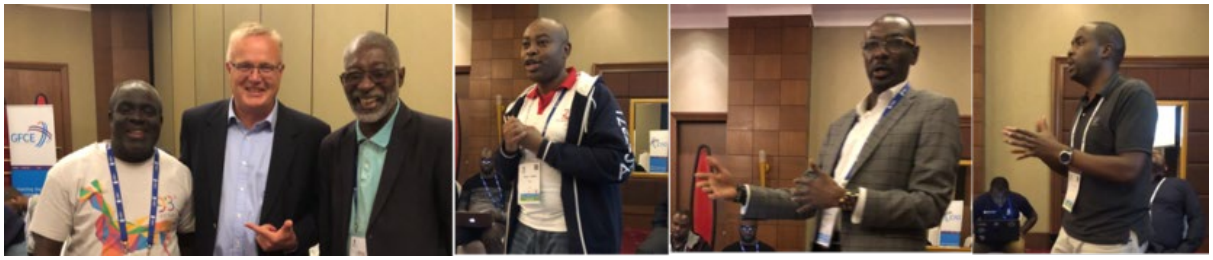
GFCE Triple-I Meeting @AIS2019 in Kampala, 6 June 2019

Triple-I (the ***I**nternet **I**nfrastructure **I**nitiative*) is a GFCE Initiative with the objective to enhance justified trust in the Internet and email through open internet security standards and sharing good practices on a global level. Triple-I aims to organize capacity building workshops in different regions with the support of the GFCE community, as well as from members of the global "technical community". The Initiative seeks to facilitate awareness raising and capacity building in the region, and thus sets local priorities and stimulates local action. People from government, the technical community, Internet service providers, business and academia come together to explore opportunities and commit to action.

On Sunday 16 June, the African Internet Summit hosted the GFCE Triple-I Internet Infrastructure Security Day for the second year in a row. This workshop was supported by AfriNIC, AfricaCERT, AFNOG, WACREN, ICANN, Internet Society, and the Dutch Ministry of Economic Affairs and Climate. The aim of the workshop is to look for ways forward towards more trusted use of the Internet and email in the region. Participants in this workshop included global and regional experts, and regional Internet stakeholder groups, including the government, business and technical community, who all contributed in finding solutions to strengthen an open end-to-end Internet. This is the fifth of a series of workshops organized globally, after Dakar, Senegal (also hosted by the African Internet Summit), Almaty, Kazachstan (hosted by RIPE NCC), New Delhi, India (hosted by INSIG and the Indian Ministry of Electronics and IT), and Daejeon, South Korea (hosted by APRICOT).

Towards a safer use of the Internet in Africa

The workshop session was opened by Mr. Nii Quaynor, who 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. He also highlighted the good experiences with the AFNOG capacity building trainings. Maarten Botterman explained that 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. It was noted that GFCE partnership with the regional registries and has been setting up Capacity building events with this workshop being the second in Africa. The first workshop was held in Dakar (see Report).



Some of the speakers at GFCE Triple-I @AIS2019, left to right: Alain Aina, Maarten Botterman, Nii Quaynor, Michuke Mwangi, Adiel Akplogan, Kevin Chege

©Maarten Botterman

During the first block, we focused on Open Internet standards that could already be applied today, and Alain Aina (WACREN) discussed with Adiel Akplogan (ICANN) about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF, and IPv6.

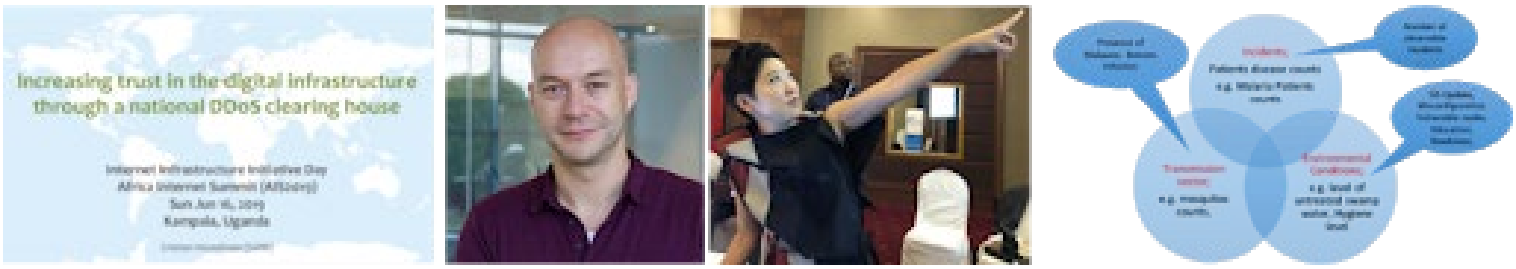
DNSSEC, TLS and DANE are important in ensuring integrity of routing and of the data exchange itself. The challenge is the overhead and action needed by all players in the value chain to be fully effective. The successful first root KSK rollover cycle completed recently was mentioned. All in the room were invited to participate and ask questions or contribute where useful. It was point out that based on the recent statistics published by NRO, for RPKI adoption for IPv4 and IPv6; this region is not doing badly. Effort must continue and the RPKI BoF planned for the end of AFNOG2019 was well welcomed.

During the discussion on the use and usefulness of these Open Internet Standards, Alain stressed the need for all to understand what an open standard is, as there are many definitions when it comes to this and also a lot of confusion. He referred to the recent effort by IETF, IAB, IEEE, W3C, etc. to promote a proven set of principles that establish The Modern Paradigm for Standards. He mentioned the five (5) principles of the modern Paradigm of Standards published in RFC 6852 as important guidance for further standards preparation. Adiel highlighted the challenge to understand what the meaning of open standards is, and pointed out that there is a need for choosing appropriate standards that are suitable for different business and economic environments. Sometimes the implementation of standards, as open as they can be, add operation costs that small ISPs or network operators will not be able to handle given their already tight margins. Sometimes the additional costs are real and unavoidable, but sometimes they are just a matter perception and much could be done without the additional costs. It is therefore important to raise awareness and share relevant good practices. It was also noted that for some governments and telecom operators, adoption by ITU of specific IETF standards will stimulate implementation.

A very good tool to measure the use of these standards by websites and mail servers is the website www.internet.nl. On this website, it is possible to fill in any website or email address to check whether it is up-to-date in its use of these open standards. As the source code has been made available to regional initiatives, adopting this and setting up a regional website seems very worthwhile. Daniel Nanghaka (ILICIT Africa) shared his interest to take the lead to deploy an Africa Open Standards Platform on this basis, in order to support the open internet standard adoption in Africa.

Inspiration from Good Practices

During the second block, space is given for the sharing of inspirational practices and useful ways forward. Cristian Hesselman: head of SIDN Labs (the research team of the .NL operator) and SSAC Member, explained the concept of a DDOS Radar, which facilitates a proactive and collaborative DDoS mitigation strategy. It resolves around providers of critical services (e.g. ISPs, banks, government agencies, and hosting providers) continually collecting information on potential and active DDoS sources and automatically sharing this information with each other.



Cristian Hesselman on DDOS mitigation and Yurie Ito pointing at the "Public Healthcare approach towards cybersecurity" ©Maarten Botterman

Abuse mitigation was the subject of a panel led by Jean-Robert Hountomey (AfricaCERT), with Yuri Ito (CyberGreen) and Adiel Akplogan (DAAR – ICANN). There is a need for resources to help detect and act against abuse as it was also mentioned that the Internet is not good or bad in itself: it is how it is used that matters. Early detection of abuse (whether purposefully or by mistake) will help to contain damage by being able to alert users and actively take measures against the abuse. Measuring abuse helps us understand where the weakest spots are, which then informs the prioritization of appropriate measures. Examples of global action include CyberGreen and DAAR, basically providing information to the public about specific abuse.

Michuki Mwangi gave a presentation on Mutually Agreed Norms for Routing Security (MANRS) and called upon network operators around the world to join the Routing Resilience Manifesto Initiative, and to agree to the Mutually Agreed Norms for Routing Security (MANRS) Principles. There is a clear need for a culture

of collective responsibility whereby best practices on routing security are shared among the stakeholders. For consumers it is wise to choose a reliable router supplier that agrees to the MANRS Principles.

The Internet of Things (IoT) comes with opportunities for citizens as well as the digital economy. Maarten Botterman highlighted the fact that many internet-connected devices, and in particular those sold to consumers, often lack basic cyber security provisions, which is an increasing concern for citizens and governments. There are basically two risks: 1) vulnerability of individual devices themselves to tampering; and 2) wider society faces an increasing threat of large scale DDOS attacks launched from large volumes of insecure IoT devices. How to reduce those risks is a high interest topic in many countries and regions. Kevin Chege expanded on the need to for the adoption of IoT trust frameworks to improve security in and around IoT, and recommended the adoption the OTA IoT Trust Framework as a guideline for safer IoT implementation. Verengai Mabika reported that most of the people in Africa are consumers of IoT devices and are not involved or aware about the Security of the IoT. Reference was made to Senegal with the process on which they are doing to improve on IoT Security. More information can be found on https://iotsecurity.sn.

Market place for actions to improve trust

Following the introductions about Open Internet Standards that can help enhance justified trust in using 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 can we do, together, to improve justified trust in using the Internet and email in the region*".

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

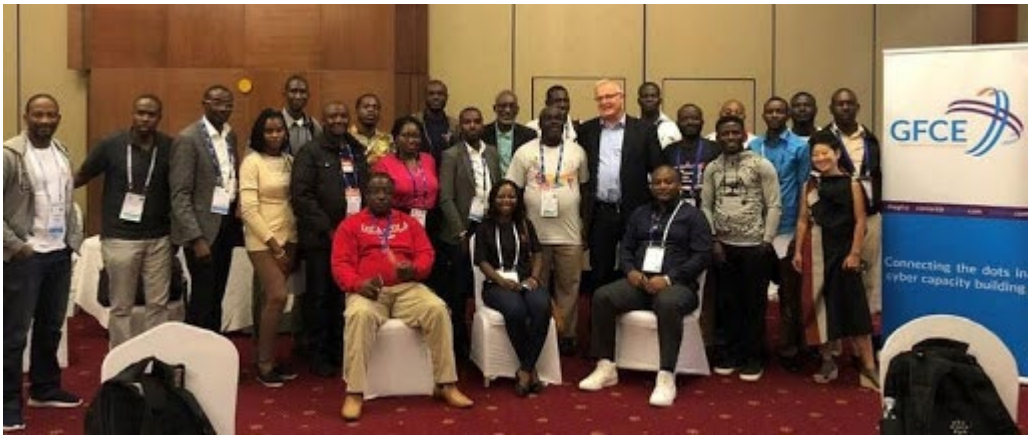
1. Awareness raising on key global Internet Standards is a first step to deeper adoption of those, and that will help make the Internet in the region more trustworthy. As too few people are aware of this, ISPs do not see it as a business priority for investing. However, this is likely to change if abuse continues to grow, and if some service providers in the region start offering more secure services. Soawareness raising needs to take place on all fronts: consumers, politicians, business decision makers and service providers. When moving forwards on this, the website www.internet.nl can be very useful, and it may be possible to set up local applications of the code that will be shared under an open software license.

2. DDOS mitigation through collaboration: Here, it was recognized that dealing with DDOS attacks is key towards being able to rely on infrastructures and services – even more so for critical applications and infrastructures than for others

3. The big opportunity seems to be in working together and sharing both DDOS attack sinking facilities and information about attacks, as soon as they are recognized.

4. The number of IoT devices continues to surge with estimates indicating that the number of devices will exceed 2.5 times the population of earth by the year 2020. For these devices to be trusted and used properly, users need to be educated early on what IoT devices are as well as the risks and opportunities IoT devices present. Manufacturers need to ensure that IoT devices are secure by design from the beginning, following broadly recognized Principles and Guidelines on IoT design such as the OTA IoT Trust Framework Guidelines. Network providers need to make sure they filter and sink abuse of the networks when it is detected. Cloud providers need to ensure adequate protection of their services as well. Overall, next to mitigating the short-term risks, longer term solutions need to be developed and adopted. For this, much can be learned from other countries.

5. Capacity building workshops – there was mention of AFNOG capacity building workshops (Nii Quaynor), and IoT security capacity building workshop (Kevin Chege, Internet Society). In addition, most of the attendants agreed that it would be useful to bring back the GFCE Triple-I workshop in 2020, during AIS2020.



Participants to the Triple-I workshop after an inspirational day ©Maarten Botterman

Conclusions

Many of the good practices presented on subjects like Open Standards adoption, joint DDOS mitigation, better abuse detection and prevention, and IoT security were confirmed to be important by the well-informed group of participants of this workshop during AIS2019. A lot of emphasis was put on awareness raising – both within the industry, and to politicians and the larger public. This comes hand in hand with (intra- and cross-sectoral) collaboration, as many of the challenges faced are the same or similar. As for Open Internet Standards, the suggestion came up to consider setting up regional or national "platforms" of multiple stakeholders to jointly set appropriate standards for a safer use of Internet and e-mail.

More information

This was the fifth of a series of Triple I Workshops that will be 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 page, including a livestream of the event provided by Internet Society. Organizations that want to get involved can contact the GFCE Triple-I facilitator Maarten Botterman at: maarten@gnksconsult.com