GFCE Triple-I Day @INSIG2023,
September 28, IIT Guwahati, India

# Increasing Justified Trust in the use of the Internet in India

Report by Maarten Botterman, Satish Babu, Amitabh Singhal and Anand Raje

## Summary

On Sunday 28 September 2023, the India School for Internet Governance (InSIG) and the Indian Institute of Technology Guwahati (IITG) hosted the GFCE Triple-I Day for the fourth time in India. The workshop is initiated by the Global Forum for Cyber Expertise (GFCE), and is supported by APNIC, ICANN, Internet Society (ISOC) and its Indian chapters, as well as the Indian Ministry of Electronics and Information Technology (MEITY).

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. An initial Action Plan was presented and discussed to further enhance justified trust in the use of the Internet in India. 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 Satish Babu, Amitabh Singhal and Anand Raje, as well to the people from the Indian ISOC Chapters and the Indian Institute for Technology Guwahati for their support from the outset to help make this workshop happen.*

## Opening Session

***Satish Babu***, inSIG2022 host, welcomed all, and explained that this time the starting point is different than during the first three workshops. Measuring has helped provide a starting point for better understanding and thus action, and we started to develop an Action Plan that should serve us when executed together throughout India. India is the most populous country in the world, and the Internet is a valuable tool for progressing the economy and society. With that, he set the ambition to get more concrete in moving forward, together.

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 the Digital India policy plan, and builds upon the first three workshops that have taken place in India as well as on the growing global knowledge and experience relating to digital technologies and the Internet that connects us all.

On behalf of the Indian Institute of Technology Guwahati **Professor Sukumar Nandi** thanked GFCE and InSIG for organizing this important workshop on cybersecurity and cyber capacity building in Guwahati. IITG is looking forward to contribute from the academic site. The Government of India is co-founder of GFCE, and the MEITY Secretary is Co-Chair of GFCE since 20217. Great to see consistency and continuity. In the current world we need to embrace the Internet, and make sure it can be used well, and in a safe way. The awareness raising the Triple-I facilitates in different parts of the world is crucial in this. All stakeholders need to work together in this. Next to security, it is also important that local languages can be used – in particular in India. Core to this all is interoperability. Standardization is key in that, and the IETF serves the world in proposing voluntary standards that work. More Indians need to be involved, in particular in agenda setting at global institutions, yet we do have some Indian leaders, both in technology bodies and in governance. Also, in Universal Acceptance (UA) and promoting the use of Internationalized Domain Names (IDNs) India is a key leader. With regards to the modern Internet standards, more progress is urgently needed. Indian stakeholders need to be stimulated to step up, not only in

deployment within India, but also at the global level. The Indian industry needs to go to the next level. Hackathons across India and other activities will help mobilize the Indian potential to step up. Capacity building is a key building stone for progressing the Internet in, and with India.

Maarten concluded that India steps up to the plate more and more, and is very welcome to do so. It is clear that India has a vision, as expressed in the Digital India policy, and this provides very fertile ground for progressing together.

For the 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 India. 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.

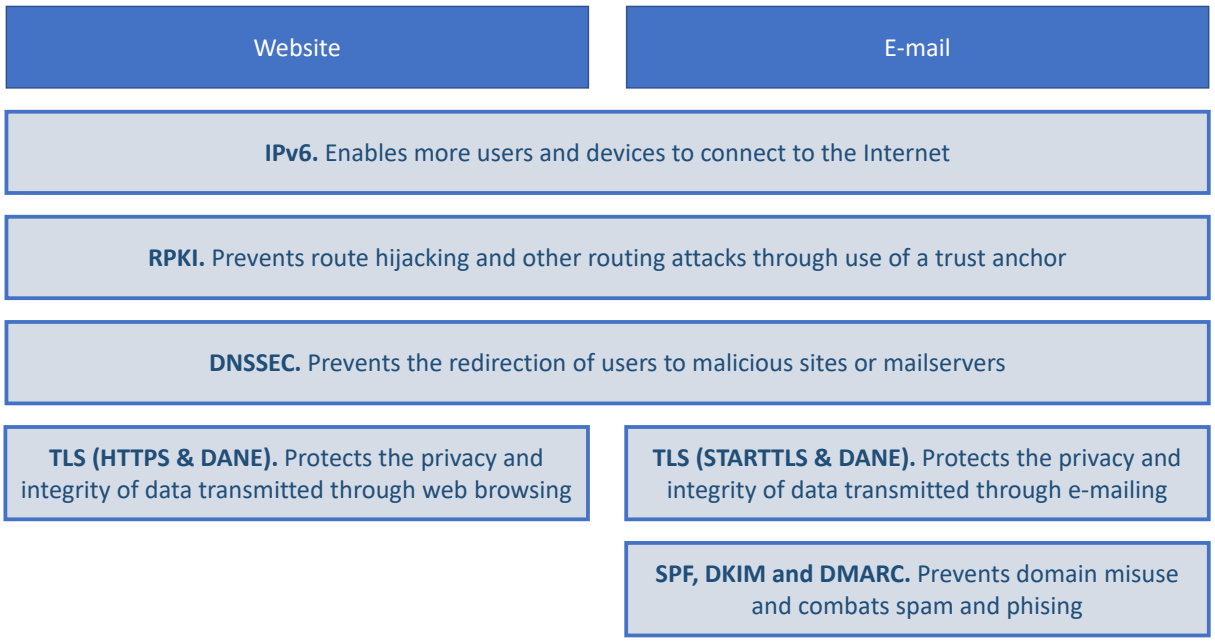


Fig.1 – Today's modern open Internet standards with in-build security considerations

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 below a diagram indicating how these standards interrelate:

After an introduction on the value and status of different standards, we also looked into a tool developed by internet.nl that allows checking for the state of those standards – and what it takes to implement the code for local use. We also presented the "current state of adoption" of key standards based on checking a "basket" of popular Indian websites against the standards.

## DNSSEC, TLS and DANE

Yazid Akanho from ICANN (OCTO), calling in via zoom from the African Internet Summit, 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. He agreed that the stakes nowadays are high, and everything we can do to ensure "justified trust" should be done.
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. And 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.

Jia Rong concluded that ICANN stands ready to help anyone with implementation of these standards – feel free to reach out via the websites or directly via email. All stakeholders need to come together, and ICANN stands ready to support.
Anurag Bhatia asks: "Most other systems using cryptography automatize encryption: with DNSSEC this is much more difficult. Why is it not automated?" Yazid explains that if you follow the guidelines, the likelihood of getting in trouble is almost zero. We deployed guidelines that help overcome this challenge. Currently, every three months new key signing takes place – and without problems other than incidents. The protocol is designed to be impossible to break it, but agreed: on initial implementation there is still some challenges on which the community works to further improve.

Prof. Sukumar Nandi asks: "Accessibility to the DNS Server is the biggest challenge, as most organization place a firewall. How to overcome this?" Yazid responded that we still need to do more research and measurement around this: deployment with very heavy keys leads to longer resolution time. ICANN stand ready to support both in terms of recommended ways forward, and what alternatives exist.

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.

## RPKI and ROA

Terry Sweetser (APNIC) focused on the role of Resource Public Key Infrastructure (RPKI) and Route Origin Authorizations (ROA), and discussed the challenges with

routing (involving the IP addresses). He explained that, for internet routing, it is important that the IP address before and after the specific address are registered. Basically, routing runs on BGP, a trust model that originally wasn't built to be secure, but to work, and in which interruptions can cause disruptions. Over time, increasingly leakages of routes have caused outages – whether by purpose or by mistake.

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.

RPKI and ROA are high on the agenda in India, and by far most Indian Government websites are signed by RPKI ROA. However, this is not always the case, and this merits attention.

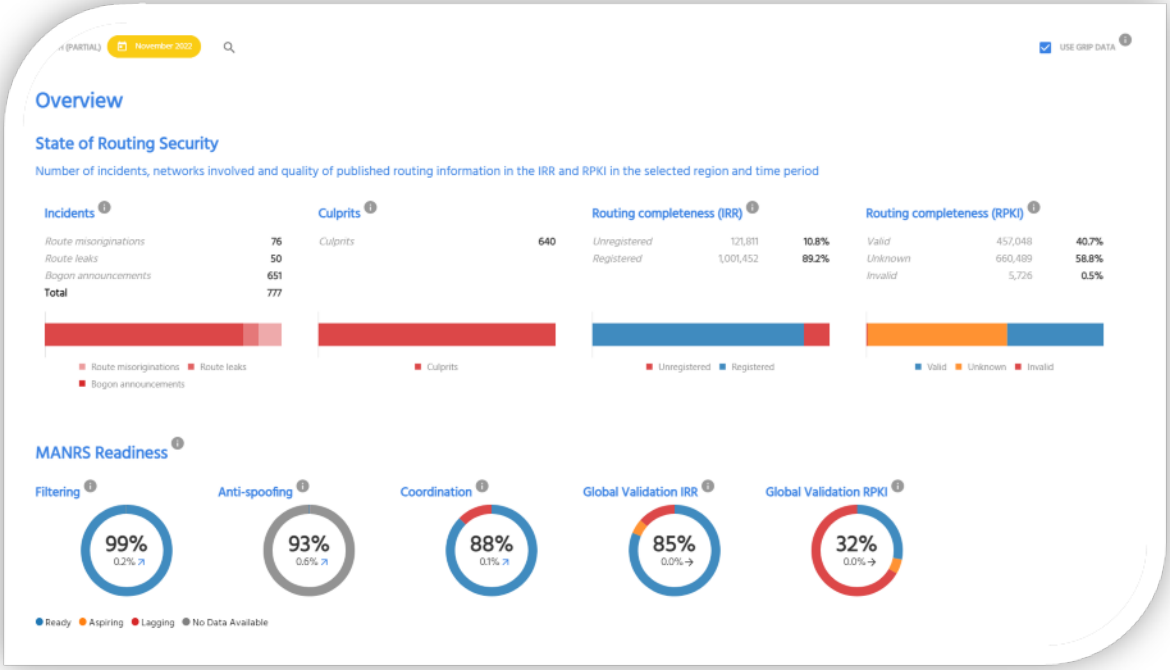


Fig.2 – ROA progress according to MANRS

India is "on the average". Hence, more can be done by promoting signing of the routes within the country. Signing in India requires attention, but is already moving forward.
A bigger challenge is validation. This occurs when everyone signs, but nobody validates, and as a consequence, the signing itself has little value. Here, progress has been made, as major (global) providers start filtering not signed routes (for list: see https://isbgpsafeyet.com). In India, some major operators are checking for signature, but not rejecting yet. As this may only be part of the chain for routing, there may still be any drop of customer traffic. This is bound to progress over time, as at some point, those operators that are not filtering will become the exception – and pressure will go up to also start filtering. APNIC will continue to raise attention and promote uptake. Are your routes signed and have you started to drop invalid routes?

*For more information: go to https://blog.apnic.net/2021/07/13/readthedocs/, and for more data go to https://labs.apnic.net/measurements/.*

A question was raised about the quality of the key itself – will that be sufficient towards the future. Terry explained that we are working on solutions towards quantum proof algorithms once 2K and 4K encryption keys are no longer sufficient. As everybody has the same problem, Terry has no doubt solutions will be found.

Maarten concluded that 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.

## 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.

Today, the problem is that anyone who is on the Internet can send an email on your behalf. India is the third most targeted country by phishing campaigns. 83% of organization in India say phishing attacks are on the rise. 42% of Indians have experienced financial fraud using the Internet.

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. Yet it is important to use DMARC well – today, a policy that just "rejects" emails tat 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.

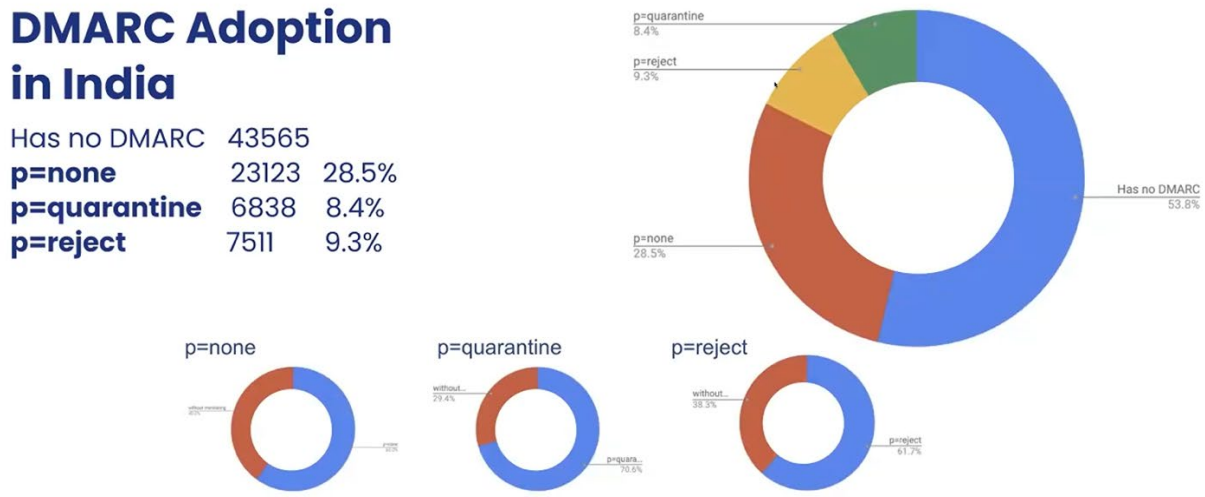


Fig.3 – DMARC Adoption in India

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.

Gerasim 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

Anurag Bhatia (Hurricane Electric) 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.

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.

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. The large Indian ISPs all support IPv6, and so do most high volume traffic websites, but there is many who still don't support it. Overall, India has amongst the highest level of IPv6 availability. Yet it is not always implemented. A lot of potential though! In particular thanks to the mobile operators.

| CC | Country | IPv6 Capable | IPv6 Preferred | Samples |
|---|---|---|---|---|
| IN | India, Southern Asia, Asia | 78.43% | 78.15% | 71,363,259 |
| MY | Malaysia, South-Eastern Asia, Asia | 66.84% | 65.24% | 3,080,196 |
| FR | France, Western Europe, Europe | 66.81% | 66.21% | 6,523,565 |
| BE | Belgium, Western Europe, Europe | 66.68% | 66.26% | 996,143 |
| DE | Germany, Western Europe, Europe | 63.52% | 63.04% | 4,659,688 |

Fig. 4 IPv6 capable counties according to https://stats.lab.apnic.net/ipv6/IN measurements

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.

### 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.

*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 and auCheck in Australia help users better understand what the situation is.*

## BLOCK II - Inspiration from Good Practice Actions

The second block of the day, presentations and discussions were held on a number of global and regional good practices. Measuring is key – Sarah Lake (ISOC) presented the results for India 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 (Anand Raje, MANRS Ambassador), and ICANN developed KINDNS, a program to assist in deployment of DNS best operational and security practices (Yazid Akanho, ICANN OCTO).

Specific points of attention were with DDOS mitigation, IoT Security, and Universal Acceptance and Internationalized Domain Names.

### Internet Resilience measuring

Sarah Lake 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. She 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. Results of recent measuring are depicted below.

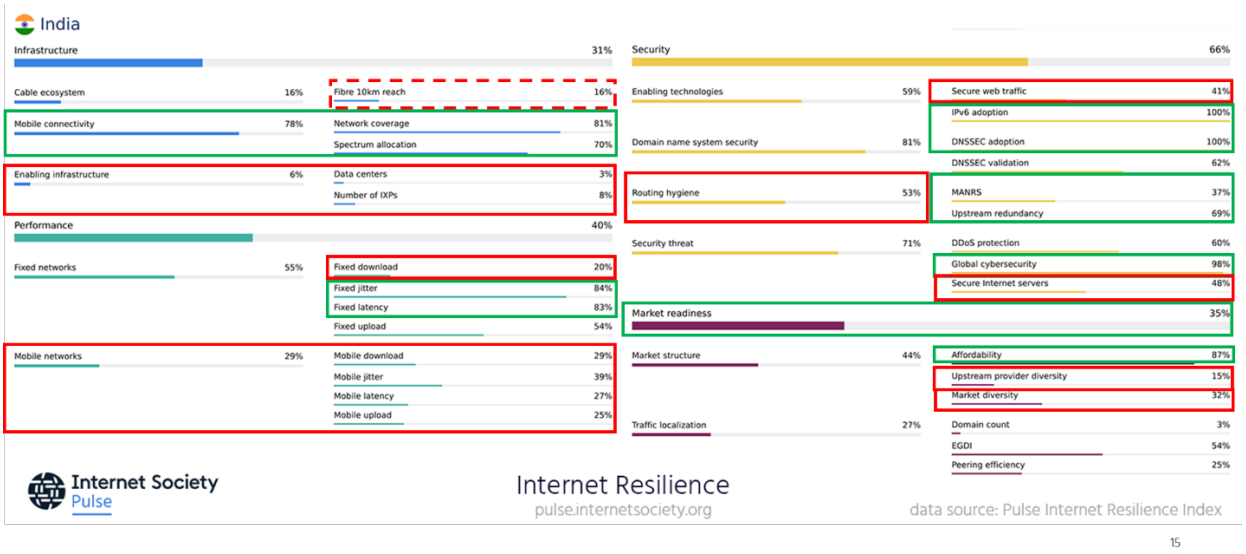


Fig. 5 Resilience aspects of the Internet in India (Sep 2023)

With regards to India, the overall resilience is 43% - average in the region. In the above figure, those factors where India is moving well are emphasized with green, those where India is currently lagging behind are emphasized in red.

It should be noted that the data are pulled from external public 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.

Swapneel (APNIC) asked whether the Index took into account Open Resolvers available in a country. Sarah explained that the various indexes go back to 25 different open sources. Actually, it is an example of opportunities to further improve and/or better explain the Index.

## MANRS - Advancing Routing Security

***Anand Raje*** (MANRS Training Ambassador 2023) 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. As Internet Exchange responsible he adopted MANRS as a way of working, and as Ambassador he steps up to help improve MANRS and help stimulate wider MANRS adoption.

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.

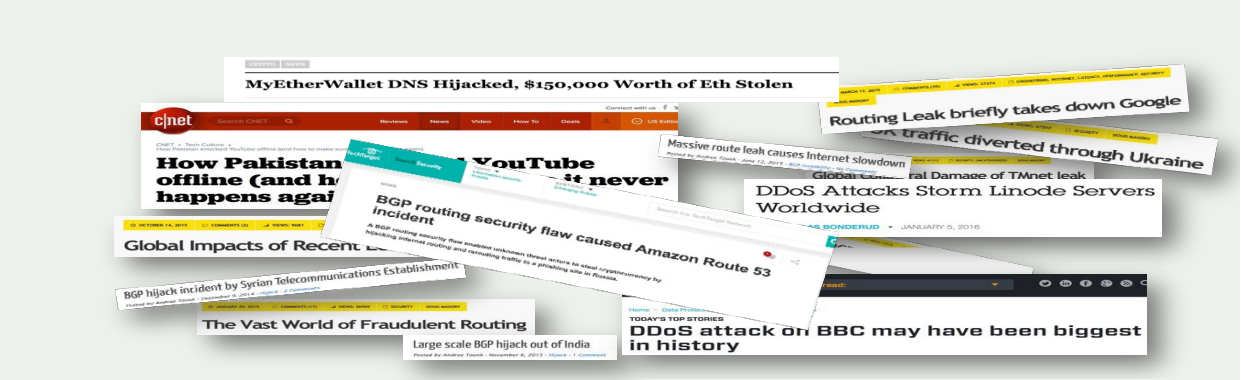


Fig. 6 – clipping of relevant articles in newspapers – courtesy ISOC

In 2019 alone, over 10,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more. About 40% of all network incidents are attacks; 3.8% of all Autonomous Systems on the Internet were affected. Incidents are global in scale,

with one operator's routing problems cascading to impact others. With that, insecure routing is one of the most common paths for malicious threats.

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

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure. Network's safety depends on a routing infrastructure that eradicates damaging actors and accidental misconfigurations that wreak havoc on the Internet. The more network operators work together, the fewer incidents there will be, and the less damage they can do.


Fig. 7 MANRS Actions for Network Operators (source: ISOC)

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.

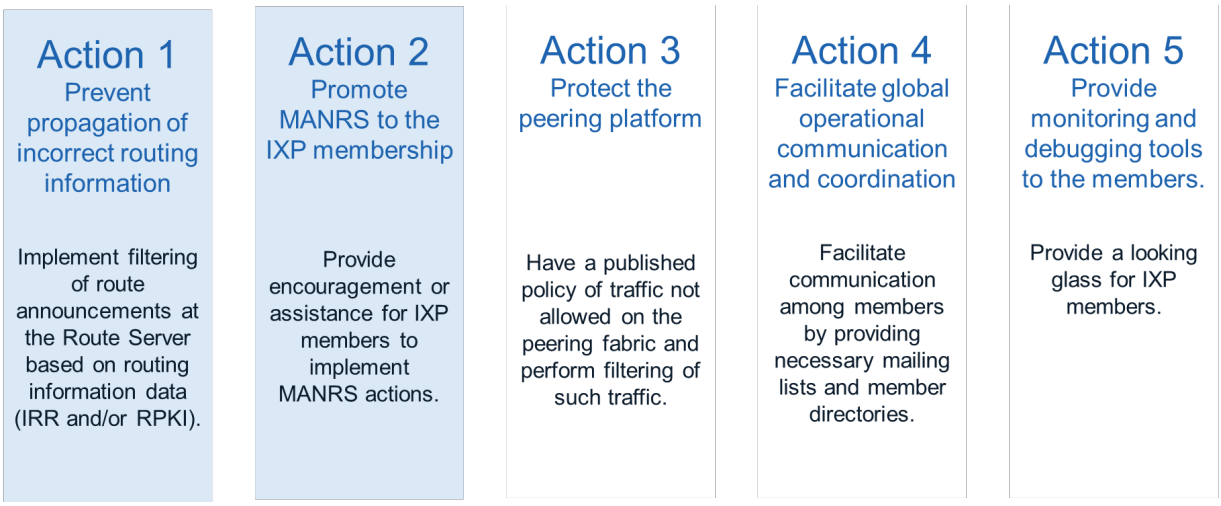


Fig. 8 MANRS Actions for Internet Exchanges (source: ISOC)

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.

In India, MANRS readiness has gone up over the last couple of years, with in particular RPKI uptake to be further improved. As of today, according to MANRS website 10+ Network Operators are MANRS compliant. However as per MANRS observatory, we see a larger percentage of stakeholders are showing MANRS readiness, by adopting routing security best practices (Filtering 99%, Anti-spoofing 79%, Coordination 99%, Sharing Routing information 98% and implementing RPKI 98%) a study involving 2715 AS operating from India. There is a dire need to work with the small players of rural India and diverse geographic regions for an inclusive routing security regime across India. With more content, and IoT at the edge there will be more AS routing at the edge. . MANRS is an initiative that needs collaborative efforts from all the relevant stakeholders, as the initiative started as a collaborative effort of network operators understanding the very need through their operational experiences. Anand called for all to join, as together we are strong: measure, grow awareness, and act.

Questions:
*>What strategies and mechanism can MANRS adopt to mitigate the risk associated with propagation of inaccurate or malicious RPKI ROAs and how can MANRS incentivize Internet service providers and organizations to actively participate in the validation of BGP route announcements against RPKI data further enhancing security and reliability of global routing?*
Anand responds that MANRS participation may be used as a marketing tool or a conformance of a secured and resilient Internet experience to the customers, which increases the reputation of the network provider in the market. On propagation of inaccurate or malicious RPKI ROAs, Route Object Validation (ROV) is used to validate the BGP prefix-origin pairs against route origin authorizations (ROAs) before they are considered. An autonomous system (AS) performing ROV is less vulnerable to BGP hijacking than an AS not doing so.

*>Why do you spend so much time on MANRS, as IXP?*
Anand responds that he truly believes this serves the users better. Working with the community on increased adoption of routing security best practices and other incentives is something that keeps him occupied.

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

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 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.

Go to the website for more information, and join us. 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.

Question from Swapneel: Is there an incentive for having implemented the standards, i.e. a kind of "certificate" for being a "good actor"? Swapneel asks whether it is self-validation, or can the KINDNS system validate assessments as well. Yazid responds that the aim is to upgrade the tool to be able to confirm compliance. He explains that next steps are under discussion: a kind of certificate or "badge" for being KINDNS compliant, but this is not agreed yet.

*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

Octavia de Weerdt, is Chair of the AntiDDoS Coalition, and General Director of NBIP NaWAS, the Dutch National Scrubbing Center against DDoS attacks. Since 2014, the NaWas has been in operation, providing connected members with automated 24/7 DDoS attack mitigation. Through the combination of capacity, technology, knowledge, and expertise, the NaWas effectively combats DDoS attacks. It achieves this by separating contaminated and clean internet traffic and routing the clean traffic to members via a separate VLAN. By neutralizing DDoS attacks, the NaWas ensures the continued availability of systems and services for its members.

Building on the initial experiences, cyber security researchers worked together to create a European "Cookbook" on DDOS attack mitigation. This document describes the concept of Anti-DDoS Coalitions and the DDoS Clearing House, a platform used for sharing measurements of DDoS (meta) data between organizations. By sharing data and expertise of DDoS attacks, organizations broaden their view of the DDoS landscape to an ecosystem wide one, which enables a more proactive and collaborative stance in fighting DDoS attacks.

The initial experiences with setting up and running such a Coalition in The Netherlands brought a number of lessons that are reflected in the Cookbook:

- The first lesson learned is that the problem of collaborative DDoS mitigation is much more organizationally rooted than technically. Therefore, a solid governance model is paramount to the success of an anti-DDoS coalition. The membership-based structure of the Dutch national anti-DDoS coalition has proven to be effective in this regard. Membership fees ensure (to an extent) participation in the coalition's activities and reduce freeloaders.

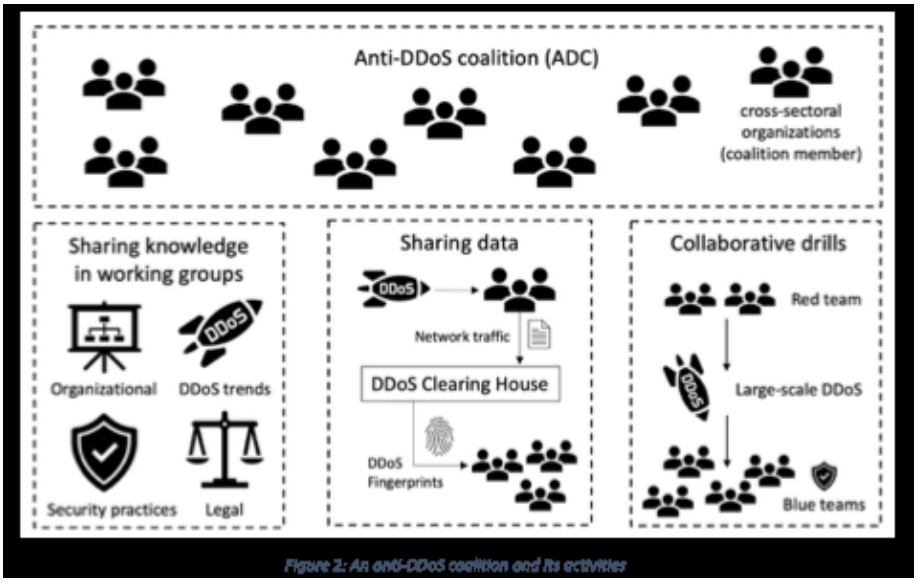


Fig.9 – Example of an Anti-DDoS Coalition and its activities (see Cookbook)

- Second lesson is the importance to follow changes in the market. Over the last years, a shift in DDoS mitigation strategies took place. Organizations move from mostly on-premises DDoS mitigation to fully outsourcing their DDoS mitigation.
- Third lesson learned, touching upon the development of the technical system, is the benefit of a modular approach and well-defined interfaces for the DDoS Clearing House. It allowed to develop the various system components separately from each other, without the need to use the entire system. This allowed us to develop the system's components in parallel, while having only agreed on the interfacing between the components. As a result, we were able to develop the software in a demo-driven way,
- Fourth and final lesson learned is that forming coalitions around a specific topic – such as Anti-DDoS Coalitions – is useful not only to improve collaboration on that specific topic but also because it grows and further interconnects the network formed by all organizations and people, which communicate on many more topics concerning cybersecurity.

It is important to set up a proactive and collaborative DDoS mitigation strategy, ideally before DDoS attacks have been causing damage. 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. The information consists of a digest of the DDoS traffic that a critical service provider needs to handle (a so-called "DDoS fingerprint").

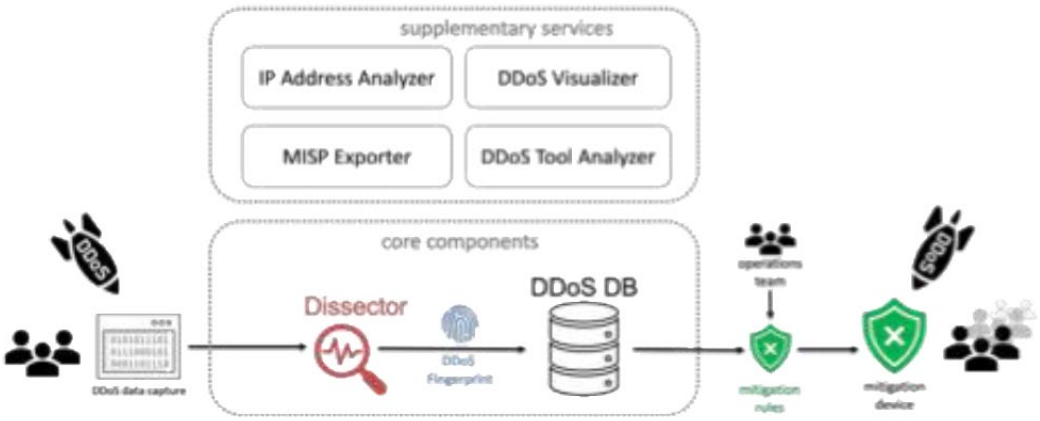


Fig.10 – DDOS Clearing House schematic overview

Sharing of fingerprints provides an additional layer of Internet security on top of to the (commercial) DDoS scrubbing services that service providers need to use as well, which separate DDoS traffic from benign traffic.

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.

## IoT security

An important point of attention in ensuring future security of the Internet is focusing on securing the advancing deployment of the Internet of Things – again a network of networks, and an increasing role for autonomous operations within a wider context.

Ihita Gangavarapu (Indian IoT security researcher from the International Institute of Information Technology, Hyderabad (IIT-H) provided a short intro about the penetration and potential of IoT, and with a specific focus on security aspects to be taken into account. Maarten Botterman (IGF DC IoT) complemented this by sharing some insights from the most recent deliberations of the Internet Governance Forum's Dynamic Coalition on the Internet of Things.

Ihita mainly focused on the IoT security challenges, the various efforts from multiple standardization bodies including recent developments in India and the focus areas going forward. She explained that the domain of IoT security is a complex space with developments happening regularly. In addition to shortage of IoT security experts, she highlighted the following challenges with securing IoT devices:

- Resource constrained devices: Constraints in terms of processing capability, memory, energy
- Heterogeneity and complexity of ecosystem: Encompassing diverse devices, communication protocols, and applications, present formidable challenges for establishing uniform security measures
- Vast attack surface: The sheer number and diverse types of interconnected devices, each with its own set of functionalities and potential vulnerabilities adds to this.
- Expectation of low cost: Users and manufacturers tend to prioritise operational and functional requirements over security.
- Fragmentation of standards and regulations: Gaps in standardisation not only hampers interoperability yet creates loopholes that malicious actors can exploit

Initial standardization and regulation efforts at global level include Here are some global developments in the standardisation and regulation space.

- ITU-T SG17/20;
- ISO/IEC 27400:2022;
- ENISA Baseline security recommendations for IoT;
- ETSI 303 645;
- GSMA IoT Security Guidelines and Assessment;
- oneM2M TS-0003;

Interoperability of IoT applications is key for many applications. This led to exploring and implementing the oneM2M Standard for many M2M/IoT solutions. The technical specifications created by multiple standardisation bodies including TSDSI from India came up with a horizontal common service layer for ensuring interoperability between a number of use cases of IoT. The TS-0003 document of oneM2M has various security methods and mechanisms such as for access control policies and dynamic authorisation. IIIT Hyderabad has been using the implementation of oneM2M standard called OM2M for their various smart city applications such as air pollution monitoring, water quality monitoring and energy monitoring.

Within the Indian context, the following efforts are made towards adoption of IoT/M2M security standards,

- Adoption of oneM2M as national standard for M2M/IoT;
- MTCT(Mandatory testing and certification of telecom equipment) framework: Development of ITSARs by NCCS;
- TEC Security by Design for IoT device manufacturers 2023;
- National Trust Center for IoT: certification of M2M devices and applications (hardware and software);

The need for labeling and certification is also recognized, as to ensure users are more aware of the security status and requirements when deploying IoT. Examples include

- Cyber Security Agency of Singapore (CSA)
- NIST: Minimum requirements and desirable attributes

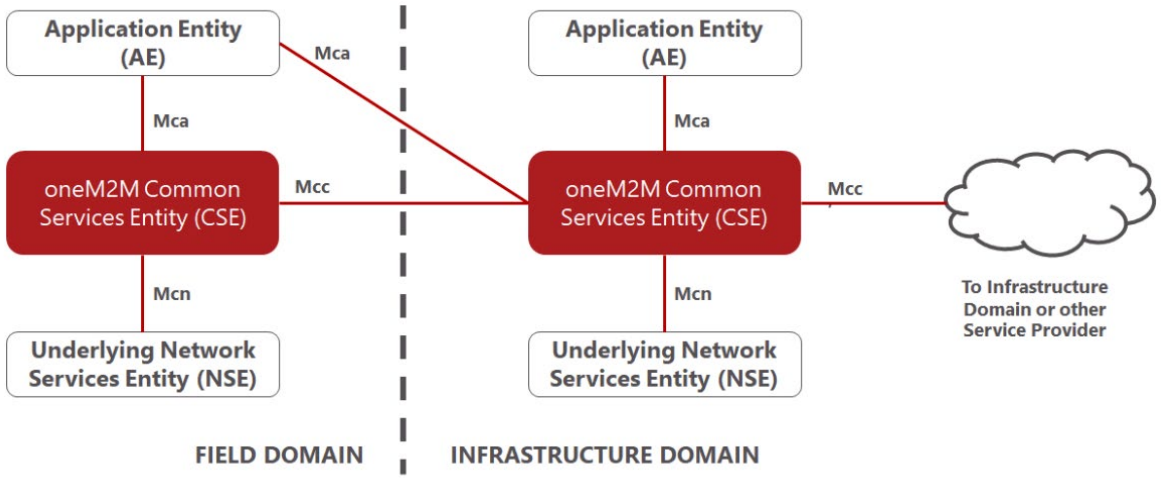


Fig 11: Separation of Nodes into the "Field Domain" and the "Infrastructure Domain"

Therefore, Ihita suggests that the following two areas in particular require attention from a implementation perspective for securing the IoT ecosystem going forward:

1. Exploring implementations of the oneM2M standard for IoT applications
2. How to go about the implementation of the labelling scheme in India?

Maarten Botterman adds that this is not a solely Indian problem, yet very much a global challenge, as we are still far away from global norms in this – something that would be important because many IoT devices are developed around the world, and deployed in different regions of the world. During a recent panel discussion at the APrIGF the need for labeling and certification was very much underpinned recognizing that currently users get confronted with many different devices without any guidance on their vulnerabilities. User guides mostly don't include good practice instructions. And today's labeling and certification activities, taking place in different countries around the world are so far mostly developed in isolation, with the exception of the oneM2M initiative, and first explorations for standards through IEEE and the IETF.

India's stakeholders are encouraged to pay both attention to good practice in implementation within India as in development of standards for interoperability, labeling and certification at the global level.

## Universal Acceptance and IDN status overview for India

Anil Jain (Chair of the Universal Acceptance Study Group UASG) explained the importance of improving Universal Acceptance to new Domain Names and internationalized scripts for Domain names and email. He presented the Call to Action for the upcoming year, as expressed by the UASG. The Action Plan calls:

**For Businesses:**

* Organize internally your business' systems to be compliant with UA standards;
* Update your own IT systems to be UA-ready. See UASG026 UA-Readiness Framework, UASG004 test cases, free code samples, and EAI Self-Certification Guide;

**For Governments:**

* Evaluate the possibility of including UA requirements in procurements;
* Coordinate with your national ccTLD managers and ICANN Governmental Advisory Committee (GAC) delegates to participate in and strengthen UA-related actions;

**For Academia:**

* Upgrade email systems to support EAI;
* Update IT curricula to include teaching and learning of UA and software internationalization-related concepts.

India is a leading country in adoption of Internationalized script. Currently, India has 15 IDN ccTLDs (.bharat) available, covering 22 Indian languages representing 11 scripts. As per the reports of the Universal Acceptance Study Group (UASG), the global Email address internationalization (EAI) acceptance rate is currently close to 8%, and India's EAI acceptance rate is around 11%.
The Government has formed a committee to work on "Multilingual Internet", following a published roadmap to universal acceptance and a multilingual Internet. Specific projects include progressing:

- Raj mail
- IDN domain & email to "Mera Gaon Meri Dharohar".
- IDN domain & emails to MSME – Registrations

The objective is to achieve "Universal Acceptance" (UA) leading to acceptance of Internationalized Domain Names (IDNs) equally by all Internet-enabled applications, devices, and systems – irrespective of the script used.

Ultimately, catalyzing the multilingual and inclusive Internet will help bring the next billion users online, of which 500 million in India, and empower the use of local language identities– in particular those that are non-English.

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

During this block, Maarten drew attention to the conclusions of the previous September 2022 Hyderabad GFCE Triple-I meeting, where it was generally agreed that Standards matter and incentives are needed to move the needle, as the cost goes before the benefit. In all this, awareness is Key. The discussion in 2022 resulted in the following two proposed actions:

1. work towards deployment of the compliance testing tool in India.
2. develop an Action Plan for Raising Awareness of Security Standards for the purpose of enhancing justified trust in the use of the Internet in the region.

Recognizing that policy and legal measures already exist, Amitabh Singhal had suggested to take the following steps:

1- Bring all stakeholders on a common platform;
2- Initiate & Ramp up Conversations and Awareness;
3- Maintain & operate the Common Platform;
4- Setting up an Indian platform for checking on the state of protection of websites and mail servers, and advising & implementing security protocols, wherever found missing;
5- Conduct regular Online and Offline campaigns - Build a Roadmap with Yearly Plans, programs & tasks.

Amitabh Singhal has since then worked with Anand Raje and Satish Babu and Maarten Botterman on this, resulting in the following Project Plan, hereinafter referred to as the Trusted India Internet Initiative (the T3I Project) which was unveiled and presented at this session.


Fig 12 – Announcing the aim to set up a "Trusted India Internet Initiative"

**Project T3I's** aims to set up an Online Tool/System/Indexation Mechanism, comprising a series of websites, links, UIs and APIs for Diagnosing the Security Postures of websites, Apps, Services, Content and promoting thereto, the Adoption and Use of State-of-the-Art Internet Security Standards throughout the Cyberspace/elsewhere, so as to Enhance Justified Trust in the use of the Internet.

**Project T3I Deliverables include:**

(i) The Project will Provision a Sophisticated Near Real Time, Multilingual capable, Testing, Measuring, Analysis and Reporting platform/Portal, namely Trusted Internet Internet Initiative (TIII), to Assess, Diagnose and Report the Vulnerabilities, Security & Safety status of all/most content, applications and services on the Internet,
(ii) To guide and encourage providers of content on the Internet to implement and keep their services updated with all essential security standards and protocols and
(iii) Eventually Build an Internet Trust Maturity Index, for Internet Users and all legitimate stakeholders to gauge and rely on the Trustworthiness Scores/Safety Grades of sites, services and applications.

*Towards further developing the Project T3I, the Team is reaching out to potential financial collaborators/contributors and look forward to connecting to others that are willing to help make this happen. Please contact Amitabh Singhal, Satish Babu or Anand Raje if you or your organization wants to collaborate and support the Project T3I.*

*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.*

# Annex I – Initial Terms of Reference for an Action Plan for Raising Awareness on Security Standards (RPKI, DANES, TLS, STARTTLS, DMARC, DNSSEC, MANRS, etc.)

Based on the discussions, a number of people are planning to take forward an awareness raising activity, both informing stakeholders about the need to adopt security standards and providing assistance in doing so, effectively. An initial plan will be developed and (co-)funding will be sought. Contributions are welcome.

Initiator/coordinator: Amitabh Singhal

## A. Trust Issue runs Deep:

**(i) Cybercrime victim India among top five victims of cybercrime: FBI report**

**May 30, 2022 - Updated 08:24 pm IST...**Among the complaints received, ransomware, business e-mail compromise schemes, and the criminal use of cryptocurrency were among the top incidents reported (BusinessLine News Report).

**(ii) Phishing/Vishing/ Smishing/Pharming** was the top crime type with 323,972 reports received in 2021. It was followed by Non-Payment/Non-Delivery, Personal Data Breach, Identity Theft and Extortion with 82,478, 51,829, 51,629 and 39,360 reports received, respectively (Hindu Businessline Report).

**(iii) 5 of the top cybercrimes affecting businesses and individuals in 2022:**

- Phishing Scams.
- Website Spoofing.
- Ransomware.
- Malware.
- IoT Hacking

**(iv) 87% of Organizations suffer DNS Attacks:** Zero-day attack. The attacker exploits a previously unknown vulnerability in the DNS protocol stack or DNS server software.

- Cache poisoning. ...
- Denial of service (DOS). ...
- Distributed Denial of Service (DDoS). ...
- DNS amplification. ...
- Fast-flux DNS.

**B. Need for Safer Internet is a necessity - Potential STEPS**

1. Bringing all stakeholders on a common platform;
2. Initiating & Ramping up Conversations and Awareness;
3. Maintaining & operating the Common Platform;
4. Setting up an Indian platform for checking on the state of protection of websites and mailservers, and advising & implementing security protocols, wherever found missing;
5. Regular Online and Offline campaigns - Build a Roadmap with Yearly Plans, programs & tasks.

**C. Some Operational Methods:**

1. Live Measure, Monitor, Analyze traffic and Develop Database of Breaches/Incidents (e.g. use and further develop Platforms like AIORI, etc.);
2. Investigate & Pinpoint the security gaps - technical/human;
3. Provide an online platform that stakeholders can use to check the state of protection;
4. Recommend Appropriate Steps to concerned stakeholders (operators, pvt/public orgs,

**D. Policy & Legal Measures Exists:**

India already has policies and laws to recognize and report breaches

1. Harmonization between current policies/laws and actual practices needed.
2. Propagate voluntary Enforcement of mitigating actions/ramping up security protocols or via regulatory actions where/if needed.

**E. Stakeholders:**

1. Telecom Operators
2. ISPs
3. Data Center/Cloud Service providers
4. E-Commerce Platforms - Both govt and private sector
5. Domain Registries & Registrars/DNS Service providers
6. CDN operators
7. Govt, Public sector and private Enterprises
8. LEA entities at both Central and State levels
9. Security/threat mitigation service providers
10. Central Govt and State Govt Ministries and Departments (MeITY, CERT-IN, Deptt of Telecom, State TERM Cells), etc.
11. IXP operators
12. Any other

# ANNEX II – Workshop Agenda

GFCE Triple-I workshop

Day Zero INSIG2023, India Institute of Technology, Guwahati, India, 28 September 2023

***Agenda***

***09:00 Opening by Host and Moderator: Welcome and intent of the day***

Welcome address by Satish Babu, India School for Internet Governance
Introduction to the day by the GFCE Triple-I coordinator, Maarten Botterman
Special address by Prof Sukumar Nandi, Senior Professor, Department of Computer Science & Engineering, India Institute of Technology Guwahati

***09:30 Block I: Better Use of Today's Open Internet Standards:***

Moderated discussion about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF and IPv6 (with invited experts [to be named] in the room to inform participants). These standards are also discussed in the GFCE Triple-I Handbook, which is available at [website address], and technical tests for the state of implementation are available at www.internet.nl.

Section 1: DNSSEC, TLS and DANE: Yazid Akanho and Jia Rong Low (ICANN)
Section 2: RPKI and ROA: APNIC – Terry Sweetser (APNIC)
Section 3: DMARC, DKIM, SPF – Gerasim Hovhannisyan (EasyDMARC)
Section 4: IPv6: Anurag Bhatia (Hurricane Electric)
section 5: Current status of adoption based on internet.nl measuring: and on the plans to set up on Indian site for measuring adoption levels of modern Internet standards: Anand Raje

11:00 Coffee/Tea

***11:15 Block II part 1: Inspiration from Good Practice Actions***

(We foresee a number of other good practices from the region, and beyond, to be presented during this "Block II", with a mix of international and regional speakers. This information will be updated as soon as we know.)

a- Internet Resilience Index: providing a snapshot of a country's Internet resilience in terms of infrastructure, performance, security, and market readiness.: Sarah Lake (ISOC)
b- MANRS: rationale, development and deployment in India: Anand Raje (MANRS Ambassador)
c- KINDNS: rationale, development and deployment in India: Yazid Akanho and Jia Rong Low (ICANN)

12:30 Lunch

***13:30 Block II part 2: Inspiration from Good Practice Actions***

d- DDOS mitigation: more about a European “cookbook” on DDOS attack mitigation (see https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf), Octavia de Weerdt, NBIP (https://www.nbip.nl/en/).

e- IoT security short intro about the penetration and potential of IoT, and with a specific focus on security aspects to be taken into account: Maarten Botterman (IGF DC IoT) and Ihita Gangavarapu (Indian IoT security researcher International Institute of Information Technology)

f- UA/IDN status overview for India – where is it, and what’s next. How can stakeholders help: Jia-Rong Low (ICANN), Anil Jain (NIXI/UASG)

15:00 Tea

***15:15 Block III: Planning for a More Trusted Internet: Marketplace for Action***

Facilitated brainstorm, based on the input discussed over the day, and an introduction on a possible way forward leveraging the “justified trust in the use of the Internet and email” throughout India, with some suggestions by Amitabh Singhal.

16:45 Conclusions and Closing Remarks

***17:00 Ends***