

Projet S8 SISN  
**Labellisation Cyberedu**



**CENTRALE  
MARSEILLE**



Groupe n°6 :  
*Florine Maureau - Maud Saint-Amand - Léa Salavert*  
Tuteur : *Pascal Préa*

Soutenance : vendredi 25 mai 2018

## Remerciements

Nous tenons particulièrement à remercier Pascal Préa qui nous a permis de travailler sur ce projet et nous a accompagnées tout au long du semestre pour s'assurer de son bon déroulement.

Aussi, nous remercions les intervenants que nous avons rencontrés et qui ont répondu à nos questions. Il s'agit de Denis Lugiez et Geoffroy Desvernay.

Finalement, nous remercions l'équipe enseignante de Centrale Marseille pour ce S8 qui nous a permis une nouvelle fois de nous former à la gestion de projet sur un sujet au coeur de ce S8.

## Introduction

Dans le cadre de notre option de S8 SISN, plusieurs projets à mener tout au long du semestre nous ont été proposés. Nous avons choisi celui proposé par Pascal Préa portant sur l'étude de faisabilité de certifier la formation de Centrale Marseille par CyberEdu. Ce choix s'est fait naturellement car, outre le fait qu'il ne soit pas axé codage pur, nous étions intéressées par la démarche d'élèves apportant une plus-value aux futurs élèves. La formation de Centrale Marseille se construit au fur et à mesure et pouvoir y apporter notre contribution est une fierté.

De plus, le thème de la sécurité informatique est plus que jamais d'actualité. Comme le dit Bruce Schneier, cryptologue américain reconnu, *«Si les produits informatiques que nous achetons étaient sûrs par défaut, nous n'aurions pas besoin de dépenser des milliards chaque année pour les rendre plus sûrs.»* En effet, à l'heure où Internet et les réseaux envahissent notre quotidien et nos plus simples habitudes, il est primordial d'adopter des mesures d'hygiène informatique pouvant éviter des fuites d'information et de confidentialité majeures.

Dans ce rapport, nous expliquerons notre démarche d'investigation. Nous expliciterons les avantages d'obtenir une telle labellisation, son contenu, les difficultés de sa mise en place et comment l'intercaler au fil du cursus. Ce dossier pourra être présenté en vue d'une future commission des études pour permettre son entrée dans la formation centralienne.

# Table des matières

<b>Remerciements</b>	1
<b>Introduction</b>	1
<b>Table des matières</b>	2
<b>I. Qu'est-ce que la labellisation CyberEdu ?</b>	3
I.A. La jeune association CyberEdu	3
I.B. Modalités d'obtention de la labellisation	3
I.C. Le label CyberEdu, quel intérêt pour Centrale Marseille ?	4
I.D. Les formations déjà labellisées	4
<b>II. Comment obtenir la labellisation ?</b>	5
II.A. Enseignements conseillés d'aborder	5
II.B. Formation centralienne et sécurité informatique	5
II.C. Répartition modulaire en fonction des années	6
<b>III. De la formation au label : propositions et perspectives d'intégration des enseignements Cyberedu dans le cursus de l'élève centralien</b>	6
III.A. Perspectives d'intégration	6
III.B. Propositions d'intégration	7
III.B.1. Comment relier Cyberedu à l'enseignement existant	7
III.B.2. Sous quelle forme peut être dispensé Cyberedu ?	8
III.B.3. Quel volume horaire et quels professeurs sont nécessaires à la réalisation du projet ?	9
<b>Conclusion</b>	10

## I. Qu'est-ce que la labellisation CyberEdu ?

Dans un premier temps, et pour bien saisir l'intérêt de CyberEdu, il convient de présenter cette jeune labellisation et son processus. Nous en discuterons à travers les différents aspects caractéristiques de l'association.

### **I.A. La jeune association CyberEdu**

CyberEdu est une association créée en 2013 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Dans ce contexte, on peut parler de CyberEdu comme d'une structure qui découle de l'ANSSI. L'association a pour objectif, comme mentionné sur son site, « *d'introduire les notions de sécurité dans l'ensemble des formations dans le domaine du numérique en France* ». Autrement dit, elle promeut l'éducation à la sécurité informatique, tâche qui auparavant était assurée par l'ANSSI, en intervenant auprès du grand public à travers différentes actions.

Une des prérogatives de CyberEdu est qu'elle peut délivrer un label qui certifie les formations qui intègrent dans leur contenu pédagogique des éléments relatifs à la sécurité numérique. CyberEdu est une association pionnière dans le sens où c'est la seule en France à pouvoir délivrer un label de ce type. Ce label, qui n'existe que depuis 2016, ne doit pas être confondu avec celui que délivre l'ANSSI. Ce dernier n'est destiné qu'aux formations en informatique (label SecNumEdu), alors que le label CyberEdu se caractérise par le fait qu'il est beaucoup plus souple, et ne repose que sur un engagement moral de la part des formations qui en font la demande. Autrement dit, c'est à la formation qui considère qu'elle initie suffisamment aux enjeux de sécurité informatique de demander le label.

### **I.B. Modalités d'obtention de la labellisation**

L'obtention du label repose sur la compatibilité entre les critères d'obtention du label CyberEdu. L'association fournit des cours qui sont disponibles en ligne sur le site de l'ANSSI, et qui constituent la base pour évaluer si une formation peut demander le label ou non. Ces cours constituent en effet la "mallette pédagogique" à intégrer dans la formation (sous différentes formes possibles) pour pouvoir faire la demande du label. Ce contenu pédagogique n'est pas à reprendre exactement tel quel, mais doit être présent dans les enseignements. Au regard de ces modalités, la question se posait donc pour nous de savoir où l'enseignement à Centrale rejoignait le contenu de ces cours, et s'il le rejoignait suffisamment pour demander le label.

D'autre part, il est à noter qu'il n'existe pas de contrat pédagogique. La formation s'engage sur la base de sa volonté individuelle à intégrer les aspects nécessaires, et en retour, l'association ne réalise pas d'audit pour vérifier si cet engagement est respecté. Elle compte sur un rapport à jour de la part de la formation concernée pour évaluer si ses critères continuent d'être respectés. La formation ne s'engage que dans la mesure où elle signe la charte CyberEdu.

### **I.C. Le label CyberEdu, quel intérêt pour Centrale Marseille ?**

Etant donné le fait que le label est très jeune (2 ans), les retours sur son impact sont faibles et il est donc difficile d'évaluer réellement son intérêt pour les formations qui l'obtiennent et leurs étudiants. Pour le moment, on ne peut quantifier son effet qu'à travers le nombre de formations qui en font la demande, et qui, selon Mr Denis Lugiez (correspondant régional de CyberEdu), tend à augmenter.

Le label constitue néanmoins un avantage pour les formations, les étudiants qui en sont issus et indirectement les entreprises qui recrutent ces étudiants dans la mesure où il représente un gage de qualité, de sérieux, mais également de modernité. La labellisation donne en effet droit à la formation d'apposer le logo CyberEdu dans les publications des formations. A ce titre, l'ANSSI souligne que « cette mention permettra aux étudiants et aux employeurs de repérer facilement et rapidement les formations en informatique qui dispensent le minimum nécessaire de cybersécurité. ».

A noter également que les aspects dits « d'hygiène informatique » ne concernent pas seulement les informaticiens, mais tous les individus qui utilisent un ordinateur ou toute autre machine leur permettant de se connecter à internet. Autrement dit, tout le monde, à peu de choses près, est aujourd'hui concerné par ces « bonnes pratiques ». Ainsi, en plus d'être un gage de qualité, la sensibilisation aux risques informatiques que promeut CyberEdu s'impose comme une responsabilité pour chacun, car chaque individu se servant d'une machine peut non seulement être victime d'un de ces risques, mais aussi exposer d'autres personnes à ces mêmes risques.

### **I.D. Les formations déjà labellisées**

Sur l'année 2017, CyberEdu a délivré le label à 7 formations, qui constituent un panel représentatif du type de formation auxquelles s'adresse la labellisation. On retrouve, parmi les formations labellisées en 2017, des licences, DUT, BTS, voire des instituts dans leur globalité. Ce panel vient vérifier plusieurs points mis en avant par CyberEdu :

- D'abord, la labellisation concerne aussi bien les formations au niveau licence que celles au niveau master,
- Elle peut concerner une école entière comme une formation particulière au sein d'une école,
- Elle ne concerne pas exclusivement les formations spécialisées en sécurité numérique,
- Elle n'a été délivrée à aucune école d'ingénieur généraliste ni à aucune formation au sein d'une école de ce type.

Au regard de ces éléments, l'enjeu pour l'Ecole Centrale de Marseille est double ; si elle obtenait le label CyberEdu, elle serait non seulement la première école dans la région de Marseille mais aussi la première école d'ingénieur généraliste à en bénéficier. Ainsi, Centrale Marseille peut-elle relever le défi ?

## II. Comment obtenir la labellisation ?

La labellisation Cyberedu ne s'adressant qu'aux écoles non spécialistes de la sécurité informatique, elle laisse une marge de manœuvre importante concernant les enseignements à aborder pour l'obtenir.

En effet, l'école qui prétend à cette labellisation est responsable des notions liées à la sécurité qu'elle enseigne et s'auto-évalue pour déterminer si ce contenu est suffisant pour prétendre à la certification. Il s'agit d'une relation de confiance entre l'ANSSI et l'école signataire de la charte CyberEdu.

### **II.A. Enseignements conseillés d'aborder**

Pour faciliter la tâche aux écoles, l'ANSSI fournit des supports de cours qui peuvent être réutilisés tels quels ou modifiés selon convenance. Ils sont au nombre de 4 sous forme de modules :

*Module 1* : Cybersécurité : notions de base

*Module 2* : Les règles d'hygiène informatique

*Module 3* : Cybersécurité : les aspects réseaux et applicatifs

*Module 4* : La gestion de la cybersécurité au sein d'une organisation

Tous ces modules n'ont pas à être abordés dans leur globalité pour obtenir la labellisation mais ils offrent un bagage de base complet sur la sécurité informatique pour des élèves en formation d'ingénierie générale. C'est la raison pour laquelle nous choisissons d'aborder 3 des 4 thèmes, répartis différemment au cours de la scolarité.

De plus, nous pensons qu'il serait préférable d'ajouter un module sur le droit des systèmes informatiques avant d'aborder ceux énoncés précédemment. Ce cours supplémentaire permettrait de comprendre plus facilement les notions -très présentes- de droit inhérentes à la sécurité informatique. La répartition en volume horaire sera explicitée plus tard dans ce rapport.

L'existence de ces modules tout faits sous forme de diapositives est un réel avantage pour les professeurs et intervenants de Centrale qui auront à dispenser la formation. En effet, ils représentent un gain de temps pour ces derniers, ils sont officiels et donc totalement dans le sujet et ils peuvent être transmis par la suite aux élèves en guise de rappel si ils souhaitent s'y référer.

### **II.B. Formation centralienne et sécurité informatique**

A ce jour, il est évident que prétendre à la labellisation Cyberedu sans ajouter de cours est inimaginable.

Après étude des plaquettes de la formation, nous avons constaté que la seule introduction à la sécurité informatique est en 1<sup>ère</sup> année lors du « Bonjour du CRI ». Ceci n'est donc pas suffisant.

Le master spécialisé que Madame Fossati est en train de créer portera sur la sécurité des systèmes et non pas sur la sécurité informatique au sens de Cyberedu. Cette option ne pourra donc pas non plus couvrir les thèmes recommandés par Cyberedu d'autant plus qu'elle ne concernera qu'une poignée d'élèves.

## **II.C. Répartition modulaire en fonction des années**

Cyberedu offre deux types de labellisation : la labellisation Bac +3 et la labellisation Bac +5. Dans le cadre de la formation à Centrale Marseille, nous n'envisagerons que la première car elle représente un volume horaire déjà bien important et que le niveau demandé correspond tout à fait aux attentes d'une école généraliste. La seconde demanderait un réarrangement des cours trop conséquent pour les enseignements principaux de la formation.

Nous avons envisagé de ne labelliser qu'une partie de la formation en intégrant les modules à la 3A digitale mais après réflexion, cette option desservirait l'école. Elle ne toucherait qu'une trentaine d'élèves et l'école ne pourrait pas prétendre être précurseur d'une telle certification dans sa globalité, ni même apposer le logo Cyberedu dans ses plaquettes.

Nous cherchons donc à intégrer cette formation sur l'ensemble du cursus centralien, afin que tout le monde en bénéficie. Après avoir discuté avec des professeurs et des membres de la DSI de Centrale, il nous semble favorable de ne pas dispenser la totalité des enseignements sur une année mais plutôt de les éparpiller sur les 3 ans de formation, tout en labellisant l'ensemble de la formation centralienne.

Comme les 4 modules n'ont pas à être abordés dans leur totalité pour obtenir la labellisation, nous avons décidé de dispenser les 2 premiers à tous les élèves durant leur tronc commun de 1<sup>ère</sup> et 2<sup>ème</sup> année ; et le dernier durant la 3A digitale. Ceci nous permettra de certifier la formation entière et de garder le 4<sup>ème</sup> volet, plus technique et approfondi, pour les élèves s'intéressant davantage au domaine du numérique, les 2 premiers modules étant des bases que tout le monde se doit d'avoir en sortant d'une grande école d'ingénieur. De cette manière, nous souhaitons attirer l'attention de tous les élèves sur l'importance de la sécurité informatique, qu'ils s'intéressent au domaine informatique ou non. Ils doivent comprendre que la sécurité informatique n'est pas à diaboliser et concerne chacun d'entre nous.

## III. De la formation au label : propositions et perspectives d'intégration des enseignements Cyberedu dans le cursus de l'élève centralien

### **III.A. Perspectives d'intégration**

Le label Cyberedu se décline sur plusieurs thèmes de cours. Néanmoins, tous ne doivent pas obligatoirement être enseignés durant la formation de l'ingénieur pour prétendre à l'obtention du label Cyberedu. Ainsi, trois, voire quatre, thèmes pourraient être intégrés à la formation. Ils apparaissent en adéquation avec l'enseignement proposé par Centrale Marseille et viendraient alors approfondir ou orienter vers de nouvelles perspectives les enseignements déjà abordés. Il s'agit des « notions de base », de « l'hygiène informatique » et de « la gestion de la cybersécurité au sein d'une organisation ».

Afin d'intégrer un pan aussi conséquent que le label CyberEdu à la formation déjà bien complète de l'élève centralien, plusieurs problématiques peuvent être soulignées. Il s'agit d'une part de relier de tels enseignements à ceux déjà existants, afin de continuer à intéresser l'élève au-delà de ses activités traditionnelles, pour lui faire envisager l'ampleur et l'importance des notions de cybersécurité dans son parcours, et plus loin : dans sa vie quotidienne et son futur professionnel.

D'autre part, il convient de réfléchir à la manière dont peuvent être dispensés ces cours. Si l'association CyberEdu fournit effectivement une mallette pédagogique très complète et détaillée sur les thèmes à aborder, leur forme reste libre.

Enfin, parallèlement à la question de la forme prise par le cours associé à CyberEdu, se posent les problèmes pratiques traditionnels de toute école : quels professeurs seraient en mesure d'aborder et d'enseigner, de manière pertinente, pédagogique et dynamique, les thèmes de CyberEdu, qui sortent de l'ordinaire en n'étant pas considérés comme une matière à part entière. Par ailleurs, l'épineuse question du volume horaire et l'intégration à proprement parler de CyberEdu dans la formation centralienne doit évidemment être soulevée.

### **III.B. Propositions d'intégration**

#### III.B.1. Comment relier Cyberedu à l'enseignement existant

L'enseignement à l'Ecole Centrale se divise schématiquement et dans la majorité des cas en trois temps.

##### *III.B.1.i. Temps 1 : le tronc commun*

Un premier temps correspond au tronc commun qui dure trois semestres (S5, S6 et S7). Bien que chaque année, la promotion entrante compte toujours plus d'élèves, il s'agit d'établir une estimation moyenne : une promotion peut être considérée comme un ensemble de 300 élèves, à l'horizon 2018-2019. Le tronc commun, réformé à partir de l'année prochaine, va s'articuler autour de matières clés, indispensables et obligatoires pour tous, accompagnées d'un choix de matières optionnelles. Ce tronc commun doit être considéré comme un premier champ d'action pour l'implantation du label CyberEdu, profitant que tous les élèves soient encore réunis dans un même parcours, à un niveau sensiblement identique de connaissances informatiques.

##### *III.B.1.ii. Temps 2 : le S8*

Un deuxième temps correspond à la deuxième partie de deuxième année, le « S8 ». Une partie de la promotion est alors hors des murs, l'autre partie est divisée entre différents parcours, sans tronc commun apparent. A partir de ce constat, il apparaît comme difficilement réalisable de poursuivre CyberEdu au S8.

##### *III.B.1.iii. Temps 3 : la troisième année*

Un troisième et dernier temps correspond au retour en troisième année. Une partie de la promotion est alors définitivement partie en double diplôme à l'étranger ou dans une université partenaire. Ces élèves ne sont donc a priori pas focalisés sur la poursuite d'une formation orientée sur l'informatique et partenaire de CyberEdu. Restent alors les élèves centraliens, qui, bien que spécialisés dans des parcours dont un en informatique (« parcours digital »), partagent encore un tronc commun. Ce dernier représente une dernière

opportunité de poursuivre la formation CyberEdu en faisant profiter un maximum d'élèves du label mais surtout de ses enseignements, indispensables à notre époque et encore plus à la veille de leur entrée sur le marché du travail, par leur stage de fin d'études.

Il existe donc deux champs d'actions sur lesquels l'implantation de Cyberedu semble opportune et réalisable.

### III.B.2. Sous quelle forme peut être dispensé Cyberedu ?

L'enseignement supérieur présente l'avantage de pouvoir dispenser des cours sous différentes formes et à travers différents supports. Chacun possède ses avantages comme ses inconvénients, chacun se prête plus naturellement à un type d'enseignement. Néanmoins, le choix de la diversité dans la présentation d'un enseignement aussi inédit que CyberEdu peut être une manière de garder l'élève intéressé et dynamique jusqu'à la fin de sa formation.

#### *III.B.2.i. Le cours magistral*

L'Ecole Centrale s'est dotée d'une nouvelle structure, encore en travaux, qui devrait à terme pouvoir accueillir l'intégralité d'une promotion en un seul et même espace.

L'intérêt du cours magistral se trouve justement dans le fait qu'il permette de réunir la promotion en un cours, pour dispenser le même contenu en maximisant le temps et l'espace. Néanmoins, la difficulté que présente le cours magistral, qui est d'autant plus vraie que CyberEdu est un enseignement inédit et pas forcément pertinent aux yeux de tous les élèves, se trouve dans le choix de l'enseignant. La personne en charge d'un tel format de cours doit y être habituée et suffisamment habile pour garder éveillé, voire susciter l'intérêt, de son public peu familier avec les règles de la sécurité informatique.

#### *III.B.2.ii. Le cours restreint*

Le cours restreint est ici entendu comme un cours dispensé en salle de cours traditionnelle, par un seul professeur ou intervenant, devant un groupe réduit d'élèves – une trentaine.

Ce format tient son intérêt au fait que le professeur et les élèves peuvent interagir plus aisément, plus librement, que dans un amphithéâtre. D'autre part, devant un groupe aussi restreint, un intervenant - hors du corps professoral - peut également enseigner : moins d'agitation, plus de contacts avec les élèves, qui sont souvent plus attentifs, personnalisation du cours, adaptation du contenu selon les questions. Cependant, le cours restreint présente plusieurs inconvénients : division de la promotion en groupes, besoin de salles et de professeurs donc coût financier sans doute à prévoir.

#### *III.B.2.iii. Le MOOC*

Comme évoqué précédemment, le label CyberEdu requiert un enseignement sur différents thèmes. Toutefois, aucune forme ni aucune contrainte particulière ne sont indiquées. Le MOOC a été évoqué parmi les propositions pour intégrer plus facilement CyberEdu dans les formations déjà bien chargées des élèves centraliens. Il ne concernerait évidemment pas l'intégralité du label, mais peut soulager la formation dans ses points de tensions.

Ce format n'est qu'une suggestion et la piste n'a pas été suffisamment creusée, mais l'idée se devait d'apparaître comme une possibilité.

#### *III.B.2.iv. Les séminaires*

Par « séminaires », il s'agit d'entendre un volume horaire consacré exclusivement à Cyberedu, mais ne se répétant pas de manière hebdomadaire.

L'idée tenait ici à proposer une série de demi-journées obligatoires, réparties sur les trois premiers semestres (S5, S6 et S7) et le S9, afin d'assurer l'enseignement CyberEdu. Il s'agirait de banaliser une demi-journée sur chaque semestre afin de traiter un thème de CyberEdu.

L'intérêt consiste à ne pas surcharger les semaines pleines des élèves centraliens, notamment sur le tronc commun, tout en traitant de manière effective et efficace les thèmes de CyberEdu.

### III.B.3. Quel volume horaire et quels professeurs sont nécessaires à la réalisation du projet ?

Dans son essence même, CyberEdu a été créée pour sensibiliser et informer les élèves à des sujets rencontrés au quotidien à notre époque, mais porteurs de problématiques et de responsabilités importantes. Ainsi, les thèmes de CyberEdu ne sauraient être bâclés dans leur enseignement : si l'Ecole Centrale fait le choix de se lancer dans cette démarche, en sélectionnant trois, voire quatre, thèmes, alors il s'agit de les enseigner correctement et en acceptant le volume horaire qui y est nécessairement imputé. Chaque thème est estimé à un volume horaire de cinq à six heures chacun. Néanmoins, il s'agit d'observer quelle répartition effective peut être appliquée afin d'optimiser l'enseignement.

#### *III.B.3.i. Propositions de répartition horaire*

Les thèmes n°1 (« notions de base ») et n°2 (« hygiène informatique ») sont abordables pour des élèves de tronc commun. Il s'agirait de répartir dix à douze heures de cours sur trois semestres cumulés. Deux propositions sont alors à débattre : soit ce volume est réparti sous la forme d'un module sur le tronc commun, à raison de tranches de deux heures par semaine et par élève ; soit il est scindé sous forme de « séminaires », de trois ou quatre heures chacun, à raison de un séminaire par semestre.

Le thème n°4 (« gestion de la cybersécurité au sein d'une organisation ») représente six heures de cours par élève également. Néanmoins, au vu de son niveau technique, il s'agirait de l'implanter dans le tronc commun de troisième année – voire uniquement dans le tronc commun du parcours digital. Là encore, la forme reste à définir.

#### *III.B.3.ii. Equipe enseignante*

Quant aux professeurs susceptibles de participer au projet, ils viennent de divers horizons. L'équipe pédagogique strictement informatique, qui a motivé ce projet au nom de Monsieur Pascal Préa, pourrait assurer une part des enseignements. Des professeurs de matières transversales peuvent également être sollicités : en sciences sociales et plus particulièrement en droit des données, des remises à niveau seront très certainement à faire et devront alors impliquer des professeurs spécialisés dans ce domaine. Enfin, les intervenants du CRI, qui participent déjà à l'enseignement informatique en tronc commun, peuvent aussi prendre part au développement de ce projet : ils sont avertis sur le sujet et possèdent un regard parfois différent, plus concret, que les professeurs, au vu de leurs expériences professionnelles et informatiques.

## Conclusion

Ce projet, portant sur l'analyse de la faisabilité de la mise en place du label CyberEdu à l'Ecole Centrale de Marseille, a pu révéler plusieurs perspectives quant à l'avenir de l'établissement autant que de ses élèves.

Il apparaît aujourd'hui totalement inenvisageable de laisser des élèves ingénieurs entrer dans le monde du travail en toute indifférence des notions de base de cybersécurité. Effectivement, les élèves de l'ECM, de par leur cursus et leur profil, sont appelés à tenir des postes à fortes responsabilités dans la société de demain, qui sera encore plus numérisée qu'à présent. Il incombe ainsi à l'Ecole Centrale de fournir aux élèves, outre le bagage scolaire d'excellence scientifique et les multiples compétences entrepreneuriales, une conscience des risques dans le cyberspace, qui prennent divers visages – du technique au juridique – auxquels l'ingénieur centralien sera confronté sans exception. Par ailleurs, outre cette responsabilité de sensibilisation et de formation qui appartient à l'Ecole Centrale, le label Cyberedu représente un enjeu de taille quant au prestige de l'établissement. En effet, il paraît important de rappeler, encore une fois, que seules des formations exclusivement informatiques ou techniques ont jusqu'ici été labellisées. L'Ecole Centrale de Marseille pourrait être la première école d'ingénieur généraliste à proposer une formation intégrant un enjeu d'actualité et d'avenir qu'est la cybersécurité, ce qui représente un atout non négligeable pour son rayonnement auprès des étudiants comme envers ses consœurs.

Finalement, le label CyberEdu, bien que dérivant de la très sérieuse ANSSI, apparaît avant tout comme réellement désireux d'éveiller les ingénieurs de demain aux problématiques de sécurité informatique. Ainsi, les différents thèmes abordés par le cursus concernent certes la matière informatique, mais sous le prisme de la polyvalence. Les cours sont abordables, sont réalisables, et sont certainement suffisamment variés pour attirer l'attention de tous les élèves. Quant à la mise en place du label au sein de l'établissement, elle demande des efforts d'organisation et une mobilisation de ressources – humaines et financières – qui n'apparaissent pas plus importants que pour la mise en œuvre d'une matière « classique », et pourrait apporter à l'ECM un attrait et un rayonnement inédit.