DAKSHIN
Development and Knowledge Sharing Initiative
GLOBAL SOUTH CENTRE OF EXCELLENCE

RIS
Research and Information System for Developing Countries
विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

DAKSHIN Workshop
Cyber Security in Digital Public Infrastructure

5 December 2024

Report

Digital India
Power To Empower

DBT Bharat
Apna Adhikar, Apna Daar

AADHAAR

ONDC
Open Network for Digital Commerce

DigiLocker

Views expressed in the report are personal.
Usual disclaimers apply.

Published by

RIS
Research and Information System for Developing Countries
विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

DAKSHIN
Development and Knowledge Sharing Initiative
GLOBAL SOUTH CENTRE OF EXCELLENCE

Zone IV B, 4th Floor, India Habitat Centre
Lodhi Road, New Delhi 110 003, India
Tel.: +91-11-24682177-80; Fax: +91-11-24682173-74
E-mail: dgoffice@ris.org.in
Website: www.ris.org.in

Contents

Concept Note

DAKSHIN- Global South Centre of Excellence works towards the identification and implementation of scalable and sustainable solutions for the Global South. It supports the exchange of ideas, best practices, capacity building, and opportunities for development under the South-South Cooperation framework. To facilitate idea sharing and continuous dialogue among the countries of the Global South, DAKSHIN organized workshops on topics of common interest. The latest in this series was a workshop on cybersecurity, with a specific focus on Digital Public Infrastructure (DPI) in the countries of the Global South.

Cybersecurity was recognized as essential for ensuring the confidentiality and integrity of data, systems, and networks. Securing DPI from malicious actors was emphasized as crucial for uninterrupted governance. Since DPI relies on the Internet, its global connectivity makes it important to remain vigilant about potential cyber risks such as data breaches, malware, or unauthorized access, which can emerge from various sources worldwide.

While the potential of digital transformation in developing countries is immense, many nations continue to face challenges in establishing robust cybersecurity frameworks. Issues such as limited infrastructure, inadequate resources, shortage of technical skills, and insufficient policies for threat management were identified as key vulnerabilities that leave DPI exposed to large-scale risks.

The workshop on cybersecurity served as a platform for stakeholders to discuss the importance of robust cybersecurity policies in the countries of the Global South and to deliberate on the evolution of threat management systems for a secure digital future.

Aim of the Workshop

The workshop aimed to enhance understanding of evolving cyber threats and their potential impacts on developing countries. It provided an opportunity for cybersecurity experts and policymakers from various countries of the Global South to share and discuss innovative approaches to safeguarding their digital ecosystems. The workshop also facilitated networking among key stakeholders, encouraging partnerships for future initiatives on cybersecurity.

Agenda

5:00 pm – 5:05 pm	**Welcome Remarks** • **Professor Sachin Chaturvedi,** Director General, RIS
5:05 pm – 5:10 pm	**Overview of Cyber Security in Digital Public Infrastructure** • **Mr. Anish Kumar,** Advisor [DPA-III], Ministry of External Affairs, Government of India
5:10 pm – 5:15 pm	**Building Secure Information Systems for the Government** • **Mr. Magesh Ethirajan,** Director General, Centre for Development of Advanced Computing (CDAC), India
5:15 pm – 5:20 pm	**Cyber Resilience approaches for Cyber Physical Systems** • **Dr. Krishna Kumar Balaraman,** Associate Professor, School of Management & Entrepreneurship, IIT Jodhpur, India
5:20 pm – 5:25 pm	**Securing Government IT Infrastructure** • **Dr. Jatin Patel,** Director(I/C) and Asst. Professor (IT), Rashtriya Raksha University School of Information Technology, Artificial Intelligence and Cyber Security (SITAICS), India
5:25 pm – 5:30 pm	**Use of Secure Products in Digital Public Infrastructure** • **Ms. Smitha Sriharsha**, Senior Manager Platform Security Engineering, F5 Networks, India
5:30 pm – 6:10 pm	**Special Remarks from Representatives of Global South Countries** • **Mr. Issam Lotfi,** Chief Strategy Officer, Royal Institute for Strategic Studies (IRES), Morocco • **Mr. Russell Woruba**, CTO, Department of ICT, Government of Papua New Guinea, Papua New Guinea • **Ms. Sarai Faleupolu Tevita,** ICT Director, National University of Samoa, Samoa
6:10 pm – 6:25 pm	**Open Discussion**
6:25 pm – 6:30 pm	**Concluding Remarks** • **Professor Gulshan Sachdeva,** Chief Coordinator, DAKSHIN, RIS

Summary Report

DAKSHIN organised the seventh workshop entitled "Cyber Security in Digital Public Infrastructure Thursday" on 5 December 2024. This workshop is the seventh workshop from DAKSHIN on digital solutions that facilitated the exchange of ideas, best practices, capacity building and opportunities for development, under the South-South Cooperation framework.

Prof. Sachin Chaturvedi, Director General, RIS, welcomed the panelists and participants, emphasizing the significance and relevance of DPI for the Global South. He noted that DPI-related challenges extend beyond technology to encompass economic and developmental dimensions, with cybersecurity emerging as a key area of concern for developing countries. Prof. Chaturvedi also highlighted that during India's G20 Presidency, particular emphasis was placed on reducing transaction costs and enhancing access to citizen-centric services, while ensuring appropriate safeguards and security measures to maintain effectiveness and trust.

Mr. Anish Kumar, Advisor [DPA III], Ministry of External Affairs, Government of India, provided an overview of cybersecurity in DPI. He emphasized that DPI is central to the economic transformation of countries such as India and Singapore, built on digital IDs, payment systems, and data exchanges. Highlighting the growing role of Artificial Intelligence (AI) in DPIs, he noted that while AI enhances efficiency through real-time data analysis and automated threat detection, it also introduces new cybersecurity risks.

Mr. Kumar underscored the importance of safeguarding the vast volumes of sensitive data generated by DPIs, including biometrics, images, and voice data, and discussed the shift from centralized to federated and decentralized storage models. He pointed to blockchain as a potential solution for secure data management and noted that quantum computing poses emerging challenges to existing encryption methods. He stressed the need for quantum-safe encryption and adoption of zero-trust security architectures to ensure continuous protection. He concluded by reaffirming India's commitment to supporting the Global South through knowledge sharing and collaboration on DPI and cybersecurity initiatives.

Mr. Magesh Ethirajan, Director General, Centre for Development of Advanced Computing (C-DAC), India, highlighted the organization's role in strengthening cybersecurity and digital forensics. He explained that C-DAC has moved from a reactive to a proactive security approach, using new technologies such as blockchain for continuous auditing and maintaining tamper-proof audit trails.

Mr. Ethirajan outlined the key initiatives of the C-DAC, India, which include developing cybersecurity and forensic tools, collaborating with law enforcement agencies, and conducting IT and OT audits, while also advancing work in emerging areas such as quantum computing and health information systems. He emphasized that integrating security at the design stage is essential to strengthen and continuously improve cybersecurity measures. He highlighted C-DAC's Information Security Education Awareness Program as a major capacity-building initiative to enhance cybersecurity skills and awareness across India. Mr. Ethirajan noted that C-DAC continues to advance its efforts in implementing comprehensive cybersecurity solutions, consulting, and auditing services, and has successfully deployed these measures during major national and international events, including India's G20 Presidency.

Dr. Krishna Kumar Balaraman, Associate Professor, School of Management and Entrepreneurship, IIT Jodhpur, highlighted the importance of **cyber resilience in cyber-physical systems (CPS)**. He explained that CPS networks across sectors such as healthcare, emergency response, traffic management, manufacturing, and defense are increasingly complex and interconnected, making them more vulnerable to cyber threats and human errors. He cited real-world examples such as the Bombay power network disruption and cloud service failures to illustrate the potential impact.

Dr. Balaraman emphasized that cyber resilience ensures the continuity of essential services even during cyber incidents or natural disasters. He underscored the need to embed security at the design stage, adopt multilayer protection, and enable quick recovery from disruptions. He also noted that artificial intelligence can enhance threat detection and real-time response. He concluded that minimizing dependencies between systems and distinguishing critical from non-critical services can significantly improve overall resilience.

Dr. Jatin Patel, Director(I/C) and Asst. Professor (IT), Rashtriya Raksha University School of Information Technology, Artificial Intelligence and Cyber Security (SITAICS), India emphasized the critical importance of securing government IT infrastructure, highlighting the global imperative of protecting worldwide critical infrastructure. He stressed that each attack on critical infrastructure can disrupt essential services, impact the economy, and erode public trust. Dr. Patel called for a collective effort from policymakers, private entities, and citizens to fortify cybersecurity through robust policies, indigenous innovation, and resilience.

Dr. Patel emphasized the need to strengthen both Information Technology (IT) and Operational Technology (OT) infrastructure security. He illustrated this by explaining how altering temperature settings in medical storage systems could compromise essential supplies, highlighting the critical importance of OT security. He underscored the value of cybersecurity exercises that give stakeholders practical experience in handling cyber

incidents and referred to the National Cybersecurity Exercise 2024, where live attack simulations were conducted to enhance preparedness. Dr. Patel also stressed the importance of strategic-level exercises to improve decision-making during cyber crises. He advocated for a centralized cybersecurity command, such as the National Critical Information Infrastructure Protection Centre, supported by real-time threat monitoring and mandatory security audits. He emphasized that building cyber resilience requires advanced threat detection systems, AI-powered tools, redundancy and backup mechanisms, and comprehensive training programs and there is a need for international collaboration, research, and innovation to address evolving cyber threats. Dr. Patel concluded by calling for the adoption of global cybersecurity standards to ensure consistent security practices and safeguard both national and global critical infrastructure.

Ms. Smitha Sriharsha, Senior Manager Platform Security Engineering at F5 Networks, India discussed the challenges and advantages of the digital era, especially with the evolution of AI and disruptive innovations. In the cybersecurity space, she highlighted the increasing sophistication of attacks, often using the same technologies designed to build security products. Ms. Smitha emphasized that traditional security measures are no longer sufficient and that layered defenses are essential to protect digital infrastructure from evolving threats. She discussed key aspects of network security, highlighting the importance of adopting zero trust architecture and deploying advanced AI-enabled firewalls to address emerging cyber risks. She noted that network segmentation has become critical due to the complex deployment of applications and workloads across data centers and cloud environments.

She underlined the need for strong endpoint security platforms to protect devices used by government officials and the public, as these often store sensitive data. She stressed the use of endpoint detection and response systems, anti-malware solutions, and ransomware protection tools. She further emphasized that data protection and recovery are crucial in today's environment, where data is as valuable as gold, and highlighted the need for end-to-end encryption, secure backup systems, and effective data governance to safeguard critical information. She also noted that privacy-preserving technologies such as homomorphic encryption and anonymization play an increasingly important role in ensuring data confidentiality. She concluded that cybersecurity is an ongoing process and that integrating these measures will help organizations remain resilient, secure, and future-ready against emerging threats and technological advancements.

Mr. Issam Lotfi, Chief Strategy Officer, Royal Institute for Strategic Studies (IRES), Morocco discussed Morocco's national initiatives and progress in cybersecurity. He explained that the rapid expansion of digital technologies has improved global connectivity but has also made systems more exposed to cyber threats. He noted that the sharp rise in cyberattack costs between 2015 and 2022 underscores the need for stronger cybersecurity

frameworks. He mentioned that under the leadership of King Mohammed VI, Morocco has launched several national digitization programs, including Digital Morocco 2013, Digital Morocco 2020, and Digital Morocco 2023. These programs aim to promote digital inclusion, enhance digital development, and manage emerging cyber risks.

Mr. Issam highlighted that since 2011, Morocco has strengthened its cybersecurity infrastructure through the General Directorate for Information System Security, which coordinates inter-ministerial efforts, conducts national security audits, and builds awareness among public officials. He added that in 2020, Morocco established a Strategic Committee for Cybersecurity to develop and implement the national cybersecurity strategy with participation from key ministries and security agencies. He also mentioned that Morocco's 2012 National Cybersecurity Strategy and 2014 National Directive on Information System Security provided the foundation for these recent measures. He further highlighted that these ongoing efforts have placed Morocco among the top 25 countries globally in cybersecurity, according to the Global Security Index. Despite experiencing more than 52 million cyberattacks in 2023, Morocco continues to strengthen its cybersecurity ecosystem. He explained that the 2024 strategic vision focuses on creating a secure, reliable, and resilient national cyberspace that supports digital transformation through better governance, capacity building, and international cooperation. Mr. Issam concluded by highlighting Morocco's commitment to personal data protection under the National Commission for the Protection of Personal Data (CNDP), for ensuring respect for individuals' fundamental rights and regulating the processing of personal data across sectors.

Mr. Russell Woruba, Chief Technology Officer, Department of ICT, Government of Papua New Guinea, shared the country's ongoing digital transformation initiatives. He highlighted the progress made since 2019, including studying digital transformation models from India, Estonia, Singapore, and Australia, which informed the development of Papua New Guinea's first Cybersecurity Policy in 2021 and the enactment of the Digital Government Act in 2022. The Act provides a legal framework empowering the Department of ICT to coordinate government-wide efforts, including the establishment of a National Cybersecurity Center. Complementary policies, such as the Cloud Policy and the Data Governance and Protection Policy, were also introduced to accelerate digital transformation, safeguard citizens' data, and ensure interoperability in service delivery.

Mr. Woruba explained the structure of the government's technology stack, noting that cybersecurity is integrated across all layers to ensure secure and resilient digital services. Within this framework, he announced the release of the PNG's Digital ID Policy for public consultation, aimed at providing citizens with secure, verifiable digital credentials accessible through mobile devices. Papua New Guinea plans to scale the Digital ID system to five million citizens by the end of next year and reach one million issuances by mid-year. He encouraged public feedback on the policy and emphasized the importance of

regional cooperation to achieve shared digital and economic goals. He also underscored the importance of cloud assurance and regular security audits to maintain the integrity and reliability of government systems, including automated software integration and delivery pipelines, as well as cloud infrastructure, to ensure adherence to international best practices.

Ms. Sarai Faleupolu Tevita, ICT Director at the National University of Samoa, shared insights on implementing cybersecurity within Samoa's Digital Public Infrastructure (DPI). She highlighted the country's recent efforts during the Commonwealth Heads of Government Meeting in October 2024, where cybersecurity was a top priority. A dedicated team, comprising experts from the Pacific region and Australia, established a Security Operations Center to safeguard government networks and event venues. She noted that this experience underscored the need for continuous training, awareness, and education on cybersecurity for both public officials and the wider community. The Ministry of ICT is currently reviewing the national cybersecurity strategy and ICT policy, recognizing cybersecurity as an essential element of governance in the Pacific. The National University of Samoa has also adopted an incident response plan focused on technology security. Ms. Tevita concluded that cybersecurity in DPI is not merely a technical concern but a governance and societal imperative, requiring a multi-stakeholder approach that integrates technology, policy, and education to ensure trust, privacy, and resilience.

Outcomes

The key outcomes of the workshop are

- The workshop underscored that cybersecurity must be integrated at the design stages of digital infrastructures and recognized that Digital Public Infrastructure (DPI) serves as a key driver of inclusive and sustainable development, extending beyond technology to build trust, ensure resilience, and safeguard the integrity of digital services.
- Experts highlighted the growing role of emerging technologies such as Artificial Intelligence (AI), blockchain, and quantum-safe encryption in strengthening cybersecurity, while emphasizing the parallel need for ethical governance and risk management frameworks.
- Strengthening the protection of critical infrastructure emerged as a global priority, requiring coordinated efforts among governments, private sector entities, academia, and civil society. Participants underscored the importance of live cybersecurity exercises, real-time threat monitoring, and regular security audits. Industry experts further emphasized the adoption of modern defense strategies such as zero-trust architectures, network segmentation, AI-powered firewalls, and advanced endpoint security systems to counter increasingly sophisticated and automated cyberattacks.
- A shift from reactive to proactive cybersecurity measures was emphasized, focusing on continuous auditing, digital forensics, and tamper-proof monitoring systems to prevent and detect cyber incidents in real time. Discussions also highlighted the need to strengthen cyber resilience in critical cyber-physical systems (CPS) through multilayered security, redundancy mechanisms, and rapid recovery capabilities to ensure uninterrupted delivery of essential services.
- Country experiences from Morocco, Papua New Guinea, and Samoa demonstrated strong regional commitment to advancing national cybersecurity strategies, developing digital governance frameworks, and promoting South–South collaboration for shared resilience.
- The discussions reinforced the importance of sustained investment in capacity building, digital literacy, and public awareness to cultivate a culture of cybersecurity readiness across institutions and communities.

Glimpses

RIS

Research and Information System for Developing Countries

विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

RIS specialises in issues related to international economic development, trade, investment and technology. It is envisioned as a forum for fostering effective policy dialogue and capacity-building among developing countries on global and regional economic issues. The focus of the work programme of RIS is to promote South-South Cooperation and collaborate with developing countries in multilateral negotiations in various forums. Through its following centres/forums, RIS promotes policy dialogue and coherence on regional and international economic issues.

DAKSHIN – Global South Centre of Excellence

The word "DAKSHIN" (दक्षिण) is of Sanskrit origin, meaning "South." The Hon'ble Prime Minister of India, Shri Narendra Modi, inaugurated DAKSHIN – Global South Centre of Excellence in November 2023. The initiative was inspired by the deliberations of Global South leaders during the Voice of the Global South Summits. DAKSHIN stands for Development and Knowledge Sharing Initiative. Hosted at the RIS, DAKSHIN has established linkages with leading think tanks and universities across the Global South and is building a dynamic network of scholars working on Global South issues.

AIC – ASEAN-India Centre at RIS

AIC at RIS has been working to strengthen India's strategic partnership with ASEAN in its realisation of the ASEAN Community. AIC at RIS undertakes research, policy advocacy and regular networking activities with relevant organisations and think-tanks in India and ASEAN countries, with the aim of providing policy inputs, up-to-date information, data resources and sustained interaction, for strengthening ASEAN-India partnership.

CMEC has been established at RIS under the aegis of the Ministry of Ports, Shipping and Waterways (MoPS&W), Government of India. CMEC is a collaboration between RIS and Indian Ports Association (IPA). It has been mandated to act as an advisory/technological arm of MoPSW to provide the analytical support on policies and their implementation.

FITM – Forum on Indian Traditional Medicine

FITM is a joint initiative by the Ministry of Ayush and RIS. It has been established with the objective of undertaking policy research on economy, intellectual property rights (IPRs) trade, sustainability and international cooperation in traditional medicines. FITM provides analytical support to the Ministry of Ayush on policy and strategy responses on emerging national and global developments.

BEF – Blue Economy Forum

BEF aims to serve as a dedicated platform for fostering dialogue on promoting the concept in the Indian Ocean and other regions. The forum focuses on conducting studies on the potential, prospects and challenges of blue economy; providing regular inputs to practitioners in the government and the private sectors; and promoting advocacy for its smooth adoption in national economic policies.

FIDC – Forum for Indian Development Cooperation – भारतीय विकास सहयोग मंच

FIDC, has been engaged in exploring nuances of India's development cooperation programme, keeping in view the wider perspective of South-South Cooperation in the backdrop of international development cooperation scenario. It is a tripartite initiative of the Development Partnership Administration (DPA) of the Ministry of External Affairs, Government of India, academia and civil society organisations.

FISD

FISD aims to harness the full potential and synergy between science and technology, diplomacy, foreign policy and development cooperation in order to meet India's development and security needs. It is also engaged in strengthening India's engagement with the international system and on key global issues involving science and technology.

SACEPS

As part of its work programme, RIS has been deeply involved in strengthening economic integration in the South Asia region. In this context, the role of the South Asia Centre for Policy Studies (SACEPS) is very important. SACEPS is a network organisation engaged in addressing regional issues of common concerns in South Asia.

NeST – Network of Southern Think-Tanks

Knowledge generated endogenously among the Southern partners can help in consolidation of stronger common issues at different global policy fora. The purpose of NeST is to provide a global platform for Southern Think-Tanks for collaboratively generating, systematising, consolidating and sharing knowledge on South South Cooperation approaches for international development.

DST SPR – Department of Science and Technology Satellite Centre for Policy Research at RIS – STI Diplomacy

DST-Satellite Centre for Policy Research on STI Diplomacy at RIS aims to advance policy research at the intersection of science, technology, innovation (STI) and diplomacy, in alignment with India's developmental priorities and foreign policy objectives.

— Policy research to shape the international development agenda —

Core IV-B, Fourth Floor, India Habitat Centre, Lodhi Road, New Delhi-110 003, India
Tel. +91-11-24682177-80, Email: dgoffice@ris.org.in, Website: www.ris.org.in

Follow us on:

www.facebook.com/risindia @RIS_NewDelhi www.youtube.com/RISNewDelhi