KM9 : Normes et certifications de cyber-sécurité

Objectifs du module

Bienvenue dans le module de connaissances sur **les normes de cybersécurité**, dans le cadre du projet GFCE-Afrique.

Les participants à ce module de connaissances acquerront des connaissances sur les considérations politiques et techniques pour le développement et la mise en œuvre de normes de cybersécurité à travers le partage des meilleures pratiques, des études de cas, des exercices et des réflexions.

À la fin du module, vous serez en mesure de répondre aux questions suivantes et de trouver des ressources supplémentaires les concernant :

- Que sont les normes liées à la sécurité ?
- Que sont les normes ouvertes ?
- Organismes de normalisation et comment s'engager
- Qui sont les parties prenantes à la normalisation ?
- Quelles initiatives sont disponibles pour la création de capacité de normalisation ?

1. Introduction

La Stratégie de transformation numérique pour l'Afrique (2020-2030) a pour but d'activer la transformation numérique et l'industrialisation, et de soutenir l'économie numérique et la mise en œuvre de la Zone de libre-échange continentale africaine (AfCFTA). Cette stratégie met l'accent sur l'utilisation de normes ouvertes dans la création d'une infrastructure de confiance transfrontalière interopérable pour la protection des données personnelles et de la confidentialité.

Il est par conséquent impératif pour les décideurs politiques de comprendre l'importance du développement et de la mise en œuvre de normes liées à la sécurité. Différentes approches peuvent être utilisées pour évaluer la capacité de cybersécurité d'un pays. Le modèle de maturité de la capacité de cybersécurité (CMM) pour les nations traite de l'utilisation de la technologie et des normes de cybersécurité pour protéger les individus, les organisations et l'infrastructure nationale. En outre, le modèle CMM traite de la connaissance et des capacités de cybersécurité, y compris la disponibilité de programmes formels de formation à la cybersécurité et de programmes de formation professionnelle.

Ce module couvre les normes de cybersécurité, les organismes de normalisation (SDO), et explore les opportunités d'implication des parties prenantes africaines

dans le développement de normes. Le module examine également les opportunités de développement de capacité via la certification des institutions et du personnel.

2. Pourquoi les normes sont-elles importantes ?

Les normes représentent des ensembles de règles convenues qui nous indiquent comment effectuer certaines actions. Une norme définit les exigences, les spécifications, les directives ou les caractéristiques concernant un matériau, un produit, un procédé ou un service. Les normes sont rassemblées dans des documents techniques « conçus pour être utilisés comme des règles, des directives ou des définitions et décrivent un moyen de réaliser une certaine opération qui repose sur un consensus et est reproductible » (CEN).

Les normes sont essentielles à la gestion de la qualité et du risque, elles dynamisent l'innovation et contribuent à la croissance des marchés via la création de produits d'une qualité et d'une performance cohérentes. Les normes sont importantes pour la protection de la santé et de la sécurité des employés ainsi que du grand public.

Les normes internationales de l'IEC fournissent des instructions, des directives, des règles ou des définitions utilisées pour concevoir, fabriquer, installer, tester et certifier, gérer et réparer les appareils et systèmes électriques et électroniques, et sont élaborées sur la base d'un consensus mondial. Selon l'Union Internationale des Télécommunications, les normes sont importantes pour assurer la sécurité, la stabilité, la fiabilité, l'interopérabilité, l'innocuité pour la santé humaine et l'efficacité énergétique des technologies de l'information et des communications (ICT).

Réflexion : Normes utilisées dans un smartphone

Identifiez les normes supplémentaires utilisées dans un smartphone, outre celles qui sont illustrées dans la Figure 1 ci-dessous.

Figure 1 : Nous vivons dans un monde « normalisé » Source : ETSI

3. Normes formelles

Un écosystème de protocoles, normes, technologies, pratiques et organisations assure l'ouverture, la stabilité, la sécurité et la résilience d'internet. Les normes garantissent que le matériel et les logiciels développés ou fabriqués par différentes entités fonctionnent ensemble de la manière la plus transparente possible, ou sont interopérables. L'adoption et le déploiement de normes internet liées à la sécurité contribuent à créer une infrastructure internet et un cyberespace sûrs et résilients.

Les normes formelles sont homologuées par un Organisme de normalisation (SDO) formel. Les SDO comprennent l'International Electrotechnical Commission (IEC), l'International Organisation for Standardization (ISO) et l'Union Internationale des Télécommunications (UIT). Des organismes quasi-formels, parmi lesquels l' Institute of Electrical and Electronics Engineers (IEEE), le 3rd Generation Partnership Project (3GPP) et l'Internet Engineering Task Force (IETF), les forums de l'industrie et les consortiums jouent un rôle majeur dans le développement de normes de sécurité pour internet.

La participation du gouvernement, des régulateurs, des universités et d'autres parties prenantes aux SDO devrait être alignée sur les priorités et obligations nationales, telles que définies dans la stratégie nationale de cybersécurité, les conventions internationales ou régionales. Cela aiderait les gouvernements à déterminer les domaines de normalisation prioritaires, la représentation de l'état ou

d'organismes non-étatiques dans différents SDO et l'engagement des ressources. Internet lui-même repose principalement sur des « normes » développées par l'IETF qui ne sont pas formellement homologuées par les États, mais reposent simplement sur le travail de volontaires de différents organismes du monde entier. La participation est ouverte à tous et l'influence est basée sur les mérites (savoir-faire et compétences techniques). Dans l'IETF, les participants ne représentent pas des organismes ou des gouvernements, et tous participent sur un pied d'égalité. Il existe donc une possibilité de voir des experts originaires d'Afrique contribuer à la normalisation selon leurs propres mérites. Les normes générées sont « volontaires » et généralement adoptées parce qu'elles fonctionnent (« consensus brut et code de fonctionnement ») et contribuent à assurer l'interopérabilité d'Internet.

4. Organismes de normalisation

4.1. L'IETF

Les normes techniques d'Internet sont principalement développées par l'Internet Engineering Task Force (IETF). Les principales normes internet développées par l'IETF comprennent le protocole Transmission Control Protocol/Internet Protocol (TCP/IP), le système de noms de domaine (DNS) et la couche secure sockets layer (SSL).

Autres normes importantes développées :

- Révision récente du protocole Transport Level Security protocol (TLS) TLS 1.3 : protège la confidentialité et l'intégrité des données transmises
- Authentification des entités nommées basée sur DNS (DANE) : améliore l'efficacité de la norme TLS
- Protocole d'environnement automatisé de gestion des certificats (Automated Certificate Management Environment, ACME) : permet de configurer un site Web sécurisé en quelques secondes
- Domain Name System Security Extensions (DNSSEC) : empêche la redirection des utilisateurs d'internet vers des sites ou des serveurs de messagerie malveillants
- IPv6 : permet à de multiples utilisateurs et appareils de se connecter à internet et fournit des capacités de sécurité
- Normes mutuellement convenues pour la sécurité du routage (Mutually Agreed Norms for Routing Security (MANRS)) : présente les mesures concrètes permettant de réduire les menaces les plus fréquentes pour le routage sur les réseaux

4.1.1. Comment participer au développement de normes au sein de l'IETF

Les spécifications techniques de l'IETF sont publiées dans des documents RFC et sont d'abord des ébauches-internet (I-D) avant d'être adoptées, améliorées et révisées par un groupe de travail. Un I-D peut être créé par un individu ou un groupe et entre en vigueur dans l'IETF s'il est adopté par un groupe de travail ou approuvé en tant que RFC. Une liste complète de tous les groupes de travail actifs, avec des liens vers leurs chartes, des listes d'e-mails de discussion et d'autres informations est disponible sur IETF Datatracker.

Le Programme de politiques de l'IETF est un programme virtuel de quatre semaines qui s'adresse aux responsables officiels, aux décideurs politiques et aux régulateurs. Ce programme donne de la visibilité à l'environnement des normes de l'IETF et couvre trois pistes thématiques :

- L'histoire de l'internet et de l'IETF
- Le fonctionnement interne d'internet
- La façon de relever les défis d'internet

Les participants ont une opportunité de communiquer avec des experts et des responsables au sujet des questions de pointe concernant la technique et les politiques, et de s'immerger dans le processus de développement de normes en participant aux sessions des groupes de travail de l'IETF.

4.2. L'IEC

L'IEC élabore des normes internationales dans différents domaines, y compris, sans toutefois s'y limiter : la cybersécurité, l'intelligence artificielle (IA), l'internet des objets (IdO), le transport, les objectifs de développement durable (ODD), l'énergie, les villes et les communautés, la fabrication intelligente. Ces normes forment la base des tests et de la certification.

Les normes internationales de l'IEC ISO/IEC 27001 et IEC 62443 sont des normes horizontales, adaptées à tous les secteurs. La série de normes IEC 62443 établit les consignes et spécifications en matière de cybersécurité applicables à un certain nombre de secteurs et d'infrastructures critiques, notamment aux transports. La norme est compatible avec l'infrastructure de cybersécurité de l'US National Institute of Standards and Technology (NIST). La norme ISO/IEC 27000:2018 fournit une vue générale des systèmes de gestion de la sécurité des informations (ISMS) ainsi que les conditions et définitions couramment utilisées dans la série de normes ISMS. La norme ISO/IEC 27001:2013 spécifie les exigences pour établir, mettre en œuvre,

gérer et améliorer en continu un système de gestion de la sécurité des informations dans le contexte de l'entreprise.

Ces normes horizontales sont complétées par des normes verticales, qui couvrent les besoins spécifiques en termes de sécurité dans l'industrie nucléaire, l'automatisation industrielle, les soins de santé et l'industrie maritime, entre autres. Ces normes comprennent IEC 62645 Centrales nucléaires – instrumentation, contrôles et systèmes d'alimentation électrique – exigences en termes de cybersécurité, série IEC 61850 pour les réseaux de communications et les systèmes destinés à l'automatisation du réseau électrique, série IEC 60870 pour l'équipement et les systèmes de télécontrôle et série IEC 61162 pour la navigation maritime et les équipements et systèmes de radio-communication.

Le programme de cybersécurité industrielle IECEE teste et certifie la cybersécurité dans le secteur de l'automatisation industrielle, conformément à la série de normes IEC 62443. Aujourd'hui, des entités publiques et privées recherchent des certifications tierces pour garantir la conformité de leur système de gestion de la sécurité de l'information (ISMS) à la norme ISO/IEC 27001. Les organismes qui vérifient la conformité devraient être certifiés et enregistrés sous la norme ISO/IEC 27006.

4.2.1. Comment participer au développement de normes au sein de l'IEC

L'IEC encourage la participation à ses travaux par le biais de centres régionaux. Le Centre régional africain de l'IEC (IEC Africa Regional Centre, IEC-AFRC) a été mis en place pour promouvoir la sensibilisation à l'IEC dans la région Afrique, augmenter l'adoption et l'utilisation des normes internationales de l'IEC et des systèmes d'évaluation de la conformité de l'IEC et soutenir la participation et renforcer les contributions actives au travail de l'IEC.

Le Programme des pays affiliés à l'IEC (IEC Affiliate Country Programme) donne l'occasion aux pays en développement et nouvellement industrialisés de participer à des activités de normalisation internationale et d'évaluation de la conformité sans subir le fardeau financier lié à l'adhésion. On peut rejoindre l'IEC Affiliate Country Programme sur invitation du Secrétaire général et PDG de l'IEC.

Un pays peut accéder au statut Affiliate Plus en déclarant officiellement l'adoption d'au moins 50 normes internationales de l'IEC en tant que normes nationales et en établissant un NEC avec des représentants des secteurs privé et public. Les pays affiliés sont soutenus pour répondre à leurs besoins spécifiques dans le cadre du Programme de mentorat de l'IEC qui établit des partenariats entre les membres de l'IEC et des pays affiliés

Figure 2 *: Avantages du Programme des pays affiliés à l'IEC* Source *: IEC*

La Commission électrotechnique africaine de normalisation (African Electrotechnical Standardization Commission, AFSEC) est établie par statut comme un organisme affilié sous les auspices de la Commission africaine de l'énergie. L'AFSEC dispose de membres statutaires et affiliés. Les pays qui sont membres statutaires participent aux travaux de l'AFSEC via un Comité électrotechnique national (NEC).

Les normes sont développées sur la base de la soumission d'une Proposition d'étude nouvelle (New Work Item Proposal, NWIP) considérée en fonction du processus d'approbation.

4.3. L'ISO

L'ISO est une organisation internationale non-gouvernementale et indépendante comptant 165 membres qui sont des organismes nationaux de normalisation. L'ISO développe des normes de sécurité informatique, la plus célèbre étant la norme ISO/IEC 27001 qui fournit des exigences de système de gestion de sécurité des informations (ISMS).

Les autres normes comprennent la norme ISO/IEC 27032:2012 qui fournit des directives en matière de cybersécurité et la norme ISO/IEC 27005 sur la gestion des risques pour la sécurité des informations, conçue pour favoriser la mise en œuvre satisfaisante de la sécurité des informations en fonction d'une approche de gestion du risque, avec la compréhension des concepts, modèles, processus et terminologies dans les normes ISO/IEC 27001 et ISO/IEC 27002.

Les autres normes pertinentes comprennent la norme ISO 27005: 2018 Technologie de l'information – Techniques de sécurité – Gestion des risques pour la sécurité des informations et la norme ISO 31000: 2018 Gestion des risques – Directives.

La norme ISO/AWI 22336 Sécurité et résilience — Résilience des organisations — Formulation des politiques de résilience et mise en œuvre de la stratégie, est en cours de développement et fournira des conseils aux organisations sur la manière

de formuler une politique d'entreprise et de mettre en œuvre une stratégie visant à renforcer la résilience de l'organisation. Cela aidera aussi les organisations à articuler leur vision et leurs buts, à définir des objectifs stratégiques et à mettre au point leurs actions pour renforcer leur résilience.

La norme ISO/IEC JTC 1/SC 27 – iSécurité des informations, cybersécurité et protection de la confidentialité – a développé des normes pour la protection des informations et l'ICT, y compris des méthodes génériques, des techniques et des consignes pour gérer à la fois les aspects de sécurité et de confidentialité, notamment la gestion de la sécurité de l'ICT et des informations ainsi que les exigences en termes d'audit.

4.3.1. Comment participer au développement de normes au sein de l'ISO

Les SDO appliquent des processus et des procédures en matière de normalisation qui passent par la proposition, l'ébauche, l'approbation et la publication. L'IEEE SA propose des adhésions d'individus et d'entreprises. Le développement d'une norme africaine ou d'une série de normes connexes peut être initié via de nouveaux éléments d'étude dans les comités techniques existants et déclaré par le conseil de l'Organisation africaine de normalisation (ARSO). L'ARSO harmonise les normes et les procédures d'évaluation de conformité africaines, afin de réduire les obstacles techniques au commerce et d'améliorer le commerce intra-africain et international, l'industrialisation et l'intégration en Afrique.

À cet effet, l'ARSO, associé à l'IEEE SA, a développé la stratégie africaine de normalisation et la feuille de route de la quatrième révolution industrielle en vue de promouvoir l'harmonisation des normes afin de renforcer la compétitivité de la Zone de libre-échange continentale africaine (AfCFTA).

Réflexion :
Faire référence au livre blanc de l'IEEE SA sur la stratégie de normalisation de la 4e révolution industrielle en Afrique (2021-2025)

Discuter des raisons pour lesquelles l'Afrique devrait disposer d'une stratégie de normalisation. Quelles problématiques cette stratégie devrait-elle aborder ?

4.4. Union Internationale des Télécommunications

L'Union Internationale des Télécommunications (UIT) est organisée en trois secteurs : les Radiocommunications (ITU-R), le Développement (ITU-D) et la Normalisation (ITU-T).

Le secteur de la normalisation des télécommunications de l'UIT a développé les recommandations UIT-T X.series : réseaux de données, communications sur les systèmes ouverts et sécurité. Ces normes/recommandations sont développées par des groupes d'étude dans le secteur de normalisation des télécommunications de l'UIT.

4.4.1. Comment participer au développement de normes au sein de l'UIT

L'adhésion aux trois secteurs de l'UIT est ouverte aux gouvernements, à l'industrie et au monde de l'enseignement. L'UIT encourage une participation accrue des pays en développement aux activités de normalisation, y compris leur participation aux réunions, la soumission de contributions, l'occupation de postes à responsabilité et l'accueil de réunions/d'ateliers conformément aux dispositions de l'Assemblée mondiale sur la normalisation des télécommunications (Hammamet, 2016), à la Résolution 54 sur la création de, et la participation à des groupes régionaux.

Il existe actuellement 8 groupes régionaux africains dans le secteur de la normalisation de l'UIT :

- Groupe d'étude 2 de l'UIT-T : Aspects opérationnels de la prestation de services et de la gestion des télécommunications
- Groupe d'étude 3 de l'UIT-T : principes des tarifs douaniers et principes comptables et problèmes politiques et économiques internationaux des télécommunications/de l'ICT
- Groupe d'étude 5 de l'UIT-T : Environnement, changement climatique et économie circulaire
- Groupe d'étude 11 de l'UIT-T : Exigences en termes de signalétique, protocoles, spécifications de test et lutte contre la contrefaçon
- Groupe d'étude 12 de l'ITU-T : Performance, qualité du service (QoS) et qualité de l'expérience (QoE)
- Groupe d'étude 13 de l'UIT-T : Réseaux futurs, mettant l'accent sur l'IMT 2020, l'informatique dans le cloud et les infrastructures réseau fiables
- Groupe d'étude 17 de l'UIT-T : Sécurité
- Groupe d'étude 20 de l'UIT-T : Internet des objets (IdO) et villes et communautés intelligentes (SC&C)

Ces groupes sont conformes aux dispositions de l'Assemblée mondiale sur la normalisation des télécommunications (Hammamet, 2016), à la Résolution 44 visant à Réduire l'écart en matière de normalisation entre pays en développement et pays développés.

Le programme Réduire l'écart en matière de normalisation (BSG) a pour but de faciliter la participation efficace des pays en développement au processus de normalisation de l'UIT, de diffuser des informations au sujet des normes existantes et d'assister les pays en développement dans la mise en œuvre des normes.

Figure 3: Cinq piliers stratégiques du programme BSG Source *UIT*

- Sensibilisation : le programme PSG a pour objectif de sensibiliser au processus de normalisation et de favoriser le savoir-faire
- Savoir-faire : acquisition des compétences et capacités adéquates pour la normalisation internationale
- Communauté : groupes régionaux des groupes d'étude de l'UIT-T apportant une assistance à l'élaboration de programmes nationaux de normalisation, aux plans de coordination avec les SDO et aux organisations et universités régionales pertinentes.
- Engagement et Participation : participation aux réunions des groupes d'étude et aux réseaux des anciens élèves de BSG
- Partenariat : opportunités d'héberger, de parrainer et de financer les activités du BSG

4.5. L'IEEE

L'IEEE Standards Association dispose de plusieurs programmes sur les normes de sécurité dans les segments verticaux, notamment les infrastructures critiques, l'énergie, les biens de consommation et les soins de santé, ainsi que les normes relatives à l'infrastructure d'IdO.

Voici la liste de certaines activités de normalisation de la cybersécurité qui sont en cours ou publiées au sein de l'IEEE-SA. Un préfixe « P » devant le numéro indique qu'il s'agit d'un groupe de travail actif qui développe actuellement la norme ; dans de nombreux cas, la norme P possédera aussi une version publiée, puisque le travail sur la prochaine révision est en cours.

Normes de l'infrastructure IdO axées sur la sécurité

- IEEE 2413-2019, Norme pour une infrastructure architecturale pour l'internet des objets
- IEEE P2994 : norme pour l'infrastructure d'évaluation de la sécurité pour les déploiements d'applications sur l'internet des objets (IdO)

Soins de santé/Produits portables/Biens de consommation :

- Série de normes IEEE 11073 : la série IEEE 11703 comprend une partie consacrée à la cybersécurité pour les appareils médicaux en vertu de l'ébauche de norme P11073-40101 – IEEE – Informatique de la santé – Interopérabilité des appareils – Partie 40101 : Cybersécurité – Processus d'évaluation de la vulnérabilité IEEE P1912 : norme de l'architecture de confidentialité et de sécurité pour les appareils de grande consommation sans fil
- Groupe de travail IEEE 2621 : norme relative à l'assurance sécurité des appareils sans fil utilisés dans le secteur de la santé

Cette infrastructure comprend 3 normes

- IEEE P2621.1 : Norme relative à l'assurance sécurité des appareils sans fil de surveillance du diabète : programme d'évaluation de la sécurité des produits
- IEEE P2621.2 : Intitulé du projet : Norme relative à l'assurance sécurité des appareils sans fil de surveillance du diabète : profil de protection des appareils connectés de surveillance du diabète
- IEEE P2621.3 : Intitulé du projet : Norme relative à l'assurance sécurité des appareils sans fil de surveillance du diabète : consignes relatives aux appareils mobiles

- IEEE PHD (Dispositifs de santé personnels) : Feuille de route des normes de sécurité – Livre blanc
- IEEE SA Rapport de travail préalable à la norme : Validation des données cliniques d'IdO et Interopérabilité avec la Blockchain – Livre blanc
- IEEE P2933 : Norme relative à l'interopérabilité des données et dispositifs d'Internet des Objets (IdO) cliniques avec les principes TIPPSS – Confiance, Identité, Confidentialité, Protection, Sûreté, Sécurité
- IEEE 2410-2020 : Norme IEEE relative à la confidentialité biométrique
- IEEE P2418.6 : Norme relative à l'infrastructure de l'utilisation de la Technologie des registres distribués (DLT) dans les soins de santé et dans les sciences de la vie et les sciences sociales

Énergie/Réseau intelligent

- IEEE C37.240-2014 : Norme IEEE relative aux exigences de cybersécurité en matière d'automatisation, de protection et de systèmes de contrôle des sous-stations
- IEEE 1686-2013 : Norme IEEE relative aux capacités de cybersécurité des appareils électroniques intelligents
- IEEE P2030.102.1 : Norme relative à l'interopérabilité de la sécurité des protocoles internet (IPsec) utilisés dans les systèmes de contrôle des réseaux de services publics
- IEEE P1711 : Norme relative à un protocole cryptographique pour les liaisons de communication du système d'alimentation électrique (EPS)
- IEEE P1711.1 : Norme relative à un protocole cryptographique pour la cybersécurité des liaisons en série des sous-stations : protocole de protection en série des sous-stations
- IEEE P2658 : Guide des tests de cybersécurité dans les réseaux d'alimentation électrique
- IEEE 802.15.4-2020 : Ébauche de norme IEEE approuvée relative aux réseaux sans fil à faible débit
    - Le protocole IEEE 802.15.4 est utilisé dans les applications de réseau intelligent (compteurs intelligents) et possède plusieurs fonctions de sécurité comme le contrôle d'accès, l'intégrité du cadre et la confidentialité
- La norme IEEE SA est également à l'origine de certains travaux clés sur la blockchain axés sur l'énergie
    - IEEE P825 : Guide de l'interopérabilité des réseaux électriques transactifs avec l'infrastructure électrique (construction du réseau d'activation des ressources d'énergie distribuées)
- IEEE P2418.5 : Norme relative à la blockchain dans l'énergie
- IEEE 692-2013 : La norme IEEE relative aux critères pour les systèmes de sécurité pour les centrales de production d'énergie nucléaire, développée par le groupe de travail WG 3.2 – Systèmes de sécurité, traite de l'équipement des systèmes de sécurité pour la « détection, l'évaluation, la surveillance, le contrôle d'accès, la communication et l'acquisition des données ».
- Les nombreuses normes IEEE relatives aux systèmes de réseaux intelligents[6] comprennent un certain nombre de règles axées sur la sécurité, notamment IEEE C37.240-2014 – les exigences de cybersécurité de la norme IEEE pour les systèmes d'automatisation, de protection et de contrôle des sous-stations développée par les normes 240 WG – PC37.240 relative à la cybersécurité et IEEE 1686-2013 – la norme IEEE relative aux capacités de cybersécurité des dispositifs électroniques développés par le groupe de travail WGC1 – Sous-stations C1.

FinTech :

- IEEE P1940 : Profils des normes pour les services d'authentification ISO 8583

  - La norme IEEE P1940 se concentre principalement sur les transactions financières (par ex. points de vente (POS), distributeurs automatiques de billets (ATM), transactions de retrait d'espèces, etc.). Ces services comprennent l'authentification biométrique (telle que définie par la norme IEEE Std. 2410), avec les méthodes d'authentification par code PIN, d'identification rapide en ligne (FIDO), mais aussi de mot de passe unique (OTP) et d'OTP temporaire (TOTP) y compris les mesures de défense contre les attaques de présentation (PAD)

Mobilité/Automobile :

- IEEE P1609.2 : norme d'accès sans fil dans les environnements de véhicule - Services de sécurité pour les applications et les messages de gestion

Logiciels :

- Comité IEEE des normes de cybersécurité et de confidentialité dans la société informatique
- Série IEEE 1619 sur la protection par cryptage des dispositifs de stockage :
  - IEEE 1619-2018 : la norme IEEE relative à la protection par cryptage des données sur les dispositifs de stockage axés sur les blocs
  - IEEE 1619.1-2018 : la norme IEEE relative au cryptage authentifié avec extension de longueur pour les dispositifs de stockage
  - IEEE P1619.2 : la norme de cryptage à blocs larges pour les supports de stockage partagés
  - IEEE P2883 : norme relative au nettoyage du stockage
- IEEE 1667-2018 : norme IEEE relative à la découverte, l'authentification et l'autorisation dans les accessoires hôtes des dispositifs de stockage
- IEEE P2986 : pratique recommandée en matière de confidentialité et de sécurité pour l'apprentissage machine fédéré (C/AI)
- IEEE P2994 : norme pour l'infrastructure d'évaluation de la sécurité pour les déploiements d'applications sur l'IdO (COM/Mobile)

Normes IEEE 802 :

- La norme IEEE 802.1AE définit un protocole de sécurité de couche 2 appelé Medium Access Control Security (MACSec) qui fournit une sécurité de point à point sur les liaisons ethernet entre les nœuds pour sécuriser les réseaux LAN filaires.
- La norme IEEE 802.11 inclut aussi des fonctions de sécurité : Service Set Identifier (SSID), utilisée pour contrôler l'accès à un point d'accès (AP), la liste des contrôles d'accès (ACL) pour empêcher les accès non-autorisés et le protocole Wired Equivalent Privacy (WEP)
- IEEE 802.11bh : fonctionnement avec des adresses MAC randomisées et changeantes (LAN/MAN)
- IEEE 802.11bi : service amélioré avec protection de la confidentialité des données
- IEEE 802E : considérations relatives à la confidentialité pour les technologies IEEE 802

Les normes IEEE sur la Blockchain :

- L'IEEE compte environ 30 à 40 normes concernant la Blockchain, dont certaines sont mises en évidence dans le cadre du secteur vertical de l'énergie et des soins de santé ci-dessus
- Le comité des normes IEEE relatives à la Blockchain et aux registres distribués
    - La série de normes IEEE P3200 est en cours de développement par ce comité, qui se concentre sur l'identité, l'interopérabilité et la sécurité (la série IEEE 3200 compte environ 10 normes)

Programmes de connexions de l'industrie de cybersécurité IEEE (avant normalisation) :

- IC20-021-01 : Méta questions de cybersécurité
- IC20-011 : Sécurité de l'écosystème de l'IdO
- La cybersécurité à l'âge de l'informatique agile dans le cloud
- IEEE SA soumet ses réponses aux consultations ou aux demandes publiques ouvertes, y compris les documents de politiques NIST

4.5.1. Comment participer au développement de normes au sein de l'IEEE

Le programme d'engagement du gouvernement de l'IEEE sur les normes (GEPS) est un programme sur mesure destiné aux officiels des gouvernements. Par le biais du programme, les officiels des gouvernements peuvent obtenir des informations stratégiques au sujet de la normalisation IEEE et ses membres peuvent contribuer à des discussions à l'intersection de la technologie, des normes et des politiques. Les

membres reçoivent des informations sur mesure et des ressources, comprenant des webinaires sur mesure et des consultations bilatérales avec des experts de la technique et des normes.

Le GEPS propose une adhésion gratuite et actuellement, 12 organismes gouvernementaux africains participent au programme, dont le ministère du développement de l'économie numérique et des postes du Burkina Faso, le ministère de la Communication, de l'ICT et des Médias (MINCOTIM) et l'Autorité de régulation des télécommunications et de l'ICT (ARCT) du Burundi, l'Autorité nationale de régulation des Télécoms (NTRA) d'Égypte, l'Autorité nationale des Communications (NCA) du Ghana, le ministère de l'ICT et de l'innovation (MINICT) et l'Autorité de régulation des services publics (RURA) au Rwanda, le ministère de l'Économie numérique et des télécommunications de la République du Sénégal, l'Autorité de régulation des communications (TCRA) de Tanzanie, la commission des Communications (UCC) de l'Ouganda et l'Autorité des Technologies de l'information et des communications (ZICTA) de Zambie.

Étude de cas

***Entretien** : utilisation des normes mondiales dans la création de politiques : Entretien avec un représentant du GEPS de l'IEEE pour l'Égypte, Ramy Fathy, Autorité nationale de régulation des Télécoms (NTRA)*

Pour aider les ingénieurs à mieux répondre aux exigences de normalisation futures, le programme IEEE Blended Learning (BLP) se concentre sur la création de capacité. Le BLP de l'IEEE offre un ensemble de cours complet sur l'IdO, l'EMI/EMC, le Wi-Fi, la gestion de l'innovation, et le lancement d'une formation à la cybersécurité est attendu.

4.6. ETSI

L'Institut européen des normes de télécommunication (ETSI), ajouté au CEN et au CENELEC, est un organisme européen de normes (ESO) qui développe des normes européennes (NE).

Par le biais de comités techniques et de projets de partenariat soutenus par des groupes de travail, l'ETSI développe des normes de sécurité dans les communications mobiles/sans fil, les télécommunications d'urgence, l'infrastructure de technologies de l'information, les cartes à puce, les communications fixes et les algorithmes de sécurité. TC CYBER travaille sur des rapports techniques et un guide relatif à la protection des données personnelles et des communications, la sécurité et la confidentialité de l'IdO grand public, la cybersécurité pour les infrastructures nationales, la sécurité des réseaux et des outils et guides de cybersécurité.

Ces éléments comprennent : TS 103 645: ‘cybersécurité dans l'Internet des Objets’, TR 103 309 : ‘Adoption de la sécurité par défaut – technologie de sécurité des plateformes’, TR 103 331 : ‘Partage d'informations au sujet des menaces structurées’, TR 103 303 : ‘Mesures de protection pour l'ICT dans le contexte des infrastructures critiques’, TR 103 304 : ‘Protection des informations personnellement identifiables (PII) dans les services mobiles et dans le cloud’ et TR 103 306 : ‘Écosystème de la cybersécurité mondiale’. Le livre blanc Sécurité de l'ICT - le travail de l'ETSI, publié chaque année, offre un bref aperçu du développement des normes dans différents domaines, y compris la cybersécurité.

4.6.1. Comment participer au développement de normes au sein de l'ETSI

Il existe actuellement quatre organisations membres originaires d'Afrique du Sud, du Botswana et du Lesotho. La candidature à l'adhésion à l'ETSI requiert la conformité aux Directives de l'ETSI et aux décisions prises par l'Assemblée générale.

4.7. ICANN

L'Internet Corporation for Assigned Names and Number (ICANN)est une entreprise internationale à but non-lucratif destinée au grand public qui développe et met en œuvre des politiques pour les identifiants uniques sur Internet afin de préserver sa sécurité, sa stabilité et son interopérabilité. Dans le cadre d'une approche ascendante, gérée par le consensus et à multiples parties prenantes, l'ICANN développe des politiques de gestion des adresses Internet Protocol (IP), l'attribution d'identifiants de protocole et les domaines et serveurs racine utilisant des codes génériques (gTLD) et nationaux (ccTLD).

L'ICANN travaille sur des normes de partage des connaissances et d'instantiation pour le DNS et la sécurité de dénomination (KINDNS). Ces directives ont encouragé l'adoption d'opérateurs pour les bonnes pratiques en termes de sécurité DNS. Sur une base régulière, l'Office du responsable en chef de la technologie (Office of the Chief Technology Officer, OCTO) de l'ICANN rédige et diffuse des Publications de l'OCTO afin de présenter les positions sur les différents sujets liés aux identifiants internet.

4.7.1. Comment participer au développement de normes au sein de l'ICANN

L'organisation African Regional At-Large Organisation (AFRALO) a pour but de renforcer la participation des utilisateurs finaux aux décisions et à la création de politiques de l'ICANN, en formulant des normes techniques ayant un objectif spécifique dans les domaines de la confidentialité, la transparence et la responsabilité, et en tenant compte de la diversité culturelle et des intérêts du public mondial. L'AFRALO comprend actuellement 68 structures At-Large (ALSes) réparties dans 32 pays et territoires, ainsi que 16 membres individuels et trois observateurs.

L'AFRALO fournit à ses membres des informations, des ressources, un développement de capacité et des outils de partage des informations pour le développement des ICT et contribue aux activités de création de politiques qui influencent la coordination technique des systèmes de nom de domaine (DNS). L'AFRALO et l'AfriCANN gèrent une référence à l'espace de travail des déclarations à utiliser lors de différentes réunions de l'ICANN.

L'ICANN propose des cours et organise des webinaires pour prendre en charge la mise en place de capacités de création de politiques et d'évolution des normes, et pour partager les bonnes pratiques. Plus précisément, DNS 101 et DNSSEC 101 sont recommandées pour les décideurs politiques.

4.8. ENISA

L'Agence de l'Union européenne pour la Cybersécurité (ENISA) contribue à la recherche et au développement des normes de l'UE en matière de gestion des risques et pour la sécurité des produits, systèmes, réseaux et services électroniques, conformément à la réglementation (UE) 526/2013. Référence à la Réglementation (UE) 2019/881 (Loi sur la cybersécurité). L'ENISA prépare également des programmes de certifications candidats en référence à l'infrastructure de certification de la cybersécurité européenne pour les produits, services et

processus d'ICT. En outre, l'ENISA collabore avec l'ETSI, le CEN, le CENELEC pour produire des publications dans le domaine de la normalisation et de la certification.

L'ENISA a participé au développement de normes formelles et de facto utilisées dans la gestion des incidents de cybersécurité et la protection des infrastructures critiques qui peuvent être adoptées et utilisées dans les pays africains.

4.9. 3GPP

Le 3rd Generation Partnership Project (3GPP) se compose de membres ou d'organismes partenaires issus de sept organisations de normalisation de télécommunications (Association of Radio Industries and Businesses (ARIB), Alliance for Telecommunications Industry Solutions (ATIS), China Communications Standards Association (CCSA), ETSI, Telecommunications Standards Development Society, India (TSDSI), Telecommunications Technology Association (TTA) et le Telecommunication Technology Committee (TTC). Le projet produit des rapports et des spécifications qui définissent les technologies 3GPP dans le domaine des télécommunications cellulaires, y compris l'accès radio, le réseau central et les capacités de service.

Le 3GPP a produit des spécifications de sécurité dans la série 33. La participation aux réunions du 3GPP est limitée aux organismes partenaires. Les non-membres souhaitant participer doivent rechercher l'éligibilité via un organisme partenaire. Les catégories d'adhésion comprennent les partenaires, les membres individuels, les représentants de l'ITU, les observateurs et les invités.

4.10. Normes de facto

Les normes de facto sont adoptées, reconnues et largement utilisées par l'industrie et ses clients, et ne sont pas officiellement approuvées par les SDO.

Il existe des normes de facto pour les équipes de sécurité, y compris les équipes de réponses aux incidents de cybersécurité (CSIRT) et les équipes de réponse aux incidents de sécurité des produits (PSIRT). Par exemple :

- Protocole Information Sharing Traffic Light Protocol (FIRST TLP v1.0)

  Cette norme fournit un ensemble de règles hautement pragmatique et mondialement accepté en matière de partage de l'information. Cette norme est adoptée par les équipes accréditées par TI pour tout le partage d'informations.

Ressource : définitions du Traffic Light Protocol

TLP :ROUGE = Pas de diffusion, informations exclusivement destinées aux participants

TLP : ORANGE = Divulgation limitée aux organisations des participants

TLP : VERT = Diffusion limitée, informations destinées à la communauté

TLP :BLANC = Informations libres de diffusion

- RFC-2350

En utilisant le modèle ou le formulaire de cette norme, un CSIRT peut communiquer à ses membres les services qu'il propose, sa politique et ses procédures, et les attentes de l'équipe de ses membres. Depuis mai 2009, il est obligatoire de remplir et de publier le formulaire RFC-2350 pour les équipes accréditées par TI.

- Infrastructure de services CSIRT

FIRST, avec le soutien de la communauté des Groupes de travail CSIRT (TF-CSIRT) et de l'Union Internationale des Télécommunications (UIT), gère l'infrastructure des

Services CSIRT. L'infrastructure fournit une liste complète des services que les CSIRT pourraient éventuellement fournir à ses membres.

- Modèle de maturité pour la gestion des incidents de sécurité (SIM3)

SIM3 prend en charge la mesure de maturité de la réponse à un incident ou de l'équipe de sécurité, en fonction de quatre critères : organisation, aspects humains, outils et processus. Ce modèle prend en charge l'infrastructure de Certification TI et est utilisé dans l'auto-évaluation des équipes.

- Code de pratiques TI CSIRT (CCoP v2.4)

Le code fournit des conseils relatifs aux exigences en termes informationnels, de coopération, de gestion juridique et de gestion des vulnérabilités. L'utilisation du Code de pratiques de TI CSIRT est recommandée, mais facultative pour les équipes accréditées TI

- Taxonomie des incidents eCSIRT.net

La taxonomie fournit une classification et des exemples d'incidents de sécurité, ainsi qu'une description/explication. Des travaux plus approfondis sont nécessaires pour gérer la taxonomie et assister à la mise en œuvre de systèmes à double-ticket ou de systèmes de partage automatique pour l'utiliser.

5. Normes ouvertes

Les progrès technologiques rapides et les exigences qui s'intensifient en termes de délai de mise sur le marché et d'attentes des consommateurs poussent l'industrie à adopter des moyens plus efficaces pour définir des normes mondiales. Un modèle de normes complémentaire, géré par le marché, permettant l'innovation, la collaboration et l'excellence technologique est désormais utilisé dans le développement de normes internet par les organismes W3C, IETF et IEEE.

Les normes internet ouvertes permettent aux développeurs de définir de nouveaux services sans demander d'autorisation. Ces normes autorisent les utilisateurs à copier, distribuer et utiliser la technologie librement ou moyennant un coût modéré. Les organismes, y compris les agences gouvernementales qui choisissent d'utiliser des normes ouvertes, permettent la transformation numérique en autorisant l'interopérabilité des systèmes, la durabilité grâce à la réduction des coûts et en améliorant l'accès aux opportunités, y compris les contrats informatiques.

Ressource : Document politique du gouvernement du Royaume-Uni - Principes des normes ouvertes

Ces principes décrivent la manière dont le gouvernement britannique spécifie et sélectionne les normes ouvertes et la manière dont ces normes peuvent être mises en œuvre en source ouverte et dans les logiciels propriétaires. Ils soutiennent les stratégies de données ouvertes et numériques définies dans la Stratégie de transformation gouvernementale 2017-2020 et la Stratégie numérique du Royaume-Uni.

Les normes sélectionnées permettent l'interopérabilité des logiciels par le biais de protocoles ouverts et d'échange de données entre logiciels et magasins de données.

Les 7 principes de sélection de normes ouvertes à utiliser dans le secteur gouvernemental sont les suivants :

1. Les normes ouvertes doivent répondre aux besoins des utilisateurs.
2. Les normes ouvertes doivent offrir aux fournisseurs un accès égal aux contrats avec le gouvernement.
3. Les normes ouvertes doivent prendre en charge la flexibilité et le changement.
4. Les normes ouvertes doivent prendre en charge des coûts durables.
5. Sélectionner les normes ouvertes en prenant des décisions éclairées.
6. Sélectionner les normes ouvertes en utilisant des processus équitables et transparents.
7. Spécifier et mettre en œuvre des normes ouvertes en utilisant des processus équitables et transparents.

L'initiative OpenStand est un mouvement dédié à la promotion d'un ensemble de principes existants qui établissent le paradigme moderne en termes de normes soutenues par des organismes tels que l'IEEE, l'IETF, l'Internet Architecture Board (IAB), le World Wide Web Consortium (W3C) et l'Internet Society.

Vidéo : la communauté OpenStand se réunit au SXSW. Avec Tim Berners-Lee (W3C), Padmasree Warrior (CISCO) et Dave McAllister (ADOBE).

Figure 4 : 5 principes essentiels pour le développement de normes ouvertes. Source : Open-Stand

5.1.1. Open Cybersecurity Alliance

L'Open Cybersecurity Alliance fonctionne selon l'interopérabilité des produits, étendant les avantages de l'interaction des produits de cybersécurité proposés par de multiples fournisseurs à la communauté de cybersécurité. L'OCA développe et promeut des ensembles de code commun, des modèles et des pratiques visant à activer l'échange de données entre outils de cybersécurité sur un bus de messagerie commun et standardisé au sein du cycle de vie de gestion des menaces. L'interopérabilité au niveau des communications et des données garantit que des informations et résultats critiques ne sont pas manqués et limite l'enfermement des fournisseurs.

Ressource
Vidéo : Découvrez l'Open Cybersecurity Alliance

5.1.2. OASIS OPEN

La mission d'OASIS OPEN est de 'favoriser le développement équitable et transparent de logiciels en source ouverte et de normes ouvertes grâce au pouvoir de la collaboration mondiale et de la communauté'. La participation à OASIS est ouverte et son travail est soutenu par un parrainage annuel et par les frais d'adhésion.

OASIS Open est un organisme de normalisation à but non-lucratif dans lequel des individus, des organismes et des gouvernements collaborent pour relever les défis techniques par le biais du développement de codes ouverts et de normes ouvertes. OASIS Open propose des projets – y compris des projets en source ouverte – un parcours de normalisation et une approbation de jure qui servent de référence dans les politiques et approvisionnements internationaux.

Les personnes et les organisations rejoignent OASIS pour faire avancer des projets de cybersécurité, de blockchain, d'IdO, de gestion des urgences, d'informatique dans le cloud, d'échange de données légales et plus encore.

Exemples de comités techniques qui travaillent sur les normes de cybersécurité :

- Open Command and Control (OpenC2) TC, *crée un langage normalisé pour la gestion et le contrôle de technologies qui fournissent ou soutiennent des mesures de cyber-défense.*

- Collaborative Automated Course of Action Operations (CACAO) for Cybersecurity TC *développe une norme de mise en œuvre d'un modèle de parcours à suivre dans les opérations de cybersécurité.*
- Cyber Threat Intelligence (CTI) TC prend en charge *le partage d'informations automatisé favorisant la sensibilisation situationnelle à la cybersécurité, la défense des réseaux en temps réel et l'analyse approfondie des menaces. Le TC développe et normalise selon le processus des normes ouvertes OASIS : STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) et CybOX (Cyber Observable Expression).*
- Common Security Advisory Framework (CSAF) TC : *Normalisation de la divulgation automatisée des problèmes de vulnérabilité pour la cybersécurité*

5.1.3. I am the Calvary

I am the cavalry est une organisation de base composée de bénévoles, 'qui se concentre sur l'intersection entre sécurité numérique, sécurité publique et vie humaine' dans quatre domaines : dispositifs médicaux, transports, maisons connectées et infrastructure. Les dispositifs de l'Internet des Objets (IdO) sont déployés pour surveiller à distance et réaliser d'autres fonctions dans une infrastructure critique et par conséquent, l'organisation s'efforce d'encourager des protections de sécurité plus responsables et mieux adaptées afin de garantir la sécurité de l'infrastructure et du public.

5.1.4. OpenRAN

Différentes collaborations entre intervenants de l'industrie travaillent au développement de spécifications de sécurité pour les réseaux 5G Radio Access Networks (RAN) ouverts.

Cela comprend les travaux de l'O-RAN ALLIANCE sur des spécifications de RAN ouvertes, intelligentes, virtualisées et interopérables, et l'adhésion est ouverte aux opérateurs mobiles, fournisseurs ou établissements de recherche et d'enseignement.

L'Open RAN Policy Coalition est un groupe d'entreprises qui promeut des politiques qui feront avancer l'adoption de solutions ouvertes et interopérables dans le réseau Radio Access Network (RAN). Par le biais de la promotion de politiques, la coalition soutient l'application d'interfaces ouvertes. Ces politiques comprennent la prise en charge de technologies sans-fil ouvertes et interopérables, encouragent le soutien par le gouvernement de solutions ouvertes et interopérables, la diversité des fournisseurs et la suppression des obstacles au déploiement de la 5G.

6. Mise en œuvre et conformité aux normes

Les tests et la mise en œuvre de normes sont recommandés comme un moyen de comprendre et de s'engager en faveur du processus de normalisation.

Bonne pratique : Créer un site Web de sensibilisation aux normes

La création d'un site Web de sensibilisation aux normes internet est identifiée comme une bonne pratique. Ce site Web doit fournir un service gratuit et public qui favorise la sensibilisation, l'utilisation et le déploiement de normes. L'utilisation d'un langage simple et non-technique apporterait :

- une documentation compréhensible de soutien sur les normes internet
- des arguments et la description des écueils concernant le déploiement de normes internet
- une vérification en temps réel de la conformité aux normes

Le site Internet.nl est un portail et un outil de test et représente un bon exemple de l'établissement d'une collaboration entre de multiples parties prenantes pour promouvoir des normes internet liées à la sécurité. Le portail permet aux utilisateurs de vérifier que leurs site Web, messagerie et connexion Internet utilisent des normes internet modernes et fiables.

L'Open Standards Everywhere (OSE) de l'ISOC encourage les administrateurs et opérateurs de serveurs Web à déployer les toutes dernières normes et les derniers protocoles ouverts. L'OSE utilise le portail Internet.nl pour vérifier la prise en charge par les sites Web des normes internet modernes, y compris les normes IPv6, DNSSEC, HTTPS et les options de sécurité. L'ISOC informe, éduque, collabore et donne l'exemple pour soutenir les administrateurs de serveurs Web et de sites Web dans le déploiement des toutes dernières normes ouvertes.

Bonne pratique : Donner l'exemple

Donner l'exemple est une bonne pratique identifiée par le GFCE dans l'utilisation de normes liées à la sécurité. Les gouvernements peuvent donner l'exemple en :

- Mettant en œuvre les normes liées à la sécurité et autres dans les systèmes et réseaux existants et par le biais de processus d'approvisionnement.
- Faisant la promotion de l'utilisation de normes internet et de bonnes pratiques dans l'infrastructure des organismes officiels.
- Assurant une affectation appropriée des ressources, y compris le personnel et le budget, pour mettre en œuvre et configurer les normes.
- Intégrant les exigences de normes pour les produits ICT aux procédures et politiques d'approvisionnement.
- Adoptant des normes internet dans leurs plans d'ICT stratégiques.
- Développant des feuilles de route qui soulignent les activités de mise en œuvre tactique et opérationnelle et les responsabilités des parties prenantes.

Étude de cas : Les normes d'ICT dans le gouvernement

Le mandat élargi de l'autorité d'ICT au Kenya comprend l'application de normes d'ICT dans le gouvernement et le renforcement de la supervision de ses communications électroniques.

Cette autorité a publié et applique une conformité aux normes dans l'architecture des entreprises gouvernementales, l'informatique dans le cloud, le centre de données, la gestion des enregistrements et données électroniques, l'équipement des utilisateurs finaux, le développement du capital humain et des effectifs dans l'ICT, la sécurité des informations, la gouvernance informatique, le réseau, les systèmes et les applications d'ICT.

Étude de cas : le groupe régional de l'UIT pour la mise en œuvre de normes

africaines

Lors de la dernière réunion de l'UIT-T SG17 'Sécurité', en virtuel du 24 août au 3 septembre 2021, l'Afrique (Kenya, Ghana et Sénégal) a enregistré deux références de contribution pour la recommandation X.1060 : Infrastructure pour la création et l'utilisation d'un centre de cyber-défense (CDC). Ces contributions étaient les suivantes :

C1098 : Mise en œuvre de l'infrastructure de centre de défense de cybersécurité X.1060 : cette contribution a donné lieu à une requête pour l'ébauche, au 3e trimestre 2017, d'un supplément à la Recommandation X.1060 afin d'aider les États membres à mettre en œuvre la Recommandation. Cette requête devrait être ajoutée au programme de travail du 3e trimestre 2017 et si nécessaire, une nouvelle étude dans ce domaine devrait être mise en place

C1099 : Proposition d'enquête 'Évaluation des centres de cyber-défense en Afrique', dont les résultats devraient renforcer la capacité et l'efficacité des CDC en Afrique grâce au partage de bonnes pratiques en matière de fourniture de services, mais aussi fournir une opportunité de mise en réseau et de développement des capacités.

La participation des membres du Groupe régional pour la mise en œuvre de la Recommandation en Afrique a permis de comprendre le processus de normalisation, l'engagement des parties prenantes et la publication d'un questionnaire visant à évaluer, planifier et renforcer les services de cybersécurité dans les CDC en Afrique.

Les normes internationales sont souvent adoptées par des pays ou des régions qui souhaitent en faire des normes nationales ou régionales. La conformité aux normes est généralement rendue obligatoire par le biais de réglementations, gérées par une autorité nationale ou régionale.

L'utilisation des normes peut être obligatoire ou volontaire, selon les exigences réglementaires en vigueur dans un pays ou une juridiction. Dans l'idéal, les gouvernements souhaitent que les entités se conforment volontairement aux exigences des normes. Il est cependant recommandé que les entités publiques et privées ayant une obligation légale de rapporter les problèmes de sécurité mettent en œuvre les normes via des réglementations. L'utilisation de normes par ces entités leur permettrait d'identifier la norme la plus appropriée et d'influencer les mises à jour ultérieures ou les propositions de nouvelles normes, en réduisant le risque de sanctions, de poursuites judiciaires ou d'arrestation pour non-conformité.

Bonne pratique : Fourniture d'incitations économiques et réglementaires afin d'encourager l'adoption de normes internet.

Les incitations économiques et réglementaires afin d'encourager l'adoption de normes internet se traduisent notamment ainsi :

- Des réductions fiscales pour les entreprises qui adoptent la norme IPv6 en Corée du Sud
- Des déductions fiscales sur le prix d'achat d'équipements IPv6 (routeurs, commutateurs)
- Des logos et certifications pour les appareils IPv6 appliqués au Japon et en Corée du Sud
- Une réduction sur les frais d'abonnement aux domaines signés DNSSEC par registraires accrédités et registres de codes nationaux
    - Des campagnes de remises sur les enregistrements de domaines signés DNSSEC de registres internet : AFNIC (France), EURid (Europe, registre .eu), NORID (Norvège) et SIDN (Pays-Bas).
    - SIDN 'Programme de carte de score de registraire' pour encourager l'adoption des normes DNSSEC et IPv6

Réflexion

Les gouvernements ont un rôle majeur à jouer dans la promotion et l'utilisation de normes. En prenant l'exemple de votre pays, quelles incitations économiques et politiques le gouvernement devrait-il envisager ?

7. Certification

L'évaluation/l'accréditation/la certification institutionnelles, professionnelles et des produits offrent aux consommateurs une confirmation indépendante et impartiale indiquant qu'un produit ou un service est conforme ou répond aux exigences et caractéristiques décrites dans une norme ou dans des spécifications techniques publiées. La vérification de la conformité aux exigences qui peut inclure les impacts en termes de performance, de sécurité, d'efficacité, d'efficience, de fiabilité, de durabilité ou d'environnement est réalisée au moyen de tests et/ou d'inspections.

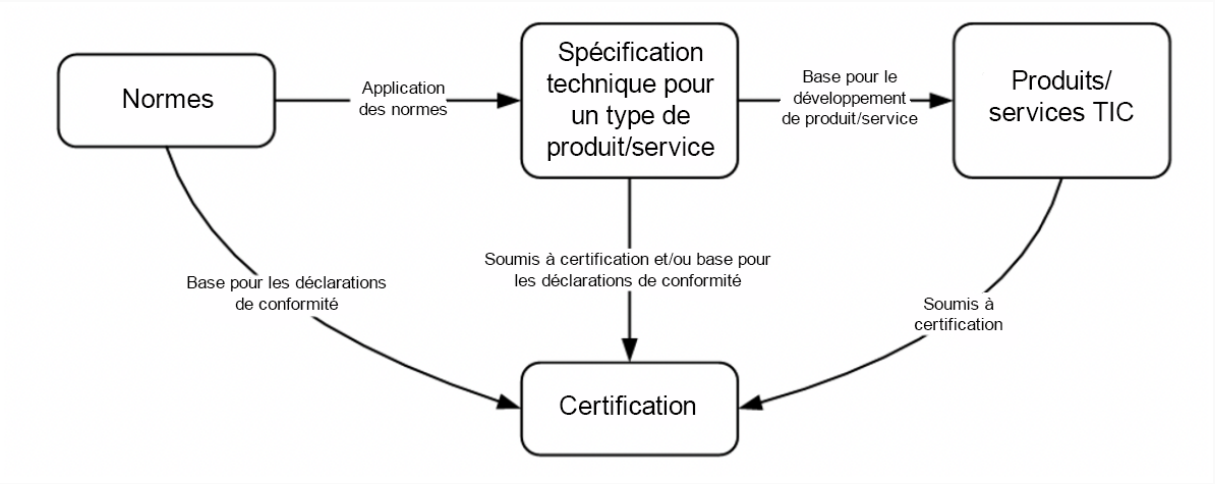


Figure 5 : Rôle des normes dans les certifications *sources : ENISA*

Le programme de certification de la cyber-sécurité de l'IECEE teste et certifie la cybersécurité de produits et systèmes électrotechniques dans la sphère électrotechnique, reposant sur les normes IEC en vigueur. Le programme est applicable à tout secteur possédant une infrastructure critique, y compris le secteur médical, les services publics et l'automobile.

Ressources :

La Réglementation (UE) 2019/881 (loi sur la cybersécurité) établit l'infrastructure européenne de certification de la cybersécurité.

L'objectif de cette infrastructure est d'assurer un niveau adéquat de cybersécurité pour les produits, services et processus d'ICT, mais aussi de garantir la cohérence des programmes de certification de cybersécurité dans l'UE. Le programme de certification de la cybersécurité est un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui s'applique à la certification de l'évaluation de conformité de produits, services ou processus d'ICT spécifiques.

En France, la certification repose sur des évaluations menées conformément aux spécifications ANSI ou aux normes conduites par l'autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI), dont la licence est octroyée par le Premier ministre français et accréditée par le comité français d'accréditation (COFRAC) selon la norme EN ISO/CEI 17025.

L'accès à internet s'effectue via des dispositifs grand public et le programme d'évaluation de la conformité (ICAP) de l'IEEE développe et met en œuvre des programmes qui associent des activités de développement standard pour contribuer à accélérer l'adoption par le marché tout en réduisant les coûts de mise en œuvre. Consommateurs, fabricants, prestataires de services, revendeurs à valeur ajoutée et entreprises attendent des produits fiables, efficaces, sûrs et interopérables.

Les professionnels peuvent recevoir une certification en suivant des cours proposés par des organisations certifiées selon la norme ISO/IEC 17024:2021. Les cours certifiés présentent de nombreux avantages : confiance, reconnaissance mutuelle et échange global de personnel. L'International Information System Security Certification Consortium, Inc. (ISC)2 propose différentes certifications de sécurité des informations, y compris le certificat professionnel de sécurité des systèmes d'information certifiés (CISSP) destiné aux responsables possédant une bonne compréhension de la stratégie et des opérations de cybersécurité. La certification professionnelle peut être obtenue via l'ISACA et le COMPTIA.

Dans la gestion des cyber-incidents, les CSIRT participent et gèrent le statut des accréditations et des certifications d'une équipe au sein de la communauté Trusted Introducer (TI), ce qui est un prérequis à l'adhésion sur les réseaux internationaux comme FIRST.

8. Mappage des parties prenantes au développement de normes de sécurité

L'établissement d'une coopération nationale entre de multiples parties prenantes pour promouvoir les normes internet relatives à la sécurité est identifié par le GFCE comme une bonne pratique.

L'élaboration de normes impliquant un certain nombre de parties prenantes dans le cadre d'une coopération volontaire d'intervenants étatiques et autres augmente le niveau de sensibilisation aux normes de sécurité internet et soutient la création d'un environnement et de partenariats favorables.

Bonne pratique : Établissement d'une coopération nationale entre de multiples parties prenantes pour promouvoir les normes internet liées à la sécurité.

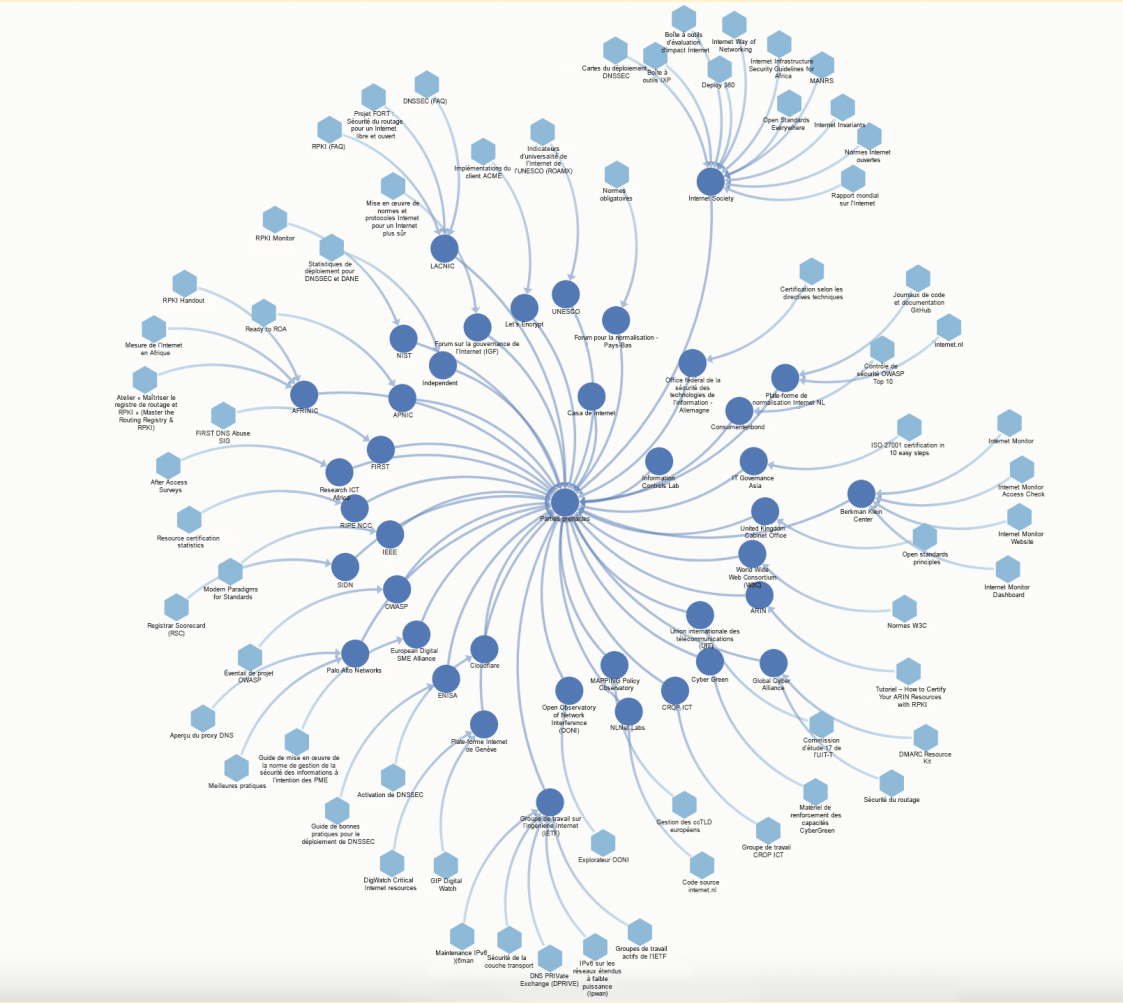
La coopération sur la base du volontariat entre les parties prenantes favorise l'amélioration de la sensibilisation à la nécessité de mettre en œuvre des normes internet et l'utilité de la formation collaborative via un partage d'expertise qui contribue finalement à la création de capacité dans les entités participantes.

La collaboration entre les parties prenantes a été établie sous différentes formes, y compris les groupes de travail IPv6 afin d'encourager l'adoption de la norme IPv6 en Algérie, en Égypte, au Kenya, à l'île Maurice, au Nigeria, en Afrique du Sud, au Sénégal et en Tunisie. En 2012, l'AfriNIC, le Registre internet régional pour l'Afrique, a lancé le groupe de travail africain sur l'IPv6 (AF6TF).

Ressource : Infographie : Cartographie des parties prenantes aux normes

Les parties prenantes sont représentées par des cercles bleus et les initiatives par des hexagones.

En cliquant sur une icône spécifique, vous pourrez vous familiariser avec des parties prenantes individuelles et leurs initiatives respectives.



***Source** : GFCE*

Étude de cas : Participation de multiples parties prenantes à la mise en œuvre des normes — Cameroun

Le Cameroun dispose d'un processus pour identifier les domaines dans lesquels des normes sont requises, évaluer quelles normes utiliser pour combler les lacunes et mettre en œuvre les normes. Par le biais d'un processus à multiples parties prenantes, les entités (entreprises du secteur privé, infrastructures critiques et éventuellement organisations gouvernementales) identifient et rapportent les problèmes de sécurité (ou leur besoin d'établir une norme technique) à une agence gouvernementale du ministère de l'ICT. Le ministère transmet ensuite la question à un comité composé de représentants du gouvernement, du secteur privé et du monde universitaire. Le comité recommande l'application d'une norme particulière, que l'agence approuve, puis met en œuvre par le biais d'une réglementation.

Source : réunion GFCE ACE à La Haye

Réflexion :

La coopération entre de multiples parties prenantes au niveau national est importante pour promouvoir les normes internet en matière de sécurité, en prenant l'exemple de votre pays.

- Identification des intervenants au développement de normes.
- Comment la collaboration d'une partie prenante est-elle mise en œuvre ?
- Quels sont les défis ?
- Quel est le calendrier de mise en œuvre ?

9. Initiatives de création de capacité

9.1. GFCE Internet Infrastructure Initiative - Triple-I

Une infrastructure internet robuste, ouverte et résiliente est essentielle pour contrer les infractions et les menaces. Le GFCE Triple-I est une initiative du GFCE qui, via la favorisation d'une prise de conscience et l'utilisation des expériences de bonnes pratiques pour améliorer une confiance justifiée dans les connexions internet et les échanges d'e-mails, encourage l'utilisation de normes ouvertes en matière de sécurité.

GFCE Triple-I promeut l'utilisation des normes Internet suivantes :

- **IPv6** : une extension majeure de la plage d'adresses internet et un catalyseur des capacités de sécurité
- **DNSSEC** : des extensions de sécurité pour l'infrastructure de noms de domaine internet
- **TLS, HTTPS, DANE et STARTTLS** : des connexions sécurisées entre les utilisateurs et les services internet
- **RPKI, ROA** : empêche le détournement et les autres attaques de routage grâce à l'utilisation d'un ancrage de confiance
- **DKIM, SPF et DMARC** : des mesures anti-hameçonnage et anti-usurpation

En outre, les ateliers GFCE Triple-I réunissent des parties prenantes qui partagent de bonnes pratiques dans les domaines de la cyber-hygiène (par ex. MANRS), et qui partagent des données sur les vulnérabilités et les abus (par ex. M3AAWG, Cybergreen, ICANN DAAR).

Chaque session se compose de trois parties : partage des informations et éducation ; discussion sur les questions prioritaires et la manière de les aborder ; et conclusions sur les actions à entreprendre à l'avenir, avec des engagements volontaires des participants à s'efforcer de réaliser ces actions.

9.2. Normes Internet ouvertes pour les universités africaines

En 2019, l'Internet Society a organisé une formation pilote d'un mois aux normes Internet ouvertes au sujet de la sécurité des protocoles Internet (Internet Protocol Security, IPSec) pour familiariser la prochaine génération d'experts africains avec les normes internet ouvertes et fournir aux conférenciers des éléments de formation supplémentaires afin de soutenir les cours existants dans des universités. Ce cours

a réuni 70 étudiants de 4 universités africaines de RDC, d'Éthiopie, du Kenya et du Ghana.

9.3. International Cybersecurity Challenge

L'ENISA organisera le premier International Cybersecurity Challenge, une cyber-coupe du Monde, du 14 au 17 juin 2022. S'appuyant sur le succès des compétitions Building Capture-the-flag (CTF), l'International Cybersecurity Challenge réunira 9 équipes internationales composées de joueurs âgés de 18 à 26 ans qui s'efforceront de relever les défis des applications Web et de l'exploitation des systèmes, de la cryptographie, de l'ingénierie inversée, mais aussi les défis matériels, l'analyse rétrospective et les attaques/défenses.

9.4. Hackathon@AIS

L'objectif d'Hackathon@AIS est d'identifier, d'encourager et de faire connaître aux ingénieurs africains le développement de normes internet ouvertes en Afrique, afin qu'ils puissent contribuer au travail d'organisations comme l'Internet Engineering Task Force (IETF).

L'Hackathon@AIS 2019 organisé à Kampala, en Ouganda, à l'occasion du Sommet africain de l'Internet comprenait cinq parties :

- La *Programmabilité réseau* abordait les concepts et composants de programmabilité réseau, y compris les normes IETF comme YANG, NETCONF et RESTCONF, et les outils tels que les langages de programmation pyang, ncclient et Postman.
- *Le Temps réseau* couvrait le travail en cours pour sécuriser le serveur de temps réseau (NTS, Secure Network Time) et l'utilisation de Chrony pour la synchronisation avec le serveur de temps.
- *IPv6 abordait le protocole* IPv6 et les groupes de travail IETF IPv6 (6MAN et v6OPS), et les participants étaient invités à activer IPv6 dans plusieurs outils en source ouverte utilisant uniquement IPv4.
- *IPWAVE* couvrait les tests et la mise en œuvre d'un Internet-Draft dans le cadre du groupe de travail IPWAVE.
- *Mesure* couvrait les configurations de DNS sur TLS (DoT) et de DNS sur HTTPS (DoH) et la mesure de la performance des résolveurs de cache par rapport aux serveurs DoT et DoH à configuration locale comparés aux résolveurs DNS publiquement disponibles. Lisez un rapport concernant l'expérience du parcours de Willem Toorop, un facilitateur de NLnet Labs. Ce parcours a contribué à une mise à jour du groupe de travail IPWAVE à l'IETF.

10. Les femmes dans la normalisation

Pour encourager la participation des femmes à la normalisation, les SDO disposent de plusieurs programmes et initiatives. Cela comprend le groupe d'experts ITU Women in Standardisation Expert Group (WISE) établi en 2016. Conformément aux dispositions de la Résolution 55 – Promouvoir l'égalité des genres dans les activités du secteur de la Normalisation, le groupe vise à encourager la participation active des femmes aux activités du secteur de la normalisation de l'UIT (UIT-T), aux rôles de leadership et à l'inclusion de la prise en compte des genres dans les travaux de l'UIT-T. On peut participer au programme de mentorat WISE qui vise à promouvoir la participation active, la contribution et le leadership des femmes dans tous les aspects des activités et processus UIT-T.

IEEE Women in Engineering est un réseau mondial qui relie les femmes dans le monde de la technologie. L'objectif de la communauté est de faciliter le recrutement et la rétention des femmes du monde entier dans les disciplines techniques. L'adhésion au IEEE WIE est proposée aux membres de l'IEEE, avec des opportunités d'inspirer les femmes pour qu'elles accèdent à des postes à responsabilité. Le WIE Affinity Group offre des opportunités de mise en réseau qui sont actuellement disponibles en Égypte, au Kenya, au Maroc, en Namibie, en Afrique du Sud, en Tunisie et en Ouganda.

11. La (géo)politique de la normalisation

Les normes soutiennent l'innovation, la croissance économique, la compétitivité, facilitent le commerce international et contribuent à protéger les droits des consommateurs, les infrastructures critiques et la sécurité nationale. Dans la mesure où les normes ont des implications socio-économiques et géopolitiques étendues qui affectent l'équilibre du pouvoir entre entreprises concurrentes et/ou intérêts nationaux, elles devraient être envisagées lors de la définition des objectifs des politiques nationales.

Ressource :

Vidéo : Normes numériques, Chine et géopolitique : quels sont les enjeux ?

La Chine a récemment augmenté sa participation aux organisations de normalisation (SDO), ce qui peut être interprété comme une conséquence naturelle du développement technologique rapide du pays et comme une indication que les Chinois préfèrent s'engager dans des organisations qui soutiennent l'ordre international.

D'un côté, on peut espérer que la participation chinoise renforcera l'adoption des normes internationales en Chine. De l'autre, certains craignent que la participation accrue de la Chine soit guidée par des objectifs de projection politique et économique nationale, sur l'État et ses intervenants privés, ce qui pourrait nuire aux objectifs d'efficacité technique.

Deux propositions spécifiques présentées par des intervenants chinois à l'Union Internationale des Télécommunications (UIT) et qui ont attiré l'attention des médias seront abordées dans notre discussion : une proposition visant à inciter l'UIT-T à s'engager dans la conception d'un nouveau protocole (la proposition « Nouvel IP ») et une proposition relative à la normalisation des systèmes de reconnaissance faciale dans la vidéo-surveillance.

Le 2 février 2022, la Commission européenne a lancé la Stratégie de l'UE en matière de normalisation - Définition de normes mondiales pour soutenir un marché unique de l'UE résilient, écologique et numérique. Cette stratégie a pour objectif de renforcer la compétitivité mondiale de l'UE, de favoriser une économie numérique résiliente et écologique et d'intégrer les valeurs démocratiques aux applications technologiques.

> *'Les normes techniques présentent une importance stratégique. La souveraineté technologique de l'Europe, l'aptitude à réduire les dépendances et la protection des valeurs de l'UE reposeront sur notre aptitude à définir des*

normes mondiales' (Thierry Breton, Commissaire responsable du Marché intérieur).

La stratégie se compose de cinq séries d'actions clés : anticiper, prioriser et gérer les besoins de normalisation dans les domaines stratégiques, améliorer la gouvernance et l'intégrité de la normalisation européenne, renforcer le leadership européen dans les normes mondiales, soutenir l'innovation et mettre en place la prochaine génération de normalisation.

Cette stratégie est considérée comme une réponse au rapport de la Chambre de commerce de l'Union européenne en Chine (Chambre européenne) La voie de l'avenir : la course au contrôle de la normalisation technique, publié en décembre 2021. Ce rapport identifie le cadre de normes techniques comme un champ de bataille sur lequel les États combattent pour la domination des technologies stratégiques, comme la 5G, l'intelligence artificielle et les nouveaux véhicules électriques.

12. Principaux enseignements

Une norme de sécurité, comme toute autre norme, est une spécification technique ou un critère visant à être utilisé de façon cohérente, comme une règle, une consigne ou une définition. Les normes sont développées dans le cadre d'un processus de création de consensus dans des organisations internationales, régionales ou nationales.

Dans ce module, nous avons examiné différentes organisations de normalisation, les normes de cybersécurité qu'elles ont élaborées et les opportunités d'engagement. Compte tenu du fait que les pays en développement ne sont pas suffisamment représentés dans le processus de normalisation, un effort a été fait pour combler ce fossé grâce à différentes initiatives. Ces initiatives, parmi lesquelles l' African Standardization Strategy et la feuille de route de la quatrième révolution industrielle, s'efforcent de promouvoir l'harmonisation des normes afin de renforcer la compétitivité de la Zone de libre-échange continentale africaine (AfCFTA). L'engagement d'un pays à participer au développement de normes de cybersécurité internationale devrait s'articuler autour de sa stratégie nationale de cybersécurité pour faire en sorte que des experts et des ressources s'engagent dans ce processus.

Réflexion : les points importants

Notez cinq points essentiels qui vous semblent importants et qui ne sont pas inclus dans ce module.