accessible à tous, cet outil vise à aider les élus dans l'évaluation des faiblesses potentielles de leurs infrastructures numériques. Développé par les spécialistes en cybersécurité de la gendarmerie nationale, en lien étroit avec l'AMF et le dispositif Cybermalveillance.gouv.fr, il permet d'avoir une démarche proactive face à la menace grandissante des cybercriminels dont les collectivités locales sont très régulièrement victimes.

Cette évaluation en 10 questions simples mais fondamentales, couvrant par l'acronyme I.M.M.U.N.I.T.É.Cyber, permet à chaque élu de mesurer lui-même le niveau de sécurité numérique de sa collectivité.

Sous l'autorité des préfets, les commandants des groupements de gendarmerie de vos départements, en lien avec vos brigades de gendarmerie locales, se tiennent d'ores et déjà à votre disposition pour vous aider dans cette démarche, répondre à toutes vos questions sur les cybermenaces et vous guider dans les mesures de protection à prendre à votre niveau.

Vous pouvez également vous appuyer sur les ressources et services mis à disposition par le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr, tant pour améliorer votre niveau de sécurité numérique que pour sensibiliser vos agents et administrés, et même trouver une assistance en cas de cyberattaque.

En espérant sincèrement que cet outil réponde à vos attentes et qu'il puisse être utilisé par le plus grand nombre pour réduire les risques de cyberattaques.

Nous vous prions de croire, Madame la Maire, Monsieur le Maire, en l'expression de notre considération distinguée.

Jérôme NOTIN
Directeur général du dispositif
cybermalveillance.gouv.fr

Gérald DARMANIN
Ministre de l'Intérieur

François BAROIN
Président de l'AMF

LE LABEL EXPERTCYBER

L'objectif :

- Reconnaître l'**expertise** en sécurité numérique
- Sur les **activités** d'installation, maintenance et assistance
- Pour les clients (TPE-PME / Associations / Collectivités)

**EXPERT
CYBER**

LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr

 RÉPUBLIQUE FRANÇAISE

Pensé par et pour l'écosystème :

- Avec les représentants du secteur :
- En partenariat avec :


syntec numérique


FÉDÉRATION
EBEN
ENTREPRISES DU BUREAU
ET DU NUMÉRIQUE


CINOV
NUMÉRIQUE


Fédération Française
de l'Assurance


afnor
GROUPE

LES MENACES ET BONNES PRATIQUES

L'ACTUALITÉ DE LA
CYBERMALVEILLANCE

NOUS DÉCOUVRIR

VICTIME D'UN ACTE DE
CYBERMALVEILLANCE ?

DES SERVICES POUR : TOUS PUBLICS **PROFESSIONNELS**

1 - DIAGNOSTIC EN LIGNE



Victime d'acte de
cybermalveillance ?

Nous vous aidons à
qualifier votre problème



ET / OU



Des conseils et solutions vous
sont proposés pour résoudre
votre problème.

Vous pouvez faire une demande de
mise en relation avec un
professionnel spécialisé.

CLIQUER ICI

Pour commencer



En savoir plus →



SÉCURISER SON SYSTÈME D'INFORMATION

Sécurisez votre SI avec un
professionnel labellisé
ExpertCyber.

COMMENCER



SE PROTÉGER

Consultez nos bonnes
pratiques et conseils pour
vous protéger des
cybermenaces.

EN SAVOIR PLUS →



SIGNALER

Vous souhaitez signaler une
escroquerie en ligne ou un
contenu illicite sur Internet ?

EN SAVOIR PLUS →



DÉPOSER PLAINTÉ

Vous souhaitez déposer
plainte suite à une
cybermalveillance ?

EN SAVOIR PLUS →

ADOPTER LES BONNES PRATIQUES !

LES MOTS DE PASSE



Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.

LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX



Protégez l'accès à vos comptes, vérifiez vos paramètres de confidentialité et maîtrisez vos publications. Faites attention à qui vous parlez. Vérifiez régulièrement les connexions à votre compte.

LA SÉCURITÉ DES APPAREILS MOBILES



Mettez en place les codes d'accès. Appliquez les mises à jour de sécurité et faites des sauvegardes, évitez les réseaux Wi-Fi publics ou inconnus. Ne laissez pas votre appareil sans surveillance.

C'est...

- Gérer ses mots de passe,
- Rester maître de ses réseaux sociaux,
- Sécuriser ses outils quotidiens.

SANS OUBLIER...

LES SAUVEGARDES



Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

LES MISES À JOUR



Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.

LES USAGES PRO-PERSO



Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez. Ne mélangez pas votre messagerie professionnelle et personnelle et n'utilisez pas de service de stockage en ligne personnel à des fins professionnelles.

- La préservation des données,
- L'optimisation sécurisée des programmes et des plateformes,
- La différenciation des usages.

SENSIBILISATION ET PRÉVENTION

Objectifs :

- Sensibiliser aux risques
- Partager les bonnes pratiques
- Alerter

17 thématiques

6 types de contenus :

- Fiches pratiques/réflexes
- Vidéos
- Mémos et infographie
- Alertes sur les réseaux sociaux @cybervictimes
- Articles

Publics :

- Particuliers
- Entreprises
- Collectivités





**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



www.cybermalveillance.gouv.fr



Assistance et prévention
en sécurité numérique



@cybervictimes



@cybervictimes



@cybermalveillancegouvfr



FRC 2021

14ème édition

FRC 2021 LA PAROLE DES VICTIMES

Marko MAYERL
Inédit Théâtre

EDITION 2021



TABLE RONDE #2

GRANDIR DE NOS EXPERIENCES

Monsieur Cyril BRAS

Responsable de la Sécurité des Systèmes
d'Information (RSSI)
Grenoble-Alpes Métropole, Ville de
Grenoble et CCAS

Monsieur Stéphane FACOTTI

Responsable des systèmes
d'information
de la société Butachimie

Monsieur Olivier PIQUET

Directeur général/
CEO du groupe
LISE CHARMEL

Monsieur Sean GITTINS

Docteur en
intelligence artificielle
avancée
et en cybernétique
Oxford University

TABLE RONDE #2 GRANDIR DE NOS EXPERIENCES

Monsieur Olivier PIQUET

Directeur général/CEO du groupe LISE CHARMEL

**« TÉMOIGNAGE D'UN DIRIGEANT D'UNE
ENTREPRISE VICTIME »**

TABLE RONDE #2

GRANDIR DE NOS EXPERIENCES

Monsieur Cyril BRAS

Responsable de la Sécurité des Systèmes d'Information (RSSI)
Grenoble-Alpes Métropole, Ville de Grenoble et CCAS

« LES ENJEUX POUR UNE COLLECTIVITÉ LOCALE »



La Cybersécurité des collectivités territoriales

Cyril Bras

Vice-président INCRT

RSSI Grenoble alpes métropole & ville de Grenoble

INTRODUCTION



- Contexte : explosion des cyberattaques
- Pourquoi un tel « succès » ?
- Quels impacts ?
- Conclusion

INTRODUCTION



- Contexte : explosion des cyberattaques
- Pourquoi un tel « succès » ?
- Quels impacts ?
- Conclusion



- Une faible prise en considération du risque cyber du fait du faible nombre d'attaques avant 2019-2020
 - 2003, 2009 Toulouse : Contrefaçon de site officiel
 - 2005 Clichy Sous Bois : publication d'une fausse information (démission du maire)
 - 2009 Longjumeau : prise de contrôle d'ordinateurs municipaux
 - 2010 Gaillac & Croisilles: Dénaturation de site web
 - 2011 Reims : pénétration directe via un flux RSS

Source: Rémy Février, « *Toujours plus cyber-menacées : les collectivités territoriales* », *Sécurité globale 2015/3* (N° 3-4), p. 9-93.



CONTEXTE



- Les premières attaques d'ampleur débutent en mars 2018 aux USA
 - *Rançongiciel contre la Métropole d'Atlanta*
- *Puis commencent à frapper des collectivités françaises*
 - *Juillet 2018 La Croix Valmer (Var)*



OUTAGE ALERT

The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.

The City of Atlanta logo is located in the top right corner of the alert box. It features an eagle with wings spread, perched on a globe, with the text 'RESURGENCE' above and 'ATLANTA GA' below.

CONTEXTE



- 2019 Perfectionnement et industrialisation des attaques
- 2020-2021 Explosion des attaques contre les collectivités
 - Métropoles, villes, départements, régions



Source : Club RSSI



- Les systèmes industriels des collectivités nouvelles cibles ?
 - 25 février 2021 : Modification du dosage de soude caustique dans l'eau potable de Oldsmar en Floride
 - 28 juillet 2021 : National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems



Source : [Wikipedia](#) – [Wknight94](#) CC BY-SA 3.0



- Les systèmes industriels des collectivités nouvelles cibles ?
 - Juin 2021 : Oloron Sainte Marie, des pirates informatiques prennent le contrôle du système de relevage de la station d'assainissement et réclament une rançon



INTRODUCTION



- Contexte : explosion des cyberattaques
- Pourquoi un tel « succès » ?
- Quels impacts ?
- Conclusion

POURQUOI ?



- Renforcement de la sécurité des principaux acteurs
- Les attaquants se déplacent vers des cibles moins exposées
- De nombreuses campagnes d'hameçonnage visent les collectivités territoriales en 2018

Source : *Rapport annuel 2018 ANSSI, avril 2019*



POURQUOI ?



- La prise en compte des enjeux de Cybersécurité est très variable même si l'arrivée du RGPD a contribué à améliorer la situation
- La gestion de la SSI est trop souvent placée sous pavillon DSI entraînant une situation de juge et partie pour le RSSI
- Le budget alloué n'est pas à la hauteur

Source : Etude MIPS 2020, CLUSIF

ÉTUDE CLUSIF



Menaces informatiques et pratiques de sécurité en France

Édition 2020

- ▶ Les entreprises de plus de 100 salariés
- ▶ Les collectivités territoriales
- ▶ Les particuliers internautes



POURQUOI ?



- Les collectivités possèdent des données « intéressantes » qui ont une valeur importante à la revente
- Certaines collectivités opèrent des systèmes industriels relevant des OIV ou de la directive NIS
 - Eau potable, transport, énergie...
- Les aspects Cybersécurité sont souvent considérés comme exclusivement techniques alors qu'ils reposent sur :
 - La couche physique
 - La couche logique
 - La couche sémantique



POURQUOI ?



- « On s'est beaucoup plus concentrés sur le fait d'augmenter les services qu'on offrait à la population grâce au numérique qu'au fait de protéger l'architecture de ces systèmes. **Ça ne veut pas dire qu'on n'a rien fait, ça veut dire qu'on n'a pas mis assez d'efforts là-dessus.** »

Christophe Béchu, Maire d'Angers

Source : Brut, Victime d'une cyberattaque les services de la ville d'Angers paralysés



INTRODUCTION



- Contexte : explosion des cyberattaques
- Pourquoi un tel « succès » ?
- Quels impacts ?
- Conclusion

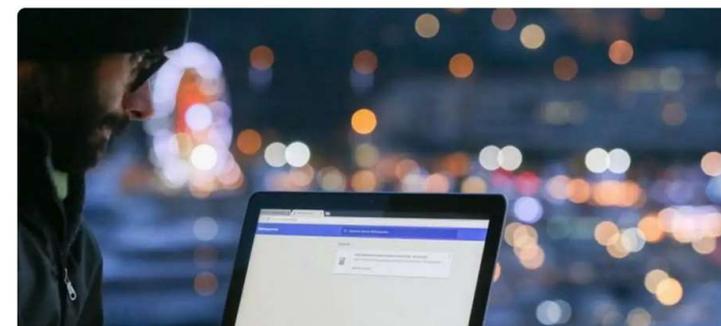
■ Typologies d'impacts

- IMPACTS SUR LES MISSIONS ET SERVICE DE L'ORGANISATION
- IMPACTS HUMAINS, MATÉRIELS OU ENVIRONNEMENTAUX
- IMPACTS SUR LA GOUVERNANCE
- IMPACTS FINANCIERS
- IMPACTS JURIDIQUES
- IMPACTS SUR L'IMAGE ET LA CONFIANCE

Cette mairie varoise victime d'une cyberattaque risque une amende de 10 millions d'euros

Depuis jeudi dernier, la mairie de la Croix-Valmer est victime d'un virus qui crypte ses données. Et avec le renforcement de la loi protégeant les données personnelles, l'amende pourrait être salée.

Andrea Morali • Publié le 02/08/2018 à 18:15, mis à jour le 08/08/2018 à 10:58



© LE DIR

- 15:40 Abonnés 07 Pr personnes é beaucoup d accueillies c
- 15:24 Les incendie créent un éq pollution atr en Corse
- 15:16 Reprise des secteurs de Grimaud
- 14:34 Incendie mc Var six sape légèrement

Source :Var-Matin

CYBERSÉCURITÉ

Les données personnelles d'agents du Grand Anancy diffusées cinq mois après la cyberattaque

Publié le 19/05/2021 • Par [Gabriel Thierry](#) • dans : [Régions](#), [Toute l'actu RH](#)

RÉSERVÉ AUX ABONNÉS



Tests « Covid-19 » ou coordonnées personnelles de plus de 1000 agents de la communauté d'agglomération ont été diffusées sur le web alternatif. Une attaque par rançongiciel avait ciblé le Grand Anancy à la fin de l'année 2020.

CYBERSÉCURITÉ

Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône

Publié le 29/07/2021 • Par [Alexandre Léchenet](#) • dans : [actus experts technique](#), [Régions](#)

RÉSERVÉ AUX ABONNÉS



Mornius / Adobestock

Lors du conseil municipal du 20 juillet, le maire de Chalon-sur-Saône a annoncé le coût de la cyberattaque subie par la ville et la communauté d'agglomération en février dernier. Plusieurs embauches sont en cours.

Source : *La Gazette des Communes*

INTRODUCTION



- Contexte : explosion des cyberattaques
- Pourquoi un tel « succès » ?
- Quels impacts ?
- Conclusion

CONCLUSION



in d t v Déclaration de vulnérabilité EN CAS D'INCIDENT ALERTES PRESSE RECRUTEMENT

ACTUALITÉS CYBERSÉCURITÉ : PROTÉGER LES SERVICES PUBLICS ET LES COLLECTIVITÉS TERRITORIALES AVEC FRANCE RELANCE

Dans le cadre du plan France Relance, l'ANSSI bénéficie d'une enveloppe cybersécurité de l'État et des territoires sur la période 2021-2022. L'objectif est de renforcer la cybersécurité de l'État, des collectivités, des établissements de santé et de développer le tissu industriel français de cybersécurité.



LES OFFRES DE SERVICE

- L'ANSSI propose aux acteurs publics :
- un dispositif de sécurisation des systèmes d'information existants
- un accompagnement financier des collectivités (CSIRT).

La démarche de l'ANSSI est destinée à bénéficier à tous les acteurs de la cybersécurité.

LES BÉNÉFICIAIRES

Label « Ville Cyber Responsable »

L'ACTU INTERCO ET TERRITOIRES DOSSIERS ET ENQUÊTES SOLUTIONS LOCALES PRATIQUE JU



Pratique

FÉVRIER 2021

Cybersécurité : un guide pour favoriser "prise de conscience" des élus

Les collectivités sont devenues des cibles d'attaques informatiques de plus en plus nombreuses. Pour sensibiliser les élus et leurs équipes à ce sujet, l'AMF et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) publient un guide leur permettant de vérifier l'état de préparation de leur collectivité tout en leur apportant des conseils méthodologiques. Les élus peuvent aussi consulter l'ANSSI (www.ssi.gouv.fr), ses régionaux et la plateforme cybermalveillance.gouv.fr (www.amf.asso.fr_ref_BW40406)



Numérique, réseaux

LES MENACES ET BONNES PRATIQUES L'ACTUALITÉ DE LA CYBERMALVEILLANCE NOUS DÉCOUVRIR VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?

Accueil → Les actualités → Article

Vigilance face aux cyberattaques : les collectivités sont toutes concernées !

Publié le 11 févr. 2021

Collectivités territoriales cyberattaque témoignage

8513 Temps de lecture : 9 min

« DANS CE COMBAT PERMANENT, QUE L'ON PEUT CROIRE À TORT EXCLUSIVEMENT TECHNIQUE, LA VICTOIRE APPARTIENT À CELUI QUI SAURA SE RENOUVELER ET INNOVER, TANT DANS SES MODES D'ACTION QUE DANS SES ORGANISATIONS. »

GUERRILLA 2.0 BERTRAND BOYER #SNC3

**MERCI DE VOTRE
ATTENTION**

 **IN.CRT**
CYBER - RESILIENCE - TERRITOIRES

- GENERAL (2S) MARC WATIN - AUGOUARD - PRÉSIDENT
- M. CYRIL BRAS - VICE- PRÉSIDENT
- M. ERIC LAMBERT - DIRECTEUR GENERAL
- WWW.CYBERTERRITOIRES.FR

TABLE RONDE #2

GRANDIR DE NOS EXPERIENCES

Monsieur Stéphane FACOTTI

Responsable des systèmes d'information
de la société Butachimie

**« RETOUR D'EXPERIENCE ET PREVENTION DU
RISQUE CYBER À BUTACHIMIE »**

November 8, 2021

Stephane FACOTTI / RSI

CYBERSÉCURITÉ : Retour d'expérience et Prévention du risque cyber



Confidentiel – Propriété de Butachimie


Fabrication du **Nylon 6-6**

Butachimie : une Joint Venture de 45 ans



Propriété de Butachimie

La Fabrication d'intermédiaires pour le Nylon 6.6

Production :



35%
capacité
mondiale
d'ADN

**Site Butachimie
de Chalampé**

INVISTA: Propriétaire de la Technologie ADN

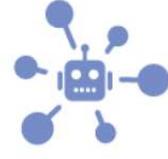
BASF: Propriétaire de la Technologie HMD

Propriété de Butachimie

La cybersécurité – les menaces à Butachimie

TOP 15 CYBER THREATS



1  Malware	2  Web-based attacks	3  Phishing	4  Web application attacks	5  Spam
6  DDoS	7  Identity theft	8  Data breach	9  Insider threat	10  Botnets
11  Physical manipulation, damage, theft and loss	12  Information leakage	13  Ransomware	14  Cyberespionage	15  Cryptojacking

* Agence de l'Union européenne pour la cybersécurité

Propriété de Butachimie

Attaques fréquentes

Attaques à fort potentiel de gravité

La cybersécurité – les menaces à Butachimie

Retour d'expérience des attaques du mois de septembre 2021

Type d'attaques :	Fréquence	Origine
Botnet *	5x /mois	Canada
Cheval de Troie	3x / mois	Allemagne
Vulnérabilité logiciel	1x / mois	Angleterre
Vulnérabilité OS * + Réseau	9x / mois	US

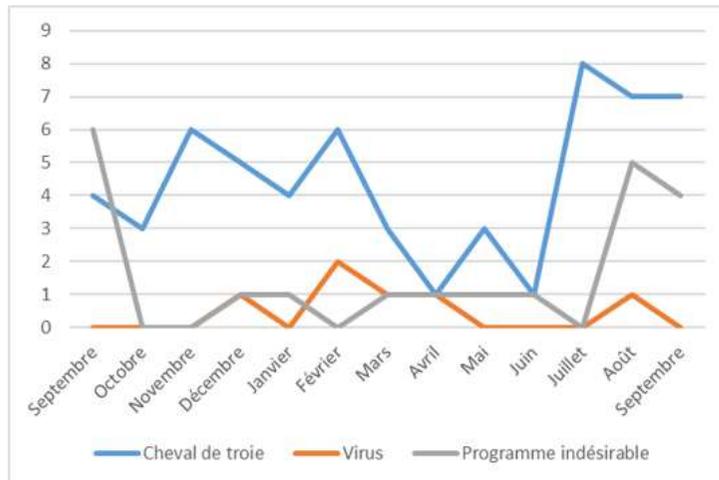
* Botnet : Programme type Robot

* OS : Windows 10

Propriété de Butachimie

Exemple Statistiques: Anti-virus / Poste PC utilisateur

Type de menace	Septembre	Octobre	Novembre	Décembre	Janvier	Février	Mars	Avril	Mai	Juin	Juillet	Août	Septembre
Cheval de troie	4	3	6	5	4	6	3	1	3	1	8	7	7
Virus	0	0	0	1	0	2	1	1	0	0	0	1	0
Programme indésirable	6	0	0	1	1	0	1	1	1	1	0	5	4



Aucun virus sur le mois de Septembre.
Nouveaux utilisateurs par rapport au mois précédent
Sensibilisation des personnes effectuée.

Propriété de Butachimie

La cybersécurité – notre socle

- Disposer d'un Corpus permettant de traiter globalement les risques cyber
- PSSI (Plan de Sécurité du Système d'Information)

Politique de Cybersécurité:
Charte IT
Formation nouvel arrivant
Politique d'architecture réseau et autres composants IT
Analyse de risque (Classe 1, 2, 3)

Plan de continuité (PCA ou PRA)
Sauvegarde journalière et externalisation
Processus de réponse à une attaque (gestion de crise)
Un contact avec ANSSI

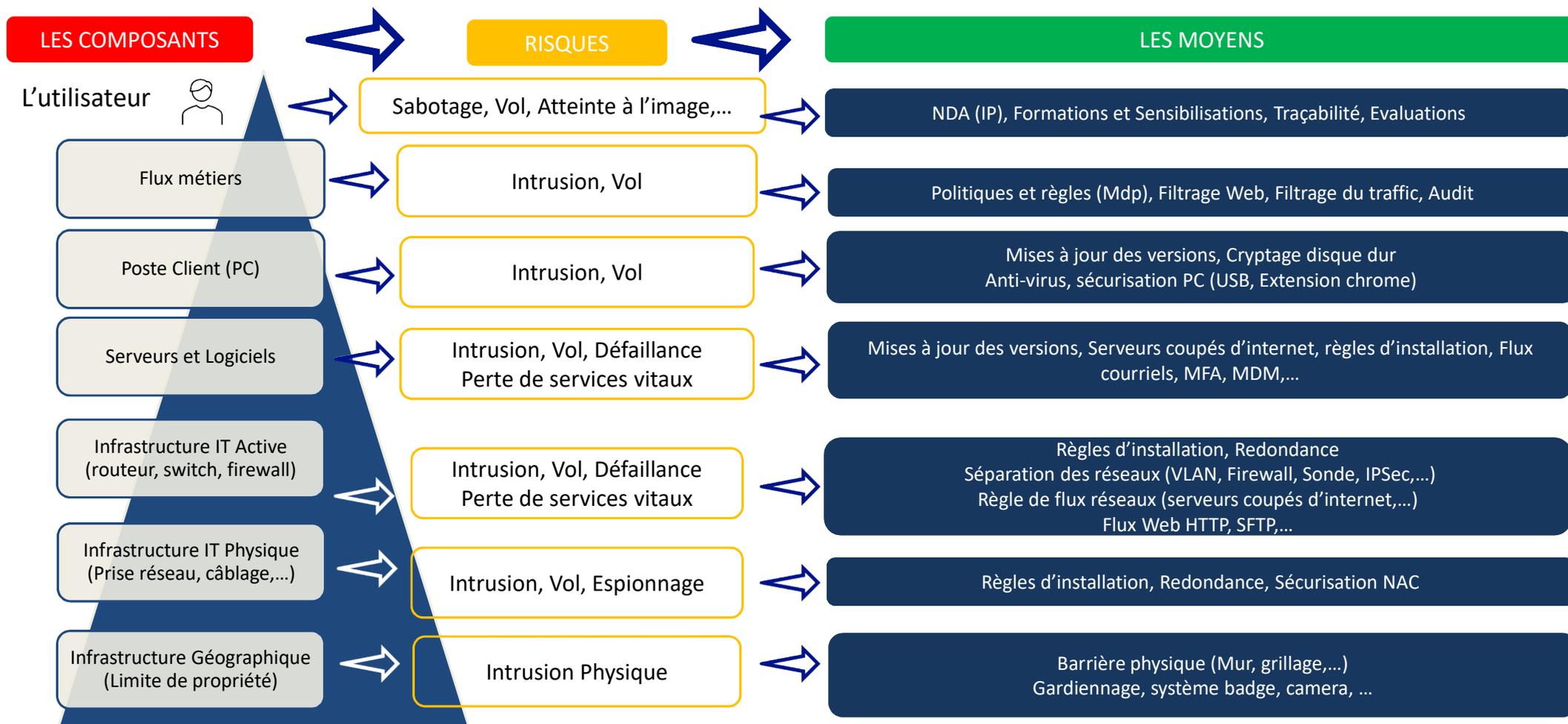
IT *

OT *

- IT : Information Technology
- OT : Opérational Technology

Propriété de Butachimie

La cybersécurité : nos réponses



Propriété de Butachimie

TABLE RONDE #2

GRANDIR DE NOS EXPERIENCES

Monsieur Sean GITTINS

Docteur en intelligence artificielle avancée et en
cybernétique
Oxford University

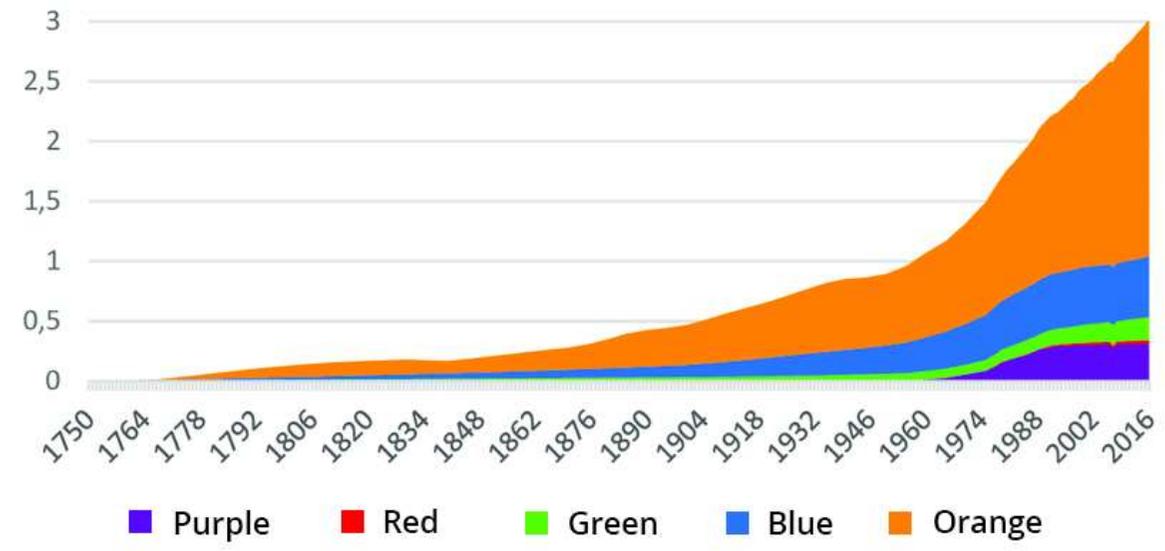
« RETOUR D'EXPERIENCE »

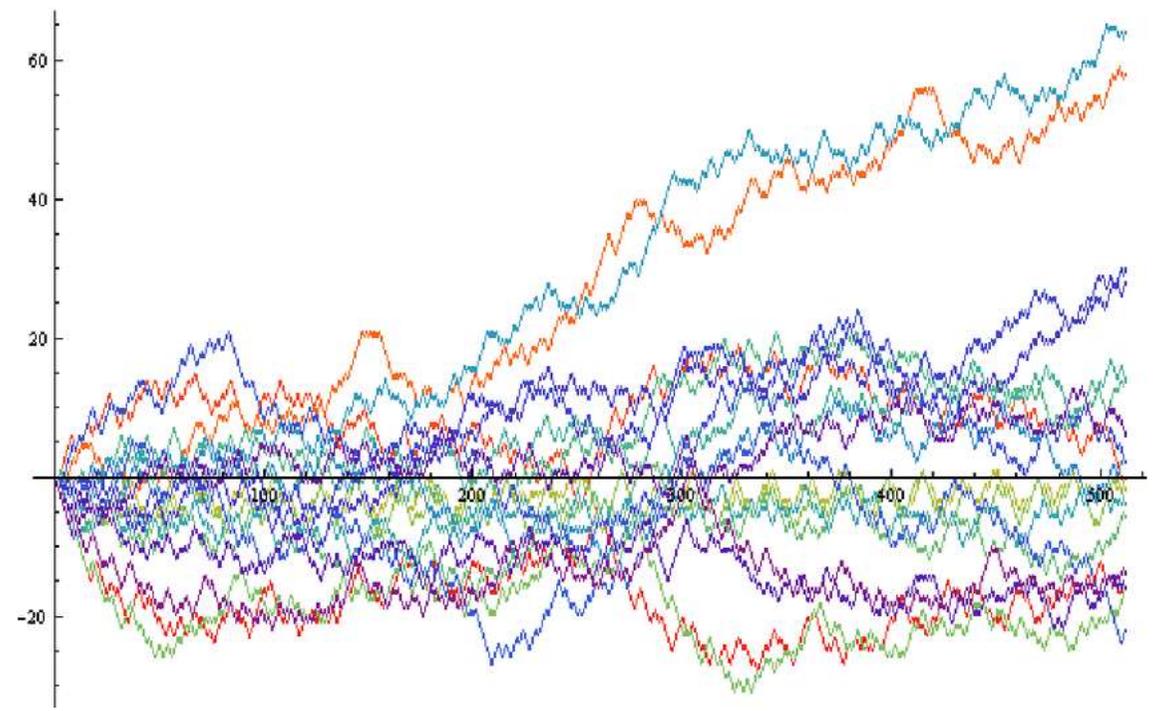


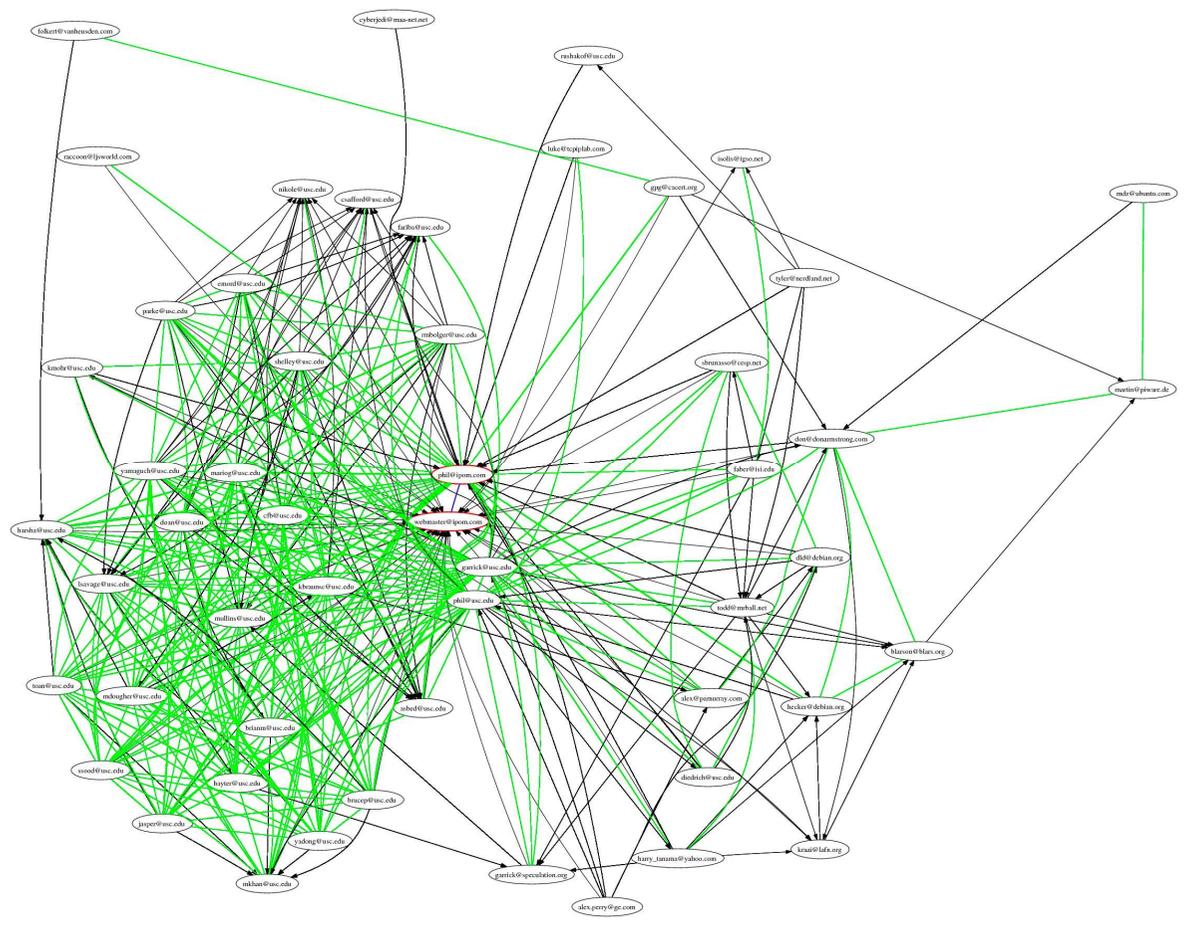
Sean Gittins
Doctor in Advanced Artificial Intelligence and Cyber Buffering

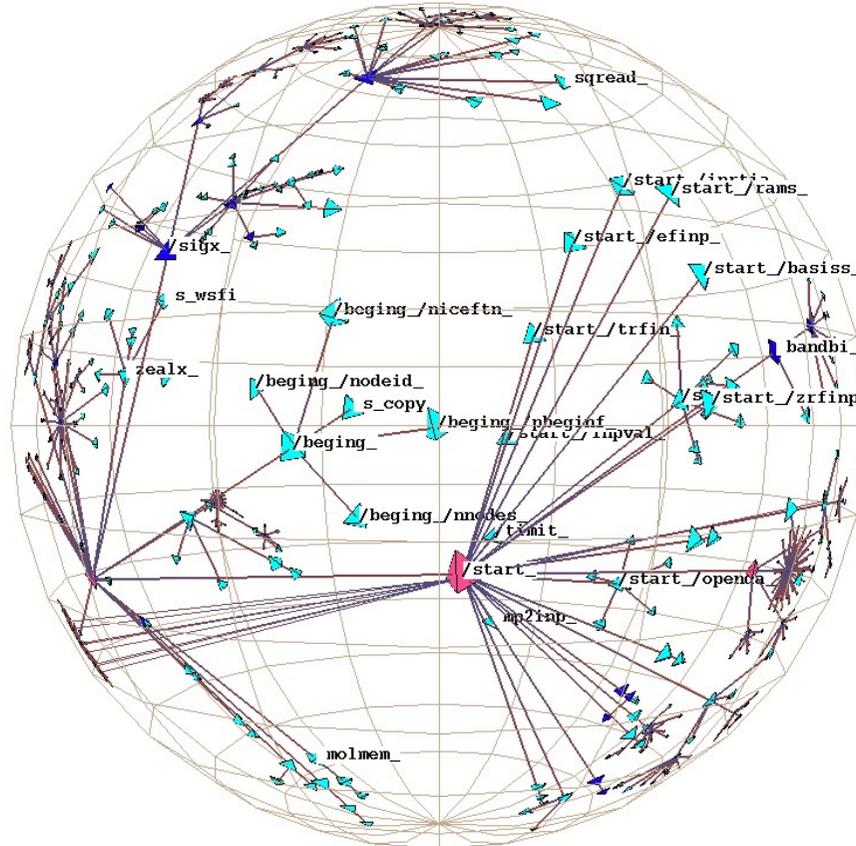


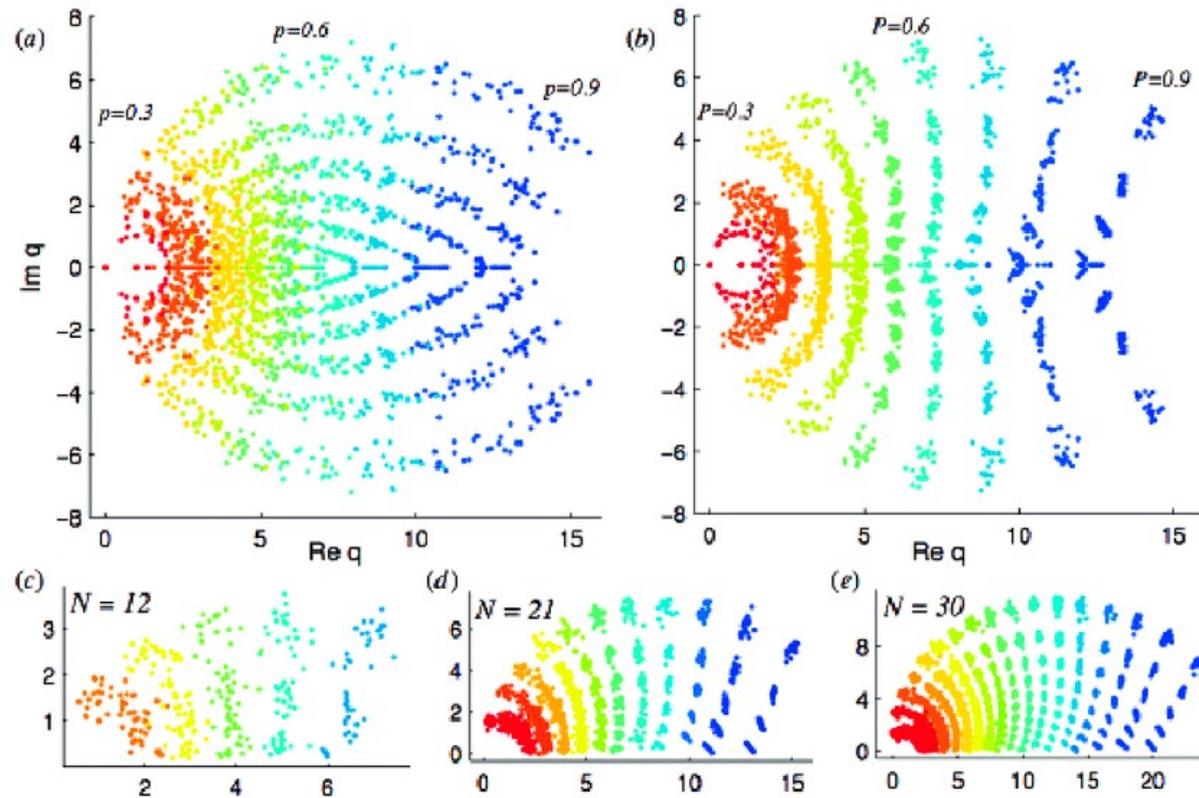
Sean Gittins
©2021

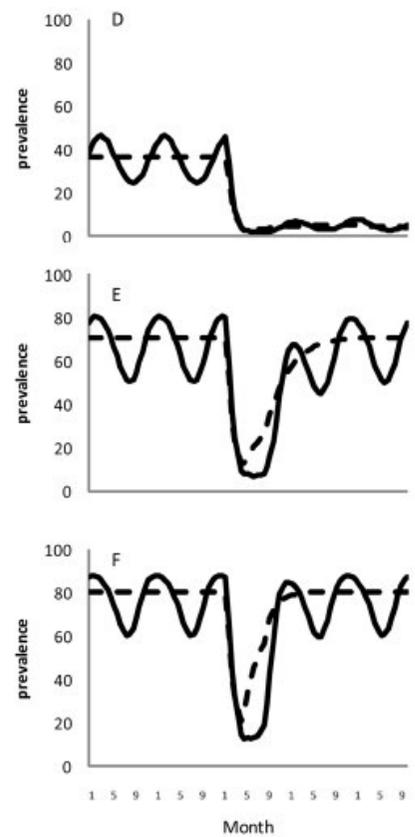
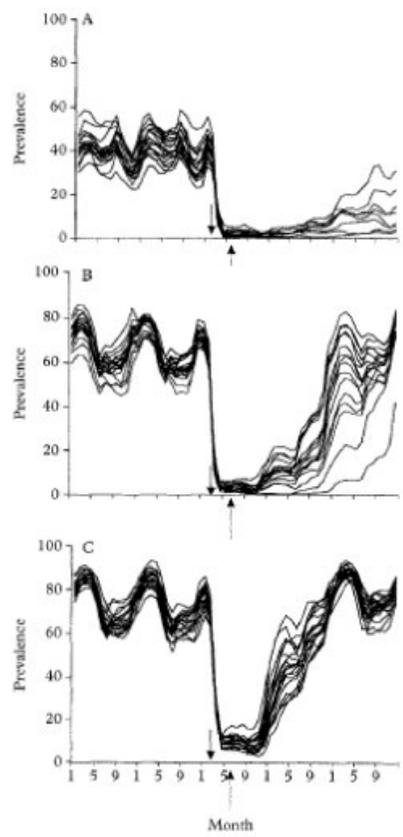


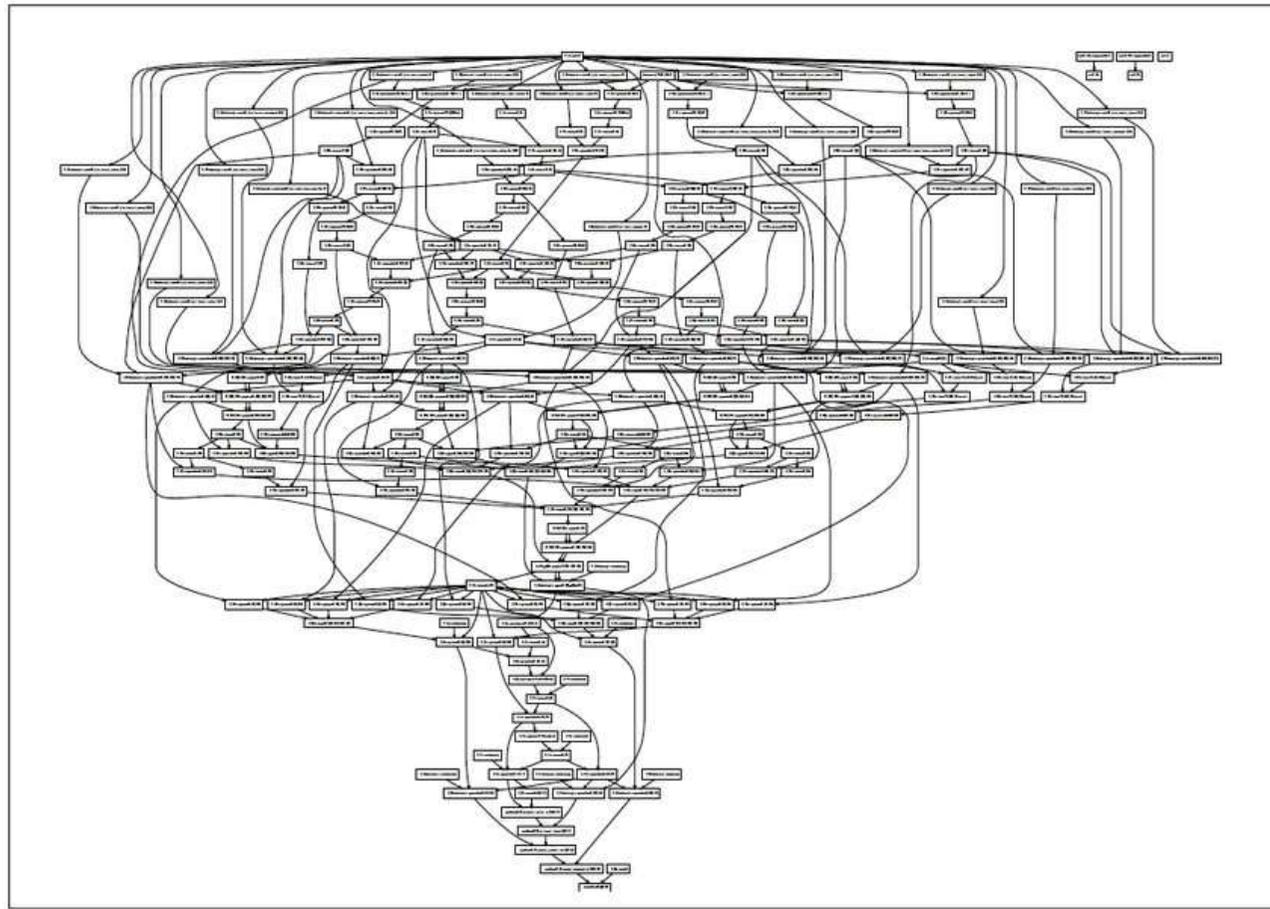


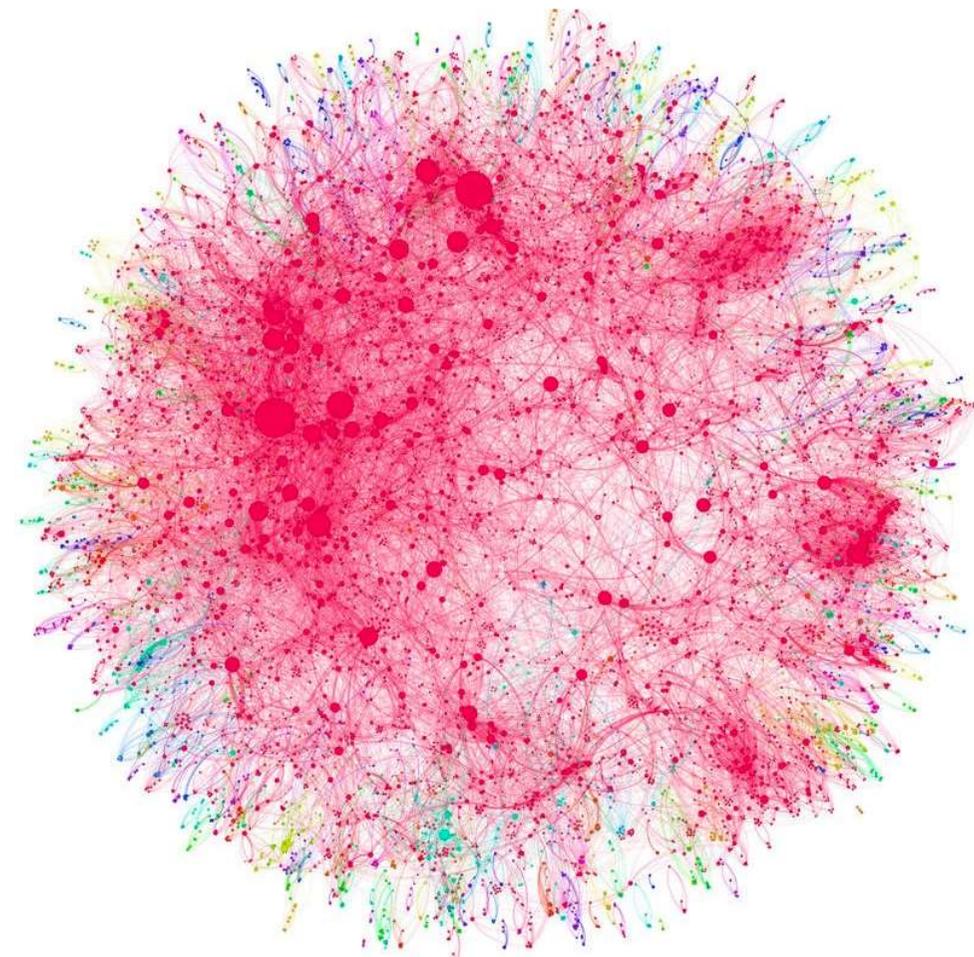
















Sean Gittins
Doctor in Advanced Artificial Intelligence and Cyber Buffering



Sean Gittins
©2021



CONFÉRENCE DE CLOTÛRE

Général d'armée (2S)

Marc WATIN-AUGOUARD

Fondateur du Forum International de la
Cybersécurité (FIC)

Président de l'Institut National pour la
Cybersécurité et la Résilience des Territoires

LA GENDARMERIE, LA RCDS & AD HONORES

**Général
Jude VINOT**

**Monsieur
Gilbert GOZLAN**

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



Président association AD HONORES



FRC 2021 : REMERCIEMENTS

A hand is shown holding a glowing globe. The globe is composed of a wireframe mesh and is surrounded by a network of white dots connected by thin lines, creating a digital or network-like appearance. The background is dark blue with a gradient and some bokeh light effects.

L'équipe d'organisation

Elony GONCALVES
Emmanuelle HAASER
Ludovic HAYE
Hervé HUMBERT
Sophie MARTIN
Didier SCHERRER
Jonathan WEBER

Daniel GUINIER
Margot HARTOIN
Isabelle HUCK
Col. Didier LIMET
Adj. Pierre MEYER
Adj. Elena VALLEJO

FRC 2021 : REMERCIEMENTS

Laurent SALLES



FRC 2021 : REMERCIEMENTS



Marko MAYERL
Sean GITTINS

15ème FRC 08/11/2022

www.adhonores.alsace

