GFCE Triple-I Workshop @GC3B2023, 28 November 2023, Accra, Ghana

Report by Daniel Nanghaka and Maarten Botterman

Summary

On Tuesday 28 November 2023, during the GFCE Annual Gathering prior to the GC3B Global Conference on Cyber Capacity Building, the 3rd African GFCE Triple-I workshop took place. This workshop was supported by GFCE, ICANN, Internet Society, EasyDMARC, Global Cyber Alliance, and IS3 Coalition. . Aim of the workshop was to look for ways forward towards more trusted use of Internet and email in regions throughout Africa, building on the results of the previous workshop in Kampala, Uganda, hosted by AIS (2019). Participants in this workshop included global and regional experts, and regional Internet stakeholder groups, including government, business and technical community representatives, who all contributed in finding solutions to strengthen an open end-to-end Internet.

The Workshop started with opening remarks by Dr. Moctar Yedaly (GC3B Special Envoy) and Prof. Dr. Nii Quaynor. *Mr. Nii Quaynor* called for active participation, and emphasized the importance of continued joint action across the African continent. He encouraged the participants to work together on development and implementation of new actions to improve trust in the Internet in the region. We need to have the experts, so we need to leverage the existing organizations that already exist today. Cryptography is one of those skills that we will need importantly towards the future. And the experts need to be local – they need to connect the world's best knowledge to local needs. *Moctar Yedaly* called for a global adoption of the standards and highlighted the disruption in the standards which has been caused by segmentation and geopolitics. He highlighted that the number of users is increasing, and that the Internet infrastructure is rapidly developing. He warns that users get confronted with vulnerabilities, once online. Taking appropriate measures to reduce those risks is crucial. Adopting specific modern Internet standards is key. Moctar expressed his worry that some providers are excluded by some superpowers when it comes to the development of superconductors. Excluding global players results in development of other standards that are not necessarily interoperable – this is not what we want: we want "One Internet" for the world. He called for avoiding fragmentation, and called for adopting common standards, that are interoperable.

Maarten started with highlighting the World Economic Forum Global risk report 2022 with the compelling risks relating to cybersecurity – noting that cybersecurity failure is seen as an important threat for the coming decade. Whereas "Internet access" may be the main challenge in many regions throughout Africa, it is

important to recognize that, as soon as someone gets online, that person is confronted with a sophisticated user base including both good faith and bad faith actors. It was noted that GFCE partners with regional stakeholders and has been setting up a number of Capacity building events with this workshop being the third in Africa.

The main Purpose of the day was to derive ways to improve the justified trust in using the Internet and email in the region. There is a need to conduct an evaluation of the Internet and decision making in the internet ecosystem through proper assessment of the trends in Internet growth in Africa and through constant planning and mitigation of risk related to the Cyberspace. The nature of the space requires collaboration and cooperation working together to create a bigger space.

Maarten Botterman explained the organization of the day, basically build up in three blocks: Block I aimed at awareness raising on a number of Open Standards, and how their deployment can help enhance justified trust; Block II seeking to inspire by sharing of excellent practices building on this; and, finally, Block III action planning – insight and inspiration is great, but in the end it is all about getting things done!

Block I: Better Use of Today's Open Internet Standards

The first Block was moderated Alain Aina, and laid the foundation for understanding the current landscape of Open Internet Standards, their practical implications, and the collaborative efforts required to enhance their implementation in Africa. The interactive format allowed participants to contribute to the dialogue, fostering a shared understanding of the challenges and opportunities in this critical aspect of internet governance.

The workshop commenced with a focused session on the exploration and assessment of Open Internet Standards. The moderator explained that an "open standard" is one that is openly accessible and usable by anyone. Next to the global work on Open Standards via institutions like IETF, IEEE, ISO and ITU, standard development also takes place in national institutions etc. The session aimed to discuss the use and relevance of key open standards crucial for a robust and secure internet infrastructure. The following standards were addressed:

These standards are all "open" and adhere to the five principles as published by IEEE, IETF, IAB, ISOC and W3C:

- Cooperation
- Adherence to principles:
    - Due process
    - Broad consensus
    - Transparency

    - Balance
    - Openness
- Collective empowerment
- Availability:
    - royalty-free to fair, reasonable, and non-discriminatory terms (FRAND).
- Voluntary adoption

Decisions are made with equity and fairness among participants. No one party dominates or guides standards development. Standards processes are transparent, and opportunities exist to appeal decisions. Processes for periodic standards review and updating are well defined, and allow for all views to be considered and addressed, such that agreement can be found across a range of interests.

The Global Forum for Cyber Expertise recommends priority adoption for the following standards:

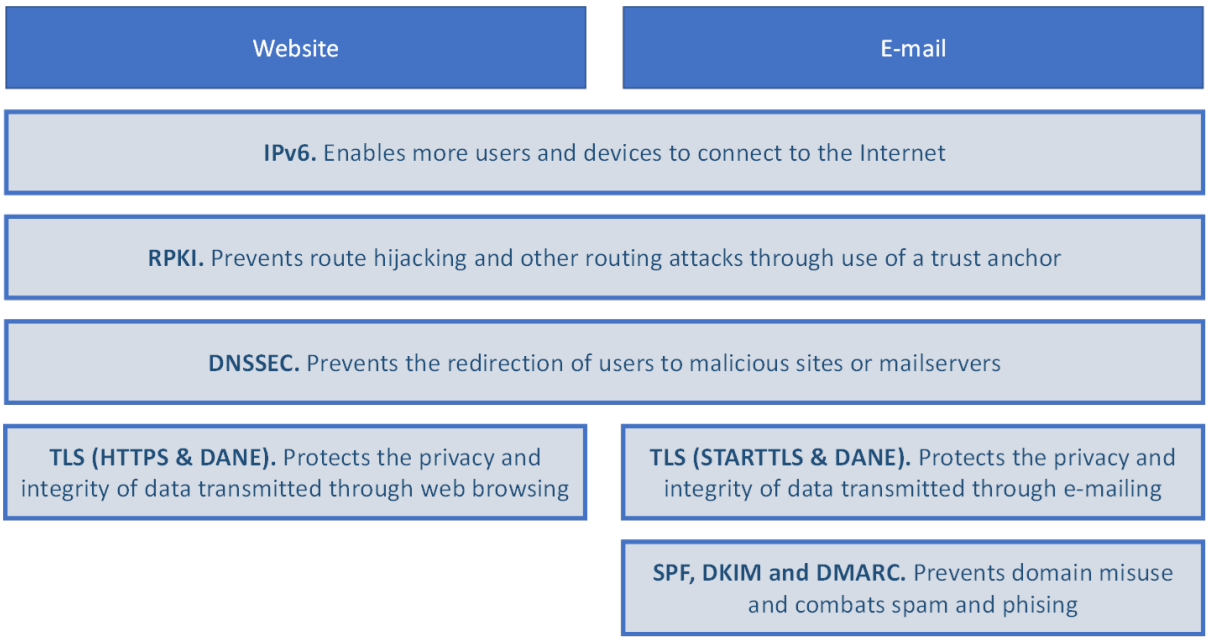

Fig. 1 – GFCE recommended Open Internet Standards (see GFCE Handbook)

These Standards organizations provide advance public notice of proposed standards development activities, the scope of work to be undertaken, and conditions for participation, and maintain easily accessible records of decisions and the materials used in reaching those decisions are provided.

Public comment periods are provided before final standards approval and adoption. Standards activities are not exclusively dominated by any particular person, company or interest group, and standards processes are open to all interested and informed parties.

These Open Standards are foundational to the global Internet as we know it, today, and the voluntary processes lead to standards that are inherently interoperable.

DNSSEC, TLS and DANE

Yazid Akanho from ICANN led the discussion on the practical implementation and significance of DNSSEC, DANE, and TLS in securing the Domain Name System (DNS) and ensuring data integrity during transmission. For its best functioning, it requires Registry operators and Registrants to sign their domain. This should be facilitated by Registrars and DNS hosting providers. And DNS Operators, Internet Service Providers, mobile operators, hosting providers etc. should activate DNSSEC validation for signed domains. Signing and validation complement each other in this. A DNSSEC deployment checklist of adjustable action items that aims to simplify your journey into DNSSEC deployment can be found in the DNSSEC Deployment Guidebook.

Global deployment of DNSSEC validation is just over 30% according to the APNIC Labs statistics.

Transport Layer Security (TLS) is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet by ensuring authentication, confidentiality and integrity, allowing client/server applications to communicate over the Internet in a secure way (prevent eavesdropping, tampering, and message forgery), using digital certificates signed by a third party (Certificate Authority).

In combination with DNS-based Authentication of Named Entities (DANE: a protocol that helps authenticate the identity of internet endpoints using the DNS infrastructure protected by DNSSEC) users will have the best assurances for integrity of data and end points.

ICANN support on DNS and DNSSEC capacity development and much more : reach out to TE or GSE teams, download the Guidebook, or check out the KINDNS program that is set up to promote best practices for DNS operators.

In the discussion Abdul-Hakeem Ajijola brought up that it is important not only to focus on the problems, but also the opportunities – what would inspire young Africans to truly commit to this? He also raised the importance to accelerate adoption of IPv6 and called l for African governments to insist by default on any infrastructures they invest in to demand inclusion of modern Internet standards.

RPKI and ROA

Amreesh Phokeer from ISOC provided insights into the Resource Public Key Infrastructure (RPKI) and Route Origin Authorization (ROA) standards, emphasizing their role in securing the internet's routing infrastructure. Routing is originally based on trust – and trust is less obvious with many more players and higher stakes. It has become a very common thing for routes to get highjacked. The routing protocol as such is very fragile and security needs to be built in.

RPKI allows the legitimate holder of an IP prefix to publish an authoritative statement about which Autonomous System is authorized to originate their prefixes in the Border Gateway Protocol. Network operators around the world can use the collection of these statements to filter unauthorized route origins. It complements the DNS protection by DNSSEC (signing the domain, and securing the DNS resolution – transition from Names to Numbers), by protecting the integrity of the routing (originator and path) as well.

Currently, Route Origin Validation takes place for about 25% according to APNIC Labs statistics. All Regional Internet Registries actively support further implementation, and information can also be obtained via MANRS.

DMARC, DKIM, SPF

Gerasim Hovhannesyan from EasyDMARC delved into the importance of DMARC (Domain-based Message Authentication, Reporting, and Conformance), DKIM (DomainKeys Identified Mail), and SPF (Sender Policy Framework) in email authentication and protection against phishing attacks. Spoofing (pretending someone else is the sender) is possible without the proper precautions. The two big changes in 2023 are:

1- Detecting Phishing emails has become much more challenging due to the use of AI;
2- Volume and target areas of phishing attacks have dramatically increased.

Of all successful attacks, 93% would have been avoided when proper email security would have been applied. It is crucial to establish mechanisms to verify the authenticity of the sender, and the integrity of the message. The standards mentioned above, together, handle this to a high extend. SPF allows domain owners to specify which mail servers are authorized to send emails on their behalf. DKIM adds a signature to very that the content has not been altered and that the message was indeed sent by the claimed sender. And DMARC builds on SPF and DKIM to provide additional protection and reporting by enabling domain owners to specify how their emails should be handled if they fail SPF and/or DKIM checks. DMARC makes email really safe, and once you start monitoring implementation is relatively easy.

As with DNSSEC and RPKI, much is to be done, but thanks to the uptake of these standards by governments, industry giants, and awareness and incentive programs, the adoption rate is accelerating.

Where are we today in adopting the standards in Africa

Daniel Nanghaka presented an overview of "current state of art" in adoption of modern Internet standards in Africa, based on a test using the internet.nl tool (with kind support of the internet.nl team). In order to have a peek of where we stand in Africa, we built a list of websites consisting of government websites and top 10 use websites throughout Africa. SO – it is an impression of the adoption – not necessarily an authoritative percentage.

GFCE TRIPLE - I

We came to the following percentages:

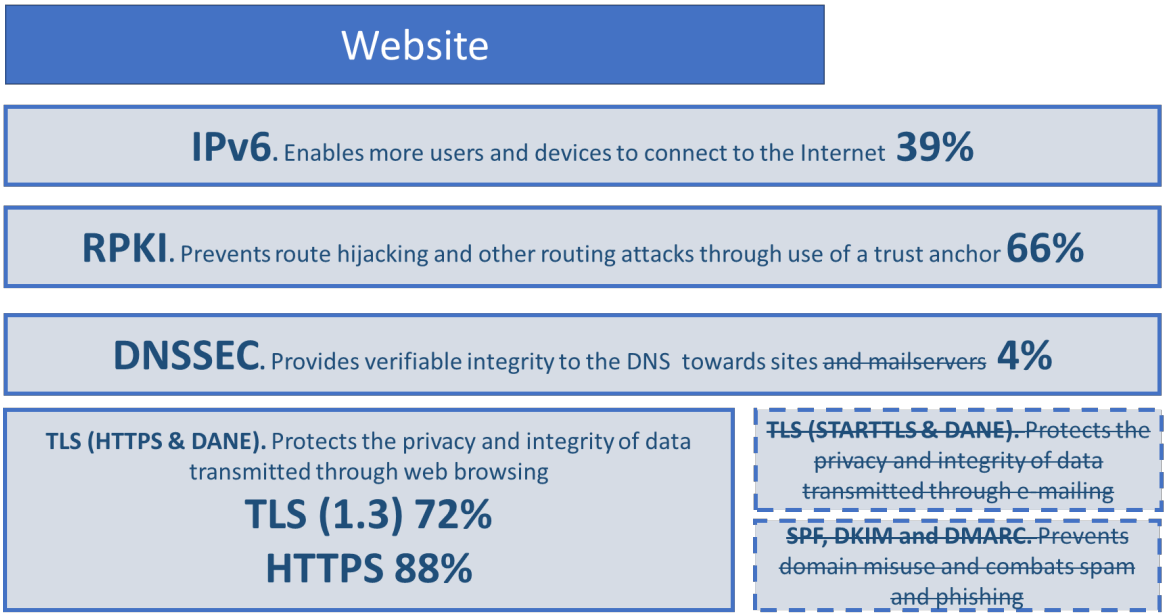

Fig. 2 Current state of uptake of modern Internet standards of the basket of African websites (measured Sep 2023 using the Internet.nl tool)

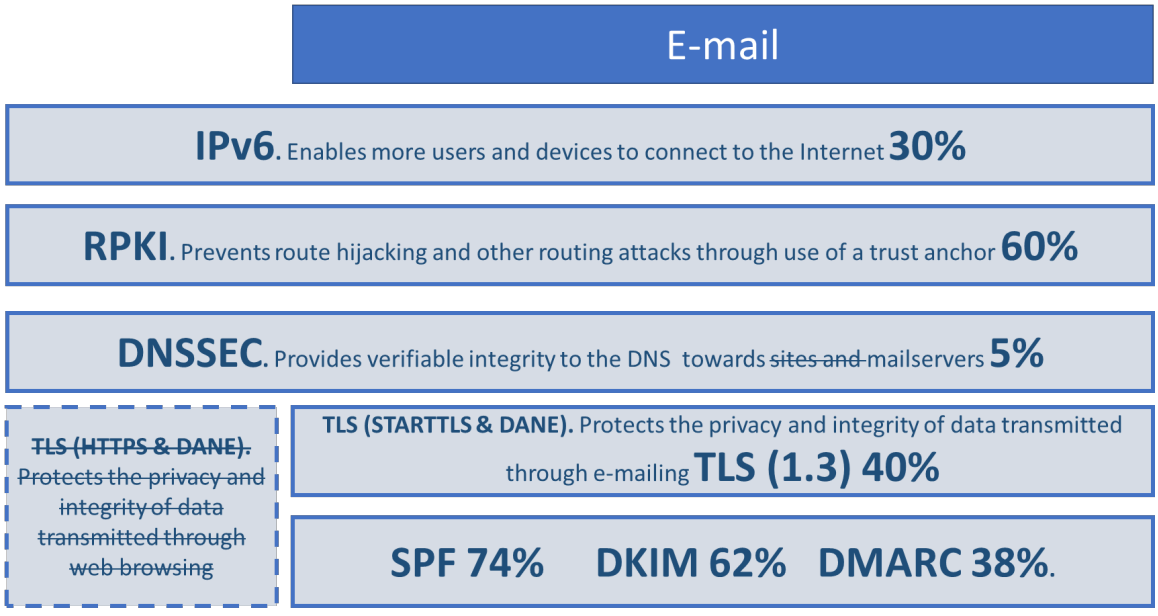

Fig. 3 Current state of uptake of modern Internet standards of the basket of African website mail servers (measured Sep 2023 using the Internet.nl tool)

Overall, it is clear there is a need to do better. Please note that some countries are more advanced in take-up than others. We believe that these numbers give a good impression, and can be used to focus attention on priority.

It was also stated that it is crucial that governments and regulators get on board to progress the most needed standards.

It was also noted that the discussion has been going on for some time and some progress has been made since, but we still lag behind. If we want to step up in the Digital Economy – we need to step up. Governments need to take a leading role and build digital skills in our new generation is key for the future.

It is clear that if governments don't understand the importance, they will not lead the investment in the internet infrastructure and cyber security.

Daniel Nanghaka said that governments have a duty to help create the space that is safe, and that society stands ready for the future. In Block III we will focus on key actions that result as priority from our discussions.

Maarten Botterman concluded with an example on how within the Netherlands the government has "bought in" to the need to adopt modern Internet standards, and adopted the obligation to government agencies to "comply or explain". And the government asked an independent platform to measure progress of adoption at regular times. Maybe a useful model for others. Key is acting together.

A challenge is lack of effective collaboration between policy makers, private operators and regulators. Business considerations shift priority based on the evolution of the markets and business models: the question raises: how do build an effective collaboration on security best practices – and how to best progress adoption of modern Internet standards, together?

Block II: Inspiration from Good Practice Actions

The focus in this Block is on practices that may help increase justified trust in the use of the Internet in the region. Next to "indicators" for progress, we will also look at globally supported processes and practical tools that may have relevance and deserve furthering. This session was moderated by Olaf Kolkman (ISOC and GFCE Board Member) and aims at inspiring practices towards developing digital resiliency in our own environment – not what we *must* do, but what we *could* do.

Amreesh Phokeer presented the Internet Resilience Index (IRI), an indicator derived from key pillars assessing a country's Internet resilience. These pillars include Infrastructure, Performance, Enabling Technologies and Security, and Local Ecosystem and Market Readiness. Amreesh highlighted the significance of data collection from over 30 different indicators, including routing hygiene. He emphasized that country rankings can be accessed through the portal pulse.internetsociety.org.

With regards to Africa, he emphasized that there is considerable progress in Internet connectivity Internet access, overall, has grown from less that 10% in 2010 to more than 33% today, very much varying from above 80% in some

countries to less than 10% in others. Yet a common recurrent problem is that "the Internet is not reliable". Consequently, building a digital society is very difficult to build – as reliable Internet access is key.

Key factors are lack of security (routing security etc.) and lack of technical capacity, lack of Internet redundancy, IXP, encryption etc. In order to assist policy makers, tech engineers and Internet users in making better decisions, AFRINIC & ISOC collaborated to Measure Internet Resilience in Africa (MIRA in short).

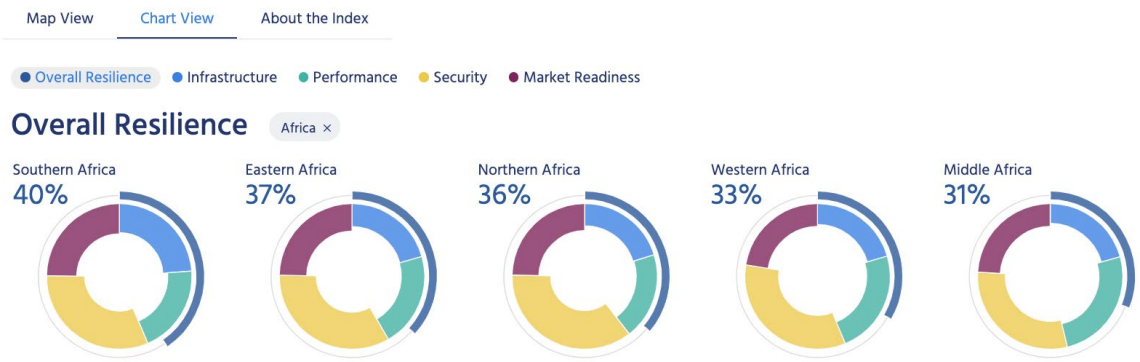

Fig.4 Overall resilience in Africa according to ISOC Pulse measurements

This resource, available freely to all, can be used by policy and decision makers to better understand local and regional differences regarding various aspect, so that targeted improvement plans can be set up. Those advocating and lobbying for more investment and targeted improvements can get a better understanding of the real "pain points" – as well as in which countries these pain points are apparently successful addressed.

Aftab Siddique emphasized the need not to overlook core components of the internet ecosystem. He highlighted the vulnerabilities associated with the Honor system, particularly the BGP flaw, which could lead to prolonged internet outages. Aftab highlighted that every cause requires MANRS which plays an important role in improving internet security: not only at physical security, but specifically at network security level. Routing security is part of network security. Ensuring the confidentiality, integrity, and availability of data as it traverses the network is essential. This includes measures like firewalls, intrusion detection systems, and VPNs.

The Internet ecosystem is rapidly evolving, new technologies, standards, protocols, platforms, and services constantly emerging. It can be challenging to develop and enforce laws and regulations that keep up with the changing nature of the Internet.

Norms are more flexible and adaptable as compared to laws, which can be rigid and slow to change. As the Internet industry evolves, norms can adapt to new technologies and practices more quickly. They are often developed collaboratively by stakeholders in the Internet industry.

We firmly believe that the Internet industry is better governed by norms rather than laws. So what are we doing:

- Building a Community of Responsible Network Operators: One of MANRS's core strengths is its ability to bring together network operators, IXPs, and other stakeholders who are committed to improving the Internet's routing security. This community-driven approach fosters collaboration and shared responsibility.
- Setting a Standard for Routing Security: By defining clear and actionable steps for network operators, MANRS provides a benchmark for routing security. Networks that adhere to MANRS are recognized for their commitment to a safer internet.
- Driving Policy : The principles and actions advocated by MANRS can influence policy makers and regulators, leading to more robust and security-focused internet governance.

The community working with MANRS is growing hand over hand. See https://observatory.manrs.org.

The moderator, Olaf Kolkman, explained that MANRS, focused at routing, is nowadays very well complemented by KINDNS, focus on the Domain Name System.

Yazid Akanho from ICANN OCTO presented the ICANN initiative KINDNS (Knowledge Sharing and Instantiating Norms for DNS and Naming Security), emphasizing the importance of configuration in providing internet services and how this program would help to do so in the best possible way. He called for increased collaboration among operators to enhance internet resilience, as well as security of the infrastructure. KINDNS is a simple framework that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices that the industry identifies for better security and more effective DNS operations. Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices:

- self-assessment is anonymous
- reports can be downloaded directly from the web site

Participants in the KINDNS initiative become a community of operators voluntarily committing to implement/adhere to agreed practices. They also become goodwill ambassadors and promote best practices – as the wider spread the best practices, the healthier the Internet.

ICANN is in the process of promoting this in multiple languages, and continues to improve the tools, based on interaction experience with those that participate and contribute. Workshops and webinars are organized to further raise awareness on KINDNS practices as part of ICANN’s overall DNS ecosystem

security awareness program. All operators are encouraged to sign up, follow the practices and contribute to the continuous improvement of the platform.

Pierre Dandjinou, the ICANN Vice President of GSE for Africa, discussed the Coalition for Digital Africa. The Coalition for Digital Africa is an initiative that aims to bring together stakeholders to expand the Internet in Africa. It promotes innovation and encourages entrepreneurial efforts aimed at strengthening Internet infrastructure to support the development of Africa's digital economy.

Pierre touched upon meaningful connectivity, language accessibility issues, and the need to build capacity to manage the internet ecosystem in Africa, recognizing its diversity. With the partners, including the ITU, AFNOG, AFTLD, Association of African Universities (AAU), ISOC, Network Startup Resource Center (NSRC), ATU, AfricaCERT, AFNIC, ICANN, LusNIC and Smart Africa, a number of initiatives are currently undertaken relating to improving the DNS Infrastructure, for instance by installing more instances from the ICANN managed root server (IMRS), as recently done in Kenya and Cario, providing meaningful connectivity for universities through universal acceptance and different scripts, and capacity development for ccTLDs. Pierre highlighted the establishment of route server instances in Kenya and Egypt, and the support by ICANN and ISOC for the creation of additional IXPs in Africa, so that traffic can reside in Africa.

The end goal is, ultimately, to ensure that the Internet continues to grow safely in Africa, in a stable manner, to bring communities, cultures, and economies together, and all Members of the Coalition agree to these guiding principles:

- *Keeping the Internet open, interoperable, and secure* - The power of the Internet comes from being a single, open and interoperable Internet that is easily accessible globally and locally, to anybody, anywhere, at any time.
- *Creating the building blocks for meaningful connectivity* - Enabling full use of the benefits of the Internet and easing barriers to help ensure that people who are already connected, and will be connected, can communicate over the Internet and access local content in their preferred languages and scripts. This provides populations with access to information and knowledge, and enables cultural and linguistic diversity.
- *Fully participating in multistakeholder Internet policy development* - Working together in an ecosystem based on voluntary participation, best practices, cooperation, and trust, the multistakeholder model engages stakeholders from different backgrounds, functions, and geographies. This ensures that the engineers, policymakers, and others who need to be involved, are at the table, developing workable policies, so that as the Internet grows, it remains open, secure and interoperable.
- *Capacity development at the individual and institutional levels to provide specialized skills and education* - Sharing expertise in the technical functioning of the Internet, the security of the Domain Name System

(DNS), the policy and operational aspects of the country code top-level domains, as well as the routing system, with relevant stakeholders in Africa helps to ensure the continuation of a stable, secure, and resilient Internet. Currently, the number of domains from African ccTLDs is very limited (with the exception of South Africa). Investing in capacity development is an investment that will lead to dividends in the enormous economic potential of the continent.

If you are ready to participate – contact ICANN or go to the KINDNS website and sign up. We can get a lot done, together.

The above contributions were about resilience of the Internet, and improvement of that. Now the attention switches to "security for users". Brian will talk about tools that can help end users to be more secure.

Brian Cute presented on the Global Cyber Alliance an organization with the mission to create and equip communities to deliver a more trustworthy Internet for all through community building, creation of concrete solutions, and measuring of the effect. GCE is very happy to work with ISOC on growing the MANRS community and impact. It is one of the things GCA does.

Another project line is developing toolkits for basic cyber-hygiene journeys. These cybersecurity toolkits for end-users, includes one focusing on SMEs (but there are also toolkits specifically developed for journalists, elections, etc.). These toolkits only work when they get in the hands of end users, and they are designed to be easily deployable. GCA works with partners all over the world to facilitate awareness and training events, including in Africa, and Ghana itself. The outreach activities of globally useable toolkits are brought with collaborating stakeholders to regions targeted to the needs of the region. What we learned is that, in order to create sustainable impact, the critical aspect is localization and contextualization of the tools to the region itself. Without adaption to local circumstances and culture, the tools are not as useable. And any project of deployment needs to be complemented with a feedback loop – "how does this work out for you?".

This feedback loop is crucial to improve cyber hygiene awareness, as well as the toolkits we continue to improve and the way we go about to raise awareness together with local partners.

The moderator explicitly recognized this point – the importance of creating feedback loops – both to create communities and to continue to improve the approach.

Wout de Natris discussed the Internet Governance Forum (IGF) Dynamic Coalition and highlighted the IS3C report and procurement challenges. Furthermore, it was noted that most countries do not procure ICT security by design and the Internet Standards are not recognized by Governments. The public core of the Internet remains unprotected and the Standards are not taught in tertiary education. Most countries have no documents especially the

global South. When focusing on IoT Security, research showed that, currently, countries draw up IoT documents in isolation. Consequently, there are differences in focus and taxonomy. And so far most documents provide guidance without demanding accountability. In the documents, there is generally little emphasis on current global modern Internet standards that matter. Governments committed to "protecting the core of the Internet" are often more aware of the hardware and cables than the software, and the modern Internet standards that are key to enhance resilience and security.

Governments themselves could lead by "informed procurement", i.e. procure explicitly for ICT that is secure by design: but that is only happening in a limited number of countries today. There is a number of initiatives that are happy to help make things happen with regards to agreeing on standards to be deployed, training decision makes and procurement departments, close the tertiary education gap and active the necessary pressure points (like responsible disclosure) to get this done outlined next steps, including the creation of a Cyber Security Hub, capacity building, and seeking cooperation with the GFCE and partners.

Following this presentation, the moderator Olaf Kolkman invited further questions from the audience.

A representative from JPCERT asked about the interdependencies between infrastructures of different countries. Olaf responded that the data scores are "indications" and always should be considered in context. For MANRS there is heavy weights for routing security – so hence relatively heigh scores for specific regional hubs are "logical". After that he invited Maarten for his take-aways.

Maarten responded that it had become even more clear how important the local context is – and that there is co-dependence between different local situations. It is also clear that there is even more excellent information on the state of the Internet that will help us understand where we should put our efforts. Some of the remarks related to: how to stimulate faster implementation of IPv6; how to further simplify adoption of modern Internet standards and good practices; what role for government to help increase resilience; how to improve awareness and knowledge, etc.

Maarten than reminded to the take-aways from the previous GFCE Triple-I workshop in Kampala, 2019, that had the following key take-aways:

(1) Measuring current state (ISOC IRI, internet.nl, MANRS, KINDNS, etc.)
(2) DDOS mitigation through collaboration
(3) IoT security
(4) More capacity building workshops

It was recognized to be key to do so in a local and regional context. One practical action point would be to set up a measuring platform like internet.nl for Africa. Another one was to set up collaboration platforms for specific objectives. Capacity building workshops were seen as key, and necessary.

Understanding where weaknesses in the routing and DNS exit, and where abuse takes place is key knowledge for effectively addressing this. It requires reliable data from reliable sources. Global sources can play an important role in that, yet it requires local "capacity" and action.

Block III: Planning for a more Trusted Internet

Following the introductions about open internet standards that can help enhance justified trust in use of the Internet and email (Block I) and the examples of good practice provided (Block II) the day was summarized with a focus on answering the question:

> *"What to do, together, to improve justified trust in using the Internet and email in the region"*

First, Martin Koyabe walked members through GFCE Capacity Building activities in Africa, emphasizing the need for collaboration among cyber experts. He mentioned that current discussions included the development of modules to enhance capacity building, the global position of Africa in cyberspace, and the implementation of the Malabo Convention. This work is very much done in partnership with others, including African Union. Focus is on strategy for enhancing and sustaining expertise in Africa, on coordination of cyber capacity building across Africa, on setting up and maintaining an institutional memory (knowledge modules), and on ensuring resilience, once build, is maintained also looking towards new developments that will also affect the digital economy on the African continent.

It has become clear that, next to the individual states of resilience, cross-border aspects should also be in scope. A digital economy needs to be built on secure foundations, and as the digital economy goes across borders, by definition, consulted efforts will be needed to take the necessary steps, together.

Lufuno Tschikalange raised the following point: before policy is to be formed there is a need for consultation on the ground – bottom up. Currently there is a lot of work in silos. We see that political will is in practice the last step. First the private sector are the ones that create the policy on security. They seldom ask governments what to do, but act to serve their clients, and often governments follow. Cybersecurity standards for small businesses is an issue – often not able to keep up to speed. The Telcos have a mandate to operate within a certain

framework but what do they do to the small business supplying. Robust use of critical information infrastructure is key.

Lufuno emphasized that for her two keywords came up: priority setting. Africa is very diverse – what is implemented in one country is not always accepted in another. And political will varies as well. Setting the agenda is more important than the program itself. It is key to consider the different circumstances in different regions.

Piere: political will is important. We need to find a way that we communicate with decision makers. Technically we can do a lot. Governments need to come in on security, and investment priorities. How can we help governments best to understand what to decide – depending on the different "state of the Internet" in different countries. And how can we ensure all stakeholders will join in to make things happen – a multistakeholder approach.

The following topics came up during the day as possible actions to pick up specifically in the region, at this point in time, in order to progress trust in the use of Internet and email in the region:

1- We need data/measurements – and will make sure we get this well organized. Clear identification of accessible sources of use, and, when possible – measuring through an online testing platform like internet.nl;
2- We need "access to knowledge" and institutional memory and curriculum building that is of value to us in the African regions;
3- We have clearly heard that a more focused action plan will need to be developed for the different regions, with the local actors in those regions as well as pan-African and global Internet organizations.
4- All this with a focus on the mission: to ensure "enhancing justified trust in the use of the Internet and email in the region". Some of it will be easy, other actions may require a more firm commitment and/or investment. All will require getting the right stakeholders around the table.

As I see it there are only two conditions for being one of those stakeholders: (a) you care about this mission; and (b) you are willing to contribute in good faith, at your best ability. Together, we can get so much done!

Triple-I meeting ended with some thoughts on an Africa Action Plan to enhance Capacity Building and Cybersecurity Resilience in Africa. In summary, the following points came forward to be considered:

- **Capacity Building**
  - Module Development: Participants emphasized the need to develop modules for capacity building in cybersecurity. These modules

could cover various aspects, including emerging technologies, such as AI, and address the specific challenges faced by Africa.
    - Maintaining Resilience: The discussion centered on the importance of maintaining resilience. Strategies for building a resilient cybersecurity ecosystem were explored to withstand evolving cyber threats effectively.
    - Global Position and Emerging Technologies: The global position of Africa in cyberspace was a focal point. Questions arose about Africa's stance on emerging technologies like AI, pondering whether AI could be used for security purposes or if security measures could be applied to AI.

- **Communication and Security Mechanisms**
    - Enhancing Communication: Participants stressed the need to increase communication to ensure a secure ecosystem. Building better security mechanisms was highlighted to fortify defence against cyber threats.
    - Reference was made to the Malabo Convention particularly the design to enhance cybersecurity in Africa. Participants emphasized the importance of implementing this convention across different African countries.

- **Building an Ecosystem and International Standards:**
    - Metrics and Ecosystem Building: Ensuring applicable metrics and building a robust ecosystem were identified as crucial tasks. The discussion touched on the challenges and strategies associated with these objectives.
    - International Standards and Collaboration: The cost implications of adhering to international standards were raised. The importance of affordable standards and creating a critical mass of assessors on the ground was emphasized. Government intervention and policy frameworks were seen as essential to managing supply and demand.

- **Education and Awareness**
    - Importance of Education: Education and awareness emerged as key elements. Building expertise, institutional memory, and incorporating best practices within educational curricula were seen as vital. The example of Kaspersky incorporating education was cited.
    - Regulatory Frameworks: A call for SMART (Specific, Measurable, Achievable, Relevant, Time-bound) regulation was made, stressing the need for effective regulatory frameworks.
    - Trusted Africa Internet Initiative: The concept of a trusted internet involving collaboration with governments and various stakeholders

was discussed. Challenges related to implementing standards when governments are not actively involved were considered.

- **Challenges and Solutions Discussion**
  - Operating in Silos: Challenges such as operating in silos, conflicts in security standards, and the need for political will were highlighted. The discussion suggested a focus on the private sector, where adherence to standards is often more prevalent.
  - Political Will: The importance of political will, especially for small businesses, was emphasized. Building political will was identified as a critical starting point for effective cybersecurity measures.
  - Capacity Building and Human Resources: Challenges in human resources understanding critical infrastructure were addressed. The consensus was that capacity building efforts need to be more robust.

- **Harmonizing Regulations and Cyber Diplomacy**
  - Harmonizing Regulation: Harmonizing regulatory frameworks and addressing the lack of data were identified as challenges. Cyber diplomacy was acknowledged as an international agenda, emphasizing collaboration and shared standards.
  - Digital Public Infrastructure: The importance of digital public infrastructure and international collaboration, particularly in open standards and security, was underscored. The discussion urged pushing for proper regulations, especially in the context of AI.

- **Key Challenges and Government Engagement**
  - Key Challenge for the Continent: A key challenge for the continent was highlighted by key experts in government, calling for a collective effort from parliamentarians and stakeholders to ensure a safe cybersecurity ecosystem.
  - Engaging Governments: Participants explored what good political will looks like and strategies for putting security into the political line. Communicating technical issues and providing governments with the right information were identified as essential steps.

The comprehensive discussion covered diverse aspects of cybersecurity, from capacity building and education to regulatory frameworks and international collaboration. It highlighted the need for a holistic, collaborative approach involving various stakeholders to address the challenges and build a resilient cybersecurity environment in Africa.

Conclusions

Following excellent exchanges during the day the conclusions during the last session provide an end point to the day, but a starting point for further activities. In this, it is very much recognized that much is already going on, and the aim is to ensure that all key issues are covered, and that all Africans can benefit from it, wherever in Africa they are.

Key is context, and coordination to ensure the many different initiatives can complement each other, recognizing that multistakeholder collaboration as well as cross-border collaboration will be important. After a draft version of this workshop report is reviewed by session contributors, and updated and finalized, the aim is to further develop an action plan in interaction with all those involved. GFCE is committed to help make that happen at its best ability and will support proposals going forward in the spirit of this meeting at their best ability. For more information about the specific action follow up please contact Maarten or Daniel Nanghaka.

This was the eights of a series of Triple I Workshops that are organized in different regions of the world. Big thanks to all contributors to this workshop – co-organizers, presenters and participants. The results and outcomes will all be shared on the Triple-I event website.

For more information: maarten@gnksconsult.com.