GFCE Triple-I Day @Caribbean IGF,
22 August 2024, Georgetown, Guyana

Stepping up enhancing Justified Trust in the use of the Internet in the Caribbean

Report by Maarten Botterman

Summary

On Thursday 22 August 2024, during the 20th Caribbean IGF, CTU Secretary General Rodney Taylor kicked off a discussion on what can be done to ensure the Caribbean can rely on a resilient and robust Internet infrastructure that is safe to use. The workshop was initiated by the Global Forum for Cyber Expertise (GFCE) in close collaboration with the Caribbean Telecommunications Union (CTU), and is supported by LACNIC, ARIN, ICANN, Internet Society (ISOC) the Global Cyber Alliance, EasyDMARC, nic.tt and Identity Digital.

This GFCE initiative is meant to facilitate awareness raising and capacity building events in different regions of the world in order to *enhance justified trust* in the use of Internet and/or email in those regions (specific priorities to be determined by stakeholders in the region). Local and regional actors are stimulated and supported in setting up and running local/regional events between regional stakeholders, bringing in local expertise, when useful. The initiative builds on the experience of multiple events around the world and is firmly embedded in the GFCE's mission of strengthening cyber resilience and capacity globally through international collaboration and cooperation.

Participants in this workshop included global and regional experts, and regional Internet stakeholder groups, including the government, business and technical community, who all contributed to finding solutions to strengthen an open end-to-end Internet. The meeting was set up as a hybrid meeting and included online participants. Initial conclusions were drawn to (1) further improve measurements on the state of the Internet in the region, and (2) step up raising awareness throughout the region, recognizing that stakeholders are dispersed across 20 economies, partly on small islands, and with a dominance of small businesses. Follow-up discussions should lead to concrete steps in 2024.

On behalf of GFCE Triple-I, thanks to everyone who helped make this happen, and with special thanks to Rodney Taylor, Nigel Cassimire and Shernon Osapa from the CTU for their support from the outset to help make this workshop happen.

Opening Session

Rodney Taylor, CTU Secretary General, welcomed all, and explained that he was happy to host the GFCE Triple-I workshop in the region to further explore what can be done to improve justified trust in the use of the Internet in the region. CTU has also become a Member organization of the Global Forum for Cyber Expertise, as part of their capacity building commitment.

After that, **Maarten Botterman** explained that the GFCE Internet Infrastructure Initiative aims to close that gap of trust in the Internet: to help build a robust, transparent and resilient Internet infrastructure. The Internet was not designed to be safe, but to be used. Now the use has grown to levels that require much higher level of resilience, security and safety. Modern Internet standards offer higher levels of resilience and justified trust in the DNS and routing, yet wider awareness and adoption are needed if we are to reap the benefits that the Internet can bring. Challenges with the Internet need to be addressed – the good news is that most challenges are already addressed at some point in the world. This workshop is essential to support improvement of the Internet infrastructure in the Caribbean region and draw upon the growing global knowledge and experience relating to digital technologies and the Internet that connects us all.

For a regional/local response to be effective, capacity building is key. This workshop contributes to that by bringing regional/local stakeholders together with global expertise. The role of GFCE is to contribute to more human capacity and better infrastructures, making the Internet safer by reducing the impact of attacks.

BLOCK I – Better Use of Today's Open Internet Standards

The first Block 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 the region. 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. Focus was on the use and usefulness of Open Internet Standards that matter for integrity and

security of the DNS, routing and email (DNSSEC/TLS/DANE, RPKI/ROA, DMARC/DKIM/SPF), and IPv6.

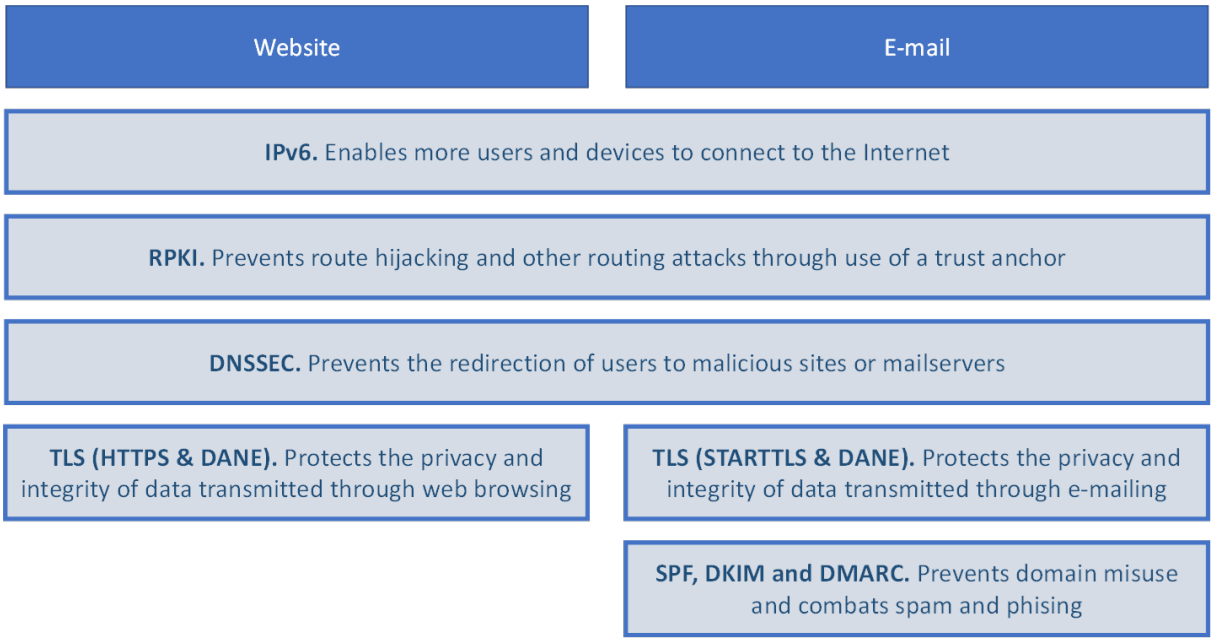

Fig.1 – Today's modern open Internet standards with in-build security considerations

These standards are globally accepted and represent state-of-the-art insights that, when applied, can already help reduce the risks of using the Internet and email today. These are also reflected in the GFCE Triple I Handbook. Please find above a diagram indicating how these standards interrelate:

Domain name security: DNSSEC, TLS and DANE

Nicolas Antoniello (ICANN OCTO), calling in via zoom presented the need for practical implementation and significance of DNSSEC, DANE, and TLS in securing the Domain Name System (DNS) and ensuring data integrity during transmission.
For the safest functioning of the DNS, it requires Registry operators and Registrants to sign their domain. This should be facilitated by Registrars and DNS hosting providers. DNS Operators, Internet Service Providers, mobile operators, hosting providers etc. should activate DNSSEC validation on the entire resolver system and should sign domains. DNS Security Extensions (DNSSEC): use public-key cryptography and digital signatures to protect the DNS data by providing (1) data origin authenticity (i.e. "Did this response truly come from the correct DNS server?") and (2) data integrity (i.e. "The data relating to the DNS server has not been modified after signing").

However, DNSSEC do not provide confidentiality for DNS data, unless combined with standards like HTTPS (DoH – RFC 8484) or TLS (DoT – RFC 7858) and achieve DNS encryption between the client and the resolver. 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).

To go beyond the protection by DNSSEC (ideally in combination with SSL/TLS or HTTPS), DNS-based Authentication of Named Entities (DANE – RFC 6698) will allow administrators of a domain name to certify the keys used in that domains' TLS clients or servers by storing them in the DNSDNS-based Authentication of Named Entities (DANE) is a protocol that helps authenticate the identity of internet endpoints using the DNS infrastructure protected by DNSSEC. It offers the option to use the DNSSEC infrastructure to store and sign keys and certificates that are used by TLS.
Through the combination of DNSSEC and DANE, users will have the best assurances for integrity of data and end points.

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.

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

Maarten Botterman referred to the first KSK re-signing happening in 2018, actually during the GFCE Triple-I workshop in New Delhi at that time. The industry did hold its breath … but except for some measures that needed to be taken it worked. Since then, it has become a regular activity that people got used to. And good to know further improvement is on its way.

Routing security: RPKI and ROA

Bevil Wooding (ARIN) had planned to present the why and what of these standards, but had a last minute conflict and couldn't deliver his contribution. Maarten Botterman explained that securing the route is improved by use of the Resource Public Key Infrastructure (RPKI) and Route Origin Authorizations (ROA). He explained that, for internet routing, it is important that the IP address before and after the specific address are registered. In short: through global RPKI deployment:

1- Networks sign their prefixes i.e. "create ROA", and:
2- Networks validate other "networks signature".

This is to prevent "prefix hijacking" (i.e. someone originating an IP block that doesn't belong to them) and "route leaking" (i.e. announcing a route which they are not supposed to) by ensuring the integrity of the sources. Signing is one thing, however, checking whether the signature is correct closes the loop (i.e. validation). This is done by RPKI.

Towards the future, Regional Internet Registries including ARIN and LACNIC are working on solutions towards quantum proof algorithms for signing with encryption keys, once 2K and 4K encryption keys are no longer sufficient. We will not only need to address current problems, but also be ahead of problems for the future, for instance related to the new paradigms of quantum computing once that is there.

Email Security: DMARC, DKIM, SPF

Hovsep Naranijan from EasyDMARC explained 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.

Today, the problem is that anyone who is on the Internet can send an email on your behalf. 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. Key is that ISPs in the region support DMARC well – which is relatively easy for those that already implemented SPF and DKIM. Confirmation of legitimate sources is increasingly important.

DMARC makes email really safe, and once you start monitoring implementation is relatively easy. Yet it is important to use DMARC well – today, a policy that just "rejects" emails that cannot be confirmed via SPF and/or DKIM will lead to many emails not reaching you at all. Quarantine is currently probably a better policy – the danger gets contained, yet can still be checked.

Hovsep stands ready to support organizations that want to make best use of these standards and set the policies. Maarten concluded reminding us that standards deployment is often triggered by things going wrong. For instance, in Australia, DMARC has gained a high priority as it has been recommended by the Australian Cyber Security Centre following an incident that involved the compromise of Australian Parliament House's network that was reported in 2019. Question is whether we need to wait for things to go wrong before we deploy modern Internet standards.

IPv6

Kevon Swift (LACNIC) explained that IPv6 is now widely deployed and the number in use is growing fast, with IPv4 addresses in scarce supply. In 2023, there are already more Internet users in the world than IPv4 addresses …let alone the IoT devices that are connected, the fact that many users have multiple devices, and so on. Besides end users, servers, API endpoints, web servers, mail servers and a lot more need addresses to communicate. To compare: if all of the IP numbers available under IPv4 would represent a space that together would have the size of a golf ball, the representation of all IPv6 numbers would have the size of the Sun.

Today, existing unused IPv4 addresses are changing hands via brokers, paying real money for it, whereas there is already an abundance of IPv6 addresses at marginal costs and increasingly in use. There is also a heavy use of (Carrier Grade) NATs, and gateways are used of convert packages to ensure interoperability between IPv4 and IPv6. NAT comes with a lot of issues … and it would be good if we can let that behind us at some point in time. It breaks to end to end connectivity between users and pushes for more server-client connectivity models. And there is a theoretical upper cap on NAT (6553 ports).

Once ISPs using NATs start hitting that, they have to find creative ways to reduce the number of active sessions. It is also very hard for lawful logging of who communicate with whom to backtrack in some legal cases.

Moving to IPv6 is really a necessity when considering the digital divide. According to the World Bank, the Caribbean's total internet penetration is about 79% so there's still 21% of people that still need to be connected to the internet, as well as an

increasing number of IoT devices. Taking this a step further, meaningful connectivity will include parameters such as high availability, regular use, quality of service, security, trustworthiness, affordability and access by appropriate devices.

A second reason is traceability of origin, and supporting the end-to-end paths that were used originally. So-called Carrier Grade Networks extend the use of IPv4 addresses by splitting access among thousands of end devices – so any attack or crime initiated from any of those is very difficult to trace back to its origin.

IPv6 implementation has become much easier as most of today's devices support IPv6. All transit free networks nowadays support IPv6 and most of them have dual stacked peering links between them.

Most improvement will be possible for fixed-line operators, where most, in particular the smaller one, still need to move towards implementation. In particular, IPv6 will help reducing the (CG)NAT load. Overall, it is less of a technology challenge, today, than a business challenge.

Governments can play a big role in the transition to IPv6 by insisting on IPv6 capable devices and services – thus setting standards by example, ensuring access using IPv6, and providing market incentives to serve IPv6, as governments are relatively large customers. Academia play a major role in research, innovation and capacity building – key they embrace IPv6 as well. LACNIC sees raising awareness on this as a priority. BTW: Guyana (host country for this year's Caribbean IGF) is relatively advanced in its uptake of IPv6 – and has made the jump to "advanced uptake" in a relatively short period starting with the pandemic.

Using a testing tool to stimulate and support uptake of modern Standards

In The Netherlands, a public-private collaboration is set up to select and stimulate the uptake of key standards that help use of the Internet to be more trustworthy. This multistakeholder platform meets regularly to discuss what improvements can be implemented next. A key tool to assist with the implementation is available at www.internet.nl – including code to test domains and email on their adoption of the selected standards – and what else can be done to enhance adherence to these standards. The source code of this tool is available for free on GITHUB, and the Dutch team is willing to support those that want to work with it, where they can. Some standards' uptake are already measured by the CTU – but more may be feasible to add based on source code available.

In the end, the key is with the users, whether commercial or non-commercial organizations, or individuals. For users to benefit most from the Internet, it is

important to know they are safe, and can trust the connections to services offered on the Internet. By making users aware of the risks and measures, users will stand up and ask their suppliers to provide services they can rely upon, and their governments to protect them from criminal acts. Websites like internet.nl help users better understand what the situation is.

BLOCK II - Inspiration from Good Practice Actions

Next to technical modern Internet standards it is important to manage the Internet resources in a good practice way. For this, we can learn from global internet practices – sometimes to adopt one-on-one, sometimes to learn from. Measuring is key – Dan York and Nancy Quiros (ISOC) presented the results for the Caribbean from the resiliency measuring index ISOC developed. Measuring is followed by action. On a global level, ISOC has initiated the MANRS program to help improve DNS security. MANRS is nowadays managed by the Global Cyber Alliance (Andrei Robachevsky), and ICANN developed KINDNS, a program to assist in deployment of DNS best operational and security practices (Nicolas Antoniello, ICANN OCTO).

Specific points of attention were with DDOS mitigation (Thijs van den Hout, SIDN), Internet Security Toolkits for Small Enterprises (Brian Cute, Global Cyber Alliance), subsea cables resilience (Dan York (ISOC) and Nicole Starosielski (Berkeley University), and ccTLD good practices (Parick Hosein (nic.tt).

Kroop a Shah (Identity Digital) shared the role of Registry Services Providers in ensuring security, stability and continuity for ccTLDs.

Internet Resilience measuring

Dan York and **Nancy Quiros** (Internet Society) 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. Dan highlighted the significance of data collection from over 30 different indicators, including routing hygiene.

Country rankings can be accessed through the portal pulse.internetsociety.org. Next to resilience, Pulse also tracks Internet shutdown; what state of deployment of technologies is critical for the evolution of the Internet; and concentration of services (how much are services concentrated in the hands of a few).

The definition of Internet resilience used is: "A resilient Internet connection is one that maintains an acceptable level of service in the face of faults and challenges to

normal operation." The focus is on the Intern-net, not on the applications and services on top of the Internet.

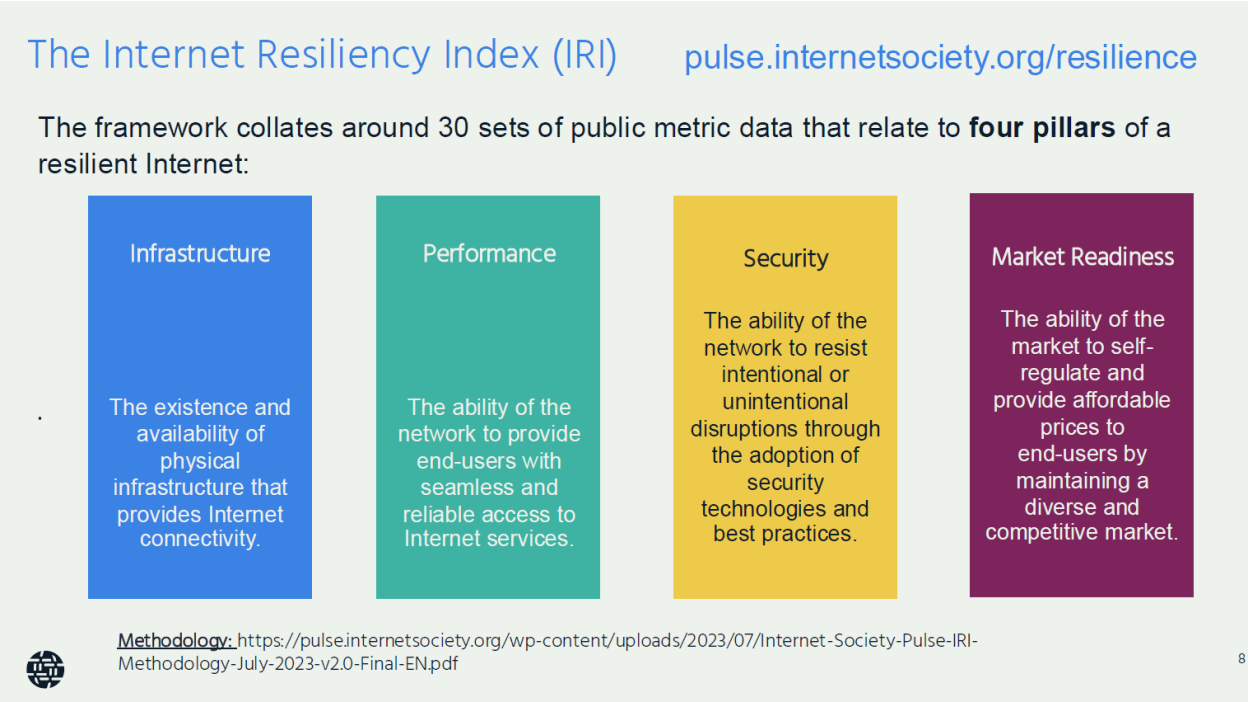

Fig. 2 Internet resilience index (Internet Society)

It should be noted that the data are pulled from external public sources (over 30 different sources), and are not always up-to-date, so this is merely indicative. Without in-country measurements, it's difficult to validate the data, yet the methodology used is reproducible, and "robust" in that sense.

This measuring 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. A request from the floor is to make the Indicators more easily addressable via the API, such as making certain selections and comparisons between (groups of) countries.

It is noted that the data are already useful to engage in analyses and debate, today … and further development is expected over the time to come.

MANRS - Advancing Routing Security

Andrei Robachevsky (Global Cyber Alliance), one of the initial architects of MANRS, presented measures that can be taken on a voluntary basis by industry players: the Mutually Agreed Norms for Routing Security (MANRS), which is a campaign originating from ISOC aimed at best practices adoption for prevention of routing incidents.

Routing is a key element of making the Internet work. There are ~70,000 core networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks. Routers use Border Gateway Protocol (BGP) to exchange "reachability information" - networks they know how to reach. Routers build a "routing table" and pick the best route when sending a packet, typically based on the shortest path.

Border Gateway Protocol (BGP) is based entirely on trust between networks. It was created before security was a concern, and assumes all networks are trustworthy. There is no built-in validation that updates are legitimate. This chain of trust spans continents, and there is a clear lack of reliable resource data. This can lead to:

- Prefix/Route hijacking: in which a network operator or attacker impersonate another network operator, pretending that a server is their client, which can cause Denial of Service attacks or traffic interception;
- Route leak: in which a network operator with multiple upstream providers announces to one upstream, provider that it has a route to a destination through another provider, which could be used for Man-In-The-Middle attack including traffic inspection, modification and reconnaissance;
- IP Address spoofing: when someone creates IP packages with a false source IP address to hide the identity of the sender or impersonate another sender: which is the root cause of DDoS attacks.

Attacks can take anywhere from hours to months to recognize, and inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage. Being vigilant and having procedures in place is therefore key for all network operators.

In order to tackle this, regulation doesn't really help, since this will lead to fragmented solutions for what is really a global issue, with global dependencies. MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure, and sharing good practice norms that are widely accepted, make a difference when applied, and are visible and measurable.

MANRS recommends four simple but concrete actions that network operators must implement to improve Internet security and reliability:

Fig. 3 MANRS Actions for Network Operators (source: MANRS)

Next to Network Operators, MANRS also addresses possible actions for Internet Exchange Points and calls upon them to adopt MANRS as working practice.

Since 2020 MANRS also includes a CDN and Cloud Provider Programme helps by requiring egress routing controls so networks can prevent incidents from happening. Leveraging CDNs' and cloud providers' peering power can have significant positive spillover effect on the routing hygiene of networks they peer with – and they serve many end users. And since 2021, MANRS also has a program for Network Equipment Vendors.

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet. Adopting MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure. MANRS sets a new norm for routing security: joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure. The commitment to adopt MANRS is truly growing throughout the industry. And the MANRS observatory truly helps to understand the preparedness from a region towards cyber hygiene and resilience. Hence the call to the industry to adopt MANRS, and to government and end users to ask for MANRS from their service providers.

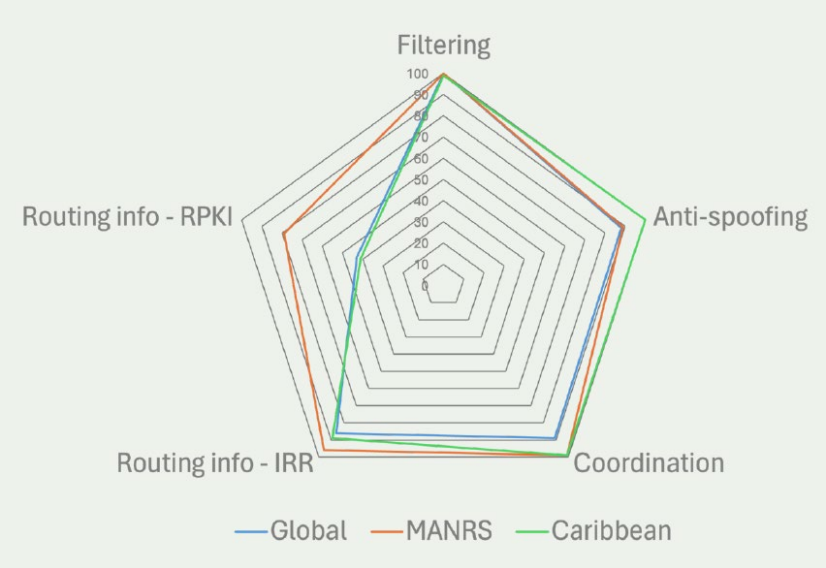

Fig.4 Relative adoption of MANRS in the Caribbean

The MANRS observatory results show that MANRS is advanced in many ways in the region, with a clear "" weak spot" on RPKI adoption. Onboarding from regional network operators and Internet exchange points will not only help to further this adoption, but will also ensure that regional actors are "on board" with the MANRS community to continue to keep Routing Security as good as it can be towards the future.

Right now, it seems to early to "require all IXPs/ISPs to be MANRS compliant" as too few currently are – yet it should be noted that the reputation of those that are compliant will be higher – both within the routing industry as with their users – and ultimately it will lower the management costs.

KINDNS - Knowledge-Sharing and Instantiating Norms for DNS and Naming Security

Nicolas Antoniello and **Albert Daniels** from ICANN 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 using KINDNS framework and use the report to correct/adjust unaligned practices:

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

One out of three participants to the self-assessment indicate as reason to help convince management of the need for implementation of best practices. 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. There is also a number of additional tools available for your use. All operators are encouraged to sign up for this voluntary community, follow the practices and contribute to the continuous improvement of the platform.

Altogether, it will be important to ensure the safest possible practices, as DNS abuse exists, even when the identified abuse seems to be declining (spam, botnets) or at least not growing (phishing, malware). Activities such as MANRS and KINDNS help the industry get a feel for where things happen and building capacity and sharing good practice to address issues arising, are important as to ensure we can continue to rely on the DNS in the years to come – with new opportunities, there will always be new potential threats to address – physical world, and online world alike.

DDOS mitigation

Thijs van den Hout (SIDN) presented a multi-stakeholder approach to DDoS mitigation. In the Netherlands, a national anti-DDoS coalition has since 2018 been tasked with engaging its (currently 20) member organizations in collaborative DDoS mitigation. Providers of critical (internet) infrastructure or services exchange information and data about DDoS attacks with each other to broaden the view of the DDoS landscape and be more prepared when a new DDoS attack eventually hits.

Anti-DDoS coalitions are governed democratically and work is carried out in five working groups: legal affairs, communications, exercises, intel & attribution, and clearing house. The DDoS Clearing House is a platform that enables organizations in an anti-DDoS coalition to share data about the DDoS attacks their receive in the form of "DDoS Fingerprints", a summary of an attack's key characteristics. With this information, other organizations can better prepare for when those attacks may hit them next. The collaboration is based on an agreed governance approach, and

includes good practice exchange on legal, communications and technical matters. Twice a year, large DDoS exercises are done on-site, and members meet face to face. To make it as easy as possible for other organizations to form anti-DDoS coalitions and exchange DDoS information, the Dutch coalition published a "cookbook" that includes all documentation, governing models, and lessons learned from the DDoS Clearing House and Dutch anti-DDoS Coalition. all contributions are open source and open access. The code for the DDoS Clearing House platform is on Github.

Resilience Toolkits for Small enterprises

Brian Cute (Global Cyber Alliance) emphasized the importance of working in community and as a community to deliver cybersecurity capacity building. In essence, it is key to understand that:

- Cybersecurity capacity building requires working with and through communities
- Working with end user communities, particularly in underserved communities and communities like the Caribbean, means understanding their specific needs and the particular cyber threats they face.
- Working through communities means bringing together a number of organizations including content and curriculum providers, funders (i.e., government, corporate, and philanthropies), implementing and training organizations who have broad engagement with identified end user communities

Impact in cybersecurity capacity building requires meeting the end users "where they are" in their digital journey and providing them with content and a learning experience that matches their cyber hygiene maturity level.

The good news: there are many free cybersecurity tools and solutions available for underserved end user communities. Toolkits and solutions that are standards based, adhere to basic cyber hygiene principles, and that meet end users where they are can be an effective approach to building capacity and community resilience to cyber threats. The Global Cyber Alliance has developed several toolkits with the help of its partners, and these are freely available from https://www.globalcyberalliance.org.

Subsea cable resilience in the Caribbean

Dan York (Internet Society) and Prof. **Nicole Starosielski** (Berkely University) presented their research and thinking relating to sea cable resilience. Based on recent events in Africa Dan drew some lessons for all dependent on sea cable – and acknowledging the key role for sea cables in communications in the Caribbean region.

Understanding the physical path of subsea cables is critical. A major outage in Western Africa in March 2024 happened largely because several separate cables wound up taking the same physical path in one area and were all damaged by an undersea rock slide.

He pointed out that Internet Exchange Points (IXPs) can play a strong role in building resilience related to subsea cables. IXPs can help reroute paths in the event of a cable cut, as they are "nodes in the network" that each could connect to other nodes for internet traffic is one connection is broken.

Another measure to reduce dependency for local action on sea cable connection is to ensure availability of local content caching and content distribution networks. Strong local technical communities are important to be able to help ensure resilience and take immediate action when necessary.

In addition: new network paths are becoming possible such as low Earth orbit (LEO) satellites. While such LEO systems may not have the capacity to replace the amount of traffic over a subsea cable, they can provide some capacity in the event of a cable failure thus to facilitate ongoing communications. This may help in case of extreme weather and disasters.

In conclusion, Dan posed that resilience is even more critical today than ever before, and for subsea cables as we face climate-related concerns, including: rising sea levels, increasing storm intensity, coastal erosion, seafloor sediment mobility, flooding, and new shipping routes. Overall, the Internet Resilience Index available from the Internet Society website helps understand the level of resilience in the region, and we continue to improve and update that.

Nicole Starosielski (University of California-Berkeley and the SubOptic Foundation) followed with a presentation of preliminary findings from the Internet Society Foundation-sponsored project, "Enhancing the Strategic Resilience of Subsea Cables in the Caribbean."

Starosielski described the significance of subsea fiber-optic cables for the region, as over 99% of international data traffic transits these lines. Despite the increase in low-earth orbit satellites, these do not currently match cables' speed, security, and cost.

Since these cables are absolutely essential to a resilient internet, and in turn, to economic stability and future investment, our project tackles the question: what can enhance the resilience of these systems?

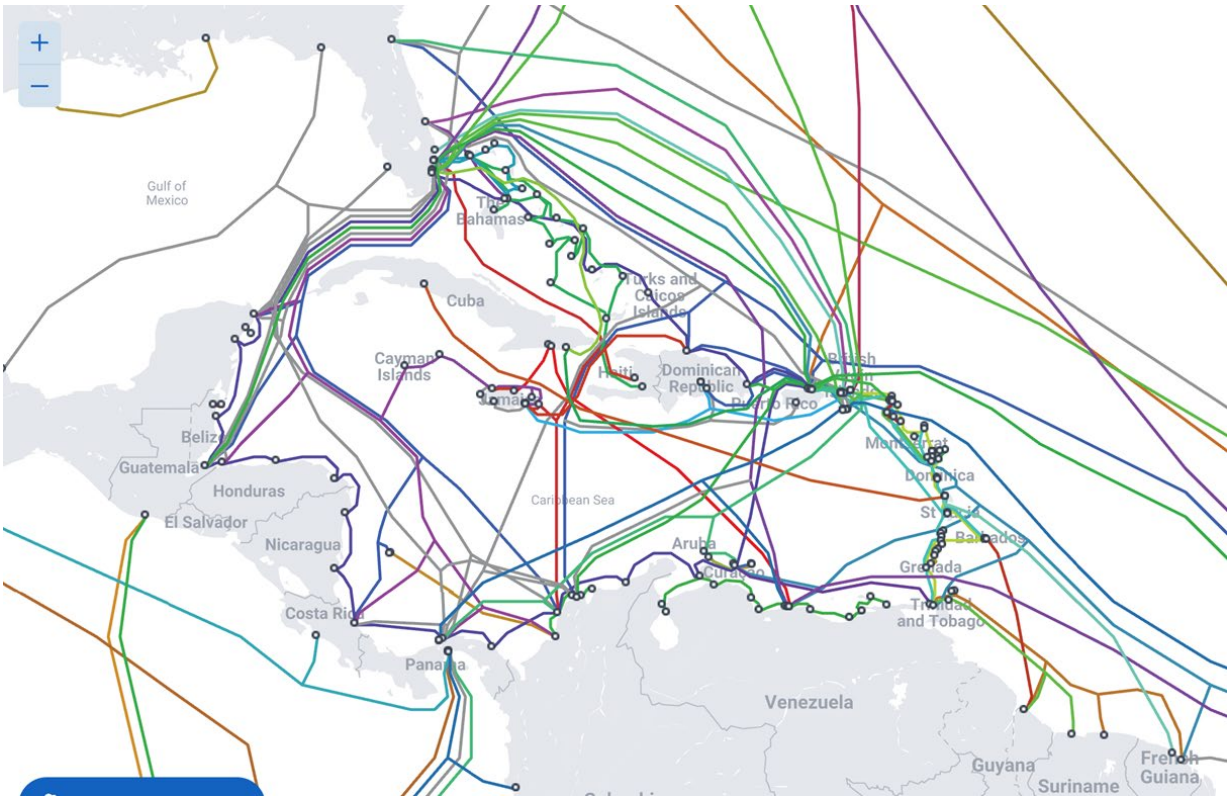

Fig. 5 – subsea cables in the Caribbean region (Nicole Starosielski, Berkeley)

Many organizations and companies currently focus on important resilience considerations for subsea cables. Resilience of marine route planning and maintenance has long been discussed by the International Cable Protection Committee (ICPC) and is well-defined by the ICPC Best Practices. Features that have enhanced resilience include cable awareness, reducing inconsistencies in permitting requirements, cable burial, and others. Resilience of subsea equipment, CLS and front-haul cable has long been the focus of individual companies that often have an economic incentive to ensure business continuity. Resilience of the cable landing point, including diversity of landing points is less well-covered but receives attention in the design process. Resilience of the network has advanced due to work on mesh networking and is a consideration for all operators who often have an economic incentive to offer multiple routes. To-date, however, there has not yet been holistic evaluation of the resilience of the subsea cable system, which considers the technology in its entirety alongside commercial factors at a regional level.

Starosielski proposed the consideration of **the strategic resilience of the subsea network**. This entails the identification and enhancement of features that will make

the entire network within a region more resilient. Some features of strategic resilience include that it is geographically specific. The features that will strategically advance resilience in one area of the world will not necessarily be translatable to other areas. Strategic resilience also requires considerations of commercial affordances and constraints. This means assessing how resilience may be hindered or enabled by existing market conditions. Its scope typically extends beyond a single cable or single network and thus requires consideration of multiple operators. Since strategic resilience focuses on the features that enhance resilience of the region's network as a whole, it can reveal challenges to resilience that cannot be remedied by design, equipment, marine route engineering, or building specifications.

What does strategic resilience mean in the Caribbean? Starosielski shared some preliminary results from interview with individuals with many years of experience in building subsea cable networks, maintaining and operating these systems, regulating island telecommunications, and representing various sectors across the Caribbean islands:

- All interviewees have argued that an increase in the number of cables connecting to Caribbean islands is the primary challenge for resilient infrastructure.
- Current subsea cables in the region are getting old -- many were built in the late 1990s or early 2000s and are now approaching their theoretical end-of-life at 25 years.
- Some islands are about to face the situation of either having no subsea cables or second-tier Internet connectivity

This is a problem, not simply of increasing resilience, but maintaining an existing level of resilience. In addition to this problem, given the heightened significance of an expanding digital economy and as well as the increase of catastrophic events due to climate change, islands will require an even higher level of resilience than they currently have.

In order to develop additional subsea cable systems, prospective builders face a significant economic challenge. Because of the market, there is not a clear business case for private investors in subsea cables. This is also underpinned by specific technical challenges – submarine cable technology cannot be deployed at a small scale. As a result, there has been a lack of investment in new subsea systems, compared to other parts of the world.

The "Enhancing the Strategic Resilience of Subsea Cables in the Caribbean" investigators are currently working to research best practices in incentives for

attracting and facilitating cable development, best practices in financing and funding, and identify scenarios for collaboration, such as the identification of timelines for participation and the navigation of relationships with large players in the subsea industry. The project welcomes input. Please contact Starosielski at nicole.starosielski@berkeley.edu to share insights and opinions.

This project is an initiative of the SubOptic Foundation, the charitable arm of the SubOptic Association, an organization dedicated to promoting the development and sustainability of global subsea fiber-optic cable.

Next to ensuring ample capacity and availability of multiple cables in the region, a challenge is to ensure access to available subsea cables in the region (as some may be privately owned – yet there is a need for shared resources) as well as competition , to ensure communications across those cables remains affordable.

Noted is the international Cable Protection Committee that has a set of best practices that cover already a lot of these policies, and so they've outlined some ideas that governments could take to facilitate the ease of implementation of new projects and the ease of investment and new projects. Something for Caribbean governments to closely pay attention to.

Caribbean DNS Observatory

Mr. **Shernon Osepa**, CTU introduced the project set up by the CTU for promoting Caribbean Internet Resilience: "The DNS Observatory Project" – currently in particular focusing on tackling DNS abuse in the region. "DNS Abuse" can be considered at two levels: the technical level (malware, botnets, phishing, farming, and spam when used for delivery of one of those) and at content level (for example, child abuse, violent extremist content, hate speech, intellectual property related and so on and so on).

He explained the importance of taking adequate measures against cyber attacks, as there are many (144 million cyber-attacks within the Caribbean last year, during six months). This happens in multiple countries, even today in Guyana – sometimes leading to state of emergency and shutdowns.

Thing is – if your infrastructure is not well protected it will be fairly easy for someone with a keen interest and a bit of computer science knowledge to disrupt your systems. Hence the initiative of the Caribbean Telecommunication Union to take action. First, this should be done at policy level – strategies, policies and legislation. Second, there should be active enforcement. All this would require capacity building – one of the reasons the CTU is now working with GFCE (and, in fact, has become a Member).

In order to further support measuring the state of resilience we intent to extend the DNS Observatory measurements with additional measurements, and look forward to working with the Dutch team from internet.nl.

ccTLD good practices for Secure and Resilient Operations

Ms. **Kroopa Shah** (Identity Digital) and Prof. **Patrick Hosein** (nic.tt) discussed best practices for secure and resilient operations for ccTLDs.

Kroopa leads the Registry Services and Management teams at Identity Digital, where she is overseeing service delivery, technical support, and account management for all of Identity Digital's registrar partners and TLD operators whose TLDs are supported on Identity Digital's registry platform. Identity Digital (formerly Afilias and Donuts) has a 23-year history of leadership and innovation in domain registry technology and domain management. This encompasses providing registry services for over 28 million domains across 460+ TLDs including a number of ccTLDs in the Caribbean.

She detailed various aspects of the role of a registry services provider in operating ccTLDs reliably including:

1. Operating the TLD in a safe, secure and reliable manner: RSPs like Identity Digital operate their supported TLDs using modern infrastructure on a cloud based platform with measures for high availability and redundancy to deliver a standards-compliant turnkey solution that meets all requirements of registry support
2. Enabling 100% DNS resolution: Provisioning global DNS infrastructure which provides 100% DNS uptime to ensure that names resolve every minute of every day without any issues.
3. Providing support to registrars: Providing support to registrars including comprehensive documentation, reporting and enabling 24 x 7 Technical Support for all registrars on a variety of topics including account funding and technical inquiries.

Identity Digital supports the TLDs under her care by implementing continuous improvement and security measures such as DNSSEC and DDoS protection, as well as continuous process improvement with a focus on adoption of global good practices by ccTLDs. Protections for its supported TLDs including DNSSEC and DDOS protection, implemented via a massively provisioned global DNS infrastructure.

She remarked that it is essential for the sustainability of TLDs to explicitly address the increase in cyber crime. DDoS attackers are not just sending a massive number of attacks: they're not attacking infrastructures just merely by the number of attacks.

Their attacks have become creative and attacks persist until businesses are offline. A well protected global DNS infrastructure is critical to the mitigation of DDoS attacks.

In addition, as DNS abuse is on the rise, it is more important than ever to implement quick response and mitigation for DNS abuse to enhance trust and reputation of the TLD. Registry Services Providers, such as Identity Digital implement robust abuse mitigation programs which have demonstrated results. For example - Abuse in TLDs supported by Identity Digital has shown a decrease in reported phishing by about 50% in six months last year. As pioneers of DNS abuse management, Identity Digital implemented DNS abuse mitigation strategies to mitigate abuse for ccTLDs in their care, including:

- Proactively detecting abuse
- Quickly reporting it to the sponsoring registrar for investigation and action
- Taking action on abusive domains if the registrar does not respond. This is key for sustained growth of TLDs, and also increases the interest of registrars to offer their services for distribution of the domains.

She also explained that Identity Digital is connected to registrars that account for 96% of the global market, and thus provides access to the TLDs it supports to a well-established channel. As an example - one ccTLD supported by identity Digital continues to see growth in the channel. The registrar channel has grown approximately 700% since the TLD transitioned to Identity Digital in 2005.

Patrick addressed the experience of their ccTLD and the activities they carry out, including the TTLAB. This is a space created by an ad-hoc group of researchers from various disciplines, which focuses on providing solutions to industry-related topics. Emphasis of the Trinidad and Tobago operation was on "community engagement" in running a ccTLD. TT.NIC exists for over 30 years and is self-sufficient – guided by a Trinidad & Tobago Multistakeholder Advisory Group. Based on the system we set up 30 years ago we have evolved, addressing challenges that came our way, and we have done so on a relatively small budget. Being close to our domains we also manage to avoid emergence of embarrassing websites. We stand ready to assist other islands as well. Currently we run 3500 websites. Thanks to many volunteers and students TTNIC manages to stay on top of current and emerging challenges.

CTU SG Rodney Taylor raised the issue of regional coordination of ccTLDs. Currently, it is not existing. Albert Daniels (ICANN) referred to a meeting some years ago with the intent to establish the relationships amongst ccTLD manager from the region but whereas there were one or two meetings, in which the intent was expressed to better share experiences (similar to LACTLD setup) it has not progressed. Patrick suggests

setting up a WhatsApp group … and possibly CTU, ICANN and other partners can help organize a better coordination.

For domain growth (a question brought up by Shernon) Patrick suggests policies such as discounts for local domain owners, as he sees it is difficult to convince people to use .tt over .com. Kroopa suggested a better focus on the registrar channel, and improvement of the understanding of the market by the TLD.

Block III: Planning for a More Trusted Internet: Marketplace for Action

The moderator summed up the key take-aways from the day and invited insights, feedback and comments. In summary, the key take-aways for potential further action are:

1- improve data collection and use by building on the DNS Observatory the CTU already has set up, and extend it with the help of external resources such as internet.nl;
2- promote uptake of standards, good practices (including MANRS and KINDNS, but also the cybersecurity toolkits from GCA) through targeted awareness raising campaigns and capacity building events throughout the region
3- stimulate closer collaboration (exchange of good practices) between Caribbean ccTLDs – possibly consider the setup of Caribbean TLD (in line with LACTLD).

Continued work with global, regional and local knowledge partners is key in this. Multiple organizations stand ready to assist – once momentum is there. The CTU stands ready to help coordinate further action in the region.

CTU SG Rodney Taylor concluded with expressing the vision for the CTU for the next five to 10 years to be to continue to build on our successes, to ensure that the organization enjoys greater support from our member states, and that the CTU continue to be in tune with member state needs, to build on the success in terms of the CTU's representation at the international level. Next to activities such as organizing meetings and (ccTLD?)networks, extending the DNS Observatory, etc. the CTU can consider helping to develop roadshows throughout the region, addressing different audiences. Albert Daniels expressed ICANN's support, in principle.

A final remark related to take into account sustainability considerations in everything that will be done. It is clear that – next to considering network resilience in times of increasing extreme weather in the region and around the world – we need to watch our ecological footprint in whatever next steps we develop.

May this session have been the start of more action, together. The intent is clear – let's further increase justified trust in the use of the Internet and email in the Caribbean, together.

-=(0)=-

For more information about GFCE Triple-I, including results of earlier events, please check out the GFCE website. Contact Maarten Botterman if you have specific questions about GFCE Triple-I, and if you are interested in improving the trusted Internet experience in your region. Contact Rodney Taylor if you have specific questions about the CTU activities.