Sécurité du numérique : enjeux et réponses pour une utilisation sereine de l'informatique

Olivier Levillain– ANSSI

Espace Mendès France – Poitiers – 15 Décembre 2017

Présentation

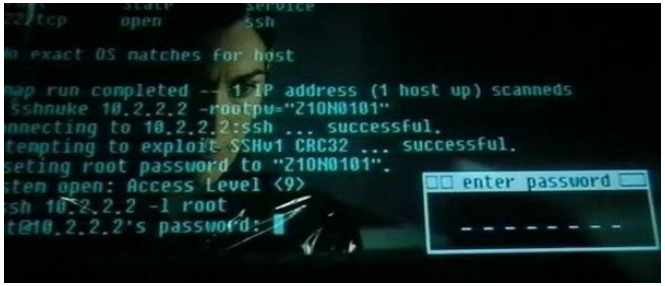
Olivier Levillain, un pictavien

- Féru d'informatique depuis tout petit
- Dans la sécurité des systèmes d'information depuis plus de 10 ans
- Et à l'ANSSI en particulier
  - Membre des laboratoires (2007-2014)
  - Thèse soutenue sur le protocole SSL/TLS (2016)
  - Responsable du centre de formation (depuis 2015)
- Mon sujet : la SSI (devenue cybersécurité, puis sécurité du numérique)

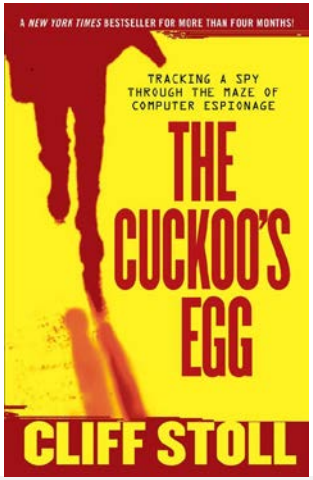
LA SÉCURITÉ DU NUMÉRIQUE : MYTHES ET RÉALITÉS

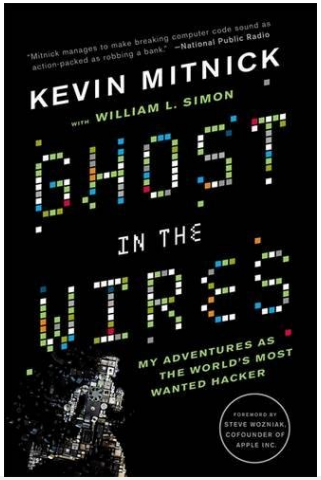
La sécurité informatique

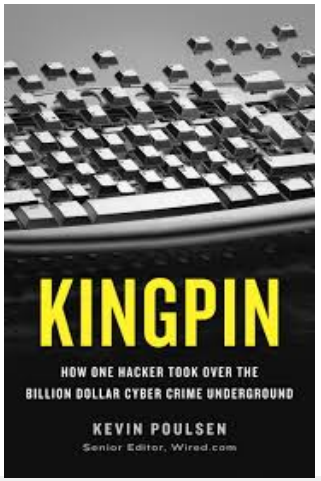
Un sujet populaire dans l'imaginaire



Et dans la littérature







Vu dans la presse : Stuxnet (2010)

Virus introduit pour saboter des centrifugeuses

- Objectif : ralentir le programme nucléaire iranien
- Prise de conscience sur les risques encourus par ces systèmes « industriels »

Vu dans la presse : l'affaire Snowden (2013)

Edward Snowden

- Ancien contractuel pour la NSA
- Un lanceur d'alerte à l'origine de la fuite de nombreux documents
- La réalité sur l'espionnage par certaines agences de renseignement dépasse (ou rejoint) la fiction

Vu dans la presse : Heartbleed (2014)

Faille critique dans OpenSSL

- Une bibliothèque logicielle sur laquelle repose en grande partie la sécurité d'internet
- Possibilité pour un attaquant d'obtenir facilement des secrets échangés sur le web
- Première occurrence d'une telle médiatisation (site web, logo, etc.)

Vu dans la presse : prise de contrôle d'une voiture (2015)

Travaux de Charlie Miller et Chris Valasek à BlackHat 2015

- Prise de contrôle complet d'une voiture à distance
- Cause : nos voitures deviennent de véritables ordinateurs connectés, mais non sécurisés

Vu dans la presse : Wannacry (2017)

LES MENACES

Motivations et profils d'attaquants

LUCRATIVE

Cyber-mercenaires
Officines
Escrocs

IDÉOLOGIQUE

Hacktivistes
Cyber-terroristes
Cyber-patriotes

ÉTATIQUE

Unités spécialisées

LUDIQUE

Adolescents désœuvrés ou non (script-kiddies)

TECHNIQUE

Hackers chevronnés

PATHOLOGIQUE

Vengeurs
Employés mécontents

Finalités poursuivies

ATTEINTE À L'IMAGE

CYBER CRIMINALITÉ

ESPIONNAGE

SABOTAGE

Évolution récente des attaques génériques

On distingue traditionnellement attaques génériques et attaques ciblées

- Depuis plusieurs années, recrudescence des attaques génériques, parfois dévastatrices

- Tout le monde est une cible potentiellement intéressante
  - Les états
  - Les grands groupes, mais aussi
  - Les petites entreprises
  - Les particuliers

- Exemple récent : les rançongiciels

Le rançongiciel Wannacry

vague mondiale d'infections par le rançongiciel WannaCry

- **Propagation** : vulnérabilité disposant d'un correctif de sécurité peu appliqué

- Réutilisation d'un **code d'exploitation** divulgué sur Internet en avril 2017

Une multitude de secteurs touchés dans le monde

Energie

GAS NATURAL et IBEROLA (gaz naturel) en Espagne

Administration civile

MINISTÈRE DE L'INTÉRIEUR et BANQUES en Russie

Santé

NATIONAL HEALTH SERVICE au Royaume-Uni

Industrie

RENAULT en France

Transport

DEUTSCHE BAHN

Telecom

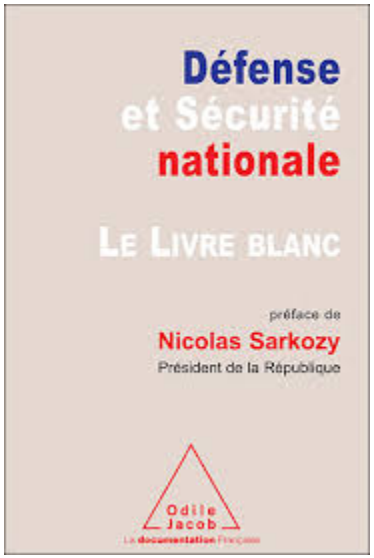
TELEFONICA
PORTUGAL TELECOM

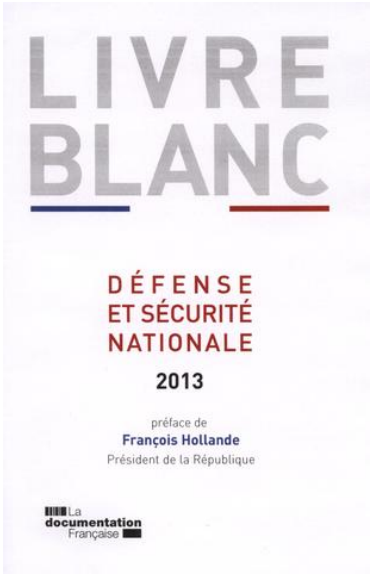
Petya / NotPetya

- Dépasse largement le cadre d'un rançongiciel
- Volonté de nuire, de détruire, de bloquer, de saboter
- Moins de victimes que WannaCry mais plus gravement touchées
- Saint-Gobain estime sa perte de CA à **250 millions d'euros**

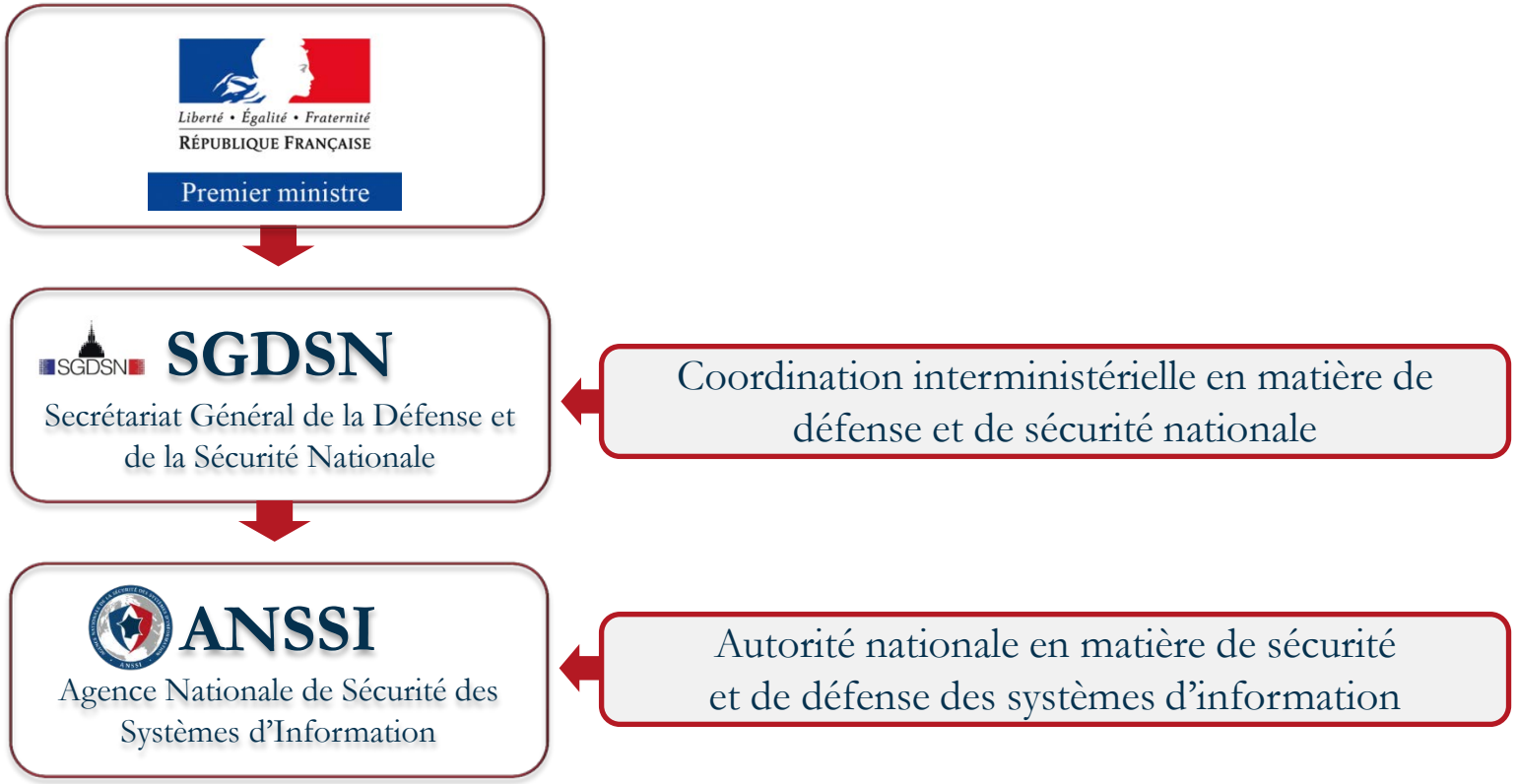
L'ANSSI

Prise en compte de la sécurité du numérique





Positionnement de l'ANSSI



Créée le 7 juillet 2009 par le décret n°2009-934, l'ANSSI est un **service à compétence nationale.**

Deux principaux domaines de compétences

-> Autorité de sécurité (prévention)

-> Autorité de défense (réaction)

~~-> Renseignement~~

~~-> Actions offensives~~

ACCOMPAGNER

500 interventions
menées en région

SOUTENIR

CONNAÎTRE & ANTICIPER

59 audits et contrôles
de sécurité

COOPÉRER, PROMOUVOIR

+120 rencontres internationales

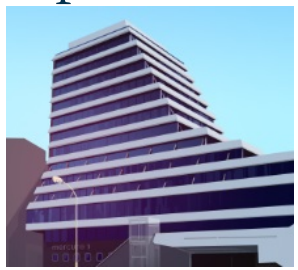
INFLUENCER & PILOTER

DÉFENDRE

20 opérations majeures de cyber-défense

Le centre de formation à la SSI

- Mission traditionnelle : former les agents du secteur public
  - 1700 personnes par an
  - Centre de formation à Paris (15e arrondissement)



- CyberEdu

CyberEdu
La sécurité par l'enseignement supérieur des NTIC

- SecNum*edu*

SecNumedu
ANSSI

- SecNum*académie*

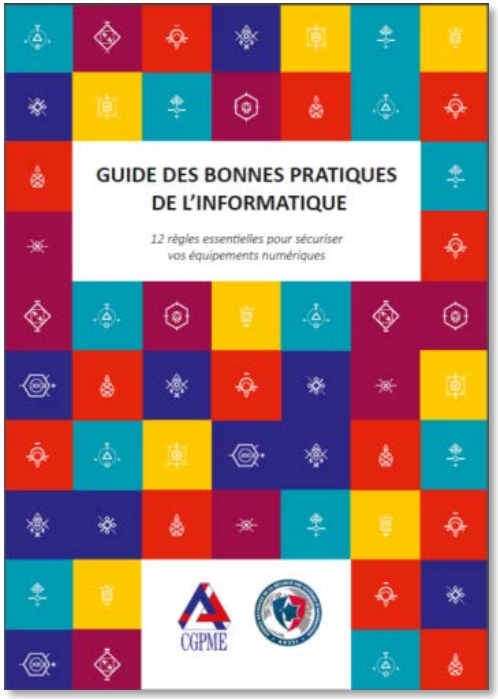
SecNum académie
ANSSI

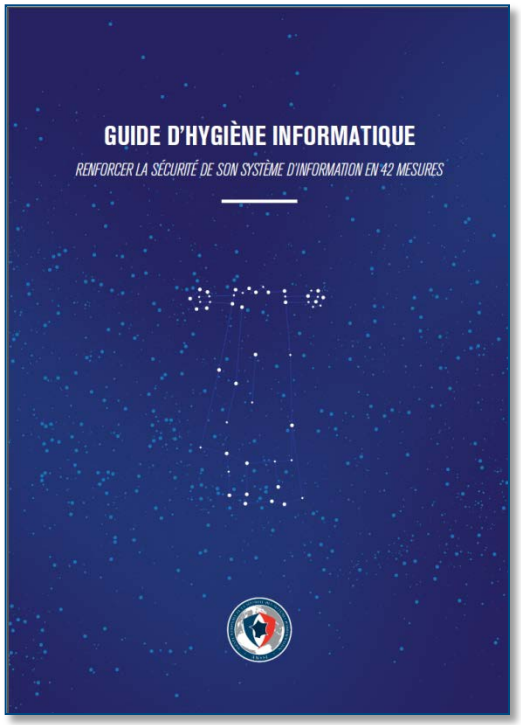
CONSTATS ET RECOMMANDATIONS

Pourquoi les attaques réussissent-elles ?

- Systèmes et applications pas à jour
- Politique de gestion des mots de passe insuffisante
- Pas de séparation des usages (utilisateur/administrateur) et des réseaux
- Laxisme dans la gestion des droits d'accès
- Absence de surveillance des SI
- Pas d'anticipation des menaces souvent pour des raisons financières
- Cloisonnement insuffisant des systèmes (propagation latérale)
- Nomadisme / télétravail incontrôlés
- Sensibilisation et maturité insuffisantes des utilisateurs

CONSEILS ET SENSIBILISATION





www.ssi.gouv.fr
www.cert.ssi.gouv.fr

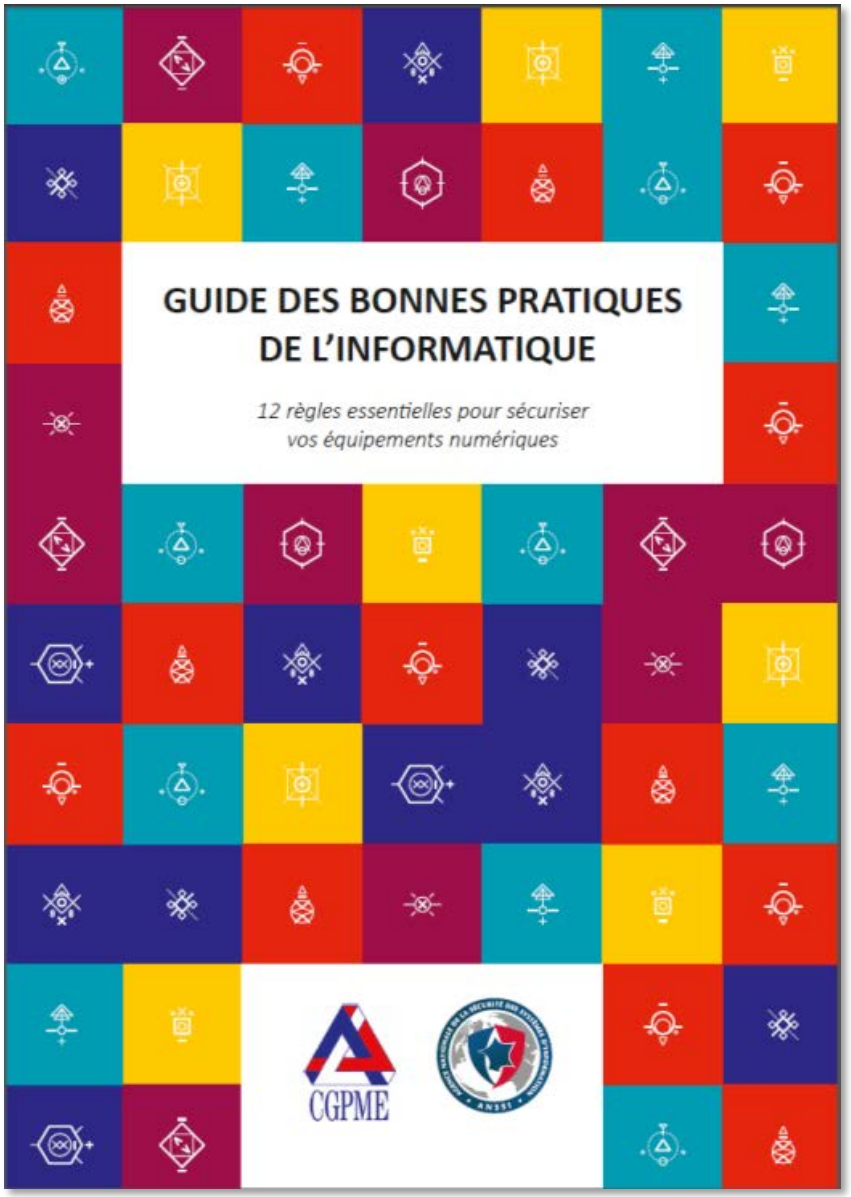


TABLE DES MATIERES

1

Choisir avec soin ses mots de passe

2

Mettre à jour régulièrement vos logiciels

4

Effectuer des sauvegardes régulières

8

Être prudent lors de l'utilisation de sa messagerie

L'hygiène informatique

- Objectif de ces guides d'hygiène informatique : un premier niveau de conscience et de prise en compte de la menace

- La sécurité est l'affaire de tous
  - Particuliers
  - Utilisateurs de l'informatique en milieu professionnel
  - Acteurs du système d'information (administrateurs, développeurs)
  - Spécialistes en sécurité du numérique

- Au-delà, il faut se rappeler que la sécurité n'est pas absolue

SECNUM*ACADÉMIE*

SecNum
académie

ANSSI

SecNum*académie*

Modules de sensibilisation à la sécurité du numérique

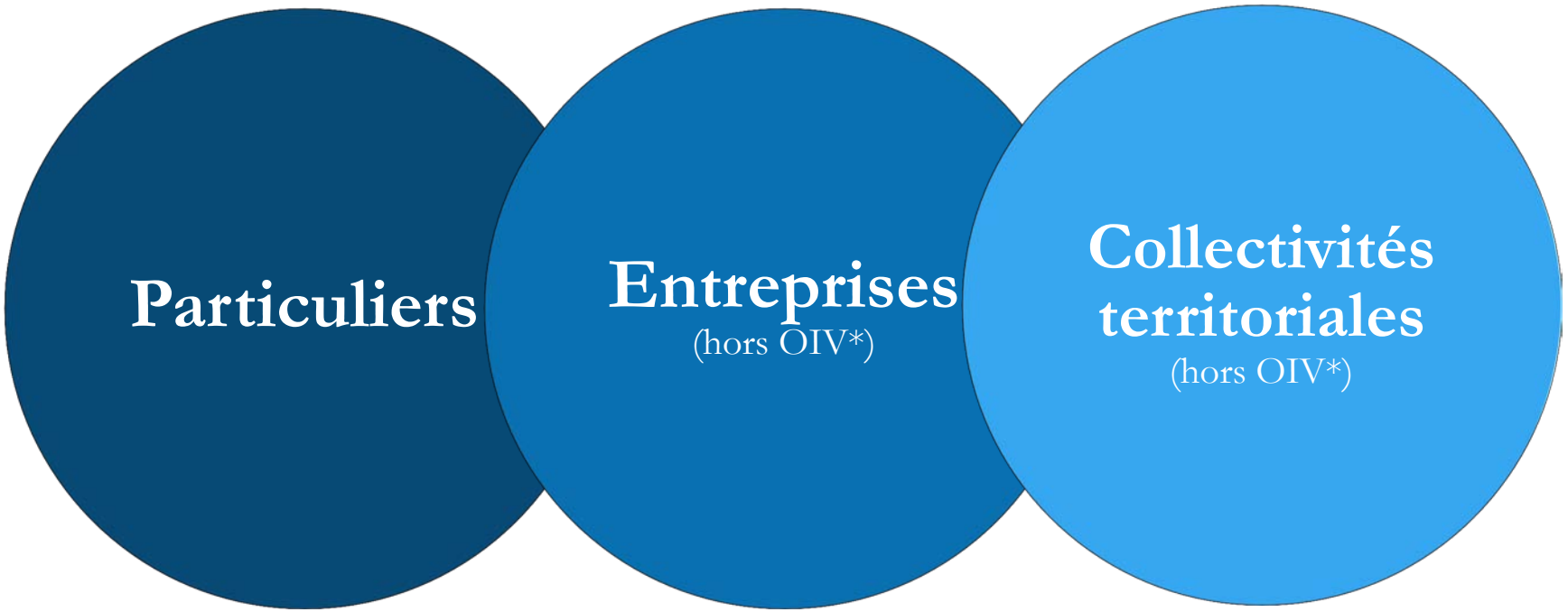
- MOOC accessible à tous gratuitement
- Disponible en continu (pas de sessions)
- Cible : les utilisateurs de l'informatique (en milieu professionnel)
- Contenu
  - Panorama de la SSI, en ligne depuis le 18 mai 2017
  - Sécurité de l'authentification, en ligne depuis le 7 septembre 2017
  - Sécurité sur internet, en ligne depuis le 12 décembre 2017
  - Sécurité du poste de travail et nomadisme, à venir début 2018

SecNum*académie* : accès aux modules

SecNum*académie* : exemple de cours

CYBERMALVEILLANCE.GOUV.FR

Dispositif national d'assistance aux victimes d'actes de malveillance



*Opérateur d'Importance Vital

Missions du dispositif cybermalveillance.gouv.fr

Assistance aux victimes d'actes de cybermalveillance

- Accueil et mise en relation avec des prestataires de proximité
- Fiches réflexe

- Prévention et sensibilisation à la sécurité du numérique
  - Mise à disposition de recommandations et de contenus
  - Campagnes de sensibilisation

- Création d'un observatoire de la menace numérique
  - Remontée d'informations et partage d'information techniques
  - Analyse des données et partages des statistiques

Merci pour votre attention

Questions ?

Planches disponibles sur paperstreet.picty.org/yeye

olivier.levillain@ssi.gouv.fr

ANSSI : www.ssi.gouv.fr

secnumacademie.gouv.fr

cybermalveillance.gouv.fr