La cybersécurité dans l'espace francophone

Etat des lieux et Enjeux

Étude réalisée par :

Belhassen ZOUARI

Novembre 2016

Sommaire Exécutif

Le présent rapport fait un état synthétique de la situation actuelle, des programmes d'action et des tendances dans le domaine de la cybersécurité au sein de l'espace francophone. Trois aspects sont particulièrement étudiés à savoir la *formation*, la mise en place de *centres d'alerte et de réaction aux attaques informatiques* (CERT) et le *partenariat international* en cybersécurité. La démarche suivie est balisée par les éléments de la stratégie de la francophonie numérique– « Horizon 2020 » établie lors du sommet de Kinshasa en octobre 2012 et dont plusieurs de ses axes touchent directement ou indirectement les exigences de la cybersécurité.

Le premier fait saillant est l'écart manifeste entre les pays avancés et les PED à l'image du fossé numérique généralement présent entre les deux catégories de pays à l'échelle mondiale. L'étude a montré qu'au sein même des PED francophones il y a deux sous ensembles de pays qui se distinguent. Le premier groupe dispose de certains éléments de stratégie en cybersécurité et de certains mécanismes d'implémentation à la hauteur des moyens nationaux. Le deuxième groupe, aucune vision n'est perceptible ni d'actions concrètes d'envergure nationale en cybersécurité. Le deuxième constat est *l'interdépendance* des trois axes (formation, CERT et partenariat international) dans le niveau d'avancement en cybersécurité. Ainsi les pays ayant une certaine politique en cybersécurité avancent sur les trois fronts en parallèle, alors que les autres ne disposent pratiquement pas d'actions dans ce sens. La formation en cybersécurité apparaît comme le pilier pour construire une stratégie et un plan d'action pertinents. En effet, le développement des capacités passe essentiellement par la formation de compétences et ne nécessite que peu d'équipements (ordinateur, accès Internet, logiciels libres). L'investissement devrait donc être orienté vers le capital humain à travers la mise en place de structures et programmes francophones permettant l'émergence d'experts spécialisés, la mutualisation des compétences, l'échange de savoir-faire et la formation qualifiante dans le domaine de la cybersécurité. Le patrimoine francophone commun est sans aucun doute un facilitateur et un facteur de réussite pour un tel investissement.

De cette étude, quelques idées ou recommandations se sont dégagées :

- Création d'un CERT universitaire francophone, *CERT-UF* par exemple, qui offrirait ses services à la communauté universitaire francophone notamment les étudiants, les enseignants et chercheurs. Sa mission serait principalement orienté vers la *recherche et le développement* d'outils innovants de cybersécurité et assurant la *veille technologique* en matières de menaces et d'outils palliatifs.
- Lancement d'un consortium francophone dont les membres seraient les CERT des pays francophones créant un espace d'échange de savoir-faire et d'expertises.
- Planifier pour la définition d'un *« label »* ou forme de « certification » pour des formations en français concernant les différentes spécialités de cybersécurité.
- Création d'un *Répertoire d'Experts* et de compétences universitaires francophones en cybersécurité afin de capitaliser le savoir-faire et l'exploiter aussi bien pour la formation que pour l'assistance à la mise en place de stratégies ou de CERT.

Table des matières

1 Introduction

La Stratégie de la Francophonie numérique–Horizon 2020: « Agir pour la diversité dans la société de l'information » représente un symbole politique fort et dresse un cadre synergique pour l'adoption du numérique dans l'espace francophone.

«Cette nouvelle stratégie apporte des innovations importantes dans l'action de la Francophonie, afin que le numérique soit un des moteurs du développement et renforce la participation citoyenne, l'expression des libertés démocratiques et la place de la langue française sur la Toile en devenant un axe prioritaire de la solidarité francophone», déclarait Abdou Diouf, Secrétaire général de la Francophonie, lors de l'adoption d'Horizon 2020 [4].

Cette stratégie appelle à lever de nombreux défis. En effet, dans la quasi-totalité de ses axes stratégiques et des champs d'intervention qui en découlent, l'édification d'un *climat de confiance* est un prérequis pour le succès et le développement des services autour du numérique. L'usager, qu'il soit simple citoyen ou entreprise, ne peut adhérer en masse aux services des technologies de l'information et des communications (TIC) si la sécurité de ses données et transactions n'est pas assurée. Or, l'univers du numérique, dont Internet est un composant incontournable, bien qu'il soit un espace ouvert et libre est semé de menaces et risques de toutes sortes. Le challenge est donc de saisir toutes les opportunités offertes par cet univers tout en évitant les dangers qui les accompagnent. De par la complexité de la question, cet objectif ne saurait être atteint sans la conjugaison des efforts de plusieurs acteurs : les gouvernements, la société civile, les entreprises, les citoyens, etc.

Cette étude tente justement de dresser un état des orientations et des différentes actions pour renforcer la cybersécurité dans l'espace francophone. Elle focalisera sur les principaux moyens de mise en œuvre des politiques de cybersécurité, en particulier la *formation*, la mise en place de *centres d'alerte et de réaction aux attaques informatiques* et le *partenariat international*. Ces différents éléments entrent dans le renforcement des capacités des pays à faire face aux menaces cybernétiques. Ils interviennent de manière transversale dans les quatre axes stratégiques de la Francophonie numérique 2020 décidés lors du sommet de Kinshasa en octobre 2012 [4] :

I. Accompagner l'innovation pour l'intégration des pays en développement (PED) dans l'économie numérique
II. Édifier des sociétés de l'information ouvertes, transparentes et démocratiques en Francophonie
III. Développer l'intelligence numérique au service de la diversité et du partage
IV. Produire, diffuser et protéger les biens communs numériques

Le développement des capacités opérationnelles passe par la formation de compétences, l'encouragement à l'innovation technologique et l'accompagnement des jeunes à l'entreprenariat. Compter sur le savoir-faire est relativement accessible aux pays en développement pour bâtir une économie numérique et maîtriser les technologies pour la sécuriser. En effet, au moyen d'un ordinateur, d'un accès Internet et d'une formation appropriée il devient possible de former des compétences en TIC en général et en cybersécurité en particulier. L'accès aux cours en ligne, comme les MOOC (de l'anglais Massive Online Open Courses), et aux logiciels libres et ouverts est un facilitateur supplémentaire. Ceci constitue une opportunité formidable pour que les PED intègrent le concert des nations avancés dans ce domaine.

La mise sur pied de centres d'alerte et de réaction aux attaques informatiques (en anglais, CERT, pour Computer Emergency Response Team) constitue l'une des réponses efficaces que peuvent apporter les pays et leurs partenaires pour contrer l'augmentation du phénomène de la cybercriminalité. On peut définir les CERT comme des structures capables de prendre en charge la prévention et la réponse à des incidents pour les systèmes d'informations publics et les infrastructures critiques. Il existe différents types de CERT. Outre les CERT gouvernementaux ou militaires, il y a des centres académiques voués à la recherche scientifique ou à la défense d'un secteur d'activité particulier, comme les secteurs financier et énergétique.

Créer des partenariats et des collaborations à l'échelle internationale permet de faire face aux menaces qui prennent souvent leurs sources derrière les frontières d'un pays. La coordination entre pays dans le domaine de la cybersécurité doit se faire à plusieurs niveaux : stratégique, académique et opérationnel pour atteindre l'efficacité recherchée.

2 Quelle démarche pour la cybersécurité ?

Tous les experts s'accordent sur le fait que la sécurité d'un système d'information obéit à deux règles :

- Le risque zéro n'existe pas, mais il faut travailler à minimiser le risque
- La sécurité est une chaîne dont la force est celle du maillon le plus faible

La première règle implique que la sécurité doit être traitée comme un processus *continu* qui vise à réduire au plus bas les risques et ses impacts. D'ailleurs la famille des normes ISO 270xx, dédiées à la sécurité des systèmes d'information, adopte une approche d'amélioration continue de la qualité basée sur le *cycle* PDCA Planifier-Réaliser-Vérifier-Réagir (PDCA de l'anglais Plan-Do-Check-Act). La deuxième règle signifie que la sécurité doit être adressée *globalement* et que tout traitement local ou partiel ne permettra pas de se protéger contre les risques les plus courants.

A l'échelle d'un pays, il est primordial d'avoir une stratégie nationale de la cybersécurité qui donnera cette vision globale requise. Ceci implique que les politiques doivent être sensibilisés et doivent s'impliquer en prenant les décisions qui permettraient de mobiliser les acteurs et les ressources nécessaires à la mise en œuvre d'un plan d'action complet. Ainsi, la stratégie cybersécurité d'un pays doit tenir compte de l'ensemble des volets suivants :

- Définir un cadre réglementaire adapté permettant de se doter des outils juridiques nécessaires pour faire face aux nouveautés apportées par les TIC qu'il s'agisse de délits, crimes, moyens utilisés, armes ou preuves utilisant ces technologies. Sensibiliser et former les différents corps de sécurité aux méthodes d'investigation numérique.
- Développer et mettre à niveau les compétences dans le domaine de la cybersécurité. Ceci passe par inclure dans les divers cursus de formation, aussi bien académique que continue, des parcours et des modules concernant les divers aspects de la cybersécurité.
- Encourager la recherche et le développement des techniques de sécurité.
- Créer les mécanismes d'implémentation et d'application de la stratégie de cybersécurité par la mise en place de structures telles que les CERT, agences spécialisées ou équivalents.
- Protéger le cyber espace national, en particulier l'infrastructure TIC ainsi que les serveurs critiques qui lui sont reliés.
- Sensibiliser les différents usagers des TIC aux menaces et dangers émergents. En particulier, les populations les plus vulnérables comme les enfants quand il s'agit de la protection de leur données privées.
- Développer des relations de coopération internationale dans le domaine aux niveaux stratégique, juridique, académique et opérationnel.

Il apparait clair que les différentes composantes d'une stratégie nationale en cybersécurité sont interdépendantes et que l'approche globale pour les traiter devient une condition nécessaire de réussite.

Dans beaucoup de pays, la grande part de la mise en œuvre d'une telle stratégie est confiée à une ou plusieurs structures spécialisées créées en l'occasion pour coordonner et mener les différentes actions d'implémentation. Ces structures sont couramment appelées CERT(en anglais, CERT, pour Computer Emergency Response Team) et consistent en des *centres d'alerte et de réaction aux attaques informatiques*. Leur mise en place constitue l'une des réponses efficaces que peuvent apporter les pays et leurs partenaires pour pallier les menaces cybernétiques. Ces mêmes structures apparaissent également sous le nom de CSIRT (Computer Security Incident Emergency Response Team) ou SIRT (Computer Security Incident Emergency Response Team).

3 Formation et développement des compétences en cybersécurité

Miser sur le facteur humain et le développement des compétences dans le domaine des TIC est un facteur clé pour réussir l'édification d'une société du savoir. Dans la stratégie de la Francophonie numérique –Horizon 2020, le champ d'intervention 2.3 stipule de « promouvoir la sécurité, les libertés et la confiance dans l'univers numérique» [4]. Pour répondre à ces exigences, la Francophonie accompagnera les PED francophones pour mettre en place un environnement de formation permettant de diffuser les meilleures pratiques en matière de sécurité des systèmes d'information. La formation en cybersécurité permettra de soutenir un espace scientifique d'excellence au service non seulement de la mise en œuvre des stratégies nationales en cybersécurité mais aussi du partage du savoir-faire au sein de l'espace francophone. La langue, étant le vecteur majeur de transmission du savoir, ne pourra que faciliter et renforcer les actions et les collaborations universitaires pour délivrer les diplômes, certifications et qualifications nécessaires au développement de compétences.

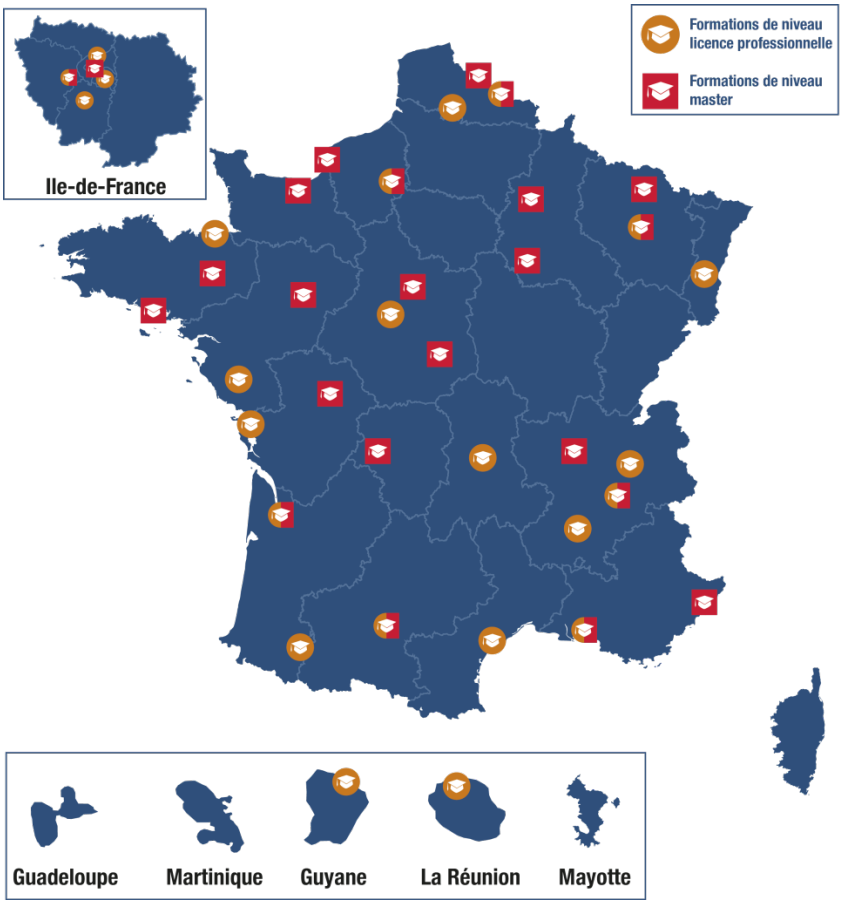
De nombreux pays, y compris dans l'espace francophone, soutiennent particulièrement les formations en cybersécurité. On distingue les *formations universitaires* classiques avec des diplômes de type License, Master ou Ingénieur. Néanmoins, la *formation continue* reste importante compte tenu du fait que les technologies visées sont très évolutives et qu'il devient impératif aux compétences actives de maintenir à jour le niveau de leurs connaissances. Afin de soutenir et compléter les efforts de renforcement des capacités, un troisième type de formation orienté *sensibilisation* est nécessaire pour protéger les particuliers et maîtriser les usages de chacun dans un monde où la cybercriminalité est en forte croissance et où il est de plus en plus difficile d'assurer la protection de ses données à caractère personnel.

L'offre de formation dans les domaines de la cybersécurité dans les pays avancés est riche. Ceci s'explique d'une part par une forte demande, issue du marché de l'emploi, des profils en cybersécurité et d'autre part par la disponibilité des moyens pour assurer ce type de formation en termes d'enseignants et formateurs qualifiés principalement.

Le journal Le Monde dans son édition électronique du 05 février 2016 titrait «Mastères spécialisés : la cyberdéfense, une priorité». Renforcer la sécurité des espaces numériques est devenu une priorité nationale en France [11]. Dans ce contexte, l'offre de formation s'est rapidement développée ces dernières années, qu'elle soit dans le domaine de la cybersécurité, c'est-à-dire la protection des données, ou dans celui de la cyberdéfense, qui prévoit la riposte. Récemment, deux nouveaux mastères spécialisés ont obtenu l'accréditation de la Conférence des grandes écoles (CGE) et sont venus s'ajouter aux cinq autres qui existaient déjà dans ces domaines.

En France, l'ANSSI (Agence Nationale française de Sécurité des Systèmes d'Information, en charge du CERT public) a collecté et publié sur son site web la liste des formations en cybersécurité délivrant un titre reconnu par l'État (ministère en charge de l'enseignement supérieur) de niveau équivalent à Bac+3 (licence professionnelle) jusqu'à Bac+5 (master, ingénieur). Cette liste a pour vocation d'informer les étudiants sur l'ensemble des programmes accessibles [12].

Carte 3.1 : Formation universitaire en sécurité des systèmes d'information en France



Les formations recensées de niveau Licence Pro sont assurées au sein de 24 établissements universitaires. Par ailleurs, on distingue 44 formations délivrées de niveau Bac+5 dont 29 Masters et 15 Ingénieurs.

Il est intéressant de noter que l'ANSSI vient d'annoncer le lancement en janvier 2017 d'un programme appelée SecNum*edu* qui consiste à attribuer un label pour les formations initiales en cybersécurité des établissements de l'enseignement supérieur [13].

L'objectif de cette labellisation est d'apporter une assurance aux étudiants et employeurs qu'une formation dans le domaine de la sécurité du numérique répond à une charte et des critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine (établissements d'enseignement supérieur, industriels…). Le programme de labellisation SecNum*edu* vise à améliorer le référencement des formations en sécurité du numérique par la mise en place d'un processus qui éprouve et garantit la pertinence de la formation par rapport à ses objectifs. Il tend également à participer au renforcement et au développement des enseignements en matière de sécurité du numérique. Le label s'appuie sur un référentiel de labellisation, dont l'élaboration a été pilotée par l'ANSSI avec la contribution d'industriels, d'écoles, du Pôle d'Excellence Cyber (PEC) et du ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche.

En Belgique, une initiative remarquable a été lancée à la rentrée universitaire 2016-2017 démontrant d'un effort conjugué de plusieurs acteurs académiques à délivrer une formation pointue en cybersécurité de type Master. Six établissements de l'enseignement supérieur proposent un nouveau Master en Cybersécurité en codiplomation impliquant quatre établissements d'enseignement universitaire : ULB, UCL, UNamur, École royale militaire et deux Hautes Ecoles : HEB et HELB. « Cette nouvelle formation, souligne Yves Roggeman – professeur à la Faculté des Sciences et coordinateur du master pour l'ULB, répond à un besoin de société et vise à former des experts à même de répondre aux défis techniques, légaux et éthiques relatifs à la sécurité des systèmes informatiques et des réseaux de télécommunications » [14].

L'Ecole Polytechnique de Montréal a renforcé pour 2016-2017 son offre de *formation en ligne* en proposant de nombreux certificats en cybersécurité dans l'objectif de développer l'expertise permettant de prendre des décisions stratégiques et d'appliquer les meilleures pratiques en défense, protection et maintien de l'intégrité des réseaux informatiques commerciaux et institutionnels sur Internet [15].

Du côté des PED francophones, on distingue une certaine disparité des moyens et des offres de formation dans les technologies de pointe en général et dans les domaines de la cybersécurité en particulier. Pour les pays comme la Tunisie et le Maroc, on observe des offres de formation qualitativement proches de ce qui est offert en France. A un degré moindre, on trouve la Côte d'ivoire et le Sénégal. Pour le reste des pays, on constate un écart notable en raison principalement du manque de moyens.

La Conférence des grandes écoles (CGE) étaye ce constat. En effet, le tableau 3.2 montre que les seuls PED francophones ayant des membres de la CGE sont le Maroc et la Tunisie [16]. Notons que la CGE est une association de grandes écoles d'ingénieurs, de management et de haut enseignement multiple ou spécifique, délivrant un diplôme sanctionnant au moins cinq années d'études après le baccalauréat et conférant le grade de Master. La CGE, organisme accréditeur de formations pour ses membres, apporte son label de qualité pour garantir l'adéquation des programmes avec les attentes du marché du travail et promouvoir, sous toutes ses formes, tant en France qu'à l'étranger, le développement et le rayonnement des établissements d'enseignement supérieur et de recherche, dans un objectif d'excellence, en liaison avec les pouvoirs publics, les acteurs de l'économie et la société.

Tableau 3.2 : établissements accrédités par le CGE offrant des formations en TIC et cybersécurité

Etablissement		**Pays**
CFVG	Centre Franco-Vietnamien de formation à la Gestion	Vietnam et France
EP Montréal	Ecole Polytechnique de Montréal	Canada
Sup'Com	Ecole Supérieure des Communications de Tunis	Tunisie
Esprit	Ecole Supérieure Privée d'ingénierie et de Technologies	Tunisie
EHTP	Ecole Hassania des Travaux Publics	Maroc
INPT	Institut National des Postes et télécommunications	Maroc
EP Louvain	Ecole Polytechnique de Louvain	Belgique

L'attribution par la CGE de l'accréditation, considérée comme un label d'excellence, à ses membres, est réalisée à travers son admission qui se fait sur des critères particulièrement exigeants portant à la fois sur la structure, les modalités de recrutement, les approches pédagogiques et l'accompagnement des étudiants dans les établissements.

Malgré cette disparité dans les offres de formation parmi les PED, on constate qu'il y a des liens de collaboration étroits et intéressants qui constitue une véritable synergie Sud-Sud. Cette dynamique est facilitée non seulement entre PED francophones en raison de la langue commune, mais aussi grâce à des coûts moins importants comparés à ceux pratiqués dans les pays les plus avancés. Un pays comme la Tunisie, présente aujourd'hui une quinzaine de Masters spécialisés dans les domaines de la cybersécurité dont huit qui se font dans des universités publiques et sept dans le secteur privé [17]. Ces chiffres ne prennent pas en compte les formations d'ingénieur en TIC ayant une orientation de cybersécurité. L'Ecole Supérieure des Communications de Tunis (Sup'Com, www.supcom.mincom.tn) dispose aujourd'hui de conventions de coopération avec l'ENSPT-Yaoundé (Ecole Nationale Supérieure des Postes et des

Télécoms) du Cameroun, l'ESATIC Abidjan (Ecole Supérieure Africaine des TIC) de la Côte d'ivoire et l'ESMT Dakar (Ecole Supérieure Multinationale des Télécommunications) au Sénégal. Pour toute ces conventions, Sup'Com assiste ses partenaires dans le montage de formation de type Ingénieur, Master ou continue dans le domaine de la cybersécurité. La collaboration avec l'ENSPT Yaoundé du Cameroun a été fructueuse et a permis depuis cinq ans la sortie de plusieurs promotions d'ingénieurs qualifiés. Aujourd'hui, cette collaboration s'est hissée au niveau doctoral en permettant à des enseignants de l'ENSPT Cameroun de s'inscrire en thèse de doctorat à Sup'Com. Cette dernière initiative permettra de créer un nouveau corps d'enseignants du supérieur capable de prendre le relais et mener de manière autonome les formations en cybersécurité initiées conjointement. Sur un autre registre, la collaboration peut être multilatérale impliquant plusieurs acteurs internationaux. Par exemple, en 2008 et 2009, certaines actions de formation financées par le CNUCED (Conférence des Nations Unies sur le commerce et le développement) ont permis de créer des compétences en cybersécurité, dans environ une vingtaine de pays francophones d'Afrique, qui sont aujourd'hui des responsables dans leur pays respectifs impliqués dans des programmes spécialisés. Ces actions ont été organisées à Tunis avec le concours de l'ANSI Tunisie qui a été déclaré par le CNUCED « Centre d'excellence » en cybersécurité. Ainsi, l'ANSI avait la responsabilité des aspects pédagogiques et logistiques de la formation et le CNUCED finançait la prise en charge des participants. Plusieurs PED francophones ont pu bénéficier de ces actions dont l'objectif était de renforcer les capacités en cybersécurité de ces pays à travers une formation pointue donnée à un ou deux de ses représentants.

4 CERT : outil d'implémentation opérationnel de la cybersécurité

On peut définir les CERT comme des structures capables de prendre en charge la prévention et la réponse à des incidents touchant les systèmes d'information et les infrastructures critiques d'entreprises publiques ou privées. Les CERT sont particulièrement efficaces pour contrer le phénomène croissant de la cybercriminalité mais peuvent se positionner aussi à un niveau plus stratégique quand il s'agit de cyber-espionnage et cyber-guerre.

Un CERT peut être vu comme un centre opérationnel spécialisé en cybersécurité qui offre des services à la carte pour le compte d'un groupe de clients. Ses clients peuvent être un département gouvernemental, un groupe d'entreprises privées, une université ou tout consortium ayant des intérêts communs à protéger leurs infrastructures et systèmes d'information TIC. Ainsi, on distingue différents types de CERT ; outre les CERT gouvernementaux ou militaires, il y a des centres qui prennent en charge la sécurité du système d'information d'entreprises ou entités d'un secteur d'activité donné. Par exemple, les CERT académiques ont une mission plus orientée scientifique et de

recherche. Par ailleurs, on observe particulièrement des CERT travaillant pour le compte d'un groupe financier où les enjeux sont évidemment majeurs. D'autres secteurs comme les télécoms ou l'énergie sont également conscients et concernés par cette question.

Dépendamment du type de CERT, les services offerts peuvent varier légèrement en adéquation avec les besoins de ses clients. Néanmoins, on peut distinguer un noyau de services communs qui forment la mission principale d'un CERT. On peut citer :

- Veille technologique aussi bien en termes de nouvelles menaces et attaques (virus, malware, etc.) qu'en termes de nouveaux outils et techniques palliatifs.
- Information et alerte dès que les résultats de la veille technologique font apparaître des menaces concrètes ciblant les systèmes d'information des clients.
- Sensibilisation et formation des usagers travaillant sur les systèmes d'information cibles.
- Surveillance et détection d'incidents (virus, attaques, etc.) ayant touchés l'infrastructure et les systèmes d'information opérationnels.
- Gestion d'incidents et réponse immédiate afin de contenir l'impact sur le fonctionnement des services dépendants des TIC du client.
- Analyse de l'incident et investigation numérique afin de tirer les enseignements permettant d'améliorer les procédures en vigueur.
- Mise en place de *plan de continuité des activités* et de reprise après incident.

En tout état de cause, un CERT est considéré par ses clients comme étant *l'expert en cybersécurité* qu'il est utile de consulter et éventuellement impliquer dans toute réflexion ou planification dans tout projet TIC. En effet, il est beaucoup plus facile, et donc moins couteux, d'intégrer la composante sécurité dès l'étape de conception. Définir directement une architecture sécurisée d'un système d'information est plus judicieux que d'implanter un système d'information puis chercher à la sécuriser.

5 Situation des CERT dans l'espace francophone

La création d'un CERT est une étape majeure dans la mise en œuvre d'un plan d'action pour la sécurité de l'infrastructure TIC et des systèmes d'information relatifs. Dans la suite, on s'intéressera au mouvement au niveau mondial ayant mené à la création de CERT.

5.1 Historique

Le premier CERT au monde est le CERT Coordination Center (CERT/CC, www.cert.org). Il a été lancé en 1988 aux états unis par DARPA (Agence américaine pour les projets de recherche avancée de défense) suite à l'attaque du ver Morris sur le réseau Internet. L'université de Carnegie Mellon abrite le CERT/CC et dirige un programme de recherche fédéral de cybersécurité. La dénomination CERT est une marque déposée de l'université de Carnegie Mellon ce qui explique l'utilisation par les autres centres de dénominations similaires telles que CSIRT et SIRT. Ensuite, sont venus plusieurs autres CERT, principalement gouvernementaux, à travers le monde. On focalisera dans la suite sur les CERT créés dans l'espace francophone.

5.2 Répartition des CERT au sein de l'espace francophone

La répartition des CERT à travers le monde et en particulier dans l'espace francophone fait apparaître la faille numérique que l'on trouve entre pays en développement et pays avancés. Le tableau suivant illustre les pays de l'OIF ayant au moins un centre de type CERT.

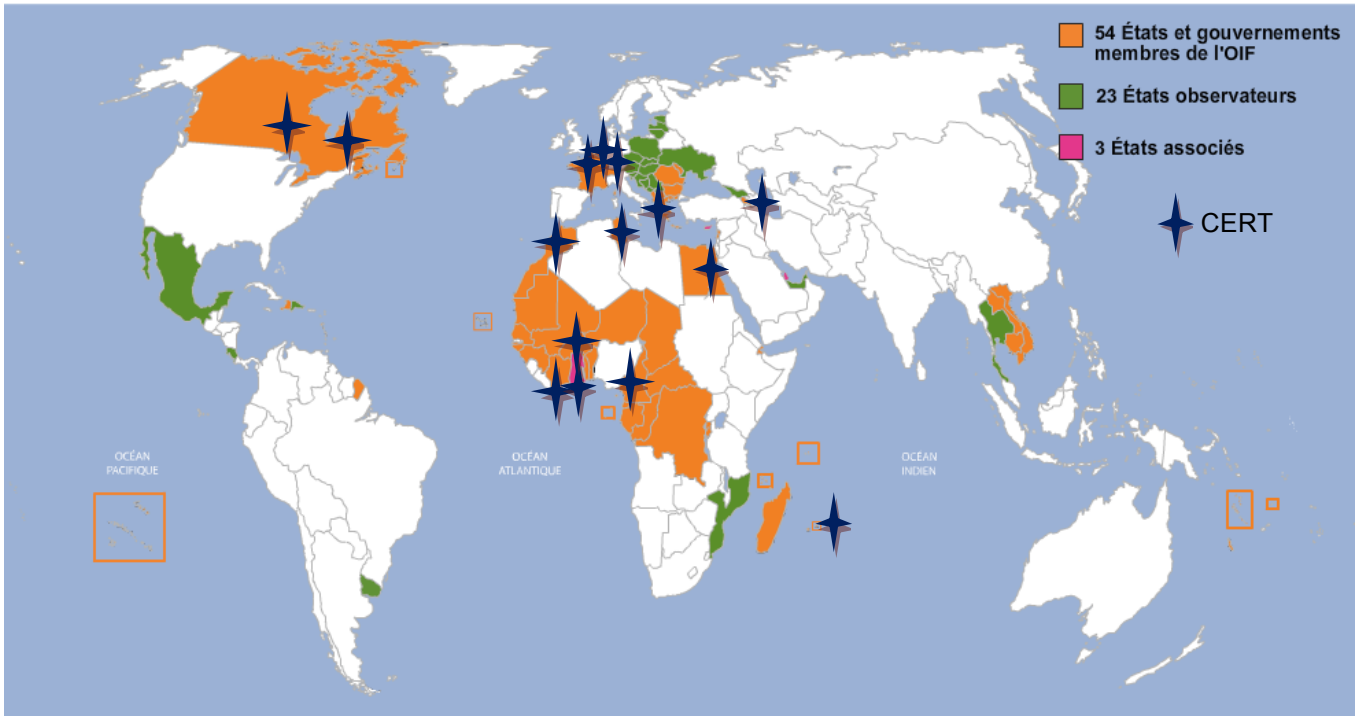
Tableau 5.1 : Pays membres de l'OIF dotés d'au moins un CERT

Albanie	Canada–Québec	Maroc
Arménie	Côte d'Ivoire	Maurice
Belgique	Égypte	Moldavie
Bulgarie	France	Roumanie
Burkina Faso	Grèce	Suisse
Cambodge	Laos	Tunisie
Cameroun	Luxembourg	Vietnam
Canada		

Vingt-deux États et gouvernements membres de l'OIF possèdent au moins un CERT à l'heure actuelle. Ce qui donne un taux de couverture de 38%. Certains pays, principalement des PED, annonce le fait qu'un centre CERT est créé bien que peu d'activité est observé à travers le site web dédié ou que le CERT est à l'état embryonnaire. L'effet d'annonce prouve du moins la volonté politique d'aller vers cette création. Néanmoins, ce projet doit entrer dans un processus plus global comme il l'a été indiqué plus haut. En effet, la création d'un CERT suppose l'existence d'un plan national de sécurité des infrastructures TIC qui doit être suivi d'une panoplie de textes réglementaires appropriés. Ensuite, vient la mise en place du centre avec tout ce que cela nécessite en termes de ressources logistiques, technologiques et de compétences humaines. Par exemple, sur la région d'Afrique, certains CERT ont été annoncés et faute de gouvernance appropriée ou de difficultés locales, ces centres n'ont pas réellement vu

le jour. Les CERT du Burkina Faso et du Cameroun sont annoncés mais on relève peu ou pas d'activités récentes sur leur site web [1]. La Côte d'Ivoire a créée un CERT gouvernemental CI-CERT sous l'autorité de régulation des télécommunications ARTCI depuis 2009 et vient de rejoindre le consortium FIRST en septembre 2016 [18]. Le Rwanda a établi un plan national de cybersécurité en mars 2015 dans lequel il est prévu de créer une agence spécialisé et un CERT [9]. Ainsi, si l'on tient compte des CERT effectivement actifs, le taux de couverture des CERT dans l'espace francophone est ramené à 35% alors que celui de l'espace non francophone avoisine les 43% [5]. Ces CERT sont en majorité gouvernementaux et vise à protéger principalement les systèmes d'information publics.

Carte 5.2 : Répartition des pays de l'OIF dotés d'au moins un CERT



Pour les pays les plus avancés, l'existence de plusieurs CERT par pays est courante. Ainsi, on assiste à des CERT gouvernementaux, sectoriels, privés ou universitaires pour un même pays. Par exemple en France, il y a au moins 11 CERT reconnus par la consortium FIRST (Cf. tableau ci-après)[5]. On retrouve le CERT gouvernemental français CERT-FR géré par l'ANSSI dont les activités étaient initialement sécuritaires et militaires et qui a ensuite élargi son champ d'action vers les acteurs de l'économie numérique. Par ailleurs, on remarque la présence de CERT sectoriels en particulier dans le domaine bancaire qui se sent très concerné par la cybersécurité. On voit également des CERT privés prestataires de services et qui démontre de la tendance SAAS (de l'anglais Security As A Service) apportant le concept de la sécurité vue comme une prestation de service. Ainsi, il est devenu habituel de voir des entreprises confier la

sécurité de leurs systèmes d'information à de tels CERT. Dans la liste du tableau suivant, il est intéressant de noter la présence d'un CERT académique à savoir le CERT-Renater. La dénomination « Renater » (pour Réseau national de télécommunications pour la technologie, l'enseignement et la recherche) désigne le réseau informatique français, créé en 1993, reliant les différentes universités et les différents centres de recherche entre eux en France métropolitaine et dans les départements d'outre-mer (www.renater.fr).

Tableau 5.3 : Liste des CERT en France

Acronyme	Nom officiel	Secteur
AiG CERT	Airbus Group CERT	Privé/aéronautique
AlliaCERT	Alliacom Computer Emergency Response	Privé/SSII
CERT SG	CERT SocieteGenerale	Privé/bancaire
CERT-AG	CERT Credit Agricole	Privé/bancaire
CERT-FR	CERT-FR	Gouvernemental
Cert-IST	CERT France Industries, Services & Tertiaire	Privé/Télécoms
CERT-LEXSI	CERT-LEXSI	Privé/SSII
CERT-Renater	CERT-Renater	Académique
CSIRT BNP	Corporate Security Incident Response Team	Privé/bancaire
ISIRT	INTERPOL INFORMATION SECURITY	Police
Orange-CERT-	Orange-CERT Coordination Center	Privé/Télécoms

Comme autre exemple de pays, le Luxembourg possède un CERT gouvernemental depuis 2011 (http://www.govcert.lu/fr/). Cette année-là, le gouvernement luxembourgeois a conclu qu'il convenait de renforcer les mécanismes de protection des infrastructures nationales et des données privées des citoyens, et qu'il paraissait important de mieux coordonner l'action des différents acteurs concernés par la lutte

contre la cybercriminalité. En 2013, le GOVCERT.LU, a notamment permis à ce pays de limiter les dégâts causés par la cyberattaque « RedOctober » (voir [8]).

Selon un communiqué en juin 2016 du Haut-Commissariat à la protection nationale (HCPN) du Luxembourg, l'agence ANSSI qui lui est rattachée et le groupement d'intérêt économique SMILE (Security made in Lëtzebuerg) annoncent une collaboration renforcée par le biais de leurs CERT respectifs dans le cadre de la cybersécurité nationale. Le Govcert est l'autorité nationale en charge de la gestion des incidents de sécurité touchant les entités publiques ainsi que les propriétaires et opérateurs des infrastructures critiques. Sur un plan européen et international, l'heure est également à la collaboration. Le Luxembourg a entrepris de réunir ses forces, son dynamise et son expertise en matière de sécurité de l'information afin de parler d'une seule voix avec ses partenaires étrangers.

Le Luxembourg est un centre financier international et un lieu attractif pour les entreprises actives dans le domaine des nouvelles technologies. La qualité et la sécurité des infrastructures de communications sont vitales pour le pays. Cette collaboration fait donc partie intégrante du plan gouvernemental qui a pour but de développer les mesures de sécurité et de protection des données privées des citoyens, des entreprises et du secteur public.

Le cas de la Tunisie est inédit dans le contexte des PED en général et dans l'espace francophone en particulier. En effet, la Tunisie s'est dotée d'une stratégie nationale en sécurité informatique depuis 2000 avec l'apparition de textes réglementaires légitimant la signature électronique et créant une autorité de certification électronique l'ANCE (www.ance.tn) autorisant les transactions électroniques. En 2004, l'agence nationale de sécurité informatique ANSI (www.ansi.tn) a été créée par texte de loi et est devenue opérationnelle dès 2005. Elle représentait le premier CERT dans la région arabe et africaine baptisé tunCERT. Il est devenu membre du consortium FIRST en 2007, centre d'excellence du CNUCED en cybersécurité en 2008 et membre actif dans d'autres associations internationales telles que le « Honeynet project » (www.honeynet.org) et l'OIC-CERT (www.oic-cert.org). La collaboration internationale a été importante et le tunCERT a assisté techniquement ou en tant que sponsor plusieurs CERT dans la région tels que ECS-CSIRT (Afrique du Sud), EG-CERT (Egypte), MA-CERT (Maroc), CI-CERT (Côte d'Ivoire) et le CERT Nigérien. Il a également été parmi les initiateurs de AfricaCERT (http://www.africacert.org/home/), un consortium africain pour échanger dans le domaine de la cybersécurité.

5.3 Evolution de l'implantation de CERT

Quand on observe l'évolution temporelle des pays francophones dans le domaine de la cybersécurité, on constate clairement le fossé numérique entre les PED et les pays avancés. Les figures suivantes montre l'évolution de l'implantation de CERT depuis 2010

à ce jour selon les données du forum mondial FIRST (Forum of Incident Response and Security Teams [5])

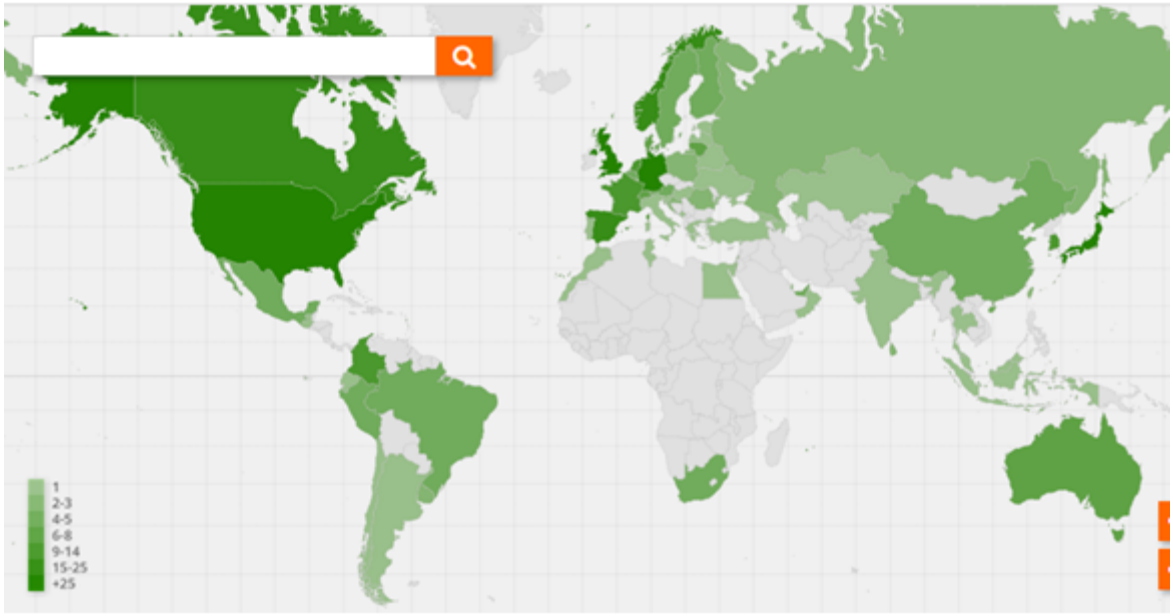
Carte 5.4 : Pays dans le monde ayant des CERT en **2010[5]**

209 CERT répartis sur 47 pays à travers le monde.

Carte 5.5 : Pays dans le monde ayant des CERT en **2014**

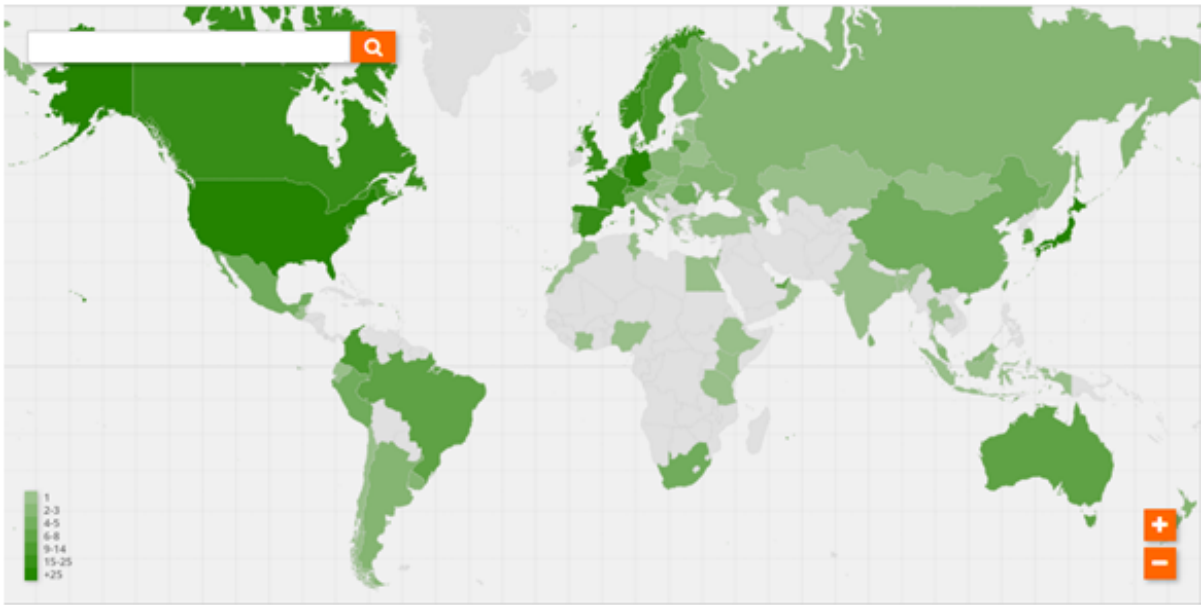
289 CERT répartis sur 64 pays à travers le monde.

Carte 5.6 : Pays dans le monde ayant des CERT en **2015**



319 CERT répartis sur 69 pays à travers le monde.

Carte 5.7 : Pays dans le monde ayant des CERT en octobre **2016**



365 CERT répartis sur 78 pays à travers le monde.

Cette évolution depuis 2010 de la répartition des PED, dans le monde en général et dans la zone francophone en particulier, selon qu'ils disposent d'un CERT ou pas, montre une légère évolution sans toutefois dissiper le fossé numérique constaté entre PED et pays avancés.

6 Partenariat et Coopération internationale

Vu les enjeux et les impacts de la stratégie nationale de cybersécurité et du caractère transfrontalier du cyberespace, il apparait indispensable pour chaque pays de se doter d'une stratégie internationale. En effet, des éléments internationaux importants ont un impact sur les efforts de protection et de réponses nationales issues des stratégies : les groupes de cybercriminels opèrent à travers les frontières nationales ; le cyber-espionnage se développe ; et les États-nations étrangères ont la capacité de lancer des attaques destructrices contre les infrastructures essentielles. Ces risques ne peuvent pas être correctement gérés sans coopération internationale. Celle-ci doit constituer un volet essentiel de la stratégie nationale.

On observe plusieurs types de groupement de CERT à travers le monde dans l'objectif de coopérer sur le plan technologique en échangeant des informations et expériences utiles et en coordonnant des actions de protection communes comme les exercices de simulation d'attaques touchant plusieurs pays d'une région (voir [7]). Ces groupements sont de divers types :

- Régional : comme le APCERT, groupant les CERT dans la région de l'Asie Pacifique [19]. L'AfricaCERT créant un espace d'échange dans les forums africains visant les pays ayant ou désirant créer un CERT.
- Institutionnel : comme l'ENISA (www.enisa.europa.eu), institution officielle de l'Union Européenne.
- Mondial : comme le FIRST [5].
- Associatif : comme le TF-CERT (www.trusted-introducer.org) [21] représentant un réseau associatif de CERT principalement européen.
- Culturel : comme l'OIC-CERT des CERT de l'Organisation des pays islamiques [23].
- Scientifique/thématique : comme le « Honeynet Project » [22] qui réunit des CERT dans un projet scientifique commun spécialisé dans la technologie « pot de miel » qui permet de partager les résultats d'expérimentation de certaines attaques cybernétiques sophistiquées.

Toute collaboration internationale apporte des avantages réels car elle permet de dresser des barrières communes aux menaces émergentes de l'Internet. L'échange du savoir-faire, d'expériences vécues, de réussites, de projets et d'exercices communs de simulation d'attaques est enrichissant pour chacun et permet de renforcer la capacité de protéger en local les systèmes d'information dont on a la responsabilité.

7 Conclusion et Recommandations

Entrer dans l'ère du numérique appelle à lancer de grands chantiers tels que le gouvernement électronique, l'administration en ligne, les « données ouvertes », formation en ligne MOOC (de l'anglais Massive Online Open Courses), services bancaires en ligne, commerce électronique. Réussir ces projets est tributaire de la confiance des usagers, citoyens ou entreprises, et de leur adhésion à utiliser les services basés sur les TIC. La cybersécurité est considérée comme le moyen incontournable pour créer les conditions d'atteindre cet objectif.

Il est établi que les pays doivent se doter d'une stratégie en cybersécurité et créer les moyens de sa mise en œuvre. Le développement de capacités et de compétences à travers la formation, la mise en place de centres opérationnels comme les CERT et la coordination internationale dans le domaine sont autant d'axes majeurs pour bâtir une cybersécurité performante. Cette étude a dressé une situation de la cybersécurité à travers ces trois axes dans l'espace francophone et a exhibé les enjeux y afférents.

Le premier constat qui émerge est l'écart conséquent observé dans ce domaine entre pays avancés et certains PED dans l'espace francophone. Des expériences réussies et des pratiques exemplaires ont été citées dans cette étude pour montrer la possibilité d'une collaboration efficace au sein de la Francophonie.

Le patrimoine francophone commun et en particulier la langue française sont un vecteur facilitateur pour l'échange de savoir-faire qu'il s'agisse de formation, d'assistance ou de collaboration entre acteurs francophones. Il apparaît donc opportun de créer les conditions et les mécanismes pour renforcer les capacités en cybersécurité dans l'espace francophone. Quelques pistes intéressantes et recommandations se déclinent de ce fait de cette étude :

- Création d'un CERT académique francophone, *CERT-UF* par exemple (pour CERT Universitaire Francophone), qui offrirait ses services à la communauté universitaire francophone notamment les étudiants, les enseignants et chercheurs. Sa mission serait principalement orienté vers la *recherche et le développement* d'outils innovants de cybersécurité et assurant la *veille technologique* en matière de nouvelles menaces (virus, malware, attaques, etc.) et de nouveaux outils palliatifs. Il jouera également un rôle dans la *mise en place de formations* de qualité (ou « certifiées ») dans les domaines de la cybersécurité au sein des espaces universitaires francophones.
- Lancement d'un consortium francophone dont les membres seraient les CERT des pays francophones créant un espace d'échange de savoir-faire et d'expertises. CERT-UF pourrait jouer un rôle de coordinateur ou animateur de cette association.

- Planifier pour la définition d'un *« label »* ou forme de « certification » pour des formations en français concernant les différentes spécialités de cybersécurité et élever ainsi le niveau et la qualité des enseignements dispensés. CERT-UF pourrait être le maître d'œuvre d'un tel projet.
- Création d'un *Répertoire d'Experts* et de compétences universitaires francophones en cybersécurité afin de capitaliser le savoir-faire et l'exploiter aussi bien pour la formation que pour l'assistance à la mise en place de stratégies ou de CERT.

9 Références

[1] AfricaCERT : http://www.africacert.org/home/

[2] Liste CERT : http://www.cert.org/incident-management/national-csirts/index.cfm

[3] http://www.francophonie.org/IMG/pdf/isoc-rapport_francophonie_numerique2014_web.pdf

[4] Stratégie de la francophonie numérique- Horizon 2020 (14e sommet de Kinshasa) : http://www.francophonie.org/IMG/pdf/horizon_2020_-_strategie_de_la_francophonie_numerique.pdf

[5] FIRST : the Forum of Incident Response and Security Teams http://www.first.org/

[6] CERT tunisien tunCERT : www.ansi.tn

[7] Cyber Drill https://www.ansi.tn/fr/pages/gallerie/pages/drill/presentations.html

[8] CERT luxembourgeois govCERT www.gouvernement.lu/1794817/16-govcert

[9] http://www.myict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/NCSP_Implementation_Plan.pdf

[10] Communiqué du HCPN http://www.gouvernement.lu/6037806/30-cybersecurite-anssi

[11] http://www.lemonde.fr/campus/article/2016/02/05/masteres-specialises-la-cyberdefense-une-priorite_4860283_4401467.html

[12] https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/

[13] Projet SecNum*edu* : https://www.ssi.gouv.fr/particulier/formations/secnumedu/

[14] Master belge en cybersécurité https://masterincybersecurity.ulb.ac.be/

[15] Polytech Montréal http://www.polymtl.ca/etudes/certificats/cheminement/cybersecurite.php

[16] CGE http://www.cge.asso.fr/nos-membres/ecoles/etablissements-etrangers?page=1

[17] http://www.mesrst.tn/francais/divers/enseignement_prive/2014/masteres_pro_fr.pdf

[18] CERT ivoirien CI-CERT : http://www.cicert.ci/

[19] AP-CERT http://www.apcert.org/index.html

[20] CERT Européen ENISA : https://www.enisa.europa.eu/

[21] TF-CERT https://www.trusted-introducer.org/services/overview/french.html

[22] Honeynet Project www.honeynet.org

[23] L'OIC-CERT www.oic-cert.org

10 Annexe 1 : Liste des Acronymes

APCERT	Asian Pacific Computer Emergency Response Teams
AUF	Agence Universitaire de la Francophonie
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Emergency Response Team
CERT	Computer Emergency Response Team
CGE	Conférence des grandes écoles
DARPA	Defense Advanced Research Projects Agency
OIF	Organisation internationale de la Francophonie
MOOC	Massive Online Open Courses
PDCA	Plan-Do-Check-Act
PED	Pays en développement
SIRT	Security Incident Emergency Response Team
TIC	Technologies de l'information et de la communication

11 Annexe 2 : Liste des Figures