

La sécurité du numérique dans l'enseignement supérieur

Olivier Levillain

Responsable du centre de formation à la SSI
ANSSI
51 boulevard Latour Maubourg
75700 Paris 07 SP

Pascal Chour

Responsable adjoint du centre de formation à la SSI
ANSSI
51 boulevard Latour Maubourg
75700 Paris 07 SP

Résumé

En 2013, le livre blanc de la Défense et de la Sécurité Nationale précisait : « [...] Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique ». Ces deux demandes sont à l'origine de deux dispositifs mis en place par le centre de formation à la SSI de l'ANSSI : SecNumedu, un programme de labellisation de formations de l'enseignement supérieur spécialisées en sécurité du numérique, et CyberEdu, une démarche qui vise à sensibiliser les futurs professionnels de l'informatique aux problématiques de la sécurité en intégrant de la sécurité dans les formations du numérique non spécialisées en sécurité.

Mots-clefs

CyberEdu, SecNumedu, SecNumacadémie, sécurité du numérique, formation initiale, formation continue, ANSSI, CFSSI.

1. Introduction

Le centre de formation à la SSI (CFSSI) a pour activité traditionnelle la formation des personnels des fonctions publiques à la sécurité des systèmes d'information. Cette activité passe par des stages courts, d'une journée à quelques semaines, et par une formation longue menant à un titre inscrit au registre national de la certification professionnelle (RNCP) de niveau I (niveau Bac+5), le titre d'expert en sécurité des systèmes d'information (ESSI).

Il est probable que pour la France, la formation de niveau BAC+5 la plus ancienne dans le domaine de la sécurité soit celle du service du chiffre qui date de 1957 (le brevet d'études cryptographiques supérieures, BECS). Cette formation a été héritée par le secrétariat central de la sécurité des systèmes d'information (SCSSI) à sa création en 1986 sous le nom de brevet d'études supérieures en SSI (BESSI), puis par la direction centrale de la sécurité des systèmes d'information (DCSSI) et enfin par l'agence nationale de la SSI (ANSSI). Le nom actuel du titre est ESSI.

Jusque dans les années 1980, cette formation était essentiellement consacrée à la cryptologie comme le montrent les mémoires des étudiants de l'époque (ce qui est normal étant donné l'orientation du programme de l'époque).

La création du SCSSI entérine le fait que la sécurité dite « logique » ne peut se résumer à la seule cryptologie. À travers le nom « système d'information », la sécurité des systèmes informatiques

devient un sujet d'étude, la cryptologie n'étant plus qu'une composante. Là encore, les thèmes des mémoires traduisent cette évolution : en 1988, sur les 8 mémoires disponibles, 4 traitent de cryptographie, 2 d'évaluation de la sécurité (les TCSEC¹ américains étaient sortis en 1984 et les ITSEC² européens étaient en cours de spécification) et 2 de la sécurité des technologies de l'information. Pour la petite histoire, concernant les aspects « évaluation », on peut aussi rappeler que la cryptographie était exclue du champ de l'évaluation faite par les laboratoires (en France, les centres d'évaluation de la sécurité des technologies de l'information, ou CESTI), celle-ci étant réservée aux agences étatiques. Les choses ont officiellement changé en France à partir de 2005).

À titre d'information, pour la promotion 2016-2017, seuls deux mémoires portaient spécifiquement sur la cryptographie, les 8 autres portant sur d'autres aspects de la sécurité informatique.

Pour autant, ce n'est pas parce qu'elle n'était pas spécifiquement enseignée, en dehors parfois de quelques modules d'un parcours informatique, que la SSI était absente des réalisations industrielles en dehors du domaine militaire.

En France, l'invention de la carte à microprocesseur par la société Bull en est un bon exemple, encore d'actualité en 2017. En dehors des aspects cryptographiques, les fonctionnalités de sécurité et l'architecture même de la carte montrent que l'on était en mesure de réaliser des produits de très haut niveau de sécurité avec des mécanismes de protection logique extrêmement sophistiqués.

On rappellera qu'à l'époque, pour l'essentiel, la sécurité (technique et toujours hors crypto) était associée à la fois à une tournure d'esprit couplée à une compétence pointue dans le domaine de l'informatique, de l'électronique (pour certains), et des réseaux. Ces fondamentaux restent indispensables en 2017 mais la professionnalisation du secteur a amené à créer des formations spécifiques permettant l'acquisition d'un socle de compétences de base dès la formation initiale. De plus, l'apparition de « nouveaux » métiers a contribué à ce besoin de formation et de spécialisation : on ne forme pas un spécialiste en cyberdéfense comme un spécialiste du développement sécurisé de logiciels.

En février 1992, le bulletin de liaison de l'AFUU³ identifiait seulement deux formations en sécurité (hors crypto pure, et en excluant la formation du SCSSI) :

- une formation de l'ENST⁴ créée en 1990 (5 étudiants diplômés en 1991) ;
- une formation de l'ENSTA⁵ créée en 1991 (13 étudiants formés en 1991).

La situation était à peine meilleure 10 ans plus tard alors que la montée en puissance de l'Internet changeait rapidement la donne.

Même s'il est toujours délicat de donner des dates précises, les années 2010 voient se multiplier les inquiétudes des industriels sur la pénurie de compétences dans le domaine. En particulier, la création de l'ANSSI et le renforcement du pôle SSI de la DGA-MI⁶ créent une demande importante de personnes spécialisées sur ces sujets ce qui amènera certains à exprimer des récriminations sur l'assèchement du marché.

C'est dans ce contexte que le livre blanc de la Défense et de la Sécurité Nationale de 2013 précisait : « [...] Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique ».

Cette volonté sera encore renforcée par la parution en 2015 de la stratégie nationale pour la sécurité du numérique du Premier ministre de l'époque.

1 *Trusted Computer System Evaluation Criteria.*

2 *Information Technology Security Evaluation Criteria.*

3 Association Française des Utilisateurs d'Unix, aujourd'hui, l'AFNeT pour association francophone des utilisateurs du Net.

4 École nationale supérieure des télécommunications.

5 École nationale supérieure de techniques avancées.

6 Direction générale de l'armement – maîtrise de l'information (anciennement CELAR).

Ces deux documents constitueront la base de légitimité permettant à l'ANSSI de lancer plusieurs actions visant à répondre à ces demandes. Les paragraphes suivants permettent de faire le point sur celles qui ont été lancées, avec les premiers retours d'expérience, et sur celles qui pourraient suivre dans les années à venir.

2. SecNumacadémie

L'objet de ce document n'est pas de traiter des actions visant la sensibilisation du grand public. Toutefois, il faut signaler le lancement par l'ANSSI d'une formation en ligne ouverte à tous (un MOOC⁷) sur la sécurité du numérique car certaines demandes tendent à montrer que ces modules de sensibilisation pourraient participer plus qu'initialement prévu à la « formation » des utilisateurs en milieu professionnel.

Le MOOC a d'abord été conçu pour permettre la sensibilisation des personnes à titre privé à la sécurité du numérique. La plateforme comportera 4 modules en mars 2018, dont deux sont déjà disponibles. L'accès est gratuit et ouvert à tous en continu (contrairement aux MOOC classiques qui fonctionnent par session).

Plusieurs organismes publics (français et étrangers) ont fait part de leur souhait de disposer de cette formation pour permettre la sensibilisation de leurs personnels en situation professionnelle. Une extension de SecNumacadémie est à l'étude pour permettre l'usage de cette formation dans ce contexte.

3. CyberEdu

Depuis plusieurs années, on entend régulièrement des annonces, en France ou à l'étranger, affirmant que les besoins en sécurité du numérique sont immenses et qu'il faut former plus d'experts en cybersécurité. Bien que ce constat soit avéré, il est important de comprendre que la sécurité du numérique ne doit pas reposer uniquement sur des experts. Chaque acteur de la chaîne des systèmes d'information (administrateur, développeur, chef de projet, etc.) doit se sentir concerné et être impliqué, afin que la sécurité soit prise en compte tout au long des projets et de la vie des systèmes. On parle parfois de « *security by design* ».

Ainsi, tout administrateur réseau devrait savoir que les adresses réseau source d'un paquet peuvent être trivialement modifiées. Cela permettra d'éviter que le filtrage par adresse MAC soit vu comme un mécanisme de défense absolu. De manière similaire, tout développeur devrait avoir quelques notions concernant les vulnérabilités logicielles classiques, telles qu'un débordement de tampon (*buffer overflow* en anglais), ainsi que les moyens de s'en protéger (en effet, demander aux utilisateurs d'un site Internet de ne pas utiliser certains caractères dans leur mot de passe n'est pas une solution acceptable).

Développer chez les étudiants cet état d'esprit, cultiver ce réflexe du questionnement, susciter la curiosité face au monde du numérique, c'est la base de la sécurité.

1. Une démarche initiée par l'ANSSI

La démarche CyberEdu, initiée en 2013 par l'ANSSI, a pour objectif d'introduire des notions de sécurité dans l'ensemble des formations du numérique en France. Deux grandes actions ont été lancées par l'ANSSI pour CyberEdu : la réalisation et la mise à disposition de supports de cours destinés aux enseignants du supérieur en informatique souhaitant intégrer des éléments de sécurité dans leurs interventions, et la tenue de colloques à destination des enseignants du supérieur en informatique.

Les supports pédagogiques développés dans le cadre de la démarche CyberEdu sont disponibles en ligne⁸ sous licence *Creative Commons Attribution* (CC-BY) et comportent :

⁷Massive Open Online Course.

⁸<https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/>

- un guide pédagogique, qui présente la démarche et propose d'expliquer quelques grands principes. Parmi ceux-ci, citons l'importance de ne pas traiter la sécurité comme un module à part, mais d'intégrer ce sujet, de le tisser autant que faire se peut au sein des cours existants ;
- un ensemble de planches de présentation, représentant un cours prêt à l'emploi d'une durée de 20 heures environ. Il est à destination des étudiants de niveau licence / DUT / BTS, en vue de leur apporter les notions de base, le vocabulaire nécessaire à la compréhension des enjeux de sécurité et pour présenter succinctement l'organisation de la cybersécurité en France ;
- des fiches sur différents sujets pour les enseignants au niveau master : les systèmes d'exploitation, le réseau, le développement logiciel, l'authentification et les composants électroniques. L'objectif est de tisser au cœur d'un cours l'étude d'un sujet lié à la sécurité.

Entre 2014 et 2017, cinq colloques ont été organisés par l'ANSSI pour les enseignants du supérieur en informatique afin de leur présenter la démarche et d'échanger sur l'intégration de la sécurité dans leurs cours. Plus d'une centaine de personnes venues de toute la France ont ainsi assisté à ces colloques. Chaque colloque, d'une durée de trois jours, a été l'occasion d'aborder aussi bien des sujets techniques (systèmes d'exploitation, réseau, développement, notions de cryptographie) que juridiques et ont également permis de présenter quelques retours d'expériences.

2. L'association

Après cette première phase (2013-2016) menée par l'ANSSI, quelques limites de cette approche ont été constatées. D'une part, il semblait important d'associer durablement des enseignants à cette démarche, puisque ce sont eux les relais au cœur du dispositif. D'autre part, les colloques ont jusqu'à présent été organisés uniquement à Paris, pour des raisons logistiques.

Afin de répondre à ces limitations, l'ANSSI a proposé d'impliquer les enseignants dans la démarche, en commençant par ceux qui avaient suivi les colloques. C'est pourquoi, le 17 mai 2016, l'association CyberEdu a été fondée. Son objectif est de reprendre le flambeau en lien avec l'ANSSI. L'agence continuera en effet de s'impliquer dans la démarche CyberEdu via une participation à divers groupes de travail de l'association.

L'association a pour vocation de porter les missions suivantes :

- maintenir à jour les documents existants et en proposer de nouveaux ;
- proposer des colloques sur l'ensemble du territoire ;
- offrir un forum d'échanges entre spécialistes et non spécialistes de la sécurité ;
- labelliser des formations « CyberEdu » (voir section suivante).

4. SecNumedu

SecNumedu est un programme qui permet à l'ANSSI de labelliser des formations supérieures en sécurité du numérique qui sont *conformes* à une charte et des critères publics. Il a été lancé en juillet 2016.

À cette date, seules les formations délivrant un grade de licence ou master, ou un diplôme d'ingénieur, ou un Mastère spécialisé de la conférence des grandes écoles sont éligibles. Une extension est à l'étude pour accepter également les certifications RNCP de niveau I et II.

Concrètement, un établissement qui souhaite faire labelliser sa formation signe une charte, remplit un dossier pour démontrer sa conformité aux critères et envoie sa demande à l'ANSSI.

Si les critères sont satisfaits, l'ANSSI délivre un label valable 3 ans et publie les informations associées à la labellisation sur son site Web. Tous les ans, l'établissement est tenu de communiquer l'actualisation des informations publiées. On notera que cette labellisation est gratuite.

Il serait fastidieux d'énumérer l'ensemble des critères d'éligibilité à la labellisation. Par contre, l'esprit dans lequel ils ont été conçus mérite d'être précisé :

- SecNumedu se veut « non intrusif ». En particulier, il n'impose pas un programme défini. Ce choix a parfois étonné. Il a été discuté lors de l'élaboration du programme de labellisation par le groupe de travail et finalement écarté. À la lumière des premières labellisations, on ne peut que s'en féliciter : les établissements d'enseignement font preuve d'une grande diversité dans l'approche de la sécurité et dans la finalité des programmes. Il aurait été impossible de traduire cette diversité dans des programmes préétablis.
- SecNumedu propose une base d'information présentée de façon homogène aux étudiants, employeurs et établissements d'enseignement eux-mêmes. Il suffit de consulter les sites Web des différents établissements pour comprendre tout l'intérêt de l'approche...
- Le dossier met l'accent sur les thèmes devant être abordés⁹ (au moins au niveau sensibilisation) et sur une mise en pratique minimum : ce sont les rares critères qui peuvent avoir un impact (normalement faible) sur l'enseignement.

À ce jour, 37 formations ont été labellisées et une dizaine d'autres pourraient l'être prochainement.

La labellisation n'est que la première étape du dispositif SecNumedu. En pratique, il a donné lieu à la constitution d'une communauté de personnes intéressées par l'enseignement dans ce domaine et qui participe, tant à l'évolution du label qu'à celle de l'enseignement. Quelques exemples permettent d'illustrer ce propos :

- La première version des critères prenait mal en compte les spécificités des formations de niveau BAC+3. Des discussions ont eu lieu avec les représentants des licences professionnelles RIMS¹⁰ et ASUR¹¹. Elles ont permis de faire évoluer les critères et accessoirement, pour l'ANSSI, de mieux connaître ces formations. D'autres discussions devraient avoir lieu avec les représentants d'autres licences professionnelles.
- Les premières labellisations ont permis de constater que certains critères devaient être améliorés pour faciliter la lecture des données publiées. La version 2 des critères, applicable depuis juillet 2017, améliore ce point. Elle a été élaborée en collaboration avec les établissements labellisés ou en cours de labellisation.
- L'ANSSI était consciente que la liste des métiers était incomplète et parfois un peu obscure. Toutefois, élaborer une nouvelle liste est un travail long et délicat. L'ANSSI a donc préféré publier les critères de SecNumedu avec la liste des métiers disponibles et se laisser du temps pour travailler sur une nouvelle liste. Suite à l'étude menée par l'OPIIEC¹² à laquelle l'ANSSI a participé, une nouvelle liste a été élaborée. Elle a été proposée aux établissements d'enseignement pour commentaires. Le résultat prenant en compte les retours a été intégré à titre expérimental dans les critères de labellisation actuels. Le travail est actuellement en cours avec les employeurs pour l'améliorer. Au final, ce sous-produit de SecNumedu devrait permettre de disposer d'une liste de métiers plus représentative de la réalité et qui remplacera celle actuellement disponible sur le site Web de l'ANSSI.
- En juin 2017, le bureau « politique industrielle » de l'ANSSI a présenté aux établissements labellisés ou en cours de labellisation un état des lieux des besoins dans le domaine des COS¹³. Suite à cette présentation, il a été décidé de monter un groupe de travail entre les industriels du secteur et les établissements d'enseignement intéressés pour identifier plus

9La liste initiale des thèmes provient du guide pédagogique CyberEdu.

10Réseaux informatiques mobilité et sécurité.

11Administration et sécurité des réseaux

12Observatoire paritaire de l'informatique, de l'ingénierie, des études et du conseil.

13Centre opérationnel de sécurité ou SOC pour *Security Operations Center*.

précisément comment faire évoluer les programmes pour répondre à la demande. Un des objectifs est aussi de déterminer ce qui est du domaine de la formation initiale et de la formation continue.

Début 2017, on estimait à environ une soixantaine le nombre de formations spécialisées en sécurité de type Licence, Master, Mastère spécialisé et Ingénieur en France. Pour information, les statistiques issues de SecNumedu montrent que près des trois quarts de ces formations ont été créées entre 2005 et 2017.

Une projection sur le flux de sortie annuel par rapport aux formations actuellement labellisées par l'ANSSI (ne prenant donc pas en compte les formations inscrites au RNCP) donne un nombre de diplômés potentiel de 1500 personnes environ.

Une étude réalisée par l'OPIIEC en mai 2017 conclut que les capacités d'accueil actuelles sont probablement suffisantes pour un marché de l'emploi en régime permanent. Il faut tempérer ce constat par le fait que l'estimation du flux de sortie est un maximum alors que beaucoup de formations ne font pas le plein pour ce que constate l'ANSSI.

On peut espérer que SecNumedu donnera une meilleure visibilité sur ce domaine et que la communauté ainsi créée améliorera encore son attractivité, tant pour les étudiants français qu'étrangers.

Mais le problème actuel est que l'on ne se trouve pas en régime permanent mais plutôt dans un régime de pénurie et que la demande instantanée semble beaucoup plus importante que le flux de sortie annuel.

La formation continue longue ou courte est probablement l'une des voies les plus prometteuses pour augmenter à court-terme le nombre de personnes formées, en particulier, via des reconversions de personnes expérimentées dont la spécialité actuelle est moins demandée.

5. SecNumedu – FC

À la date de rédaction de ce document, il s'agit encore d'un projet qui devrait voir son aboutissement avant fin 2017. Certaines informations exposées ici peuvent être remises en cause d'ici là. Il correspond à la vision de l'ANSSI à un instant donné sur le futur dispositif.

SecNumedu - FC (ou SecNumedu - Formation continue) est le nom du projet de l'ANSSI visant à référencer les formations continues courtes (quelques jours à quelques semaines) dans le domaine de la sécurité du numérique. Comme SecNumedu, il vise à donner une meilleure visibilité à ces formations. Ce référencement est gratuit. Son fonctionnement est proche de celui de SecNumedu à savoir : l'organisme de formation continue qui souhaite faire référencer sa formation s'engage sur une charte et remplit un dossier comportant pour l'essentiel 2 critères et des informations à publier :

- la certification associée à la formation doit être inscrite à l'inventaire de la CNCP¹⁴ ;

ou

la formation se réclame conforme à un cahier des charges approuvé par l'ANSSI. La liste des cahiers des charges se trouve dans le dossier de demande de référencement. À cette date, il existe deux cahiers des charges (un concernant la sécurité des systèmes industriels, l'autre la formation d'un référent sécurité du numérique pour les TPE et PME) ;

- 70 % de la formation doivent être dédiés à la sécurité.

Le projet apparaît comme moins ambitieux que SecNumedu : c'est pourquoi l'ANSSI préfère parler de « référencement » plutôt que de « labellisation ». Il ne fait dans un premier temps que répondre à une demande des industriels et de certains organismes de formation continue : améliorer la visibilité des formations dans ce domaine en les référençant sur le site Internet de l'ANSSI.

14 Commission nationale de la certification professionnelle

En première analyse, on pourrait objecter qu'un tel référencement fait double emploi avec l'inventaire de la CNCP sur lequel il s'appuie en partie.

En fait, il faut plutôt parler de complémentarité : l'inventaire de la CNCP référence des certifications professionnelles alors que l'ANSSI référence des formations. Les organismes concernés ne sont pas forcément les mêmes dans les deux cas.

Par ailleurs, les certifications professionnelles en sécurité référencées par l'inventaire sont noyées dans la masse des autres certifications. Pour beaucoup de professionnels, il apparaît plus simple de consulter un site dédié au sujet et celui de l'ANSSI est aujourd'hui considéré comme un site légitime et de référence pour de telles publications. Finalement, l'ANSSI agit comme un relais vis-à-vis de la CNCP : lorsque les certifications associées aux formations référencées sont inscrites à l'inventaire, un lien permet d'accéder directement aux informations correspondantes dans l'inventaire.

La déclaration de conformité à un cahier des charges approuvé par l'ANSSI est l'autre moyen pour faire référencer une formation. Il n'est pas antinomique avec l'inscription à l'inventaire de la CNCP.

SecNumedu-FC devrait être lancé à titre expérimental en 2017. Si le dispositif semble utile pour les professionnels, des évolutions pourront (devront) être envisagées.

6. Conclusion

L'ANSSI a mis en place plusieurs programmes complémentaires visant à promouvoir les formations en sécurité auprès des étudiants et des employeurs et à apporter une aide aux organismes de formations en facilitant par exemple, les échanges entre les employeurs et les écoles et universités.

Ces programmes ne sont pas figés. Ils peuvent évoluer, qu'il s'agisse des référentiels sous-jacents ou des services associés (animation d'une communauté par exemple).

Ils ont été pensés pour être gérables dans le temps. Pour ceux directement opérés par l'ANSSI, cela signifie que les programmes sont conçus pour être compatibles avec les ressources existantes ou prévisibles que l'ANSSI a décidé d'allouer à ces opérations. Le but n'a pas été de faire « un coup » mais bien de permettre un travail dans la durée avec les acteurs concernés par la promotion et à l'évolution du domaine.