FRANCK CHARRON
RSSI-DR

Présentation du dispositif SSI au CNRS

1 CHAINE FONCTIONNELLE SSI DU CNRS

L'organisation SSI du CNRS

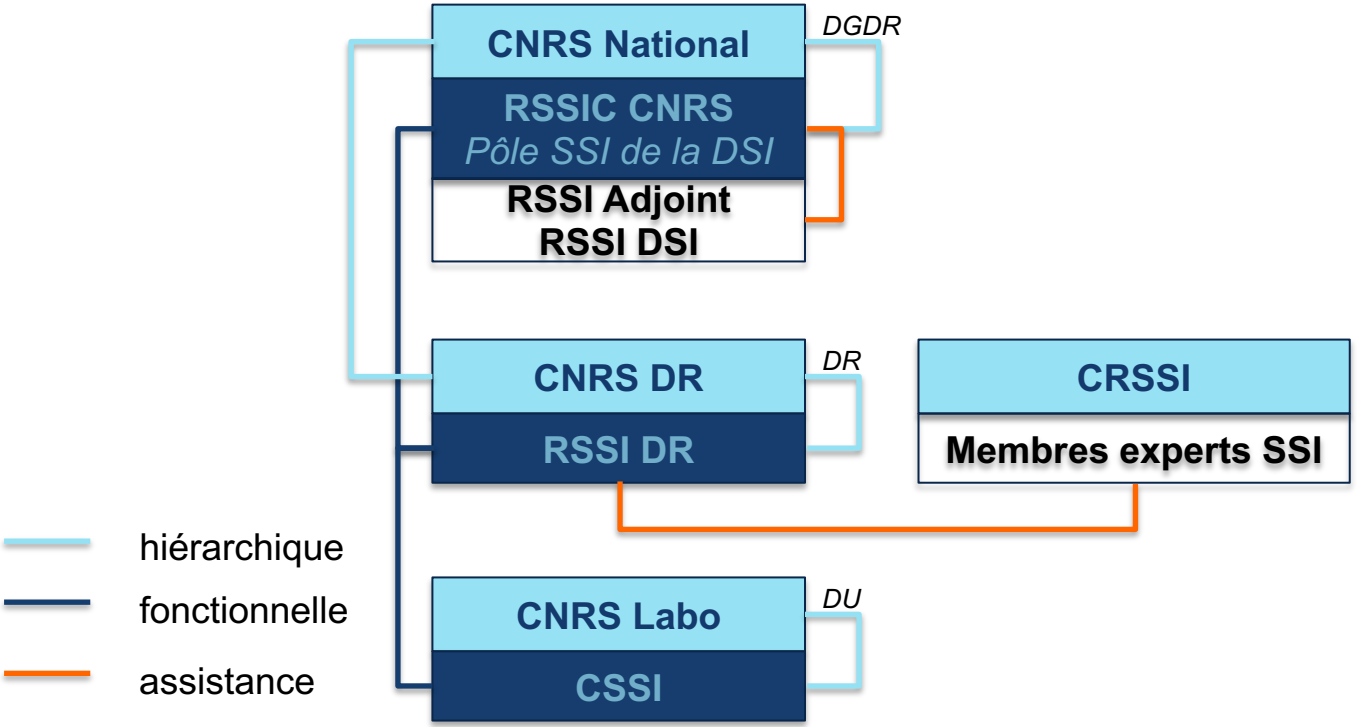
❑S'inscrit dans l'organisation SSI de l'administration FR

➢Responsabilité nationale FR : PM-SGDSN (ANSSI)
➢Responsabilité secteur Recherche : MESR

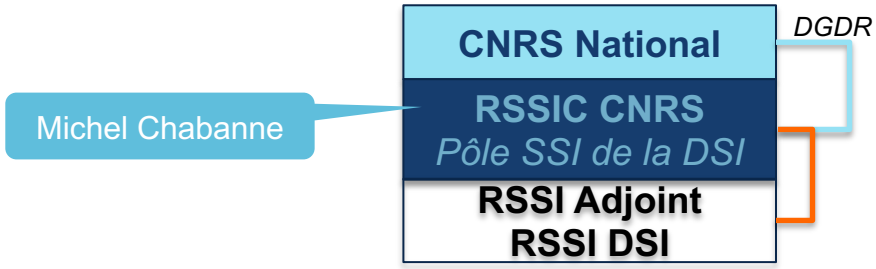
❑S'appuie sur deux composantes

➢Chaîne **Défense et Sécurité Nationale (PPST)**
oPM-SGDSN -> HFDS MESR -> **FSD CNRS ->** Correspondants Défense
➢Chaîne **Sécurité de l'Information (SSI)**
oPM-SGDSN-ANSSI -> FSSI MESR -> **RSSI CNRS** -> RSSI DR / structures / thématiques / Instituts -> CSSI dans les unités

1 CHAINE FONCTIONNELLE SSI DU CNRS



2 CHAINE FONCTIONNELLE SSI DU CNRS - NATIONAL



DROIT ET NORMES

Définir et mettre en place les normes, méthodes, procédures, outils et référentiels : Les décisions officielles : DEC111261DAJ, DEC111263DAJ

Mettre en place, suivre et rendre compte de la PSSI de l'établissement

Homologation des SI

Fonctionnaire Sécurité Défense (FSD)
Services du FSD et du SPD
RSSI-R et CSSI
Directeurs d'unités

- 2019 - Protéger les données au quotidien.pdf
- CHARTE_USAGE_SSI_DEC133249DAJ charte SSI.pdf
- CNRS - SSI - Corpus SSI 2013 - Présentation DR-DAA - 26 mars 2014 - 2.pdf
- CNRS_chiffrement ordinateurs.pdf
- DEC133249DAJ charte SSI.doc
- Fiche-pratique-appareils-mobiles.pdf
- Fiche-pratique-mots-de-passe.pdf
- Fiche-pratique-usages-pro-perso.pdf
- note aux DR sur la PSSI.pdf
- PGSI_1.0.0.pdf
- PSSIO - Laboratoires.pdf
- Voyager avec un portable.pdf

2 CHAINE FONCTIONNELLE SSI DU CNRS - NATIONAL

Mise en application de la PSSI du CNRS, rénovée, conforme à la PSSI-E

Le CNRS a défini 3 chantiers prioritaires

- Complétude de la chaine fonctionnelle SSI de l'établissement (désignation des CSSI)
- **Conformité SSI des terminaux utilisateurs, inventaire et gestion du parc, mises à jour, sauvegarde, chiffrement et prévention de l'obsolescence technique**
- **Identification et classification des données sensibles de l'unité**

2

Resinfo
Fédération des réseaux métiers d'Administrateurs Systèmes et Réseaux dans l'Enseignement et la Recherche.

racine AVOCATS

Droit de la sécurité des systèmes d'information

Schéma version 3 de mars 2018 réalisé par Eric Barbry et Léa Paravano (cabinet Bensoussan)- Laurette Chardon & Marie David pour le groupe de travail GBP, gbp@listes.resinfo.org, du réseau RESINFO (www.resinfo.org)
Mis à disposition selon les termes de la Licence Creative Commons Paternité - 

Code de sécurité intérieure

La sécurité devient "un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives", au même titre que les droits de l'homme, la liberté d'expression, la liberté syndicale

Loi relative au renseignement

- Interceptions de sécurité
- Autorisation du Premier Ministre

L'autorisation du Premier ministre sera donnée, sauf urgence, après avis de la Commission nationale de contrôle des techniques de renseignement, autorité administrative indépendante dont les missions consistent à contrôler la régularité de la mise en oeuvre des techniques de recueil de renseignement

Loi Godfrain

Loi de 1988
Première loi consacrée à la fraude informatique. Elle définit tout le droit qui protège les systèmes d'informations des intrusions, des altérations et des entraves.

Cybercriminalité

- Cyber-patrouille
- Perquisition à distance
- Infractions d'atteintes au STAD : compétence exclusive des juridictions parisiennes et mise en oeuvre d'une procédure spécifique.

- Compétence de la loi française pour tout crime ou délit commis ou tenté au moyen d'un réseau de communication électronique au préjudice d'une personne physique ou morale ayant son siège social ou sa résidence en France.

Atteinte aux STAD

(Systèmes de Traitements Automatisés de Données)

Les atteintes aux STAD comprennent de nouvelles modalités depuis 2014 (article 323-3 du Code pénal) :
- l'extraction, la détention, la reproduction et
- la transmission de données issues d'un traitement.

Ces nouvelles modalités viennent compléter le dispositif des articles 323-1 et suivants du Code pénal qui sanctionnait déjà :
- l'accès ou le maintien frauduleux, l'entrave ou l'altération du fonctionnement et l'introduction frauduleuse ou la suppression de données.

La Cour de cassation a récemment reconnu que l'extraction des données d'un STAD était susceptible de s'analyser comme un vol dans la mesure où elle impliquait la soustraction frauduleuse de données à l'insu de leur propriétaire.

Loi relative à la sécurité publique

- Traitement des données relatives aux détenus
- Interception des correspondances des détenus

Procédure d'habilitation par le ministre de la justice d'agents individuellement désignés sous le contrôle du juge administratif, exclusivement compétent. En l'absence de transmission des données en vue d'engager une procédure judiciaire, elles doivent être détruites.

Sécurité intérieure

Lutte contre le terrorisme

- Sanction des comportements visant, par l'intermédiaire des nouvelles technologies et de la manipulation de données, à entraver l'efficacité des procédures de lutte contre le terrorisme
- Répression de la consultation habituelle et sans motifs légitimes de sites internet comportant du contenu lié à la commission d'actes de terrorisme ou en faisant l'apologie

Vidéosurveillance et écoutes

Loi LOPSSI 2

Apparition du délit d'usurpation d'identité numérique

Loi pour la confiance dans l'économie numérique

- Chiffrement
- Obligations de conservation des données de connexion par les FAI et hébergeurs
- Blocage de sites et déréférencement

Loi pour une République numérique

- instauration d'un principe de neutralité de l'Internet : tout internaute doit avoir accès aux mêmes contenus quel que soit son FAI.
- assujettissement des plateformes à une obligation de clarté, de transparence et de loyauté
- assujettissement des fournisseurs de services de communication au public en ligne au secret des correspondances
- Consécration d'un droit au maintien de la connexion à Internet

Internet

Loi pour la prévention de la délinquance

Enregistrement ou diffusion d'images violentes ou d'agressions

Règlement RGPD du 27 avril 2016

Entrée en vigueur le 25 mai 2018. Modifications d'envergure :
- extension du champ d'application du droit européen des données à caractère personnel à la nationalité de la personne concernée par un traitement de données
- durcissement des sanctions applicables (4% du CA mondial)
- responsabilisation des responsables de traitements et sous-traitants (principes d'accountability et de privacy be design/default)
- suppression de certaines formalités déclaratives au profit de la constitution et du suivi d'un registre.
- création du DPO (délégué à la protection des données), désignation obligatoire dans certains cas
- consécration d'un droit à l'oubli et d'un droit à la portabilité des données, renforcement de la transparence.
- rapprochement de la CNIL et de la CADA (commission d'accès aux documents administratifs

Loi informatique et libertés

* Elle fixe les règles pour les fichiers de données à caractère personnel. Pas de traitement sans la respecter.
* A l'horizon de mai 2018, elle fera l'objet d'importantes modifications afin que la législation française soit conforme au règlement RGPD.

CNIL (Commission Nationale de l'Informatique et des Libertés) et ses attributions

Informatique et libertés

Code de propriété intellectuelle (DADVSI et HADOPI)

- Lutte contre le téléchargement illégal
- Responsabilité de l'abonné sur ses consultations
- Quasi-obligation de filtrage
- Apparition des mesures techniques de protection ou "DRM"

Propriété littéraire et artistique

Référentiels qui s'imposent à l'administration

- Référentiel Général de Sécurité (RGS) : Ce référentiel fixe des règles pour sécuriser les échanges entre les usagers et les autorités administratives et entre les autorités. : signature électronique, 'authentification etconfidentialité.
- Référentiel d'exigence PASSI (prestataire d'audit de la sécurité des SI) : permet la délivrance de certificats de conformité.
- Référentiel Général d'Accessibilité pour les Administrations (RGAA) : Liste les critères d'accessibilité que doivent respecter les sites Internet de l'Etat, des collectivités territoriales et des établissements publics qui en dépendent, et propose une méthode pour vérifier la conformité à ces critères.
- Référentiel Général d'Interopérabilité (RGI)

Public

Rapport entre l'administration et les usagers et recours à la voie électronique

Loi pour une République numérique du 7 octobre 2016 et ordonnance du 23 octobre 2015.
- droit de saisir l'administration en ligne grâce à des téléservices
- Open data : mise à disposition des données publiques dans un standard ouvert et sans demande préalable
- obligation de rendre les sites internet publics accessibles aux personnes handicapées

Loi pour une république numérique

* Création d'un droit à l'autodétermination informationnelle
* Extension des droits des personnes concernées :
- droit à la portabilité
- droit à la transparence et à l'information
- droit d'organiser le sort de ses données après la mort
- droit à l'oubli et consentement renforcé pour les mineurs
- droit d'exercer ses droits par voie électronique

Santé

Création récente du système national des données de santé, un traitement de données à caractère personnel créé par une loi du 26 janvier 2016 et dont les modalités ont été prévues par un décret du 26 décembre 2016 rendu après avis de la CNIL .
- Fichier rassemblant les bases de données déjà existantes, à des fins d'études médicales. Ce fichier repose sur une procédure de pseudonymisation.
- Accessible en permanence par certains services ou organismes publics, et sur autorisation de la CNIL pour d'autres structures.
- Conservation des donnéespendant 20 ans maximum puis archivage pendant une durée de 10 ans .

Autres

Banques

Lo- Norme de l'industrie des cartes de paiement

- Code monétaire et financier

OIV (Opérateur d'Importance Vitale

Loi de programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

Industrie

Normes pour les systèmes de contrôle industriels (SCADA)

Défense

Protection du secret de la défense nationale.

Compléments

Public : voir le site de l'ANSSI (agence nationale de la sécurité des systèmes d'information) : www.ssi.gouv.fr

Industrie : Les SCADA (Supervisory Control and Data Acquisition) sont des logiciels de supervision et de contrôle permettant d'acquérir et de traiter un grand nombre de données (mesures, signalisations, etc.) et de contrôler des équipements industriels. Les principaux risques touchant ces systèmes sont le sabotage et l'espionnage. Des normes de protection et de sécurisation ont donc été élaborées, notamment aux Etats-Unis. L'ANSSI propose également un guide disponible sur son site internet « Maîtriser la SSI pour les systèmes industriels".

Internet : La loi relative à la prévention de la délinquance du 5 mars 2007 a introduit dans le Code pénal une nouvelle incrimination, couramment appelée « happy slapping », qui sanctionne le fait d'enregistrer ou de diffuser des images d'atteintes volontaires à la personne (article 222-33-3 du Code pénal)

3 CHAINE FONCTIONNELLE SSI DU CNRS - RÉGIONAL

RSSI national
DSI du CNRS
RSSI Partenaires
CSSI en unité
Directeurs d'unités
Personnels des unités

SECURITE

Evaluer les risques et les menaces
Coordonner les 70 unités, 25 partenaires, dont 8 universités, sur 2 régions
Gérer les incidents
Sensibiliser et former les utilisateurs aux enjeux de sécurité du SI

3 CHAINE FONCTIONNELLE SSI DU CNRS - RÉGIONAL

- RGPD

  Règlement général sur la protection des données
  Protection des données, chiffrement, voyage, données sensibles traitements normalement interdits

- PPST

  Protection du Potentiel Scientifique et Technique de la nation
  Espace de confiance pour écarter les prédateurs et protéger les intérêts fondamentaux de la Nation
  PPST = ZRR -> non, il y a plusieurs niveaux avec différentes notes de 0 à 4
  Mission à l'étranger

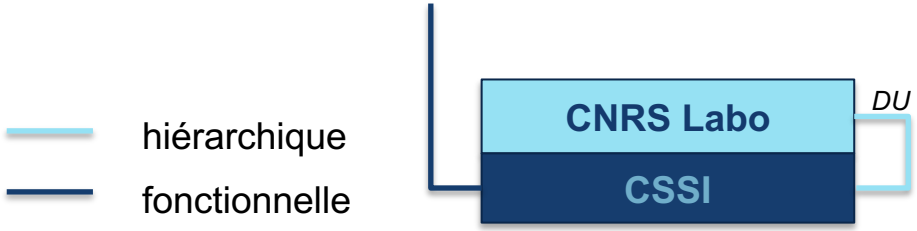
- PMS-AI

  Plan de mise en sureté – Attentat Intrusion
  Consignes Vigipirate, mise en sureté des bâtiments…

- Drones

  Chaque pilote doit être formé, chaque drone doit être déclaré

4 CHAINE FONCTIONNELLE SSI DU CNRS - DANS L'UNITE



SECURITE

Assister les directeurs d'unité dans l'exercice de leur responsabilité en matière de SSI
Sensibiliser les utilisateurs de l'unité à la SSI (notamment phishing, rançonware, président)
Transmettre les mails de la chaine de sécurité aux intéressés dans l'unité
Réunion avec RSSI et DU

Cartographie du SI de l'unité : Matériels, réseaux, applications, services client ou serveur

4 CONFORMITÉ SSI DES TERMINAUX UTILISATEURS

- Inventaire et gestion du parc
- Mises à jour (OS, logiciels et matériels)
- Antivirus (avec gestion centralisée)
- Sauvegarde (MyCore)
- Prévention de l'obsolescence technique
- Chiffrement -> note du 30/11/2018 (avant 31/01/2019)

  - Le chiffrement permet de réduire les conséquences du vol ou de la perte de l'équipement
  - Concerne tous les personnels et tous les ordinateurs et téléphones utilisés, quel que soit l'origine du financement
  - La note rappelle la responsabilité de chacun dans l'application des mesures
  - Solutions simples à mettre en place par chaque utilisateur (flyer en annexe de la note)
  - Attention : garder les clefs de « chiffrement » (=recouvrement) de par-devers soi

4 LIENS UTILES

- Site Sécurité SI du CNRS : https://securite-si.cnrs.fr/

- PSSI du CNRS : https://securite-si.cnrs.fr/pssi/
- PSSIO – Unité : https://securite-si.cnrs.fr/pssi/pssio-labos/

- Consignes et bonnes pratiques : OS, prise en main à distance, chiffrement, cloud… : https://securite-si.cnrs.fr/consignes/

- Déclarer un incident SSI : https://securite-si.cnrs.fr/urgence/declarer-un-incident/