KM9: Cybersecurity Standards and Certification

Module objectives

Introduction

Why are standards important?

Formal Standards

Standards Development Organisations

- The IETF
  - How to engage in standards development at the IETF
- The IEC
  - How to engage in standards development at the IEC
- The ISO
  - How to engage in standards development at the ISO
- International Telecommunications Union
  - How to engage in standards development at the ITU
- The IEEE
- ETSI
- ICANN
  - How to engage in standards development at ICANN
- ENISA
- 3GPP
- De facto standards

Open standards

- Open Cybersecurity Alliance
- OASIS OPEN
- I am the Calvary
- OpenRAN

Standards implementation and compliance

Certification

Mapping the stakeholders in security standards development

Capacity building initiatives

- GFCE Internet Infrastructure Initiative - Triple-I
- Open Internet Standards for African universities
- International Cybersecurity Challenge
- Hackthon@AIS

Women in Standardisation

The (Geo)Politics of standardisation

Main takeaways

Module objectives

Welcome to the knowledge module on **Cybersecurity Standards** as part of the GFCE-Africa project.

This knowledge module participants will gain knowledge on policy and technical considerations for cybersecurity standards development and implementation through sharing of best practice, case studies, exercises, and reflections.

Upon finishing the module, you will be able to respond to, and find additional resources for the following questions:

- What are Security-Related Standards?
- What are Open Standards?
- Standards Development Organisations (SDOs) and how to engage
- Who are the stakeholders in security standards development?
- What standards development capacity building initiatives are available?

1. Introduction

The Digital Transformation Strategy for Africa (2020-2030) seeks to enable digital transformation and industrialisation, and support the digital economy and implementation of the African Continental Free Trade Area (AfCFTA). The strategy promotes the use of open standards in the building of an interoperable cross-border trust framework for personal data protection and privacy.

It is therefore imperative for policy makers to understand the importance of developing and implementing security related standards. When assessing a country's cybersecurity capacity, different approaches can be used. The Cybersecurity Capacity Maturity (CMM) Model for Nations addresses the use of cybersecurity technology and standards to protect individuals, organisations, and national infrastructure. In addition, the CMM model addresses cybersecurity knowledge and capabilities, including the availability of formal cybersecurity education programmes, and professional training programmes.

The module covers cybersecurity standards, standards development organisations (SDOs), and explores the opportunities for the involvement of African stakeholders in the development of standards. The module also explores opportunities for development of capacity through certification of institutions and personnel.

2. Why are standards important?

Standards represent sets of agreed-upon rules that tell us how to do something. A standard defines requirements, specifications, guidelines or characteristics for a determined material, product, process or service. Standards are contained within technical documents 'designed to be used as a rule, guideline or definition, and are a consensus-built, repeatable way of doing something' (CEN).

Standards are essential for quality and risk management, drive innovation, and contribute to the growth of markets through the production of products with consistent quality and performance. Standards are important for the protection of health and safety of workers, as well as the general public.

The IEC international standards provide instructions, guidelines, rules or definitions that are used to design, manufacture, install, test and certify, maintain and repair electrical and electronic devices and systems, and are arrived at through global consensus. According to the International Telecommunications Union, standards are important to ensure the security, stability, reliability, interoperability, safety for human health, and energy efficiency of Information and Communications Technologies (ICT).

Reflection: Standards used in a smartphone

Identify additional standards used in a smartphone other than those shown in Figure 1 below.

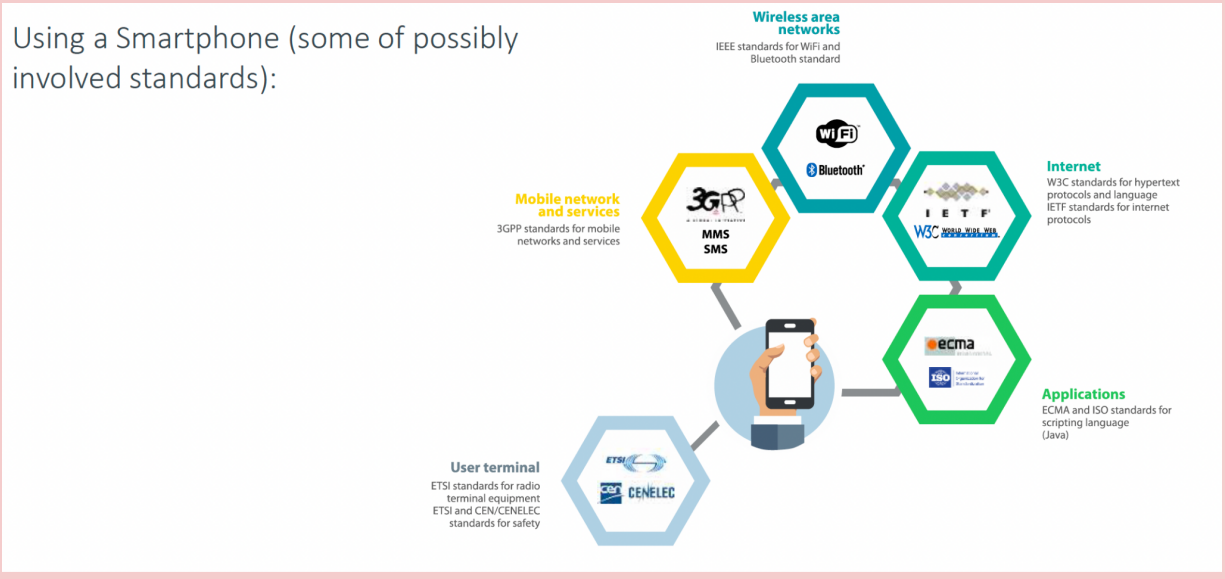


Figure 1: We live in a 'standardised' world Source: ETSI

3. Formal Standards

An ecosystem of protocols, standards, technology, practices, and organisations keep the internet open, stable, secure, and resilient. Standards ensure that hardware and software developed or manufactured by different entities work together as seamlessly as possible, or are interoperable. Adoption and deployment of security-related internet standards contribute to a secure and resilient internet infrastructure and cyberspace.

Formal standards are endorsed by a formal Standard Development Organisation (SDO). SDOs include the International Electrotechnical Commission (IEC), the International Organisation for Standardization (ISO), and the International Telecommunication Union (ITU). Quasi-formal organisations including the Institute of Electrical and Electronics Engineers (IEEE), the 3rd Generation Partnership Project (3GPP), and the Internet Engineering Task Force (IETF), industry forums, and consortia play a significant role in the development of security-related internet standards.

The participation of government, regulators, academia, and other stakeholders in SDOs should be aligned with national priorities and obligations as set out in the national cybersecurity strategy, international or regional conventions. This would help governments determine priority standardisation areas, state and non-state representation in various SDO,s and the resource commitment. The Internet itself is mainly based on IETF developed "standards" which are not formally endorsed by States but are merely based on the work by volunteers from different organisations from all over the world. Participation is open for anyone, and influence is based on merits (technical know-how and skills). In the IETF, participants don't represent organisations or governments, and all participate on equal footing; there is therefore potential to have experts from Africa contribute to standards development on their own merit. The standards generated are "voluntary" and are generally adopted because they work ("rough consensus and running code") and help ensure interoperability of the Internet.

4. Standards Development Organisations

4.1. The IETF

Internet technical standards are developed mainly by the Internet Engineering Task Force (IETF). The main internet standards developed by the IETF include the Transmission Control Protocol/Internet Protocol (TCP/IP), the domain name system (DNS), and the secure sockets layer (SSL).

Other significant standards developed:

- Transport Level Security protocol (TLS) recent revision TLS 1.3: Protects the privacy and the integrity of transmitted data
- DNS-based Authentication of Named Entities (DANE): enhances the effectiveness of TLS
- Automated Certificate Management Environment (ACME) protocol: enables the setup of a secure website in seconds
- Domain Name System Security Extensions (DNSSEC): Prevents the redirection of internet users to malicious sites or mail servers
- IPv6: Enables multiple users and devices to connect to the internet and provides security capabilities
- Mutually Agreed Norms for Routing Security (MANRS): outlines concrete actions which reduce the most common routing threats for networks

4.1.1. How to engage in standards development at the IETF

The IETF technical specifications are published in RFC documents, beginning as Internet-Drafts (I-Ds) which are then adopted, improved, and revised by a working group. An I-D can be authored by an individual or a group, and obtains standing in the IETF if adopted by a working group or approved as an RFC. A complete list of all active working groups, with links to their charters, discussion email lists, and other information is available on IETF Datatracker.

The IETF Policy Program is a virtual four-week program targeting government officials, policy makers, and regulators. The program gives visibility to the IETF standards environment and covers three thematic tracks:

- The history of the internet and the IETF
- The internet's inner workings
- Tackling internet challenges

Participants have an opportunity to engage with experts and leaders on leading-edge technical and policy issues, and immerse in the open standards development process by participating in IETF Working Group sessions.

4.2. The IEC

The IEC develops international standards in various areas, including but not limited to cybersecurity, Artificial Intelligence (AI), internet of things (IoT), transportation, Sustainable Development Goals (SDGs), Energy, Cities and Communities, smart manufacturing. These standards form the basis of testing and certification.

The IEC International standards ISO/IEC 27001 and IEC 62443 are horizontal standards, suitable for all sectors. The IEC 62443 series of standards establishes cybersecurity guidelines and specifications applicable to a variety of industries and critical infrastructure, including transportation. The standard is compatible with the US National Institute of Standards and Technology (NIST) cybersecurity framework. ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS) as well as the terms and definitions commonly used in the ISMS family of standards. ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organisation.

Such horizontal standards are complemented by vertical standards covering the specific security needs of the nuclear industry, industrial automation, healthcare, and the maritime industry, among others. These standards include IEC 62645 Nuclear power plants – instrumentation, control, and electrical power systems – cybersecurity requirements, IEC 61850 series for communication networks and systems for power utility automation, IEC 60870 series for telecontrol equipment and systems, and IEC 61162 series for maritime navigation, and radiocommunication equipment and systems.

The IECEE industrial cybersecurity programme tests and certifies cybersecurity in the industrial automation sector, in accordance with the IEC 62443 series. Today, both public and private entities are seeking third-party certification to ensure conformity of their information security management system (ISMS) to ISO/IEC 27001. The

organisations verifying conformity should be certified and registered under ISO/IEC 27006.

4.2.1. How to engage in standards development at the IEC

The IEC encourages, through regional centres, participation in its work. The IEC Africa Regional Centre (IEC-AFRC) has been set up to promote awareness of the IEC in the African region, increase the adoption and use of the IEC International Standards and the IEC Conformity Assessment Systems, and support participation and enhance active contributions to the IEC work.

The IEC Affiliate Country Programme provides the opportunity for the developing and newly industrialised countries to participate in the international standardisation and conformity assessment activities without the financial burden of membership. Joining the IEC Affiliate Country Programme is by invitation from the IEC General Secretary & CEO.

A country can attain an Affiliate Plus status by officially declaring the adoption of at least 50 IEC International Standards as national standards, and establishing a NEC with representatives from the private and public sectors. Affiliate countries are supported to meet their specific needs through the IEC mentoring programme that partners the IEC members with affiliate countries

Figure 2*: Benefits of the IEC Affiliate Country Programme* Source*: IEC*

The African Electrotechnical Standardization Commission (AFSEC) is established by statute as a subsidiary body under the auspices of the African Energy Commission. The

AFSEC has statutory and affiliate membership. Countries that are statutory members participate in the work of the AFSEC through a National Electrotechnical Committee (NEC).

Standards are developed on the basis of submission of New Work Item Proposal (NWIP) which is considered based on the approval process.

4.3. The ISO

The ISO is an independent, non-governmental international organisation with a membership of 165 national standards bodies. The ISO develops IT security standards, the most widely known being the ISO/IEC 27001 which provides requirements for an information security management system (ISMS).

Other standards include the ISO/IEC 27032:2012 providing guidelines for cybersecurity and ISO/IEC 27005 on information security risk management standard, designed to assist the satisfactory implementation of information security based on a risk management approach with the understanding of concepts, models, processes, and terminologies in ISO/IEC 27001 and ISO/IEC 27002.

Other relevant standards include ISO 27005: 2018 Information Technology – SecurityTechniques – Information security risk management and ISO 31000: 2018 Risk management – Guidelines.

The ISO/AWI 22336 Security and resilience — Organisational resilience — Resilience policy formulation and strategy implementation is under development, and will provide guidance to organisations on how to formulate corporate policy and implement a strategy to enhance organisational resilience. It will also assist organisations in articulating the organisations' vision and purpose, set strategic objectives, and define its actions to achieve an enhanced state of organisational resilience.

The ISO/IEC JTC 1/SC 27 – information security, cybersecurity, and privacy protection – has developed standards for the protection of information and the ICT including generic methods, techniques, and guidelines to address both security and privacy aspects, such as management of information and the ICT security, conformance assessment, accreditation, and auditing requirements.

4.3.1. How to engage in standards development at the ISO

The SDOs have processes and procedures for standards development from proposal, drafting, approval, and publication. The IEEE SA provides individual and corporate membership. Development of an African Standard, or a series of related standards, can be initiated through New Work Items in existing Technical Committees, and declared by the African Organisation for Standardisation (ARSO) Council. The ARSO harmonises

African Standards and conformity assessment procedures, in order to reduce technical barriers to trade, and to enhance intra-African and international trade, industrialisation, and integration in Africa.

To this end, ARSO together with the IEEE SA has developed the African Standardization Strategy and Roadmap for the Fourth Industrial Revolution to promote harmonisation of standards to enhance competitiveness of the African Continental Free Trade Area (AfCFTA).

Reflection:
Making reference to the IEEE SA White Paper on Africa 4th Industrial Revolution Standardization Strategy (2021-2025)

Discuss why Africa should have a standardisation strategy? What would this strategy address?

4.4. International Telecommunications Union

The International Telecommunication Union (ITU) is organised in three sectors, the Radiocommunications (ITU-R), Development (ITU-D) and Standardisation (ITU-T) Sectors.

The ITU Telecommunication Standardization Sector has developed the ITU-T X.series Recommendations: data networks, open system communications, and security. These standards/recommendations are developed by Study Groups in the ITU Telecommunications standardization sector.

4.4.1. How to engage in standards development at the ITU

Membership to the three sectors of the ITU is open to governments, industry, and academia. The ITU encourages increased participation of developing countries in standardisation activities including attendance to meetings, submission of contributions, taking leadership positions and hosting of meetings/workshops pursuant to provisions of the World Telecommunication Standardization Assembly (Hammamet, 2016),

Resolution 54 on Creation of, and assistance to, regional groups.

There are currently 8 Africa Regional Groups in the ITU Standardisation Sector:

- ITU-T Study Group 2: Operational aspects of service provision and telecommunications management
- ITU-T Study Group 3: Tariff and accounting principles, and international telecommunication/ICT economic and policy issues
- ITU-T Study Group 5: Environment, climate change and circular economy
- ITU-T Study Group 11: Signalling requirements, protocols, test specifications, and combating counterfeit products
- ITU-T Study Group 12: Performance, quality of service (QoS), and quality of experience (QoE)
- ITU-T Study Group 13: Future networks, with focus on IMT-2020, cloud computing, and trusted network infrastructures
- ITU-T Study Group 17: Security
- ITU-T Study Group 20: Internet of things (IoT) and smart cities and communities (SC&C)

These groups are pursuant to provisions of the World Telecommunication Standardization Assembly (Hammamet, 2016), Resolution 44 on Bridging the Standardization Gap between developing and developed countries.

The Bridging the Standardization Gap (BSG) programme aims to facilitate the efficient participation of developing countries in the ITU's standards-making process, to disseminate information about the existing standards, and to assist developing countries in the implementation of standards.

Figure 3: Five strategic pillars of the BSG Source *ITU*

- Awareness: The BSG programme aims to create awareness and know-how of the standards-making process
- Know-how: acquiring the right skills and capabilities for international standards-making
- Community: Regional groups of the ITU-T Study Groups providing assistance in establishing National Standardization Programs, coordination plans with national SDOs and relevant regional organisations and academia.
- Engagement and Participation: Participation in study group meetings and the BSG alumni network
- Partnering: Opportunities to host, sponsor, and fund the BSG activities

4.5. The IEEE

The IEEE Standards Association has various programmes on security standards in verticals, including critical infrastructure, power, consumer and healthcare, plus IoT framework standards.

This is a listing of some of the cybersecurity standardisation activities which are currently ongoing or published within the IEEE-SA. A prefix "P" in front of the number indicates that it's an active working group, currently developing the standard; in many

situations, the P standard will also have a published version, as the work on the next revision is ongoing.

IoT Framework Standards focused on Security

- IEEE 2413-2019, Standard for an Architectural Framework for the internet of things
- IEEE P2994: Standard for Security Assessment Framework for the internet of things (IoT) Application Deployments

Healthcare/Wearables/Consumer:

- IEEE 11073 Series of Standards: IEEE 11703 has one part on cybersecurity for medical devices under the P11073-40101 – IEEE Draft Standard – Health informatics – Device interoperability – Part 40101: Cybersecurity – Processes for vulnerability assessment IEEE P1912: Standard for Privacy and Security Architecture for Consumer Wireless Devices
- IEEE 2621 Working Group: Standard for Wireless Health Device Security Assurance

  There are 3 standards within this framework

  - IEEE P2621.1: Standard for Wireless Diabetes Device Security Assurance: Product Security Evaluation Program
  - IEEE P2621.2: Project Title: Standard for Wireless Diabetes Device Security Assurance: Protection Profile for Connected Diabetes Devices
  - IEEE P2621.3: Project Title: Standard for Wireless Diabetes Device Security Assurance: Guidance for Mobile Devices

- IEEE PHD (Personal Healthcare Devices): Cybersecurity Standards Roadmap – Whitepaper
- IEEE SA Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain – White paper
- IEEE P2933: Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security
- IEEE 2410-2020: IEEE Standard for Biometric Privacy
- IEEE P2418.6: Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences

Energy/Smart Grid

- IEEE C37.240-2014: IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
- IEEE 1686-2013: IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
- IEEE P2030.102.1: Standard for Interoperability of Internet Protocol Security (IPsec) Utilised within Utility Control Systems
- IEEE P1711: Standard for a Cryptographic Protocol for Electric Power System (EPS) Communications Links
- IEEE P1711.1: Standard for a Cryptographic Protocol for Cybersecurity of Substation Serial Links: Substation Serial Protection Protocol
- IEEE P2658: Guide for Cybersecurity Testing in Electric Power Systems
- IEEE 802.15.4-2020: IEEE Approved Draft Standard for Low-Rate Wireless Networks
    - The IEEE 802.15.4 protocol is used in smart grid applications (smart metering) and has several security features such as access control, frame integrity, and confidentiality
- IEEE SA has also initiated some key work on blockchain focused around energy
    - IEEE P825: Guide for Interoperability of Transactive Energy Systems with Electric Power Infrastructure (Building the Enabling Network for Distributed Energy Resources)
- IEEE P2418.5: Standard for Blockchain in Energy
- IEEE 692-2013: The IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations, developed by WG 3.2 – Security Systems Working Group addresses security system equipment for 'detection, assessment, surveillance, access control, communication, and data acquisition'.
- The numerous IEEE smart grid systems standards[6] include a number focused on security, e.g. IEEE C37.240-2014 – the IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems developed by 240 WG – PC37.240 Cyber Security Standard and the IEEE 1686-2013 – the IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities developed by WGC1 – Substations Working Group C1.

FinTech:

- IEEE P1940: Standard Profiles for ISO 8583 authentication Services

- IEEE P1940 is mainly focused around financial transactions (e.g. point-of-sale (POS), automated teller machine (ATM) cash withdrawal transactions, etc.) Such services include biometric authentication (as defined by IEEE Std. 2410), PIN-based, Fast Identity Online (FIDO), and One-Time Password (OTP) and Time-based OTP (TOTP) authentication methods including risk and presentation attack defence (PAD) measures

Mobility/Automotive:

- IEEE P1609.2: Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages

Software:

- IEEE Computer Society Cybersecurity and Privacy Standards Committee
- IEEE 1619 series on crypto protection for storage devices:
  - IEEE 1619-2018: the IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
  - IEEE 1619.1-2018: the IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices
  - IEEE P1619.2: Standard for Wide-Block Encryption for Shared Storage Media
  - IEEE P2883: Standard for Sanitising Storage
- IEEE 1667-2018: IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices
- IEEE P2986: Recommended Practice for Privacy and Security for Federated Machine Learning (C/AI)
- IEEE P2994: Standard for Security Assessment Framework for IoT Application Deployments (COM/Mobile)

IEEE 802 standards:

- The IEEE 802.1AE standard defines a Layer 2 security protocol called Medium Access Control Security (MACSec) that provides point-to-point security on ethernet links between nodes for securing wired LANs.
- IEEE 802.11 standard also includes security features: Service Set Identifier (SSID) which is used to control access to an Access Point (AP), the Access Control List (ACL) to prevent unauthorised access, and the Wired Equivalent Privacy (WEP) protocol
- IEEE 802.11bh: Operation with Randomised and Changing MAC Addresses

(LAN/MAN)
- IEEE 802.11bi: Enhanced Service with Data Privacy Protection
- IEEE 802E: Privacy considerations for IEEE 802 Technologies

The IEEE Standards on Blockchain:

- The IEEE has about 30–40 standards focused in the area of Blockchain, some of which are highlighted as part of the energy and healthcare vertical above
- The IEEE Blockchain & Distributed Ledger Standards Committee
    - The IEEE P3200 series of standards are being developed within this committee focusing on identity, interoperability, and security (there are about 10 standards in the IEEE 3200 series)

IEEE Cybersecurity Industry Connections Programs (Pre-Standardisation):

- IC20-021-01: Meta Issues of Cybersecurity
- IC20-011: IoT Ecosystem Security
- Cybersecurity in the era of Agile Cloud Computing
- IEEE SA submits responses to public open consultations or requests, including NIST policy papers

4.5.1. How to engage in standards development at the IEEE

The IEEE Government Engagement Program on Standards (GEPS) is a tailored program for government officials. Through the program, government officials can gain strategic insights into IEEE standardisation and members can contribute to discussions at the intersection of technology, standards and policy. Members receive tailored information and resources including bespoke webinars, and bi-lateral consultations with technical and standards experts.

The GEPS is free join and there are currently 12 African government bodies participating in the program, including the Ministry of Development of the Digital Economy and Posts Burkina Faso, Ministry of Communication, ICT and Media (MINCOTIM) and Telecommunications & ICT Regulatory Authority (ARCT) Burundi, National Telecom Regulatory Authority (NTRA) Egypt, National Communications Authority (NCA) Ghana, Ministry of ICT and Innovation (MINICT) and Rwanda Utilities Regulatory Authority (RURA) Rwanda, Ministry of Digital Economy and Telecommunications Republic of Senegal, Tanzania Communications Regulatory

Authority (TCRA) Tanzania, Uganda Communications Commission (UCC) Uganda and Zambia Information & Communications Technology Authority (ZICTA), Zambia.

Case Study

***Interview**: Leveraging Global Standards in Policy Making: Interviewing an IEEE GEPS Representative, Egypt, Ramy Fathy, National Telecom Regulatory Authority (NTRA)*

To enhance engineers' ability to meet future standardisation requirements, the IEEE Blended Learning (BLP) programme focuses on capacity building. The IEEE BLP offers a comprehensive set of courses on the IoT, EMI/EMC, WiFi, Innovation Management, with the launch of cybersecurity training expected.

4.6. ETSI

The European Telecommunications Standards Institute (ETSI), in addition to CEN and CENELEC, is a European Standards Organisation (ESO) that develops European Standards (ENs).

Through Technical Committees (TCs) and Partnership Projects supported by Working Groups (WG), the ETSI develops security standards in mobile/wireless communications, emergency telecommunications, information technology infrastructure, smart cards, fixed communications, and security algorithms. TC CYBER is working on Technical Reports (TRs) and Guide (EG) for the Protection of personal data and communication, consumer IoT security and privacy, cybersecurity for critical national infrastructures, network security, and cybersecurity tools and guides.

These include TS 103 645: 'cybersecurity in the Internet of Things', TR 103 309: 'Secure by Default adoption – platform security technology', TR 103 331: 'Structured threat information sharing', TR 103 303: 'Protection measures for ICT in the context of Critical Infrastructure', TR 103 304: 'Personally Identifiable Information (PII) Protection in mobile and cloud services' and TR 103 306: 'Global Cyber Security Ecosystem'. The Security for the ICT - the work of ETSI white paper, published annually, gives a brief overview of standards development in various areas including cybersecurity.

4.6.1. How to engage in standards development at the ETSI

There are currently four member organisations from South Africa, Botswana, and Lesotho. The application for ETSI membership requires compliance with the ETSI Directives and decisions taken by the General Assembly.

4.7. ICANN

The Internet Corporation for Assigned Names and Number (ICANN) is an internationally organised, not-for-profit public-benefit corporation, developing and implementing policies for unique identifiers on the internet to keep it secure, stable, and interoperable. Through a bottom-up, consensus driven and multi stakeholder approach, the ICANN develops policies for the management of Internet Protocol (IP) addresses, protocol Identifier assignment, generic (gTLD) and country code (ccTLD) domains and root servers.

The ICANN is working on knowledge-sharing and instantiating norms for the DNS and Naming Security (KINDNS). These guidelines encouraged the adoption of operators on the DNS security best practices. On a regular basis, the ICANN Office of the Chief Technology Officer (OCTO) authors and publishes OCTO Publications to present positions on various topics in relation to internet identifiers.

4.7.1. How to engage in standards development at ICANN

African Regional At-Large Organisation (AFRALO) aims to strengthen end users' participation in ICANN decision and policy-making, formulating technical standards with specific focus on the areas of privacy, transparency, and accountability, taking into account cultural diversity and global public interests. AFRALO currently consists of 68 At-Large Structures (ALSes) located in 32 countries and territories, as well as 16 Individual Members and three Observers.

AFRALO provides members with news, resources, capacity development and information sharing tools for the development of the ICTs, and contributes to policy

activities that influence the technical coordination of the Domain Name Systems. AFRALO and AfriCANN maintains a statements workspace reference to work at various ICANN meetings.

ICANN offers courses and organises webinars to support the building of capacities in policy making and evolution of standards, and to share best practices. In particular, DNS 101 and DNSSEC 101 are recommended for policy makers.

4.8. ENISA

European Union Agency for Cybersecurity (ENISA) contributes to research and development of EU standards for risk management and for the security of electronic products, systems, networks and services, pursuant to Regulation (EU) 526/2013. Reference to the Regulation (EU) 2019/881 (Cybersecurity Act). ENISA also prepares candidate certification schemes with reference to the European cybersecurity certification framework for the ICT products, services, and processes. In addition, ENISA collaborates with ETSI, CEN, CENELEC to produce publications in standardisation and certification.

ENISA has been involved in the development of both formal and de facto standards used in cybersecurity incident management and protection of critical infrastructure which can be adopted for use in African countries.

4.9. 3GPP

The 3rd Generation Partnership Project (3GPP) consists of members or organisational partners from seven telecommunications standard development organisations (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) and the Telecommunication Technology Committee (TTC). The project produces reports and

specifications that define 3GPP technologies in cellular telecommunications technologies, including radio access, core network, and service capabilities.

The 3GPP has produced security specifications in 33 series. The participation at 3GPP meetings is limited to organisational partners. Non-members wishing to participate must seek eligibility through a partner organisation. Membership categories include partners,individual members, the ITU Representatives, observers, and guests.

4.10. De facto standards

De facto standards are adopted, recognised, and widely used by the industry and its customers, and are not officially approved by the SDOs.

There are de facto standards for security teams including Cybersecurity Security Incident Response Teams (CSIRTs) and Product Security Incident Response Teams (PSIRTs). These include:

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

  This standard provides a highly pragmatic and globally accepted set of rules for information sharing. The standard is adopted by TI Accredited teams for all information sharing.

  Resource: Traffic Light Protocol Definitions

TLP:RED = Not for disclosure, restricted to participants only

TLP:AMBER = Limited disclosure, restricted to participants' organisations.

TLP:GREEN = Limited disclosure, restricted to the community.

TLP:WHITE = Disclosure is not limited

- RFC-2350

Using the template or form in this standard, a CSIRT can communicate to its constituents the services it offers, its policy and procedures, and team's expectations of the team of its constituents. Since May 2009, filling out and publishing RFC-2350 is mandatory for TI Accredited teams.

- CSIRT Services Framework

FIRST, with support from the Task Force CSIRT (TF-CSIRT) Community, and the International Telecommunications Union (ITU), maintains the CSIRT Services Framework. The framework provides a comprehensive list of services that the CSIRTs could potentially provide to its constituents.

- Security Incident Management Maturity Model (SIM3)

SIM3 supports the measurement of maturity of an incident response or security team, based on four areas: organisation, human issues, tools, and processes. The model supports the TI Certification framework and is used in self-assessment of teams.

- TI CSIRT Code of Practice (CCoP v2.4)

The code provides guidance on cooperation, legal, informational, and vulnerability handling requirements. The use of the TI CSIRT Code of Practice is recommended, but optional for TI Accredited teams

- eCSIRT.net Incident Taxonomy

The taxonomy provides a classification of security incidents and examples, as well as a description/explanation. Further work is needed to maintain the taxonomy and assist implementers of trouble-ticket-systems or automatic sharing systems to make use of it.

5. Open standards

Rapid technological advancement and intensified time-to-market demands and consumer expectation is driving the industry to adopt more efficient ways to define global standards. A complimentary, market driven model of standards, allowing for innovation, collaboration, and technology excellence is now used in internet standards development by the W3C, the IETF, and the IEEE .

Open Internet standards allow developers to set up new services without requiring permission. These standards give users permission to copy, distribute, and use technology freely or at low cost. Organisations, including government agencies that opt to use open standards, enable digital transformation by allowing interoperability of systems, sustainability by reducing cost, and increasing accessibility to opportunities including the IT contracts.

Resource: UK Government Policy Paper - Open Standards Principles

These principles describe how the UK government will specify and select open standards, and how these standards can be implemented in open source and proprietary software. They support the open data and digital strategies set out in the Government Transformation Strategy 2017-2020 and the UK Digital Strategy.

The selected standards enable software to interoperability through open protocols and data exchange between software and data stores.

The 7 principles for selecting open standards for use in government are:

1. Open standards must meet user needs.
2. Open standards must give suppliers equal access to government contracts.
3. Open standards must support flexibility and change.
4. Open standards must support sustainable cost.
5. Select open standards using well-informed decisions.
6. Select open standards using fair and transparent processes.
7. Specify and implement open standards using fair and transparent processes.

The OpenStand initiative is a movement dedicated to promoting a proven set of principles that establish The Modern Paradigm for Standard endorsed by bodies including the IEEE, the IETF, the Internet Architecture Board (IAB), the World Wide Web Consortium (W3C), and the Internet Society.

Video: The OpenStand Community rallies at the SXSW. Featuring Tim Berners-Lee (W3C), Padmasree Warrior (CISCO), and Dave McAllister (ADOBE).

Figure 4: 5 Core principles for open standards development. Source: [Open-Stand]

5.1.1. Open Cybersecurity Alliance

Open Cybersecurity Alliance works on product interoperability, extending the benefits of integration of cybersecurity products from multiple vendors to the cybersecurity community. The OCA develops and promotes sets of common code, patterns, and practices to enable data interchange between cybersecurity tools over a common, standardised messaging bus within the threat management lifecycle. Interoperability at the communications and data levels ensures that critical insights and findings are not missed, and reduces vendor lock-in.

Resource
Video: Meet the Open Cybersecurity Alliance

5.1.2. OASIS OPEN

The OASIS OPEN mission is to 'advance the fair, transparent development of open source software and open standards through the power of global collaboration and community'. Participation to OASIS is open and its work is supported by annual sponsorship and membership dues.

OASIS Open is a non-profit standards bodiy where individuals, organisations, and governments collaborate to solve technical challenges through the development of open code and open standards. OASIS Open offers projects – including open source projects – a path to standardisation and de jure approval for reference in international policy and procurement.

People and organisations join OASIS to advance projects for cybersecurity, blockchain, IoT, emergency management, cloud computing, legal data exchange, and more.

Examples of Technical Committees (TC) working on cybersecurity standards include:

- Open Command and Control (OpenC2) TC, is *creating a standardised language for the command and control of technologies that provide or support cyber defences.*
- Collaborative Automated Course of Action Operations (CACAO) for Cybersecurity TC is *developing a standard to implement the course of action playbook model for cybersecurity operations.*
- Cyber Threat Intelligence (CTI) TC is *supporting automated information sharing for cybersecurity situational awareness, real-time network defence, and sophisticated threat analysis. The TC is developing and standardising under the OASIS open standards process: STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information), and CybOX (Cyber Observable Expression).*
- Common Security Advisory Framework (CSAF) TC: *Standardising automated disclosure of cybersecurity vulnerability issues*

5.1.3. I am the Calvary

I am the cavalry is a grassroots volunteer organisation 'focused on the intersection of digital security, public safety, and human life' in four areas: medical devices, transportation, connected homes, and infrastructure. Internet of things (IoT) devices are deployed to remotely monitor and carry out other functions in critical infrastructure and therefore the organisation is working to encourage more responsible, adaptive security protections to ensure the infrastructure and public safety.

5.1.4. OpenRAN

Various collaborations of industry players are working on developing security specifications for 5G open Radio Access Networks (RAN).

These include the O-RAN ALLIANCE works on open, intelligent, virtualised, and fully interoperable RAN specifications with membership open to mobile operators, vendors, or research and academic institutions.

Open RAN Policy Coalition is a group of companies that promotes policies that will advance the adoption of open and interoperable solutions in the Radio Access Network (RAN). Through promotion of policies, the coalition supports the application of open interfaces. These policies include the support of open and interoperable wireless technologies, encourage government support of open and interoperable solutions, vendor diversity, and removal of barriers to 5G deployment.

6. Standards implementation and compliance

The testing and implementation of standards is recommended as a means of understanding and engaging in the standards development process.

Good Practice: Create a Standards Awareness Website

The creation of an internet standards awareness website is identified as a good practice. The website would provide a free and public service that raises awareness, use, and deployment of standards. Using simple non-technical language would provide:

- comprehensible supporting documentation on internet standards
- arguments and pitfalls regarding internet standards deployment
- Real time,check for standards, compliance

The Internet.nl is a portal and test tool, and represents a good example of the establishment of a national multistakeholder collaboration to promote security-related internet standards. The portal allows users to test if their website, email, and Internet connection use modern and reliable internet standards.

The ISOC Open Standards Everywhere (OSE) has focused on encouraging web servers administrators and operators to deploy the latest open standards and protocols. The OSE uses the Internet.nl portal to check in websites' support for the modern internet standards including the IPv6, the DNSSEC, the HTTPS, and Security options. The ISOC informs, educates, collaborates, and leads by example to support web server and website administrators with the deployment of the latest open standards.

Good practice: Lead by example

Leading by example is a good practice identified by the GFCE in the use of security-related standards. Governments can lead by example by:

- Implementing security-related and other standards in existing systems and networks and through procurement processes.
- Promoting the use of internet standards and good practices in agencies' infrastructure.
- Ensuring appropriate allocation of resources, including staff and budget, for implementing and configuring the standards.
- Embedding standards requirements for the ICT products in procurement procedures and policies.
- Adopting internet standards in their strategic ICT plans.
- Developing roadmaps outlining tactical and operational implementation activities and stakeholder responsibilities.

Case Study: The ICT Standards in Government

ICT Authority, Kenya broad mandate entails enforcing the ICT standards in government and enhancing the supervision of its electronic communication.

The Authority has published and enforces compliance to standards in Government Enterprise Architecture, Cloud Computing, Data Centre, Electronic Records and Data Management, End-User Equipment, ICT Human Capital & Workforce Development, Information Security, IT Governance, ICT Network, Systems & Applications.

Case Study: The ITU Regional Group for Africa standard implementation

At the last Meeting of the ITU-T SG17 'Security', virtual, 24 August – 3 September 2021, Africa (Kenya, Ghana and Senegal) had two contribution references to Recommendation X.1060 : Framework for the creation and operation of a cyber defence centre (CDC). Those were:

C1098: Implementation of Cybersecurity Defence Centre Framework X.1060: This contribution initiated a request to Q3/17 to draft a Supplement to Recommendation X.1060 in order to assist Member States in implementing the Recommendation. This request should be added to the Q3/17 Work Programme, and if necessary, a New Work Item in this area should be established

C1099: Proposed Survey 'Assessment Cyber Defence Centres in Africa' survey and results arising are expected to enhance the capacity and effectiveness of the CDCs in Africa through the sharing of best practices in the provision of services as well as provide an opportunity for networking and capacity development.

The participation of members of the Regional Group for Africa implementation of the Recommendation resulted in understanding the standardisation process, stakeholder engagement, and the publishing of a questionnaire intended to assess, plan, and enhance cybersecurity services in the CDCs in Africa.

International standards are often adopted by countries or regions to become national or regional standards. Compliance to standards would generally be made mandatory by way of regulations, maintained by a national or regional authority.

The use of standards could be mandatory or voluntary, depending on the regulatory requirements in a country or jurisdiction. Ideally, governments should want entities to voluntarily comply with standards' requirements. It is however recommended that public and private entities with a legal obligation to report security issues implement standards through regulation. The use of standards by these entities would empower them to identify the most appropriate standard and influence subsequent updates to, or proposals for new standards, reducing the risk of sanctions, lawsuits, or arrest for non-compliance.

Good Practice: Provision of economic and regulatory incentives to stimulate the adoption of Internet standards.

Economic and regulatory incentives to stimulate the adoption of internet standards may include:

- Tax reductions to companies introducing IPv6 in South Korea
- Tax deductions on cost of purchasing IPv6 equipment (routers, switches)
- Logos and certifications for IPv6-enabled devices applied in Japan and South Korea
- A subscription fee discount for the DNSSEC signed domains by country codes accredited registrars and registries
    - Internet registries DNSSEC signed domain registration discount campaigns: AFNIC (France), EURid (Europe, .eu registry), NORID (Norway) and the SIDN (The Netherlands).
    - SIDN 'registrar scorecard' programme to stimulate the DNSSEC and the IPv6

Reflection

Governments have a significant role to play in the promotion and the use of standards. Using your country as an example, what economic and policy incentives should the government consider?

7. Certification

Institutional, professional, and product conformity assessment/accreditation/certification offers consumers an independent and impartial confirmation that a product or service complies with, or fulfils the requirements and characteristics described in a standard or published technical specifications. Verification of conformance to requirements that can include performance, safety, efficiency, effectiveness, reliability, durability, or environmental impacts is done through testing or/and inspection.

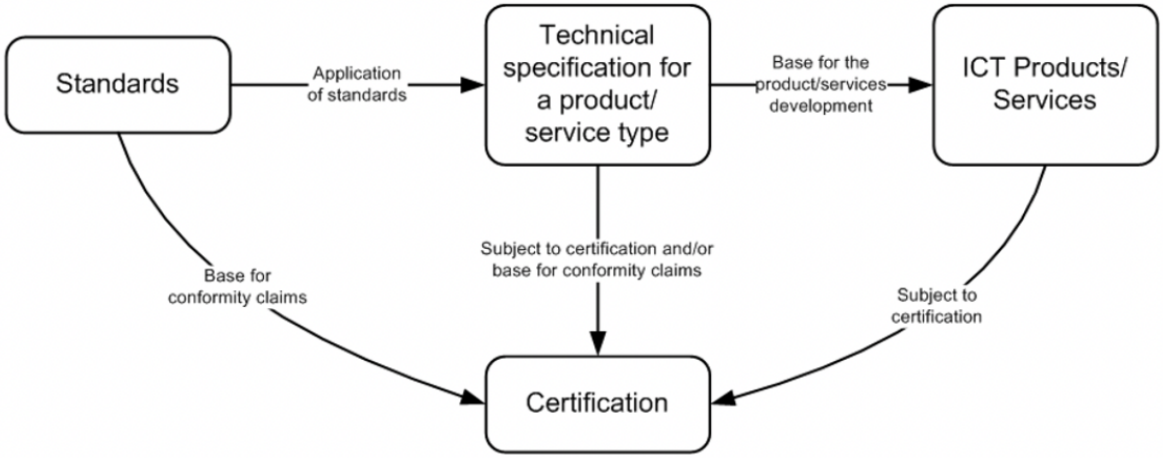


Figure 5: Role of standards in certification *source: ENISA*

The IECEE cyber security certification programme tests and certifies cybersecurity of electrotechnical products and systems in the electrotechnical sphere, based on the applicable IEC Standards. The programme is applicable to any sector with critical infrastructure, including medical, utility, and automotive.

Resources:

The Regulation (EU) 2019/881 (Cybersecurity Act), establishes the European cybersecurity certification framework.

The framework's objective is to ensure an adequate level of cybersecurity for ICT products, services and processes, as well as ensuring consistency in cybersecurity certification schemes in the EU. The cybersecurity certification scheme is a comprehensive set of rules, technical requirements, standards, and procedures that apply to the certification or conformity assessment of specific ICT products, services or processes.

In France, certification is based on evaluations conducted in accordance to ANSSI specifications or standards conducted by Information Technology Security Evaluation Facilities (ITSEF), licensed by the French Prime minister and accredited by the French accreditation committee (COFRAC), according to the standard EN ISO/CEI 17025.

Access to the internet is via consumer devices, and the IEEE Conformity Assessment Program (ICAP) develops and implements programs that couple standard development activities with conformity assessment activities to help accelerate market adoption while

reducing implementation costs. Consumers, manufacturers, service providers, value-added resellers, and businesses expect product reliability, efficiency, security, and interoperability.

Professionals can receive certification by taking courses offered by organisations certified against the ISO/IEC 17024:2021. Certified courses provide the benefits of confidence, mutual recognition, and the global exchange of personnel. The International Information System Security Certification Consortium, Inc. (ISC)2 offers various information security certifications including Certified Information Systems Security Professional (CISSP) for leaders with understanding of cybersecurity strategy and operations. Professional certification can also be obtained through the ISACA and COMPTIA.

In cyber incident management, the CSIRTs participate and maintain a team's accreditation and certification status within the Trusted Introducer (TI) community, which is a prerequisite to membership on international networks such as FIRST.

8. Mapping the stakeholders in security standards development

The establishment of a national multistakeholder cooperation to promote the security-related internet standards is identified by the GFCE as a good practice.

Standards development involving a variety of stakeholders through voluntary-based cooperation of state and non-state actors, increases the level of awareness of internet security standards and supports the creation of an enabling environment and partnerships.

Good Practice: Establish a national multistakeholder cooperation to promote the security-related internet standards.

Voluntary-based cooperation of stakeholders encourages raising mutual awareness for the need to implement internet standards and collaborative learning through sharing of expertise which ultimately contributes to building capacities of participating entities.

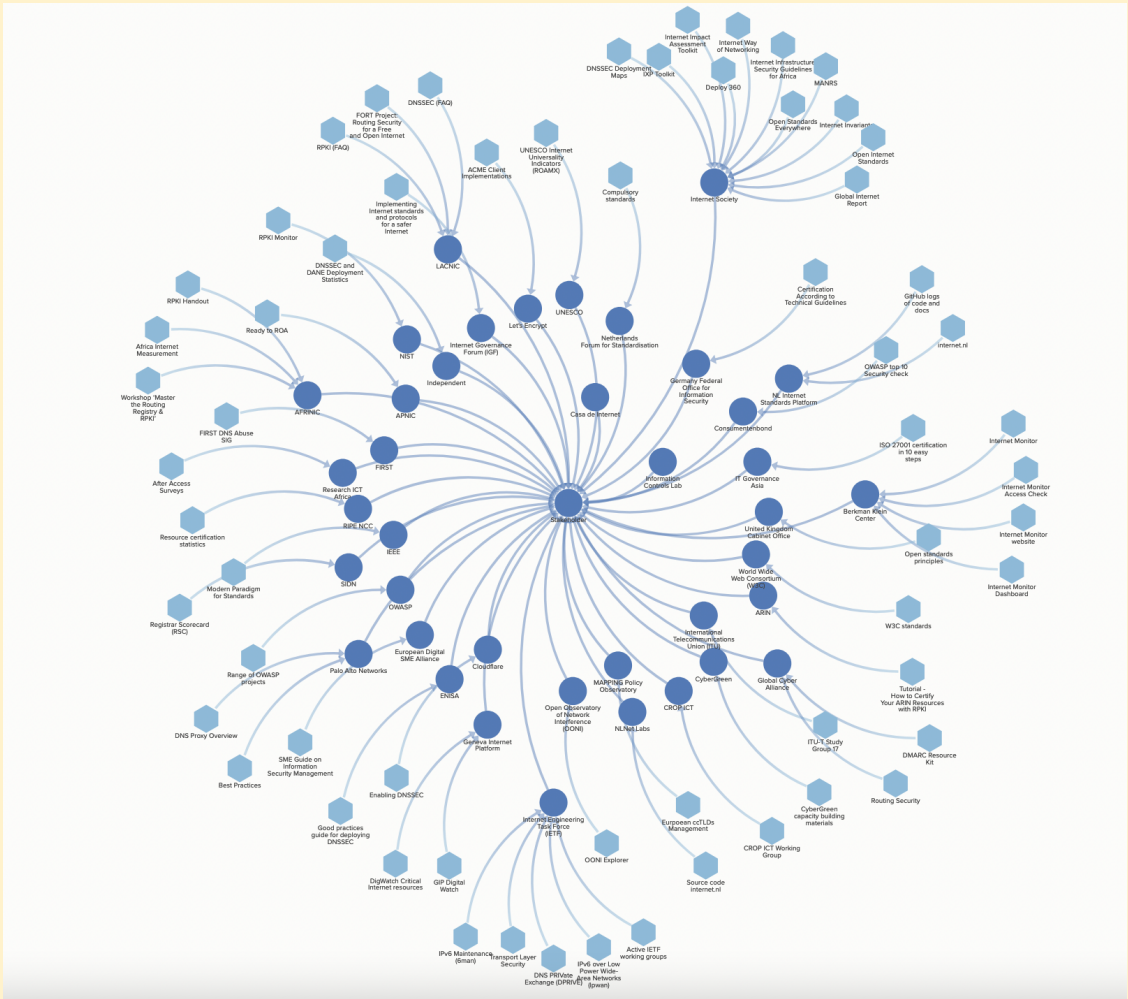
Collaboration among stakeholders has been established in various forms including the IPv6 taskforces to encourage uptake of IPv6 in Algeria, Egypt, Kenya, Mauritius, Nigeria, South Africa, Senegal, Tunisia. In 2012 AfriNIC, the Regional Internet

Registry for Africa, launched the [African IPv6 Taskforce (AF6TF)](#).

Resource: [Infographic](#): Standards stakeholder mapping

Stakeholders are presented as blue circles, whereas initiatives are hexagons.

By clicking on the specific icon you can learn about individual stakeholders and their respective initiatives.



***Source**: DiploFoundation*

Case Study : Multistakeholder participation in standards implementation — Cameroon

Cameroon has a process for identifying where standards are needed, evaluating which standards should be used to address the gaps. and implementing the standards. Through a multistakeholder process, entities (private sector, critical infrastructure, and presumably government organisations) identify and report security issues (or their need to establish a technical standard) to a government agency within the ICT Ministry. The Ministry then passes the issue to a committee consisting of government, private sector, and academic representatives. The committee recommends the application of a particular standard, which the agency approves and then implements through regulation.

Source: GFCE ACE meeting in The Hague

Reflection:

Multistakeholder cooperation at a national level is important to promote the security-related internet standards, taking the example of your country.

- Identify actors in standards development.
- How is stakeholder collaboration implemented?
- What are the challenges?
- What is the timeline for implementation?

9. Capacity building initiatives

9.1. GFCE Internet Infrastructure Initiative - Triple-I

A robust, open, and resilient internet infrastructure is critical to counter infringements and threats. The GFCE Triple-I is a GFCE initiative which, through awareness raising and building on good practice experiences for enhancing justified trust in internet connections and email exchanges, encourages the use of open security-oriented standards.

GFCE Triple-I promotes the use of the following Internet standards:

- **IPv6**: A major extension of the internet address range and enabler of security capabilities
- **DNSSEC**: Security extensions for the internet domain name infrastructure
- **TLS, HTTPS, DANE, and STARTTLS**: Secured connections between internet users and services
- **RPKI, ROA**: Prevents route hijacking and other routing attacks through use of a trust anchor
- **DKIM, SPF, and DMARC**: Anti-phishing and anti-spoofing measures

In addition, GFCE Triple-I workshops bring together stakeholders sharing good practice in the areas of cyber-hygiene (e.g. MANRS), and sharing data on vulnerabilities and abuse (e.g. M3AAWG, Cybergreen, ICANN DAAR).

Each session consists of three parts: sharing of information and education; discussion on priority issues and how to tackle them; and conclusions on actions towards the future, with voluntary commitments of participants to pursue those actions.

9.2. Open Internet Standards for African universities

The Internet Society in 2019 ran a one-month pilot open Internet Standards course on Internet Protocol Security (IPSec) to expose the next generation of African experts to open internet standards and provide lecturers with additional training material to support existing courses at universities. The course brought together 70 students from 4 African universities from DRC, Ethiopia, Kenya, and Ghana.

9.3. International Cybersecurity Challenge

ENISA will host the first International Cybersecurity Challenge, a Cyber World Cup from 14–17 June 2022. Built on the success of the Building Capture-the-flag competitions (CTFs), the International Cybersecurity Challenge will have 9 international teams with players ages 18 to 26 years taking on challenges in web application and system exploitation, cryptography, reverse engineering, hardware challenges, forensic analysis, and attack/defence.

9.4. Hackthon@AIS

The Hackathon@AIS goal is to identify, encourage, and expose engineers from Africa to open Internet Standards development, so that they can contribute to the work at organisations such as the Internet Engineering Task Force (IETF).

The 2019 Hackathon@AIS held in Kampala, Uganda, at the Africa Internet Summit had five tracks:

- *Network Programmability* covered network programmability concepts and components, including the IETF standards such as YANG, NETCONF, and RESTCONF, and tools such as pyang, ncclient, and Postman programming languages.
- *Network Time* covered the ongoing work to secure NTS (Secure Network Time) and the use of the Chrony for synchronisation with the time server.

- *IPv6 covering* IPv6 and IETF IPv6 working groups (6MAN and v6OPS) and a challenge to enable IPv6 in several IPv4 only open source tools.
- *IPWAVE* covered testing and implementation of an Internet-Draft under the IPWAVE working group.
- *Measurement* covered DNS over TLS (DoT) and DNS over HTTPS (DoH) setups and measuring the performance of caching resolvers against locally-setup DoT and DoH servers against publicly available DNS resolvers. Read a report of the experience of the track from Willem Toorop, a facilitator from NLnet Labs. The track contributed an update to the IPWAVE Working Group at the IETF.

10. Women in Standardisation

To encourage the participation of women in standards making, the SDOs have various programmes and initiatives. These include the ITU Women in Standardisation Expert Group (WISE) established in 2016. Pursuant to the provisions of Resolution 55 – Promoting gender equality in ITU Telecommunication Standardisation Sector activities, the group aims to encourage active participation of women in the standardisation sector of the ITU (ITU-T) activities, leadership roles and the inclusion of gender perspectives in the ITU-T work. One can participate in the WISE mentorship program that seeks to promote active participation, contribution, and leadership of women in all aspects of ITU-T activities and processes.

IEEE Women in Engineering, is a global network that connects women in technology. The goal of the community is to facilitate the recruitment and retention of women in technical disciplines globally. Membership to the IEEE WIE is offered to the IEEE members, with opportunities to inspire women in leadership. WIE Affinity Group offer opportunities to network and are currently available in Egypt, Kenya, Morocco, Namibia, South Africa, Tunisia and Uganda.

11. The (Geo)Politics of standardisation

Standards support innovation, economic growth, competitiveness, facilitate international trade and help protect consumer rights, safeguard critical infrastructures, and national security. As standards have far-reaching socio-economic and (geo)political implications impacting the balance of power between competing businesses and/or national interests, they should be considered when drawing up national policy objectives.

Resource:

Video: Digital standards, China, and geopolitics: What is at stake?

China has recently shown increased participation in standard developing organisations (SDOs), which can be understood as a natural consequence of the country's rapid technological development, and an indication that Chinese actors prefer to engage in organisations that underpin international order.

On the one hand, there is hope that Chinese involvement may strengthen the adoption of international standards within China. On the other hand, there are growing concerns that China's increased participation may be guided by goals of national political and economic projection – of the state and its private actors – that would trump goals of technical efficiency.

Two specific proposals put forward by Chinese actors at the International Telecommunication Union (ITU) that have attracted significant media attention will be covered in our discussion: a proposal for ITU-T to take up work on designing a new protocol (the 'New IP' proposal) and a proposal for standardising facial recognition systems in visual surveillance.

On 2 February 2022, the European Commission launched the EU Strategy on Standardization - Setting global standards in support of a resilient, green and digital EU single market. The Strategy aims to strengthen the EU's global competitiveness, to enable a resilient, green and digital economy, and to enshrine democratic values in

technology applications.

> *'Technical standards are of strategic importance. Europe's technological sovereignty, ability to reduce dependencies and protection of EU values will rely on our ability to be a global standard-setter'* (Thierry Breton, Commissioner for the Internal Market).

The strategy has five key sets of actions: anticipate, prioritise and address standardisation needs in the strategic areas, improve the governance and integrity of the European standardisation system, enhance European leadership in global standards, support innovation, and enable the next generation of standardisation experts.

The strategy is seen as a response to the European Union Chamber of Commerce in China (European Chamber) report The Shape of Things to Come: The Race to Control Technical Standardisation, published in December 2021. The report identifies technical standard setting as a battleground on which states are fighting to gain dominance in strategic technologies, such as 5G, artificial intelligence, and new electric vehicles.

12. Main takeaways

Security standard, like any other standard, is a technical specification or criteria designed to be used consistently, as a rule, a guideline, or a definition. Standards are developed through a consensus-building process at international, regional or national organisations.

In this module, we have explored various standards developing organisations, the cybersecurity standards they have developed, and opportunities for engagement. Recognising that developing countries are not sufficiently represented in the standards development process, there has been an effort to bridge the gap, through various initiatives. These initiatives, including the African Standardization Strategy and Roadmap for the Fourth Industrial Revolution, seek to promote harmonisation of standards to enhance competitiveness of the African Continental Free Trade Area (AfCFTA). A country's commitment to participate in the development of international cybersecurity standards should be articulated in its national cybersecurity strategy to ensure that experts and resources are dedicated to the process.

Reflection: Important Points

Write down five points that are important to you and are not included in this module.