CyberEdu

La cyber sécurité dans vos formations

Assemblée des Directeurs d'I.U.T.

AG du Vendredi 16 Décembre 2016

Quelques Dates

- 2006 Rapport Labordes à la demande de M.Raffarin
  - La France n'est pas préparée face aux Cyber attaques
- Nombreux rapports (sénat et AN – cf. annexes)
- Livre Blanc Défense & Sécurité Nationale 2013
  - La cyber défense devient un enjeu national
  - La cyber sécurité dans l'enseignement
  - ANSSI lance son appel d'offre
- Stratégie Nationale de la Sécurité du Numérique
  - Présenté par M. Manuel Valls le 16 Octobre 2015
    - Cyber attaque de TV5 Monde → Al Quaïda à la TV !

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) & CyberEdu

- Appel d'offre 2014 suite au Livre Blanc
  - Université Bretagne Loire et Orange
  - Support pédagogique pour l'enseignement des notions de cyber sécurité

- Colloques CyberEdu pour les enseignants
  - mallette pédagogique
  - 100 enseignants ont assisté aux 4 colloques

CyberEdu – Mallette Pédagogique

- Guide pédagogique d'intégration dans les formations
- Modules de sensibilisation
  - Syllabus (introduction) et Quizz (conclusion)
  - Module 1 → Cyber sécurité : notions de base 5h
  - Module 2 → Les règles d'hygiène informatique 6h
  - Module 3 → Les aspects réseaux et applicatifs 4h
  - Module 4 → La gestion de la cyber sécurité 3h
- Ensemble de supports pédagogiques de cours
  - Fiches sécurité des OS
  - Fiches sécurité des réseaux
  - Fiches sécurité des logiciels
  - Fiches sécurité des composants
  - Fiches sécurité authentification

ANSSI et CyberEdu – Genèse de l'association

- Besoin de porter CyberEdu sur le territoire
  - La culture de la sécurité du numérique
  - Les compétences et bonnes pratiques
- Besoin d'un réseau d'enseignants
  - Alimenter et diversifier le fond pédagogique
    - Accompagner, produire, adapter et faire vivre
    - Créer de nouveaux contenus
  - Animer et accueillir les colloques
  - Développer un label des formations CyberEdu
  - Créer une synergie transdisciplinaire
- Colloques ANSSI → recrutement des acteurs
- Constitution de l'association début 2016

CyberEdu – Association

17 Mai 2016 – Création de l'association (statuts)

Gérard	PELIKS	Président	Airbus Defence & Space Cybersecurity
Pierre	ROLIN	Vice Président	Institut Mines-Télécom
Patrick	ERARD	Secrétaire Général	Institut Mines-Télécom
Olivier	LEVILLAIN	Secrétaire Général adjoint	CFSSI de l'ANSSI
Reza	ELGALAI	Trésorier	Université Technologique de Troie
Jean-Pierre	HIVET	Trésorier adjoint	Académie de Rennes
Philippe	WERLE	Vice Président en charge des outils	Université Paris 13 - SupCIL

CyberEdu – Association (suite)

Le réseau sur le territoire

contact@cyberedu.fr

Luc	SANSELME	Vice-Président Est	Académie de Nancy-Metz
Yvon	KERMARREC	Vice-Président Grand-Ouest	Mines Télécom Bretagne
Julien	BREYAULT	Vice-Président Ile-de-France	IUT de Sénart
Dominique	LAZURE	Vice-Président Nord	Université de Picardie
Jean-Marie	PLACE	Vice-Président Nord	Université de Lille 1
Xavier	ROIRAND	Vice-Président Ouest	Université Bretagne Sud
Clara	BERTOLISSI	Vice-Présidente Sud-Est	Université Aix-Marseille
Denis	LUGIEZ	Vice-Président Sud-Est	Université Aix-Marseille
Florence	SEDES	Vice-Présidente Sud-Ouest	INIT (CNRS Toulouse 3)
Hinde	BOUZIANE	Vice-Président Sud-Ouest	LIRMM (CNRS Montpellier 2)
Marc	GILG	Vice-Président Est	Université de Haute-Alsace
Sophie	CHABRIDON	Vice-Présidente Ile-de-France	Télécom SudParis

CyberEdu – Missions

- Accompagner les enseignants (utilisation et production)
- Enrichissement du fond de supports pédagogiques
  - GT-Supports (Creative Commons BY), GT-Labellisation (ANSSI)
- Attribuer le label CyberEdu aux formations
- Adhésion des établissements → amplifier la dynamique
- Colloques sur le territoire (GT-Colloques)
- Communication et événementiel (FIC 2017 Lille, …)
- Tisser des relations avec les autres associations
  - ARCSI – Réservistes du Chiffre et de la Sécurité de l'Information
  - ADIUT et CRI-IUT en lien avec les IUTs
  - SupCIL – Informatique et Libertés dans l'Enseignement Supérieur
  - CEFCYS – Association des Femmes de la Cyber sécurité
  - AFCDP – Informatique et Libertés dans les entreprises

Atouts stratégiques pour les IUTs

- Stratégie Nationale de Sécurité du Numérique

  objectif stratégique #3 (page 27)

  - La cyber sécurité en formation initiale et continue
  - Adapter les cursus en intégrant CyberEdu (2016)
  - Porté depuis 2016 par la CPU et la CGE
- STRAtégie Numérique de l'Enseignement Supérieur

  lancé en Octobre 2013 avec 4 ambitions. Le numérique

  - au service de la réussite et de l'insertion des étudiants
  - comme outil de rénovation des pratiques pédagogiques
  - pour le développement de campus d'avenir
  - pour une université ouverte et attractive (EU et InterΘnal)

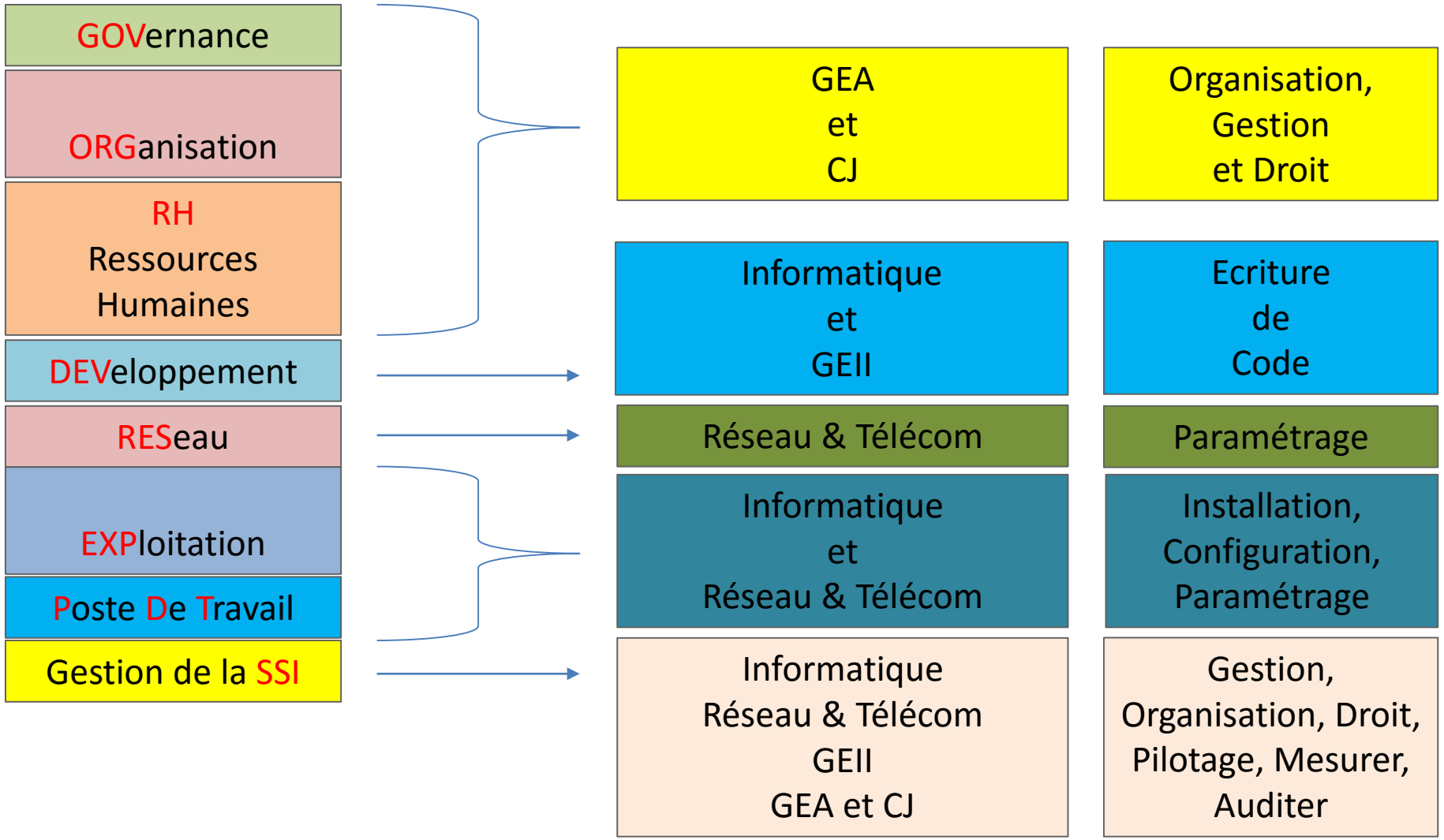
Atouts stratégiques pour les IUTs (suite)

- Développement des pratiques pédagogiques
  - Sensibilisation à la cyber sécurité par la simulation
  - Spécialisation en informatique, réseau, gestion des risques
  - La sécurité du numérique et des DCP à la conception
  - Notions légales adaptées dans chaque département
  - Notions techniques et légales en langues
- Développement d'un numérique du territoire
  - Compétences de cyber sécurité et DCP en entreprise
  - CyberEdu, Medef, ANSSI action territoriale
- Licence professionnelle
  - Formation enrichie labellisée par CyberEdu
  - Formation spécialisée labellisée SecNumEdu par l'ANSSI

Cyber sécurité dans vos formations (LicPro)

- Sécuriser à la conception (security by design)
- Respecter les DCP (privacy by design)
- Lors de l'enseignement
  - Développement de logiciel, automatisme, SCADA
  - Installation et administration système et réseau
  - Utilisation des outils numériques (bureautique, communication, réseaux sociaux, …)
  - Législation
    - Droit sur les SI (loi Godfrain 88, eIDAS 2016, RGS, …)
    - Informatique et libertés (RGPD mai 2018)

Politique de Sécurité des SI (exemple)



Merci !

contact@cyberedu.fr

information, adhésion, groupes de travail

www.cyberedu.fr

colloques, communications, contact, supports pédagogiques, labellisation

CyberEdu - Maison des Universités

103 Boulevard Saint-Michel 75005 Paris

Philippe WERLE

Vice Président outils CyberEdu

Animateur du réseau SupCIL

Annexes

Rapports parlementaires – jusqu'ici ça va …

- 2004 – Le plan de renforcement de la sécurité des systèmes d'information de l'Etat, décidé par le Premier ministre Jean-Pierre Raffarin

  Le constat sévère du Rapport Lasbordes du 26 Novembre 2005 : un retard préoccupant : « Depuis plusieurs années, les rapports annuels des départements ministériels sur l'état de la sécurité des systèmes d'information (SSI) font part des difficultés persistantes rencontrées pour améliorer la situation : compétences et capacités opérationnelles trop réduites et isolées, manque de sensibilité des décideurs aux enjeux, insuffisance de produits de sécurité dûment qualifiés combinée à des positions monopolistiques dans des segments importants du marché, prolifération d'interconnexions de réseaux mal sécurisés, réglementation nationale difficilement applicable, dimension européenne mal coordonnée. Si certaines améliorations ponctuelles sont constatées, les efforts accomplis, pour méritoires qu'ils soient, n'ont pas été à la mesure de l'évolution rapide des technologies et des menaces »

- 2008 – La cyberdéfense : un nouvel enjeu de sécurité nationale. Rapport d'information n° 449 (2007-2008) de M. Roger ROMANI, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008

Rapports parlementaires – Et maintenant ça va plus !

- 2012 – Le rapport au Sénat de 2012 de Jean-Marie Bockel – Rapport d'Information sur la Cyberdéfense

Introduction – Extraits « Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur. Aujourd'hui, le sentiment qui prédomine est que l'ampleur de la menace a été largement sous-estimée. Comme le relève le document préparatoire à l'actualisation du Livre blanc, publié en février 2012, depuis 2008, les risques et les menaces qui pèsent sur le cyberespace se sont nettement confirmés, à mesure que celui-ci devenait un champ de confrontation à part entière avec la montée en puissance rapide du cyber espionnage et la multiplication des attaques informatiques en direction des Etats, des institutions ou des entreprises. Les risques identifiés par le Livre blanc comme étant de long terme se sont donc en partie déjà concrétisés et la menace atteint désormais un niveau stratégique.

Depuis les attaques informatiques massives qui ont frappé l'Estonie en 2007, il ne se passe pratiquement pas une semaine sans que l'on annonce, quelque part dans le monde, une attaque informatique importante contre de grandes institutions, publiques ou privées, qu'il s'agisse de cybercriminalité ou d'espionnage informatique. La France n'est pas épargnée par ce phénomène, puisque notre pays a été victime de plusieurs attaques informatiques d'envergure, à l'image de l'attaque contre les systèmes d'information du ministère de l'économie et des finances, découverte fin 2010 à la veille de la présidence française du G8 et du G20, ou encore de l'affaire, révélée par la presse, d'espionnage via l'Internet du groupe AREVA. Tout récemment, la presse a révélé que même la Présidence de la République aurait fait l'objet d'une ou de plusieurs attaque(s) informatique(s) de grande ampleur. Pour sa part, votre rapporteur considère que, si ces attaques sont avérées, la Présidence de la République devrait le reconnaître officiellement et communiquer publiquement sur ce sujet car il ne sert à rien de vouloir le cacher ou chercher à minimiser les faits. Au contraire, votre rapporteur considère qu'il serait souhaitable que les grandes institutions qui ont été victimes d'attaques informatiques communiquent publiquement sur le sujet, naturellement une fois que ces attaques ont été traitées. C'est d'ailleurs ce que font les autorités américaines ou britanniques. En effet, c'est à ses yeux le meilleur moyen de sensibiliser les administrations, les entreprises ou les utilisateurs à l'importance de ces enjeux.

Dans ce contexte, la France est-elle suffisamment préparée pour se protéger et se défendre face aux attaques informatiques ? Dans un rapport de 2006 remis au Premier ministre, notre ancien collègue député M. Pierre Lasbordes dressait un constat sans complaisance des faiblesses de notre organisation et de nos moyens, notamment au regard de nos partenaires européens les plus proches. En février 2008, dans un rapport d'information présenté au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, notre ancien collègue sénateur M. Roger Romani estimait que « la France n'est ni bien préparée, ni bien organisée face à cette menace. »

Rapport parlementaire, CNIL et ANSSI

L'année 2015 fut marquée par de nombreux changements dans l'écosystème du numérique et de la cyber sécurité

- **2015 –** Sécurité numérique et risques – enjeux et chances pour les entreprises, Rapport 271 (2014-2015) de M. Bruno SIDO, sénateur et Mme Anne-Yvonne LE DAIN, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 2 février 2015**.** Ce rapport parlementaire, présenté à la presse le 14 avril par la députée Anne-Yvonne Le Dain et le sénateur Bruno Sido, confirme que la sécurité numérique est désormais un enjeu majeur à la fois pour les entreprises et pour la société dans son ensemble.
- **2015 –** CNIL – Dans le rapport d'activité 2015 la présidente Isabelle Falque-Pérotin analyse que « La protection des données personnelles est au cœur de la cyber sécurité » et fait le même constat anticipé dans le rapport effectué par OBS pour le compte du Ministère de la Défense Nationale.
- **2015** – ANSSI – Guillaume Poupard aux Assises de la Sécurité et des Systèmes d'Information 2016 – « … Guillaume Poupard a appelé à l'ouverture vers les industriels européens et la société civile car la « cyber sécurité ne peut se contenter d'un cénacle d'experts. C'est dans notre intérêt de faire monter le pays en compétence »

RGPD – Changement de paradigme

RGPD – En mai 2018 s'appliquera à l'ensemble des pays européens le règlement général de protection des données. Une évolution majeure de la règlementation qui doit être anticipé en adoptant dés à présent les bonnes pratiques puisque le RGPD implique entre autres :

- Privacy by design – La mise en œuvre de la sécurité doit passer par une prise en compte dès l'élaboration du projet et doit suivre tout le cycle de vie de la donnée. Il en va de même pour la protection de cette dernière au sens de la vie privée. Cela passe par la mise en œuvre d'un dialogue entre les métiers et la direction des systèmes d'information, et par la compréhension mutuelle des enjeux associés à ces développements. Idéalement, cette réflexion sera menée le plus tôt possible, dès la conception des projets (notion de « privacy by design »)
- Etude d'Impact sur la Vie Privée – Le Privacy Impact Assessment (PIA) est une analyse de risque produite grâce à une méthode de type EBIOS pour évaluer les risques sur les données à caractère personnelle d'un nouveau traitement que l'on étudie et évalue avant sa conception. La gouvernance a la charge de définir de façon organisationnelle et technique les mesures qu'elle va prendre à la conception du traitement pour réduire au minimum acceptable les risques en regard avec les nouveaux risques financiers qu'elle encoure en cas de sanction par la CNIL
- L'information des autorités de manière général et des individus de façon personnalisée des fuites de données occasionnées par son SI défaillant en terme de sécurité
- La charge de la preuve que la gouvernance a mis tout en œuvre d'un point de vu organisationnelle, humain, financier et technique pour protéger les données à caractère personnelle du plaignant (ex: les données RH)
- Les sanctions sont portés à 20 M€ ou 4% du chiffre d'affaire mondial. Une administration ou une université sera sensible à la sanction de 20 M€.

Documents de référence

- Cyber Securité – La SSI en France
  - Le Livre blanc sur la défense et la sécurité nationale de 2013
- Stratégie Nationales Enseignement Supérieur
- Stratégie Nationale de la Sécurité du Numérique
- Politique SSI de l'Etat
- Sensibilisation & Formation
  - Guides d'hygiène informatique
  - Précautions pour les usagers
  - Bonnes pratiques
  - Centre de Formation SSI
  - CyberEdu
  - Formations labellisées

Livres

- **La Cybersécurité au-delà de la technologie**

  Philippe TROUCHARD PwC Responsable Cybersécurité pour les directions des grands groupes et Jean-Baptiste Rudelle fondateur de Criteo – ISBN 978-2-7381-3368-7

  – Chapitre 6 – Les pieds nickelés font de la cyber sécurité : « De la débrouillardise ingénieuse au lieu d'une stratégie réfléchie » décrit une pléthore d'incidents assez graves advenus dans des organismes importants dont celui du cheval de Troie chez Areva.

- **L'homme Nu. La Dictature Invisible Du Numérique**

  Marc Dugain, Christophe Labbé - Plon Hors Collection 21 Avril 2016 – ISBN 978-2-2592-2779-7

  – 1984 d'Orwell parlait d'une dictature violente. Le monde des Big Datas à l'horizon de la moitié de ce siècle sera celui d'une hégémonie à la fois douce et totalitaire. La fin de la pensée grecque est en marche et avec elle une époque de l'humanité est bientôt révolue. On les appelle les Big Datas. Google, Apple, Facebook ou Amazon, ces géants du numérique, qui aspirent à travers Internet, smartphones et objets connectés, des milliards de données sur nos vies. Derrière cet espionnage, dont on mesure chaque jour l'ampleur, on découvre qu'il existe un pacte secret scellé par les Big Datas avec l'appareil de renseignement le plus puissant de la planète. Cet accouplement entre les agences américaines et les conglomérats du numérique, est en train d'enfanter une entité d'un genre nouveau. Une puissance mutante, ensemencée par la mondialisation, qui ambitionne ni plus ni moins de reformater l'Humanité. La prise de contrôle de nos existences s'opère au profit d'une nouvelle oligarchie mondiale. Pour les Big data, la démocratie est obsolète, tout comme ses valeurs universelles. C'est une nouvelle dictature qui nous menace. Une Big Mother bien plus terrifiante encore que Big Brother. Si nous laissons faire nous serons demain des " hommes nus ", sans mémoire, programmés, sous surveillance. Il est temps d'agir.

Livre blanc

Gouverner à l'Ère du Numérique

Dans le livre blanc – Gouverner à l'Ere du Numérique, vous pourrez découvrir les nouvelles dimensions que le numérique imposent à la gouvernance de votre organisme et comment la donnée numérique, la protection des données personnelles et la cyber sécurité constitue un nouvel axe majeur de sa stratégie. Ce nouvel axe est essentiel dans le développement de sa dimension numérique et la prise en compte de nombreux risques majeurs qui pèsent aujourd'hui sur son patrimoine informationnel. L'ère de la SSI informatique est morte, il est urgent que la gouvernance ouvre ce chantier aux dimensions stratégiques multiples.

Porté par Palo Alto et La Tribune, en collaboration avec CESIN et Solutions Numériques, ce livre blanc a été rédigé dans un langage très accessible par des acteurs majeurs

- Michel Van Den Berghe – CEO d'Orange Cyberdéfense
- Olivier Ligneul – CTO & RSSI chez EDF
- Alain Bouillé – Directeur SSI chez Groupe Caisse des Dépôts
- Ian West – Directeur Cyber défense de l'OTAN
- Mark McLaughlin – National Security Telecommunications (USA)
- Greg Day – CTO Cyber sécurité chez Palo Alto Networks
- Gregory Albertyn – Directeur conformité et Gouvernance de la Donnée chez PwC
- Maître Olivier Iteanu – Iteanu Avocats