GFCE Triple-I Day @InSIG2024,
30 September 2024, IIM Bangalore, India

Progressing improving justified trust in the use of the Internet in India, together

Report by Maarten Botterman

Summary

On Monday 30 September 2024, hosted by the India School for Internet Governance and the Indian Institute for Management Bangalore, MEITY Joint Secretary Sushil Pal opened the 5th GFCE Triple-I workshop in India. The workshop was initiated by the Global Forum for Cyber Expertise (GFCE) in close collaboration with Indian Chapters of ISOC, and received knowledge support from APNIC, ICANN, EasyDMARC, Hurricane Electric, Internet Society (ISOC), and the Global Cyber Alliance.

Purpose

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.

Discussion

This specific workshop covered various aspects of internet security, including routing security, DNS security, and email security. It highlighted the need to maintain and enhance trust in the internet as new technologies like quantum computing and AI emerge. Speakers discussed the importance of proactive measures to address potential threats, such as implementing RPKI, DNSSEC, and DMARC, as well as the role of communities like MANRS and KINDNS in promoting best practices. The discussion also touched on the challenges of funding and sustaining community-driven initiatives, as well as the need for a collaborative, multi-stakeholder approach involving governments, industry, and civil society. In addition there was a panel focused on the impact and opportunities of emerging technologies such as quantum computing and AI. The day concluded with discussions around a proposed "Trusted India Internet Initiative" (T3i) project, which aims to provide a platform for testing and monitoring the security of websites and online services in India, as well as raising awareness and building capacity throughout India’s regions.

Participation

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 enhance justified trust in an open end-to-end Internet. The meeting was set up as a hybrid meeting and included online participants, with a total participation of about 40 people.

On behalf of GFCE Triple-I, thanks to everyone who helped make this happen, and with special thanks to MEITY Joint Secretary Sushil Pal, InSIG coordinator Satish Babu, T3i coordinator Amitabh Singhal, and Anand Raje for their support from the outset to help make this workshop happen.

Opening Session

Sushil Pal, MEITY’s Joint Secretary responsible for cyber, AI , delivered the inaugural speech at the GFCE Triple-I Workshop, emphasizing India’s commitment to a cyber-resilient future. With over 940 million internet users, he highlighted the immense opportunities of digital growth alongside significant cybersecurity challenges.

India has achieved Tier 1 status in the 2024 Global Cybersecurity Index, scoring 98.49/100, showcasing leadership in legal, technical, and organizational cybersecurity measures. Notable initiatives include the **Information Technology Act (2000)** and the **Digital Personal Data Protection Act (2023)**, alongside efforts to safeguard critical infrastructure and combat threats like phishing and cyberterrorism. Agencies like CERT-In and NCIIPC ensure infrastructure protection, while capacity-building programs have trained over 3.8 lakh individuals to date.

Pal highlighted global collaborations, including India’s role in drafting the UN Convention against Cybercrime and partnerships with G20 and ITU, reinforcing a rules-based order in cyberspace. On the domestic front, efforts such as NIXI’s DNS abuse mitigation and innovative tools like M-Kavach 2 showcase India’s focus on securing its digital ecosystem.

He stressed India’s active participation in shaping the **Global Digital Compact**, ensuring innovation, regulation, and inclusivity for a sustainable cyberspace. In closing, Pal reaffirmed India’s commitment to fostering secure digital growth through strategic global partnerships and robust national policies.

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 Indian 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 and awareness raising throughout India is key. Based on the earlier workshops in India, and action plan (T3i) has been proposed that should find Indian support, both in terms of funding and volunteers, as to leverage the insights throughout India. The day is set up to further our understanding of the current situation in India in the light of global and local developments and gain more support for the T3i initiative that is set up to support Digital India.

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.

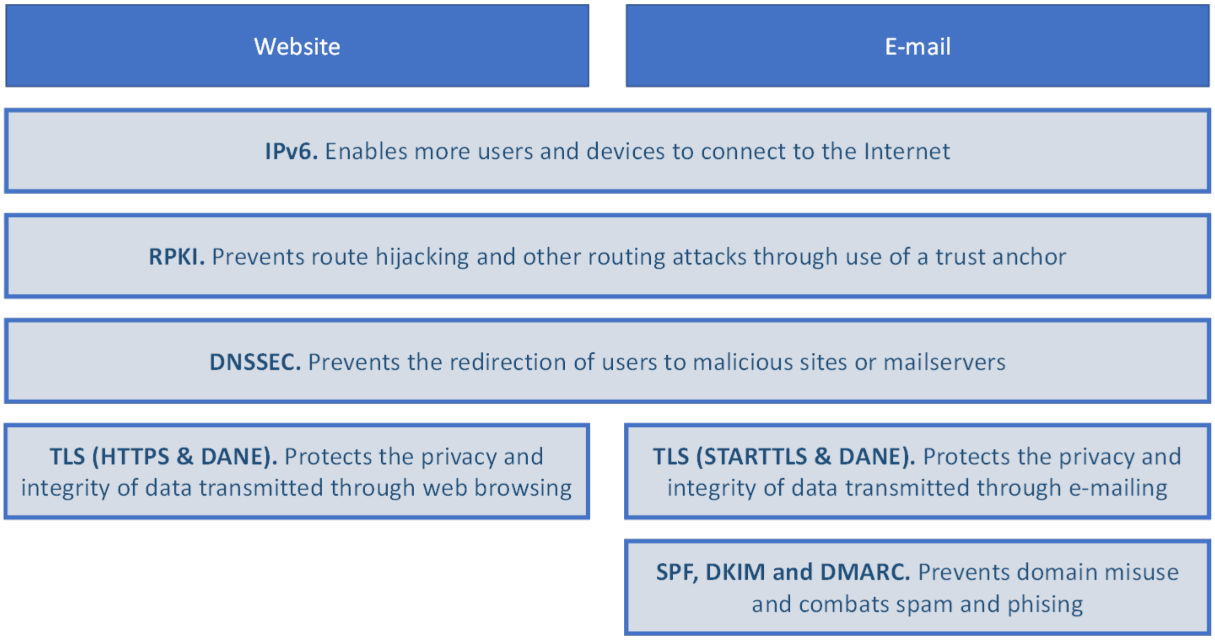

Website
E-mail
IPv6. Enables more users and devices to connect to the Internet
RPKI. Prevents route hijacking and other routing attacks through use of a trust anchor
DNSSEC. Prevents the redirection of users to malicious sites or mailservers
TLS (HTTPS & DANE). Protects the privacy and integrity of data transmitted through web browsing
TLS (STARTTLS & DANE). Protects the privacy and integrity of data transmitted through e-mailing
SPF, DKIM and DMARC. Prevents domain misuse and combats spam and phising

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.

Routing security: RPKI and ROA

David Phelan, network engineer and trainer at APNIC, presented an overview of Resource Public Key Infrastructure (RPKI) and its role in securing internet routing. RPKI is a security framework designed to protect the Border Gateway Protocol (BGP), which is used for routing data across the internet. Initially, BGP was created for a small, trusted internet where network operators knew each other, and security wasn’t a major concern. However, as the internet grew, BGP became vulnerable to attacks and misconfigurations, such as route hijacking and leaks.

One notable example of such an incident was the MyEtherWallet Hijack, where attackers hijacked Amazon's DNS service through incorrect BGP announcements and stole millions of dollars in cryptocurrency. Another example was a mistake made by Pakistan Telecom, where a technician misconfigured a filter to block YouTube, accidentally announcing Google’s IP addresses and redirecting traffic inappropriately.

RPKI addresses these issues by using public key cryptography, similar to what is used for TLS, to digitally sign route announcements. This ensures that only authorized networks (Autonomous System Numbers or ASNs) can announce specific IP prefixes.

The system involves a set of trust anchors—self-signed certificates from the five regional internet registries (APNIC, ARIN, AFRINIC, LACNIC, and RIPE NCC)—which verify the legitimacy of route announcements. Each route is associated with a Route Origin Authorization (ROA), a certificate that links an ASN to an IP prefix.

When a BGP router receives a route announcement, it can validate whether the route is authorized by checking the ROA data. This is done through the RPKI-to-Router Protocol (RTR), which reduces the cryptographic workload on routers by handling the heavy lifting externally. The router simply checks the validity of the route based on the ROA and takes appropriate action. The industry standard is now to drop invalid routes, rather than just lowering their priority.

David also emphasized the importance of proper route filtering as a best practice for network security. It's recommended to filter routes at the network's edges (both ingress and egress), but not in the core of the network. Filtering should be done at points where traffic enters or leaves the network to ensure that invalid or unauthorized traffic does not pass through.

While RPKI is an important tool for improving internet security, there are still challenges. One such challenge is the development of ASPA (Autonomous System Provider Authorization), which aims to validate the path between ASNs. This feature is still in progress and not yet widely supported by router vendors. Another challenge is BGPsec, an extension to BGP that would add security by signing route announcements with individual router keys. Although this would make the system more secure, it introduces complex key management issues and has not been widely adopted due to the scale and complexity of managing many router keys.

David also discussed global adoption trends. India is making significant progress, with about 76% of route origin authorizations (ROAs) signed. However, route origin validation (ROV) in India is still very low, with less than 1% of routes being validated. Globally, some regions like China and parts of Africa are lagging behind in adopting RPKI, while other regions like Australia benefit from indirect validation due to large upstream providers that perform route filtering, even though smaller networks may not be actively implementing RPKI.

In conclusion, while RPKI is essential for securing internet routing, its global adoption is still uneven. David emphasized that network operators should take responsibility for their own routing security by implementing proper filtering practices and adopting RPKI where possible. Although there are ongoing developments like ASPA and BGPsec, RPKI remains one of the most effective tools for improving the security of BGP-based routing.

Domain name security: DNSSEC, TLS and DANE

Champika Wijayatunga focused on several key topics, including DNSSEC (DNS Security Extensions), DNS over TLS, and DANE (DNS-based Authentication of Named Entities). The primary concern addressed was the protection of DNS data, which is publicly available and includes domain names, IP addresses, mail servers, and other essential information. This information needs to be secured to prevent issues like cache poisoning and DNS hijacking.

DNSSEC is designed to protect DNS data by ensuring authenticity and integrity. It helps prevent attacks such as cache poisoning, where DNS data is maliciously altered. DNSSEC achieves this by using digital signatures to ensure that the data received by clients has not been tampered with and originates from the legitimate source. However, DNSSEC does **not** provide encryption or privacy of DNS data. If privacy is needed, protocols like DNS over HTTPS (DoH) or DNS over TLS (DoT) should be used.

A major challenge to widespread DNSSEC adoption is that many large enterprises, especially social media platforms, are concerned about operational risks. For example, DNSSEC signatures have expiration dates, and if an administrator forgets to update them, clients may receive a "server fail" message, disrupting their access to websites. This issue could lead to customer complaints directed at ISPs, not the domain holders who are at fault for not renewing the signatures.

Despite these challenges, there are solutions in place for operators to temporarily disable validation or exclude certain domains from validation if problems arise. Educating operators about these solutions is key to improving adoption.

DNSSEC Deployment and Global Trends

Globally, over 90% of generic top-level domains (gTLDs) have deployed DNSSEC, with country code top-level domains (ccTLDs) lagging behind at around 66%. Among the 16 ccTLDs in India, all have successfully implemented DNSSEC, with many using strong algorithms like RSA-SHA256, although some operators are considering transitioning to newer algorithms like elliptic curve cryptography (ECDSA).

India has made significant progress in DNSSEC adoption, with around 60% of DNS queries being validated by DNSSEC-enabled resolvers, well above the global average of 33%. However, there is still room for improvement in both India and globally, as more operators and organizations need to enable DNSSEC validation.

DANE and TLS Integration

DANE (DNS-based Authentication of Named Entities) was introduced to address concerns about the trustworthiness of TLS (Transport Layer Security) certificates. DNSSEC is used to store and sign information about TLS certificates and certificate authorities, ensuring the integrity and authenticity of the certificates. While TLS provides encryption, DNSSEC enhances security by preventing certificate impersonation and validating the authenticity of certificates during the TLS handshake.

By combining DNSSEC and TLS, the system achieves both encryption and strong integrity protection for data exchanges between clients and servers.

Practical Challenges and Moving Forward

A key challenge in the adoption of DNSSEC, especially in large enterprises, is the fear of operational disruption. Some domain holders worry about mistakes leading to service interruptions, as expired DNSSEC signatures could prevent resolvers from validating DNS responses. This concern is especially prevalent among large enterprises, where the stakes are higher.

To overcome this, Champika emphasized that managers need to be proactive, ensuring that DNSSEC validation is enabled and that solutions are in place to address potential problems quickly. Furthermore, the upcoming key rollover event in 2026 will require operators to ensure their resolvers are updated to validate the new root keys. Pre-publication of these new keys in January 2025 will give operators time to prepare, avoiding disruptions during the actual rollover.

In response to Maarten Botterman’s question about India’s 60% DNSSEC validation rate, Champika explained that while the validation rate in India is above global and regional averages, there are still hurdles to achieving wider adoption. One of the major concerns is the operational risk, particularly for large organizations that worry about the consequences of an expired DNSSEC signature. In such cases, users may experience access failures, and the ISP would bear the brunt of customer complaints. However, with proper management and contingency measures, such issues can be mitigated. Champika also highlighted that progress is ongoing, and operators need to be encouraged to embrace DNSSEC validation. The upcoming key rollover in 2026 offers a new opportunity for operators to enhance their readiness and improve DNSSEC validation.

In conclusion, DNSSEC is a vital tool in securing the integrity and authenticity of DNS data, and while significant progress has been made globally and in India, there is still work to be done to increase adoption. Through a combination of education, *proactive management, and technical solutions, DNSSEC validation rates can continue to grow. Moreover, DNSSEC's integration with TLS through DANE provides enhanced security, ensuring the authenticity and integrity of encrypted communications.*

Email Security: DMARC, DKIM, SPF

Hovsep Najarian, a systems engineer at EasyDMARC, provided an insightful presentation on the importance and implementation of email security standards—specifically DMARC, SPF, and DKIM. The core focus of the presentation was on the necessity of securing email systems against common threats like phishing, spoofing, and invoice fraud, which make email a prime target for attackers.

Najarian began by highlighting that email remains one of the most common attack vectors due to its ease of use and low cost. Common email-based threats include phishing, spoofing, and business email compromise (BEC), which are used to manipulate recipients into disclosing sensitive information or making fraudulent transactions.

The presentation covered three key email security standards: SPF, DKIM, and DMARC.

1. **SPF (Sender Policy Framework):** Introduced in 2003, SPF helps to authenticate the servers sending emails on behalf of a domain. It works by checking DNS records that list the IP addresses or domains allowed to send emails for a particular domain.
2. **DKIM (DomainKeys Identified Mail):** DKIM uses asymmetric cryptography to sign email content, ensuring that the email has not been altered during transit. This involves adding a DKIM signature to the email header, which is verified by the recipient's server using a public key stored in the DNS records.
3. **DMARC (Domain-based Message Authentication, Reporting & Conformance):** DMARC builds on SPF and DKIM by adding an alignment mechanism to ensure that both SPF and DKIM records are properly aligned with the "From" header of the email. DMARC also provides policies for how to handle emails that fail SPF or DKIM checks (none, quarantine, or reject) and sends reports to domain owners to help monitor and improve email security.

SPF records are DNS records that list authorized IP addresses or domains for sending emails on behalf of a domain. One important feature is the "include" mechanism, where third-party email service providers (ESPs) like Google Workspace handle the SPF configuration automatically, preventing domain owners from having to update their SPF records frequently.

DKIM ensures email integrity by using public and private key pairs. The email’s content is signed using a private key, and the recipient uses a corresponding public key to verify the signature. DKIM helps ensure that the email has not been altered during transit.

DMARC serves as a layer on top of SPF and DKIM by enforcing alignment between the "From" address and the domains used in SPF and DKIM. This alignment helps ensure that the email actually came from the claimed sender, reducing spoofing and phishing attempts. DMARC also allows domain owners to set policies to manage emails that fail SPF or DKIM checks:

- **None:** No action is taken, but reports are generated to help the administrator analyze email authentication issues.
- **Quarantine:** Emails failing DMARC checks are placed in the recipient's spam or junk folder.
- **Reject:** Emails failing DMARC checks are outright rejected by the recipient's mail server.

DMARC provides XML-based reports to domain administrators, allowing them to monitor the performance of their email security protocols. These reports provide insights into how many emails pass or fail SPF and DKIM checks, which helps administrators fine-tune their configurations. It's recommended to start with a "none" policy to monitor the email traffic and adjust configurations before enforcing stricter policies like "quarantine" or "reject."

Najarian concluded with several best practices for implementing DMARC:

- Always configure SPF and DKIM before deploying DMARC.
- Start with a "none" DMARC policy to gather data before enforcing stricter policies.
- Once SPF, DKIM, and DMARC are properly configured, transition to enforcing policies for better security.
- Organizations with multiple domains, especially parked or look-alike domains, should implement DMARC with a "reject" policy to prevent misuse of those domains for phishing.

Overall, the session emphasized that while SPF and DKIM provide valuable authentication and integrity checks, it’s DMARC that ties everything together, allowing domain owners to enforce policies and protect their domains from malicious email activity.

Maarten Botterman thanked Hovsep for his excellent presentation. He highlighted the progress from SPF to DMARC and emphasized the importance of a measured *approach in deploying these email security protocols, starting with observation and moving toward enforcement.*

IPv6

In this presentation, Maarten Botterman introduces **Anurag Bhatia**, an expert on IPv6, to discuss the global transition from IPv4 to IPv6. Anurag begins by highlighting the current state of IPv6 adoption, particularly in India, where mobile operators like Jio, Airtel, and Vodafone have made significant strides in transitioning to IPv6.

Many Indian users, especially those on mobile networks, are already using IPv6 without realizing it. Jio, for example, has even switched to an IPv6-only network for its 5G users. This shift is driven by the need to address the exhaustion of IPv4 addresses, which has led to the widespread use of Network Address Translation (NAT). While NAT has allowed continued internet connectivity, it introduces limitations such as performance degradation and challenges in maintaining end-to-end communication. IPv6, with its vastly larger address space, resolves these issues and is essential for supporting the growing number of connected devices.

Despite the progress made in mobile networks, IPv6 adoption remains slow in certain sectors, particularly among smaller fixed-line ISPs and in enterprise networks. While mobile ISPs have clear incentives to deploy IPv6 due to high demand for IP addresses in densely populated areas, smaller ISPs, especially those serving businesses and enterprises, face greater resistance. As a result, many enterprises either do not deploy IPv6 or use it sparingly, resulting in little IPv6 traffic. Most enterprise networks are focused on accessing internal systems, many of which are not yet IPv6-ready.

Anurag also emphasizes the role of large global content providers like Google, Facebook, and Netflix in driving IPv6 adoption, as they have already adopted the protocol and their traffic constitutes a significant portion of global internet traffic. However, for the internet to continue growing and to avoid potential bottlenecks, further deployment of IPv6 is necessary across ISPs, servers, and websites.

The extent of IPv6 traffic in different environments can vary significantly. For example, traffic from mobile users to a website may be almost entirely IPv6, while traffic from fixed-line users may still rely heavily on IPv4. In some cases, IPv6 traffic can range from as low as 4% to as high as 90%, depending on the user base and network type.

While mobile networks are increasingly adopting IPv6, enterprise networks are lagging behind. Many enterprises see little incentive to transition to IPv6, especially since many internal applications and services are not yet compatible with the protocol. In contrast, retail ISPs have a strong incentive to move to IPv6 to reduce congestion on NAT gateways, which can improve performance and reduce overhead.

Anurag touches on the "Happy Eyeballs" mechanism, which ensures that devices can fall back to IPv4 if IPv6 is unavailable, preventing connectivity issues. However, this fallback has led some in the industry to believe that it has slowed broader IPv6 adoption, as users may not realize when IPv6 is not functioning properly.

Another point discussed is the complexity of IPv6 from an end-user perspective. IPv6 introduces several types of addresses, such as linked-local, site-local, and global addresses, which can be confusing. However, most end-users will not need to worry about these complexities, as ISPs typically handle IPv6 configuration automatically through mechanisms like auto-configuration or DHCPv6. IPv6 offers benefits for end-users, such as reducing CAPTCHA challenges, which often occur with shared IPv4 addresses in NAT scenarios. IPv6 provides more unique addresses and better security, making it easier to differentiate between users and reduce issues like CAPTCHA verification.

Finally, Anurag addresses the challenges of transitioning to IPv6. Many websites still do not support IPv6, so ISPs often use a dual-stack approach, running both IPv4 and IPv6 on their networks. While this approach can be complex and costly, some large ISPs, like Reliance Jio, have opted for an IPv6-only core network, using translation mechanisms to handle IPv4 traffic when necessary. This approach simplifies the network's operation by reducing the need for dual-stack configurations.

In conclusion, while IPv6 adoption is progressing rapidly, particularly in mobile networks, challenges remain in the enterprise and commercial sectors. Overcoming these challenges requires addressing both technical obstacles and business considerations, encouraging enterprises to upgrade their systems, and ensuring that IPv6 deployment continues across the internet's infrastructure to support the growing demand for connected devices.

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

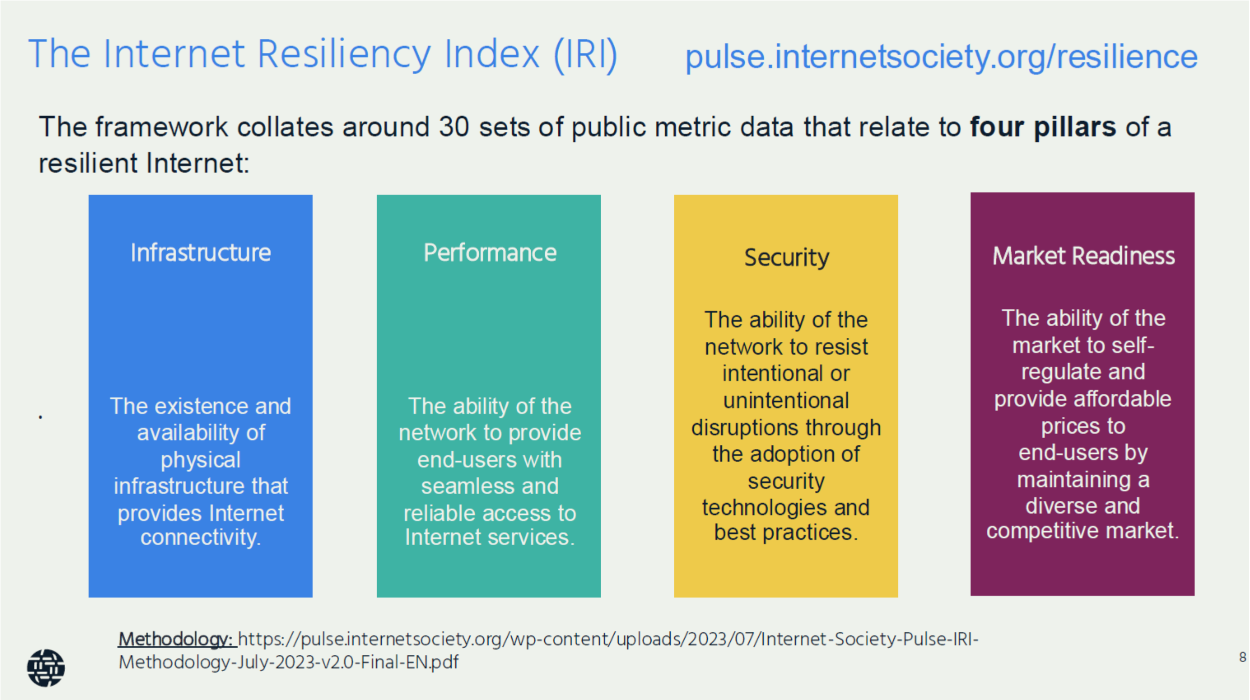
Maarten Botterman discusses the importance of internet standards and their evolution. He emphasizes that the internet was originally designed for functionality, not security, and over time, efforts have been made to enhance its security without disrupting its operation. He rejects the idea of starting over with new concepts, arguing that the internet will continue to evolve to meet growing expectations.

He also highlights the significance of global and regional efforts to improve internet security, noting the role of data in tracking progress. These data help assess the safety of the internet, identify what is implemented and what isn't, and gauge resilience by examining factors like internet providers and infrastructure, such as sea cables.

Next is Robbie Mitchell, who will explain the role of data in understanding internet resilience, followed by a discussion on KINDNS and MANRS—global communities that implement best practices for internet security.

Internet Resilience measuring

Robbie Mitchell from the Internet Society discusses the organization's efforts to improve internet resilience and health through data-driven decision-making through provision of data such as via the Internet Resilience Index (IRI),. The Internet Society, founded in 1992, advocates for an open, secure, and trustworthy internet. Their *Measuring the Internet* project, including the *Pulse* website, consolidates data from various trusted third-party sources to track global internet trends. This project helps organizations understand regional and global internet health and make informed decisions to improve resilience.
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.



The Internet Resiliency Index (IRI) pulse.internetsociety.org/resilience

The framework collates around 30 sets of public metric data that relate to **four pillars** of a resilient Internet:

Infrastructure

The existence and availability of physical infrastructure that provides Internet connectivity.

Performance

The ability of the network to provide end-users with seamless and reliable access to Internet services.

Security

The ability of the network to resist intentional or unintentional disruptions through the adoption of security technologies and best practices.

Market Readiness

The ability of the market to self-regulate and provide affordable prices to end-users by maintaining a diverse and competitive market.

Methodology: https://pulse.internetsociety.org/wp-content/uploads/2023/07/Internet-Society-Pulse-IRI-Methodology-July-2023-v2.0-Final-EN.pdf

8

Fig. 2 Internet resilience index (Internet Society)

Mitchell highlights the importance of measuring internet resilience, which the Internet Society tracks through an *Internet Resilience Index* covering 170 countries. The index evaluates four key pillars: infrastructure, performance, security, and market readiness, with a focus on ensuring countries can maintain internet connectivity during disruptions.

He provides an overview of India’s internet resilience, noting strengths like its security measures (e.g., IPv6 adoption) but also weaknesses in infrastructure and local content hosting. Mitchell also emphasizes the need for more localized data and open-source collaboration to improve resilience. India's internet market is highly concentrated, with a few providers handling the majority of the traffic, which can pose risks to resilience if one of these providers goes offline.

The Internet Society also promotes sustainable peering infrastructure and provides grants and resources to support local projects aimed at improving internet resilience, including those that address challenges during natural disasters. Mitchell concludes by stressing the importance of global cooperation to strengthen the internet and ensure its robustness across regions.

Anurag Bhatia from Hurricane Electric asks Robbie for clarification on the data about the top 1000 websites hosted in local data centers, specifically about non-

CDN-hosted sites. Robbie explains that while the data currently includes information about CDN-hosted websites, the Internet Society is working on incorporating more details about government websites and the DNS resilience of local services. Anurag also raises a point about the local data center numbers, with Robbie noting that the data depends on whether the data centers have updated their information on PeeringDB.

Maarten Botterman thanks Robbie Mitchell for his excellent presentation and for being transparent about some data challenges, particularly with HTTPS adoption in India. He acknowledges the Internet Society's ongoing efforts to improve data accuracy and encourages the sharing of any additional data or information to further build out the insights they provide. Maarten adds that the data from the Internet Society are empowering, especially for regions with limited internet data. He emphasizes the importance of continuously improving this data to support informed discussions and decisions about internet development. He encourages the audience to utilize these international data sources to help shape their strategies and make informed decisions about the future of the internet.

MANRS - Advancing Routing Security

In this segment, **Andrei Robachevsky** (Global Cyber Alliance) provides an in-depth explanation of the **MANRS** **(Mutually Agreed Norms for Routing Security)** initiative, which he describes as a collaborative effort to secure the global internet routing system. Currently hosted by the **Global Cyber Alliance (GCA)**, MANRS was originally launched 10 years ago by the Internet Society, and Andrei, who works at GCA, was one of the key individuals behind its creation. He outlines the importance of routing security and the challenges the internet faces due to vulnerabilities in the routing protocol that underpins the global internet infrastructure.

The internet is made up of about 76,000 independent networks, known as **autonomous systems (AS)**, each with its own "roadmap" for directing traffic. These systems share routing information with each other using the **Border Gateway Protocol (BGP)**. However, this system, created in 1989, was designed with scalability and resilience in mind but with little consideration for security. BGP assumes that networks are trustworthy and doesn't include built-in mechanisms for verifying the accuracy of routing information. As a result, it allows networks to send misleading or false routing information, which can cause traffic to be sent to the wrong destinations, leading to outages or, in some cases, malicious attacks.
One of the biggest threats to internet routing security is **BGP hijacking**, where one network falsely claims ownership of another network's routing information. A well-known example of this occurred in 2008, when **Pakistan Telecom** hijacked the

route for YouTube, causing a multi-hour outage for users across the globe. Another threat is **route leaks**, which occur when networks unintentionally announce incorrect routing information, causing traffic to be misdirected. Even small networks, sometimes located far from the affected sites, can cause major disruptions with a route leak. A notable incident took place in 2018 when a Nigerian ISP leaked **Google's** route, impacting its services globally.

In addition to these attacks, **IP spoofing** remains a serious concern. In this type of attack, a malicious actor can fake the source IP address of a packet, directing it to a victim’s IP address. This can then be used to amplify denial-of-service attacks, where the victim is flooded with massive amounts of traffic. Andrei highlights how, even though these vulnerabilities are well-known, the **BGP routing system** is constantly under attack, often from misconfigurations or deliberate malicious intent.

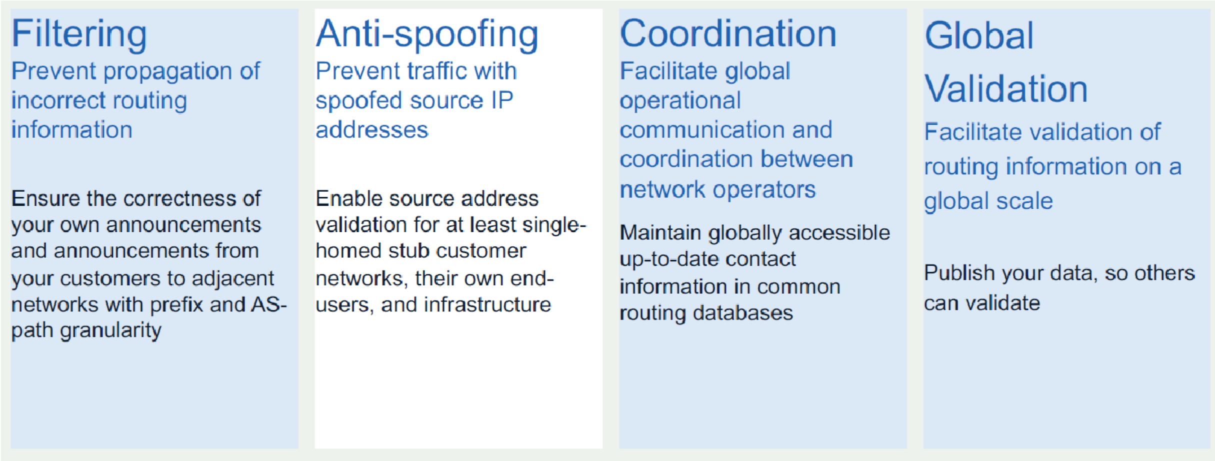
So, why is routing security still such a challenge? Andrei explains that the issue lies in what is known as the **collective action problem**. Although every network would benefit from a more secure routing system, no single entity can solve the problem alone. Effective security requires coordination and cooperation across the global internet community, which is complicated by different priorities, lack of resources, and the fact that one network's security depends on the actions of others. This means that even if one network implements the necessary security measures, it can still be vulnerable if other networks don't do the same.

Traditionally, **regulation** has been proposed as a solution, but Andrei points out that regulation doesn't work well for global systems like the internet. Due to the global nature of the internet and the interdependence of networks, regulations in one country or region often can't prevent attacks originating elsewhere. Additionally, regulation can lead to fragmented solutions that aren't universally effective. Therefore, the more promising approach to solving the problem is to make **security norms** widely accepted and easy to implement. These norms should not be overly complex or contentious but should provide a baseline that many networks can agree on and adopt.

This is where **MANRS** comes in. The initiative aims to address the routing security problem by establishing a **norm** that internet service providers and network operators can adopt. Rather than trying to enforce a single, rigid solution, MANRS sets out **minimum baseline actions** that networks should implement to help secure routing on the internet. These actions are designed to be achievable by most networks and focus on outcomes rather than overly technical details. Andrei explains that MANRS is not just a document but a **community** of networks committed to improving routing security. By encouraging network operators to implement these actions, MANRS is helping to foster a culture of cooperation and accountability.

When MANRS was first launched in 2014, it started with just nine network operators. Today, it has grown to include nearly 1,000 networks. Over time, MANRS has expanded its reach to include **Internet Exchange Points (IXPs)**, **Content Delivery Networks (CDNs)**, and **cloud providers**, all of which play a significant role in internet traffic routing. The idea behind involving these entities is that their influence can help encourage other networks to adopt MANRS' norms. MANRS also works with **network equipment vendors** to ensure that their products support the security measures required to implement the norms.

The initiative's **core actions** include four primary requirements:



Filtering
Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing
Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination
Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation
Facilitate validation of routing information on a global scale

Publish your data, so others can validate

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.

The significance of the **MANRS initiative** in promoting a collective approach to routing security is high. While the challenges are substantial, the collaborative efforts of the global internet community are helping to mitigate risks and improve the resilience of the internet. He stresses that with continued growth and adoption of these security norms, the routing system can become much more secure, ensuring a safer internet for everyone.

In this the **MANRS community** is key. It’s not just about promoting best practices but about creating a supportive community that genuinely adheres to these practices. MANRS has grown significantly over the years, and as of now, it counts over 1,200 participants spread across four distinct programs, making it a truly global initiative. One of the standout features of this growth is the local involvement, particularly seen in countries like Brazil. In collaboration with the **Network Information Center Brazil (nic.BR)**, MANRS has gained significant traction there through the Internet Safe program, which has helped raise awareness and encourage more Brazilian networks to join the community.

Robachevsky also underscores the role of **measurement and transparency** in building credibility for the initiative. MANRS has created the **MANRS Observatory**, a tool designed to track and demonstrate the commitment of its members. The tool is transparent and based on publicly accessible data, allowing anyone to verify the metrics. Unlike some approaches that require network cooperation for measurements, the Observatory works passively, meaning it can measure the status of all 76,000 networks in the global routing system without needing their active participation. it provides an overview of global routing security, displaying a variety of metrics, including the "MANRS readiness" of networks, which tracks how closely network operators are adhering to the four key MANRS actions.

Interestingly, Robachevsky points out that **India** performs better than the global average in terms of routing security. Indian networks, in general, are closer to MANRS standards than the global norm, though he emphasizes that there’s significant room for improvement, especially in terms of **anti-spoofing**. Anti-spoofing is a particularly challenging action to measure because it requires active testing within a network, which not all networks do.

Despite India’s strong performance, only four of the 2,700 networks in the country are currently part of the **MANRS program**. Robachevsky suggests that there is great potential for more Indian networks to join MANRS and, in doing so, help elevate the overall performance of India’s routing security. He presents a comparison showing that India's performance is already relatively close to MANRS standards, further highlighting the potential for growth.

To increase transparency, the **MANRS website** now displays not just the actions each participant is committed to, but also the **actual performance metrics**, showing whether the network is continuing to adhere to the commitments it made.

This approach adds accountability and highlights any gaps in adherence, offering both a form of positive recognition for committed participants and constructive pressure for those who may have lost focus on their routing security practices.

In the final part of his presentation, Andrei Robachevsky provided a brief overview of how to get involved with the **MANRS** initiative and highlighted the resources available to assist network operators in adopting best practices. He emphasized that **MANRS actions** focus on outcomes rather than specific implementation methods, and that the community has created practical **implementation guides** to help organizations adopt these practices, regardless of their network size or topology. These guides, which are available on the **MANRS website** and hosted on **GitHub**, are living documents that the community can continuously improve and contribute to.

Andrei also pointed out the availability of **tutorials** that can help operators learn how to implement MANRS actions and prepare for adoption. He addressed the question of why network operators should join MANRS, even if they are already implementing some of the security measures themselves. He stressed that while implementing these controls helps improve the security of their own networks, joining MANRS provides the added benefit of being part of a **collective effort** to improve global routing security. He highlighted how implementing these controls can prevent incidents like route leaks, which can have devastating impacts on networks.

By being part of the growing **MANRS community**, operators demonstrate that routing security best practices are not just aspirational but are becoming an **industry expectation**. The community reinforces that without these controls, network operators may be seen as unprofessional by their peers, which could ultimately harm their reputation and business. Andrei encouraged network operators to start the **MANRS adoption process** by filling out the application form, even if they are not yet fully compliant. MANRS can help them address security gaps and become fully compliant over time.

He wrapped up his presentation by providing the **MANRS website URL** which is https://manrs.org/, and the link to the **Global Cyber Alliance** website, which is https://globalcyberalliance.org/, a non-profit organization focused on improving global internet security. Andrei thanked the audience for their attention and expressed his willingness to assist anyone interested in joining the initiative.

*David's presentation, which also focused on **RPKI** implementation, complemented Andrei's message. Maarten concluded by noting the importance of strengthening* *the entire internet security fabric, rather than just focusing on the top layers, and expressed his appreciation for the work being done to build the* ***MANRS community****, particularly in countries like* ***India*** *where there is significant potential for growth.*

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

Champika Wijayatunga's presentation focuses on **KINDNS**, a framework for DNS security, designed to help operators implement best practices for a secure DNS ecosystem (website: https://kindns.org/). He emphasizes the importance of protecting the entire DNS infrastructure, from stub resolvers to authoritative servers, registries, and registrars. The goal is a collective effort to secure DNS by applying best practices at each component of the system.

Champika explains that KINDNS covers several layers of DNS infrastructure, including authoritative operators, recursive resolvers, and both public and private resolvers. Each category of operators has its own set of security recommendations. For example, authoritative DNS operators are advised to implement **DNSSEC** to sign zones, maintain redundancy with multiple DNS servers in separate networks, and ensure zone file integrity and access control. Similarly, recursive resolver operators are encouraged to implement **DNSSEC validation**, access control measures like rate limiting, and optimizations like **QNAME minimization**.

The framework encourages self-assessment through the KINDNS website, where operators can anonymously evaluate their current DNS security practices using a checklist. Based on this evaluation, they receive a score and report, which can help guide improvements. Operators who meet KINDNS standards can officially enroll and be listed as compliant, becoming part of the community of operators implementing best practices.

Champika highlights the importance of collaboration among operators, and his call to action focuses on encouraging Indian operators, particularly those from NICSI and IXPs, to join KINDNS and apply these best practices. The goal is for India to follow the example of other regions and for KINDNS to grow, making the DNS ecosystem more secure globally.

In closing, Maarten Botterman emphasizes the collective action required across different areas—ISPs, IXPs, resolvers, and TLDs—to address DNS security. He also suggests that having Indian operators join KINDNS would set a positive example, helping to drive further adoption and improving DNS security across the country.

Emerging Technologies Panel

The first session of the Triple-I workshops brought together a distinguished panel to discuss emerging technologies—specifically quantum computing and artificial intelligence (AI)—and their implications for security, trust, and policy in the digital age. The panel aimed to explore not only the current state of these technologies but also the challenges they pose as they evolve and how we can manage potential risks.

In his opening remarks **Maarten Botterman** emphasized the importance of considering how emerging technologies—while promising—also bring new risks, particularly to trust in digital systems. He asked the panel how we can ensure that justified trust remains intact as technologies like quantum computing evolve and invited the three speakers to provide their opening remarks.

Dr. Manjunath Iyer, a principal consultant at WIPRO and expert on quantum communication, discussed the security challenges posed by quantum computing. While acknowledging that current security systems might work today, he highlighted the potential threats quantum computers could pose in the future, particularly once they become widely available. Quantum computers could break conventional encryption methods, making current security mechanisms obsolete. He stressed the importance of preparing for a "quantum future" by developing quantum-safe security solutions.

Dr. Reena Dayal, CEO of the Quantum Ecosystems Technology Council of India (QETCI), expanded on the need for action in the face of quantum advancements. While some experts predict that scalable quantum computers are decades away, she noted that governments and industries are already aware of the risks and need to start planning for post-quantum cryptographic solutions. She emphasized that risk management is crucial in deciding when to act, given the uncertainty surrounding the timeline for the development of quantum technology. Dr. Dayal also called for greater collaboration between the cybersecurity and quantum communities, as well as clearer guidance from governments about regulatory timelines for these emerging technologies.

Prof. (Dr.) Charru Malhotra, a professor at the Indian Institute of Public Administration and expert in emerging technologies and public policy, shifted the discussion toward AI. He acknowledged AI’s growing role in society, from government policy to everyday applications. Drawing from his experience working with the Indian government on national AI strategies, he explained how emerging technologies like AI must serve as equalizers, reducing digital divides and democratizing access to technology. He pointed to India’s Unified Payments

Interface (UPI) as an example of how digital infrastructure can make technology accessible to all, regardless of socioeconomic status.

Regarding AI regulation, Dr. Malhotra discussed India’s approach, which seeks to avoid a purely market-driven framework (like that of the US) or a strictly risk-based approach (as in the EU). The goal is to create a balanced regulatory environment that ensures AI technologies are ethical, trustworthy, and non-biased, ensuring that the data flowing through digital systems is reliable and safe for public consumption.

In their opening remarks the panellists confirmed the importance of managing emerging technologies, particularly quantum computing and AI, in a way that maintains trust and security in the digital world. The panellists highlighted the need for proactive planning, collaboration across communities, and thoughtful regulation to ensure these technologies benefit society without compromising security or ethical standards. The discussion that followed delved deeper into the regulatory challenges posed by emerging technologies like AI and quantum computing, focusing on balancing innovation, privacy, and security.

Maarten Botterman opened by highlighting the difference between AI, which is already widely used, and quantum computing, which, although still in its early stages, is rapidly progressing. He emphasized the need for regulations that balance innovation with safeguarding privacy and security. A key example was the European Union's AI Act, which aims to prevent irreversible damage while fostering innovation. This tension between innovation and regulation was also raised in relation to privacy laws like the GDPR in Europe and India’s evolving DPDP (Digital Personal Data Protection) Act. The conversation stressed how regulators and business stakeholders must collaborate to ensure privacy and security in a rapidly advancing digital landscape.

Prof. Charru Malhotra then discussed India’s data protection regulations, focusing on the Digital Personal Data Protection Act (DPDP), which protects all citizens' data, not just personally identifiable information. She emphasized the importance of cybersecurity alongside privacy regulations and the need for a robust cybersecurity framework in India, something still lacking despite the DPDP Act. She also discussed data sovereignty and localization, stressing how foreign hardware—particularly from countries like China—poses risks by capturing and controlling data. In India, this is a significant issue, especially for startups that rely on imported hardware. Malhotra also pointed out the need for a flexible, principles-based approach to regulating AI, distinct from the EU’s risk-based model.

Reena Dayal shifted the focus to quantum computing, stressing that quantum represents a fundamental shift in computing, not just a new technology layered on top of existing systems. She warned that regulation must be approached cautiously, as quantum is still in its early stages, with many unknowns about scalability and breakthroughs. Dayal argued that regulators must be flexible, allowing innovation while still providing guidance and setting expectations, particularly in sectors like finance, which are especially vulnerable to quantum risks. She emphasized that quantum security will become a critical issue as scalable quantum computers become a reality, and suggested that regulators need to play a more proactive role in preparing for this shift.

Manjunath Iyer reassured the audience that quantum's potential risks to security are already being addressed through developments in post-quantum cryptography. He explained that these advancements could provide quantum-safe algorithms, allowing classical infrastructure to remain secure even in a quantum-powered future. Iyer emphasized that even though quantum computing may not pose a significant threat immediately, preparations through cryptographic advances are underway to safeguard against future risks. He downplayed concerns about rapid breakthroughs, noting that the technological challenges in quantum are significant, and any advancements will likely take years to materialize.

Maarten Botterman wrapped up by reinforcing the need for a regulatory framework that can adapt to the unknowns of emerging technologies, as we do not yet know when quantum computing or AI will truly disrupt existing systems. He highlighted the reality that encrypted data is already being harvested and traded on the dark web, some of which may one day be decryptable with quantum computers. This underscores the importance of forward-thinking regulation to mitigate potential risks.

Following this, other participants came in and made comments and/or asked questions:

Dr. Govind emphasized the need for light-touch regulation to allow innovation to flourish, especially for startups. He warned against rushing into stringent regulations, suggesting that too many sector-specific rules could stifle entrepreneurship. Reena Dayal added that while regulation is not an immediate concern for quantum, there are real risks, particularly with quantum's potential to break current encryption methods. She highlighted the importance of proactive action now to prepare for future threats like quantum computers with thousands of qubits.

Charru Malhotra pointed out that India is moving toward light-touch regulation, citing the DPDP (Data Protection and Digital Privacy) Act and regulatory sandboxes as examples. These initiatives aim to foster innovation while ensuring compliance. Malhotra also highlighted India's focus on the societal impact of AI, stressing transparency, explainability, and liability issues in AI systems, especially in financial and public services.

Anoop Kumar raised concerns about the economic impact of quantum technologies, asking about the costs of implementing quantum-safe systems. Manjunath Iyer explained that while quantum-safe encryption systems like Quantum Key Distribution (QKD) are expensive, they offer a way to secure communications against future quantum threats. However, scaling these systems remains costly and complex.

The conversation also touched on the growing concerns about quantum technology's potential to disrupt cybersecurity. Reena Dayal noted the phenomenon of "store now, decrypt later," where encrypted data is being hoarded now, with the expectation that future quantum computers will be able to crack it. She emphasized that while quantum computing introduces new threats, it also offers the opportunity for stronger encryption methods in the form of post-quantum cryptography (PQC).

Shivakumar Daksha Moti raised the issue of how companies will manage the costs of adopting quantum-safe technologies. Experts agreed that while the cost of implementing such systems is high, especially for QKD, the investment is necessary to protect sensitive data in the future.

The panel concluded by recognizing the importance of collaboration between governments, industry, and regulators to create balanced frameworks for emerging technologies. The consensus was that while regulations are necessary, they should not stifle innovation. Industry should help guide the development of appropriate regulations, and there is a need for international cooperation in setting standards.

In the end, the discussion emphasized that technology should remain human-centric, with an emphasis on trust, transparency, and societal good. Both innovation and regulation need to go hand-in-hand to ensure that the benefits of emerging technologies like quantum computing and AI are maximized while minimizing their risks.

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

The moderator opens the floor for the last block: action planning. Based on earlier events, a group of volunteers has worked on an Action Plan that revolves around the development of a platform aimed at raising awareness and improving the safety and trust of internet services in India.

Maarten Botterman emphasizes the need for a continuous, impactful initiative that reaches a wider audience. He acknowledges the work done by Amitabh, Satish Babu, and Anand Raju, and introduces Dr. Balaji, who represents CDAC, a key partner in the initiative.

Amitabh Singhal then takes over, reflecting on the previous year's GFC workshop and recalling his participation in the Triple-I workshop in Hyderabad in 2022. During that workshop, the conversation turned toward how to create a more concrete platform for internet security awareness in India. Amitabh, who has extensive experience in the ISP industry, recognized the challenge of building trust among India's 900 million internet users, especially regarding the safety of websites, email services, and mobile applications. He proposed an actionable plan to address this challenge.

The idea evolved into the Trusted India Internet Initiative (T3i),which is a platform of people and organizations brought together to analyze, monitor, and measure the safety of websites and services. A software testing website would be used to provide data on security breaches and offer recommendations for improving security standards. Amitabh explained that the initiative would be structured in three main components:

1- A technical platform for analysis and monitoring,
2- community engagement to spread awareness, and
3- a governing secretariat to oversee the platform's operations.

The project foresees development and deployment of a public-facing user interface for testing websites, followed by a phase that would include mobile services. Eventually, the plan envisioned issuing trust scores and certifications for services that adopt secure internet protocols. However, after facing delays in securing funding, Amitabh, Anand, and Anupam decided to bootstrap the project and launch a beta version independently, resulting in the creation of the **safeinternet.in** website. This platform allows users to test the safety of websites by checking their adherence to security protocols.

Amitabh demonstrated how the platform works, showing test results for popular websites and highlighting the varying levels of trust scores. Although the results for many websites were less than ideal, the initiative aims to improve internet security by giving users access to actionable information. Amitabh also mentioned discussions with the Ministry of IT and Dr. Balaji from CDAC about potential collaboration, as CDAC is working on a similar project. The goal is to combine efforts to create a unified platform that could be widely used across India to ensure safer and more trusted internet services.

The conversation highlights a growing effort to build trust and security in India's internet ecosystem, with the vision of empowering millions of users to make informed decisions about the online services they use.

Dr. R. Balaji elaborates on the concept of "trusted internet spaces" and outlines the challenges and potential solutions for enhancing trust online. He divided trusted spaces into three categories: globally trusted spaces, fully trusted spaces, and partially trusted spaces, each with its own set of requirements and limitations.

Dr. Balaji explained that a "fully trusted space" would require foolproof digital identities, trusted devices, and a robust system of continuous authentication, reflecting the principles of "zero trust" — where trust is only granted after verification. However, creating such a space globally is an ideal, not a practical reality, due to the expanding and ever-changing nature of the internet. Instead, he proposed narrowing the untrusted spaces and fostering trusted transactions within a confined, well-regulated framework. This would require comprehensive standardization of technologies and methods, supported by both technological advancements and policy interventions.

He also discussed the concept of a "partially trusted space," where interactions can occur with untrusted or unknown entities. Such spaces would be most suitable for non-critical exchanges, and the infrastructure could be augmented with existing technologies like DNSSEC, RPKI, and other security measures.

To address these issues, Dr. Balaji showcased the work being done at the Center of Excellence (COE) in DNS security, particularly their public DNS resolver and several tools developed to analyze and improve DNS security. These tools include a DNS health analyzer to assess domain name servers, a malicious domain checker using AI, and a tool to detect typo-squatted domain names. He emphasized that these tools are open-source and available for use by anyone, not just government entities.

Amitabh Singhal then followed up with a demonstration of the T-III (Trusted India Internet Initiative) project, particularly its beta version, which provides a platform for users to test the security of websites. Using the internet.nl platform as a starting point, the T-III project is adapting and customizing it to Indian requirements. The platform allows users to check websites for compliance with standards like RPKI, DANE, TLS, HTTPS, and IPv6, providing a score and detailed test reports that highlight any security vulnerabilities. For instance, the test results for IIM Bangalore showed areas of non-compliance, such as lacking DNSSEC and not being fully IPv6 compliant.

Both Dr. Balaji and Amitabh Singhal stressed the importance of empowering users with the ability to test and assess the security of the websites they use, ultimately helping service providers adopt necessary security standards. They emphasized the potential for collaboration between their initiatives, especially in leveraging COE's DNS security expertise and T3i's testing and monitoring platform.

The importance of building trust in the digital ecosystem is widely recognized, and there is a clear focus on developing tools and platforms that can help users and service providers assess and improve their internet security, thus empowering the users to make smarter choices, which leads to the offering of smarter choices by providers as it is more likely to pay off. Multi-stakeholder collaboration is important: collaboration between different stakeholders, including technical experts, government entities, and the broader community, is key to creating a safer and more reliable internet space for users in India and beyond.

In this conversation, a group of experts discusses the development and sustainability of a project aimed at improving the security and accessibility of the internet in India, with a particular focus on DNS security. Amitabh Singhal explains that the project is modelled after the Dutch initiative *internet.nl*, which tests websites' DNS configurations and security. The Indian version is a volunteer-driven effort, with contributions from key individuals like Anand, Maarten, and Satish Babu. The goal is to make the platform multilingual and user-friendly, allowing people to test their websites' DNS security in local languages.

However, as the initiative progresses, concerns about sustainability arise. Amitabh acknowledges that funding is a challenge, with initial plans to raise around €700,000 to cover the first three years. The team is in talks with various organizations, including MeitY (Ministry of Electronics and Information Technology) and NIXI (National Internet Exchange of India), to secure funding and collaborate on the project. They also consider models used by successful organizations like

NIXI, which was set up with seed funding from the government but became self-sustaining after a few years through services like the .in domain name registry.

The idea of a government-supported agency taking over the project after it becomes established is also suggested. This model, similar to what happened with NIXI, would allow the founders to hand over the project to a government-backed organization that could continue running it. Amitabh also discusses the possibility of collaborating with C-DAC (Centre for Development of Advanced Computing), which could provide technical resources to help scale the project.

Shivakumar Daksha asks about the promotion of the DNS security website, which has primarily been targeted at DNS ecosystem stakeholders so far. Amitabh and R. Balaji suggest that collaboration and community-driven approaches could help increase outreach and adoption. The integration of various tools and the promotion of DNS security through the community could help raise awareness and encourage broader usage.

Anurag Bhatia raises the point that for the tools to be effective, more people, especially those with less technical knowledge, need to know about them. He suggests integrating the tools with domain registrars so that when someone registers a .in domain, they could immediately receive a DNS security score, encouraging them to take necessary actions. R. Balaji acknowledges the idea and mentions that they already provide a malicious domain reporting service via an API. The suggestion to integrate DNSSEC checks into the registration process could provide significant value to non-technical users.

This leads to the realization that greater awareness and collaboration are key to driving the project forward, with support from communities and organizations like ICANN, APNIC, and MANRS (Mutually Agreed Norms for Routing Security). Everyone agrees that these initiatives need to be made more accessible, so that domain owners and administrators can improve their security practices, thus contributing to a safer and more reliable internet.

With regards to community-driven projects such as the T3i initiative in India, challenges of sustaining such projects without consistent funding remain. Maarten Botterman and Satish Babu share their thoughts on how to build and expand this initiative by leveraging networks like the ISOC Chapters in India. They emphasize the importance of a structured, multi-stakeholder approach to guide the project, involving organizations such as NIXI, CDAC, and MeitY. This would ensure broad acceptance and legitimacy, especially in producing and distributing reports about internet governance standards.

Satish Babu highlights the significance of making the project community-owned, noting that while the community may include millions of people, the focus should be on smaller groups, such as experts or ISOC Chapter members. For the project to be sustainable, it must be seen as valuable by the community, and thus, an advisory committee will be necessary. The community-driven model would also ensure continuity, but funding remains a critical challenge. While volunteer-driven projects, like the India School on Internet Governance (InSIG), have had some success in maintaining leadership continuity, the financial aspect remains a hurdle. Satish points out that InSIG has grown from two ISOC chapters to seven, but every year they face the challenge of securing funds, which impacts their ability to plan long-term.

Maarten Botterman agrees that funding is a significant issue for community-driven projects. He notes that while volunteers have historically contributed to the internet's growth, securing consistent funding has become more difficult in recent years. He emphasizes the need for both government and industry support to sustain such initiatives. The conversation also touches on the idea of establishing hubs or smaller chapters in different cities in India to rotate the GFCE (Global Forum on Cyber Expertise) activities, ensuring more local involvement and awareness.

Finally, Satish reflects on the lessons learned from InSIG, especially in ensuring leadership continuity and expanding the project across different cities, even without a local chapter. However, the financial model remains a key challenge. For the future, they are considering new models, such as paid fellowships, to reduce dependency on fundraising. This idea, although not directly linked to T3i, illustrates the broader issue of finding sustainable financial models for community-driven projects.

It is recognized that both community participation and sustainable funding are crucial for the success of initiatives like T3i and InSIG, and that these projects can only move forward with continued collaboration and support.

Other elements:

- improving website security and efficiency, particularly focusing on achieving high test scores and reliability for websites like APNIC.net. One key takeaway is that APNIC's success in achieving 100% on website tests can be attributed to the use of Cloudflare, which handles much of the backend work such as enabling IPv6 support, DNSSEC zones, and NAT caching. While Cloudflare takes care of the technical infrastructure, the APNIC team ensures compliance and effective backend management. The conversation touches on how organizations can improve their own website test scores, with suggestions to leverage tools like Cloudflare for better configuration, as well as run proper training programs.

- Testing mobile applications: a challenge presented in the conversation is testing mobile applications, which are harder to assess due to being hidden behind platforms like Apple and Google. A proposed solution is the development of a test bed to help users better understand website security. The project is in its early stages but has gathered a committed group of technical experts.
- Ensuring internet sustainability: especially in smaller regions where internet exchange points (IXPs) face financial challenges. The concern is how to keep community-driven IXPs running without relying on government control or donations. There’s an emphasis on the need for independent management to avoid regulatory interference. The importance of developing sustainable models for smaller internet communities is also highlighted.
- Comprehensive approach: there is a need for a comprehensive, multi-faceted approach to internet safety, balancing technical solutions with awareness campaigns. The complexity of cybersecurity issues, including privacy, freedom of speech, and online crimes like cyberbullying and misinformation, requires ongoing community involvement and evolving solutions. It’s emphasized that no single solution can guarantee complete safety, but continuous efforts to improve user awareness and security protocols are necessary.

Ti3 could be that ongoing project that aims to build a multi-stakeholder governance model to improve website security and reliability. Key stakeholders identified so far include ISPs, telecom providers, government agencies, academic institutions, and technical experts. The initiative aims to create a platform that makes it easier for website owners to test their site's security and compliance, raising awareness and providing tools for improvement.

As the session concludes, the importance of building a sustainable, community-driven initiative that stands ready to improve the safety and efficiency of websites is emphasized, ensuring that it evolves to meet the needs of users.

The meeting calls for ongoing collaboration and commitment from stakeholders to continue the work, with the ultimate goal of creating a safer, more reliable internet. The event is framed as a starting point for further discussion and action, and the speakers express their gratitude to all participants for their input and support.

-=(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.

Annex 1 – Meeting Agenda

GFCE Triple-I Bangalore, India

Indian Institute of Management (IIM) Bangalore, 30 September 2023

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

Warm Welcome to Mr. Sushil Pal, Joint-Secretary, Ministry of Electronics & Information Technology, Government of India to the GFCE Triple – I Workshop. Welcome by the host, Mr. Satish Babu (InSIG), and introduction to the day by the GFCE Triple-I moderator, Maarten Botterman, to ensure the best possible common understanding on how to progress the work, together.

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

During this block we will present key modern internet standards relating to integrity and security of DNS, routing and messaging . We will present the standards (and why they matter), the current deployment (measuring uptake by sampling a relevant set of websites and email addresses), and what can be done to further enhance deployment (and why that is worth doing).

-	Routing security standards:	RPKI, ROA	David Phelan (APNIC)
-	DNS security standards	DNSSEC, TLS, DANE	Champika Wijayatunga (ICANN)
-	Email security standards	DKIM, SPF, DMARC	Hovsep Najarian (EasyDMARC)
-	IPv6		Anurag Bhatia

These standards are also discussed in the GFCE Triple-I Handbook and technical tests for the state of implementation are available at www.internet.nl. We will include a status update on modern Internet standards adoption since 2023.

11:30 Coffee/Tea

12:00Block II part 1: Inspiration from Good Practice Actions

In this first part of Block II we will present some global initiatives that can inspire local action.

a- Internet Resilience Index: providing a snapshot of a country's Internet resilience in terms of infrastructure, performance, security, and market readiness.: Robbie Mitchell (ISOC)

b- MANRS: rationale, development and deployment in India: Andrei Robachevsky (Global Cyber Alliance)

c- KINDNS: rationale, development and deployment in India: Champika Wijayatunga (ICANN)

13:30 Lunch

14:30 Block II part 2: Inspiration from Good Practice Actions

This block will focus on Emerging Technologies to be aware of and to pre-empt while enhancing the infrastructure to ensure higher integrity in DNS, routing and messaging. Ensuring future proof Internet use requires awareness of new technologies evolving and planning ahead for benefiting from the new opportunities and addressing the new vulnerabilities.

- Policy aspects of AI, Quantum technologies, Blockchain and IoT ecosystems;
- Technology aspects of AI, Quantum technologies, Blockchain and IoT ecosystems

For exploring these issues, the moderator will engage with a panel of three esteemed experts in the field:

- Dr. Manjunat Iyer, Principal consultant, CTO office, WIPRO, Member of the inter-ministerial advisory group on Quantum communication and Quantum computing; Chair
- Dr. Reena Dayal, CEO Quantum Ecosystems Technology Council of India (QETCI), Steering Committee of the IEEE Quantum Initiative , Chair for the IEEE Quantum Special Interest Group in India and on the Consultative Committee for Quantum for the Government of Telangana
- Prof. (Dr.) Charru Malhotra, Professor (e-Governance and ICT) at Indian Institute of Public Administration, Delhi, India

Following short introductions, the panel will explore the key issues raised, and the floor will be opened for questions and suggestions from all workshop participants.

15:30 Tea

16:00Block III: Planning for a More Trusted Internet: Marketplace for Action

This block will be interactive inviting all to contribute to develop the best possible way forward, together. A comprehensive action plan will be presented for discussion, and we will take into account lessons learned from the discussion during the day.

Contributors during this session include Mr. Amitabh Singhal, Satish Babu, Anand Raje (Safer Internet India Action plan), and Dr. R.Balaji (CDAC).

17:15 Conclusions and Closing Remarks

17:30Ends – (followed by drinks/diner location tbc)